RR 2025-254

Från:	Kristina McConnell <kristina.mcconnell@regeringskansliet.se> för Fö RS Remissvar <fo.rs.remissvar@regeringskansliet.se>
Skickat:	den 11 juli 2025 08:47
Till:	registrator; info@centrumforrattvisa.se; info@crd.org; fortv; info@dpforum.se; registrator; exp-hkv; registrator; fra@fra.se; undom; forvaltningsrattenistockholm; svea hovratt; registrator; imy; registrator; registrator; info@lo.se; registrator; registrator; registrator kansli; pts; Regelrådet; riksarkivet; justitieombudsmannen@jo.se; registrator; registrator; info@advokatsamfundet.se; kansli@saco.se; sakint; sakerhetspolisen@sakerhetspolisen.se; press@telenor.se; martin.sjoberg@telenor.se; johanna.tham@teliacompany.com; gbg tingsratt; info; registrator; tullverket; registrator; registrator
Kopia:	fo.registrator@regerinskansliet.se; Becky Scott; FÖ Info; FÖ Remissvar; Fö RS Remissvar; FÖ Remisspublicering
Ämne:	[extern] Svar senast 2025-10-03; Remiss av utkast till lagrådsremiss Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning
Bifogade filer:	Utkast lagrådsremiss Signalspaning i försvarsunderrättelseverksamhet - en modern och ändamålsenlig lagstiftning tg.pdf; Remissmissiv tg.pdf
Uppföljningsflagga:	Följ upp
Flagga:	Slutfört
Kategorier:	Registraturen sommaren 2025
AppServerName:	public360_prod
DocumentID:	RR 2025-254:01
DocumentIsArchived:	-1

Härmed bifogas remiss av utkast till lagrådsremiss Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning.

Svar till Försvarsdepartementet **senast 2025-10-03.**

Skicka remissvar

- Remissvar mejlas till fo.remissvar@regeringskansliet.se med kopia till fo.rs.remissvar@regeringskansliet.se.

I mejlets ämnesrad

- Skriv in diarienummer Fö2024/01478 och remissinstansens namn.

Filnamn

- Filnamnen ska enbart vara remissinstansens namn. Ej diarienummer, ord, symboler eller siffror i filnamnen.

Remissvar skickas i två versioner

- En Word.
- En Pdf – som ska vara tillgänglighetsanpassad (enligt lagen (2018:1937) om tillgänglighet till digital offentlig service).

Remissvaren kommer att publiceras på regeringens webbplats.

Med vänliga hälsningar

Kristina McConnell
Assistent
Rättssekretariatet

Försvarsdepartementet
Tfn 54484
Mobil 0761-26 47 99
kristina.mcconnell@regeringskansliet.se
www.regeringen.se

Regeringskansliet

Regeringskansliet

Remiss

2025-07-11

Fö2024/01478

Försvarsdepartementet

Utkast till lagrådsremiss Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning

Remissinstanser

1. Arbetsgivarverket
2. Centrum för rättvisa
3. Civil Rights Defenders
4. Fortifikationsverket
5. Forum för Dataskydd
6. Försvarshögskolan
7. Försvarsmakten
8. Försvarets materielverk
9. Försvarets radioanstalt
10. Försvarsunderrättelsedomstolen
11. Förvaltningsrätten i Stockholm
12. Svea hovrätt
13. Institutet för mänskliga rättigheter
14. Integritetsskyddsmyndigheten
15. Inspektionen för strategiska produkter
16. Justitiekanslern
17. Landsorganisationen i Sverige (LO)
18. Myndigheten för psykologiskt försvar

Telefonväxel: 08-405 10 00
Fax: 08-723 11 89
Webb: www.regeringen.se

Postadress: 103 33 Stockholm
Besöksadress: Jakobsgatan 9
E-post: fo.registrator@regeringskansliet.se

19. Myndigheten för samhällsskydd och beredskap
20. Polismyndigheten
21. Post- och telestyrelsen
22. Regelrådet
23. Riksarkivet
24. Riksdagens ombudsmän
25. Statens inspektion för försvarsunderrättelseverksamheten
26. Stockholms universitet (juridiska fakulteten) (avsnitt 6.3 och 8)
27. Sveriges advokatsamfund
28. Sveriges Akademikers Centralorganisation (SACO)
29. Säkerhets- och integritetsskyddsnämnden (avsnitt 8)
30. Säkerhetspolisen
31. Tele2 AB
32. Telenor Sverige AB
33. Telia Company AB
34. Göteborgs tingsrätt
35. Tjänstemännens Centralorganisation (TCO)
36. Totalförsvarets forskningsinstitut
37. Tullverket
38. Umeå universitet (juridiska institutionen)
39. Åklagarmyndigheten

I utkastet till lagrådsremiss behandlas de lagförslag som lämnas i det tidigare remitterade betänkandet Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning (SOU 2024:59). I förhållande till förslagen i betänkandet har vissa ändringar gjorts. Det föreslås att begreppet strategiska förhållanden i 1 § andra stycket 3 lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska utgå. Det föreslås också en utökning av det högsta antal särskilda ledamöter som kan förordnas vid Försvarsunderrättelsedomstolen.

I remissen ligger att regeringen vill ha synpunkter på förslagen i de delar de skiljer sig från förslagen i det tidigare remitterade betänkandet. För de remissinstanser som tillkommit i förhållande det tidigare remitterade betänkandet anges inom parentes vilka delar de är särskilt berörda av.

Remissvaren ska ha kommit in till Försvarsdepartementet **senast den 3 oktober 2025**.

Skicka remissvar

- Remissvar mejlas till fo.remissvar@regeringskansliet.se med kopia till fo.rs.remissvar@regeringskansliet.se.

I mejlets ämnesrad

- Skriv in diarienummer Fö2024/01478 och remissinstansens namn.

Filnamn

- Filnamnen ska enbart vara remissinstansens namn. Ej diarienummer, ord, symboler eller siffror i filnamnen.

Remissvar skickas i två versioner:

- En Word
- En Pdf – som ska vara tillgänglighetsanpassad (enligt lagen (2018:1937) om tillgänglighet till digital offentlig service).

Remissvaren kommer att publiceras på regeringens webbplats.

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.

Utkastet till lagrådsremiss, det tidigare remitterade betänkandet och inkomna remissvar kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

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.

Mikael Andersson
Ämnesråd

Utkast till lagrådsremiss

Utkast lagrådsremiss Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning

Stockholm XXXXX

XXXXX

XXXXX
(Försvarsdepartementet)

Utkastets huvudsakliga innehåll

I utkastet föreslås en ny lag om signalspaning i försvarsunderrättelseverksamhet i krig eller krigsfara. Förslaget syftar till att möjliggöra för Försvarets radioanstalt att bedriva en effektiv och ändamålsenlig signalspaning även under sådana särskilda förhållanden.

Det föreslås även ändringar i lagen om signalspaning i försvarsunderrättelseverksamhet, som bland annat innebär följande:

- Ett nytt ändamål som möjliggör signalspaning i övningsverksamhet
- Ett reviderat ändamål om kartläggning av internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen
- Ett undantag för nödliknande situationer från det befintliga förbudet mot att inhämta signaler mellan en avsändare och mottagare som båda befinner sig i Sverige och från skyldigheten att förstöra sådana signaler
- En rätt för Inspektionen för strategiska produkter att inrikta signalspaning i försvarsunderrättelseverksamhet.

I utkastet föreslås även vissa ändringar i lagen om Försvarsunderrättelsedomstol i syfte att möjliggöra en än mer effektiv organisation och handläggning samt i lagen om behandling av personuppgifter vid Försvarets radioanstalt med anledning av det nya signalspaningsändamålet övningsverksamhet.

Den nya lagen och övriga lagändringar föreslås träda i kraft den 1 juni 2026.

Innehållsförteckning

1 Lagtext 6
1.1 Förslag till lag om signalspaning i försvarsunderrättelseverksamhet i krig eller krigsfara 6
1.2 Förslag till lag om ändring i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet 9
1.3 Förslag till lag om ändring i lagen (2009:966) om Försvarsunderrättelsedomstol 16
1.4 Förslag till lag om ändring i lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt 19

2 Ärendet och dess beredning 21

3 Signalspaning – en översikt av verksamheten och regelverket 22
3.1 Vad är signalspaning? 22
3.2 Försvarets radioanstalts uppgifter 22
3.2.1 Försvarets radioanstalts försvarsunderrättelseverksamhet 23
3.2.2 Försvarets radioanstalts utvecklingsverksamhet 25
3.3 Nuvarande reglering om signalspaning 26
3.3.1 Inriktning och ändamål för signalspaning 26
3.3.2 Inhämtning av signaler 27
3.3.3 Signalspaning kräver tillstånd 27
3.3.4 Förstöringsskyldighet 30
3.3.5 Rapportering 31
3.3.6 Underrättelseskyldighet till enskilda 32
3.3.7 Kontroll och tillsyn 32
3.3.8 Internationellt samarbete 34
3.3.9 Försvarets radioanstalts personuppgiftsbehandling 36

4 Skyddet för den personliga integriteten 39
4.1 Regeringsformen 39
4.2 Europakonventionen 40
4.3 Europarådets dataskyddskonvention 40
4.4 EU-stadgan 42

5 Signalspaning i krig och krigsfara 42
5.1 En översikt av den säkerhetspolitiska utvecklingen sedan signalspaningslagens tillkomst 42
5.2 Översiktligt om nationell reglering i krig 43
5.3 Grundläggande principer inom det svenska totalförsvaret 47
5.4 Försvarsunderrättelseverksamhet i ett allvarligt försämrat säkerhetsläge 47
5.4.1 Signalspaning i krig och krigsfara 48
5.5 Reglering av signalspaning i försvarsunderrättelseverksamhet i krig och krigsfara 49

5.5.1 En ny lag som reglerar signalspaning i försvarsunderrättelseverksamhet i krig och krigsfara ... 49
5.5.2 Tidpunkt för tillämpning ... 53
5.5.3 Inhämtningens omfattning ... 55
5.5.4 Det ska vara möjligt att tillåta ytterligare myndigheter att inrikta signalspaning i försvarsunderrättelseverksamhet ... 58
5.5.5 Ett särskilt tillståndsförfarande ... 60
5.5.6 Försvarets radioanstalt ska ha rådigheten över signalbärare ... 63
5.5.7 Kontroll och tillsyn ... 65
5.5.8 Mottagarens skydd för personuppgifter vid överföring till en utländsk mottagare ... 69
5.5.9 Tillsyn av personuppgiftsbehandling ... 71
5.5.10 Enskildas rätt till information ... 73

6 Inhämtning av signaler i elektronisk form – ett förtydligande i lag ... 74
6.1 Teknik- och telekommunikationsutvecklingens betydelse för tidigare lagstiftning ... 74
6.2 Teknik- och telekommunikationsutveckling sedan signalspaningslagens tillkomst ... 74
6.3 Ett förtydligande i lag av att signaler i elektronisk form får inhämtas oavsett var de befinner sig ... 75

7 Signalspaning i övningsverksamhet ... 81
7.1 Behov av signalspaning i övningsverksamhet ... 81
7.2 Ett nytt ändamål för signalspaning i övningsverksamhet ... 83
7.3 Inhämtning av inhemska signaler ... 86
7.4 Inriktning av signalspaning i övningsverksamhet ... 88
7.5 Tillstånd för signalspaning vid övningsverksamhet ... 89
7.6 Förstöringsskyldighet ... 90
7.7 Övningar får inte resultera i underrättelser ... 92
7.8 Internationellt samarbete ... 92
7.9 Ändamål för personuppgiftsbehandling i övningsverksamhet ... 94
7.10 Behandling av allmänt tillgänglig information ... 96
7.11 Behandling av personuppgifter i vissa fall ... 96
7.12 Överföring av personuppgifter till en mottagare utomlands ... 97

8 Inhämtning av inhemsk trafik i vissa brådskande situationer och en anpassad ändamålsbestämmelse ... 99
8.1 Förbudet mot att inhämta inhemsk trafik ... 99
8.2 Finns det behov av ytterligare undantag från förbudet mot att inhämta inhemsk trafik? ... 100
8.3 Inhämtning av inhemsk trafik i vissa brådskande situationer som innebär fara för människors liv eller hälsa eller för omfattande förstörelse av egendom ... 101
8.4 Undantag från förstöringsskyldigheten ... 107

8.5 En anpassad ändamålsbestämmelse 109
8.6 Gränsdragningen mellan försvarsunderrättelseverksamhet och brottsbekämpande verksamhet 113
8.7 Den personliga integriteten 114

9 Inriktning av signalspaning i försvarsunderrättelseverksamhet 117
9.1 Inspektionen för strategiska produkter ges rätt att inrikta signalspaning i försvarsunderrättelseverksamhet 117
9.2 Ett nytt ändamål för signalspaning införs....121

10 Övriga förslag 122
10.1 En övergripande redovisning av övrig inhämtning ska ingå i ansökan 122
10.2 Ett förtydligande av tillämplig bestämmelse 123
10.3 Underrättelseskyldigheten till enskilda upphävs 124
10.4 Försvarsunderrättelsedomstolen 126
10.4.1 Antalet särskilda ledamöter och förordnandetid för vice ordförande och de särskilda ledamöterna 126
10.4.2 Förordna och utse integritetsskyddsombud....128
10.4.3 Underrättelse till integritetsskyddsombud efter beslut från ordföranden 130
10.4.4 Deltagande i verksamheten efter att integritetsskyddsombudets förordnande upphört 132
10.4.5 Beslut om ersättning till integritetsskyddsombud....133

11 Ikraftträdande- och övergångsbestämmelser....134

12 Konsekvenser....134

13 Författningskommentar....138
13.1 Förslaget till lag om signalspaning i försvarsunderrättelseverksamhet i krig eller krigsfara ...138
13.2 Förslaget till lag om ändring i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet 145
13.3 Förslaget till lag om ändring i lagen (2009:966) om Försvarsunderrättelsedomstol....152
13.4 Förslaget till lag om ändring i lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt 154

Bilaga 1 Sammanfattning av slutbetänkandet Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning (SOU 2024:59) 157

Bilaga 2 Slutbetänkandets lagförslag....163

Bilaga 3 Förteckning över remissinstanserna 177

1 Lagtext

1.1 Förslag till lag om signalspaning i försvarsunderrättelseverksamhet i krig eller krigsfara

Härigenom föreskrivs följande.

Lagens tillämpning

1 § Om Sverige är i krig ska 5–14 §§ tillämpas.

2 § Om Sverige är i krigsfara eller om det råder sådana extraordinära förhållanden som är föranledda av krig eller av krigsfara som Sverige har befunnit sig i, får regeringen meddela föreskrifter om att 5–14 §§ helt eller delvis ska tillämpas från den tidpunkt som regeringen bestämmer.

En sådan föreskrift ska underställas riksdagen inom en månad från utfärdandet. Föreskriften upphör att gälla, om den inte underställs riksdagen i rätt tid eller om riksdagen inte godkänner den inom två månader från det att den underställdes.

3 § Under den tid som 5–14 §§ tillämpas gäller dessa bestämmelser, eller föreskrifter som meddelats med stöd av dem, i stället för avvikande bestämmelser i någon annan lag eller författning.

Regeringen ska föreskriva att bestämmelserna i 5–14 §§ inte ska tillämpas, när det inte längre råder sådana förhållanden som avses i 1 § eller 2 § första stycket.

4 § Med signalspaningsmyndighet och kontrollmyndighet i denna lag avses de myndigheter som anges i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Signalspaningens omfattning

5 § Bestämmelsen i 2 a § första stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, om att inhämtning inte får avse signaler mellan en avsändare och mottagare som båda befinner sig i Sverige, ska inte tillämpas om sådan inhämtning är av betydelse för att hantera yttre hot mot Sveriges säkerhet.

Inriktning

6 § Regeringen får meddela föreskrifter om att någon annan myndighet än de som anges i 4 § första stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet får inrikta signalspaning i försvarsunderrättelseverksamhet.

Regeringen får också besluta om detta i ett enskilt fall.

Tillstånd

7 § Tillstånd till signalspaning enligt 1 och 1 a §§ lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet får ges av den befattningshavare vid signalspaningsmyndigheten som regeringen föreskriver.

Tillstånd enligt första stycket får endast lämnas om förutsättningarna för tillstånd enligt 5 § lagen om signalspaning i försvarsunderrättelseverksamhet är uppfyllda.

8 § Tillstånd enligt 7 § ska utformas enligt 5 a § första och andra styckena lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Om det för fullgörande av inhämtningsuppdrag för vilket tillstånd getts uppstår behov av tillgång till ytterligare signalbärare eller användning av andra tillståndspliktiga sökbegrepp, gäller 5 a § tredje stycket lagen om signalspaning i försvarsunderrättelseverksamhet i tillämpliga delar.

Rådighet över signalbärare

9 § Signalspaningsmyndigheten ska ha rådigheten över sådana signalbärare som avses i 12 § första stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Signalspaningsmyndigheten ska begränsa sin tillgång till signalbärare till vad som följer av tillstånd enligt 7 §.

Överföring av personuppgifter till en mottagare utomlands

10 § Regeringen får meddela föreskrifter eller i ett enskilt fall besluta att personuppgifter som behandlas enligt lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt får överföras till ett annat land eller en internationell organisation även om förutsättningarna i 2 kap. 20 § första stycket 3 den lagen inte är uppfyllda.

Enskilds rätt till information

11 § Bestämmelserna om skyldighet att lämna information till en enskild enligt 5 kap. 2 § lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt ska inte tillämpas.

Kontroll och tillsyn

12 § Bestämmelserna om kontroll enligt 10 § första och andra styckena och 10 a § första och andra styckena lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska inte tillämpas.

13 § Integritetskyddsrådets uppgifter enligt 11 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska inte utföras.

14 § Tillsyn enligt lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt ska inte utföras.

15 § När det inte längre råder sådana förhållanden som anges i 1 § eller 2 § första stycket, ska kontrollmyndigheten kontrollera att denna lag har följts.

Vid sådan kontroll ska 10 § första och andra styckena lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet tillämpas.

16 § När det inte längre råder sådana förhållanden som anges i 1 § eller 2 § första stycket, ska det särskilda beslutandeorganet i kontrollmyndigheten tillämpa bestämmelserna i 10 a § första och andra styckena lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet på meddelanden och lagrade uppgifter som inhämtats i samband med signalspaning enligt denna lag och på tillstånd som lämnats enligt denna lag.

17 § Signalspaningsmyndigheten ska vidta de åtgärder som är nödvändiga för att underlätta kontroll enligt 15 och 16 §§.

Övriga bestämmelser

18 § Beslut enligt denna lag får inte överklagas.

Denna lag träder i kraft den 1 juni 2026.

1.2 Förslag till lag om ändring i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet

Härigenom föreskrivs i fråga om lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet[1]

dels att 11 a och 11 b §§ ska upphöra att gälla,

dels att rubriken närmaste före 11 a § ska utgå,

dels att 1–2 a, 4, 4 a, 5 a, 7–9 och 10 a §§ ska ha följande lydelse,

dels att det ska införas tre nya paragrafer, 1 a, 2 b och 12 b §§, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 §[2]	
I försvarsunderrättelseverksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet får den myndighet som regeringen bestämmer (signalspaningsmyndigheten) inhämta signaler i elektronisk form vid signalspaning. Signalspaning i försvarsunderrättelseverksamhet får endast ske i de fall regeringen eller en myndighet som anges i 4 § närmare har bestämt inriktningen av signalspaningen.	I försvarsunderrättelseverksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet får den myndighet som regeringen bestämmer (signalspaningsmyndigheten) inhämta signaler i elektronisk form vid signalspaning, *oavsett om signalerna är under förmedling eller är lagrade*. Signalspaning i försvarsunderrättelseverksamhet får endast ske i de fall regeringen eller en myndighet som anges i 4 § närmare har bestämt inriktningen av signalspaningen.

Signalspaning i försvarsunderrättelseverksamhet får ske endast i syfte att kartlägga

1. yttre militära hot mot landet,

2. förutsättningar för svenskt deltagande i fredsfrämjande och humanitära internationella insatser eller hot mot säkerheten för svenska intressen vid genomförandet av sådana insatser,

3. *strategiska förhållanden avseende* internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen,	3. internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen,
4. utveckling och spridning av massförstörelsevapen, krigsmateriel och produkter som avses i	4. utveckling och spridning av massförstörelsevapen, krigsmateriel och produkter som avses i

[1] Senaste lydelse av
11 a § 2009:967
11 b § 2009:967
rubriken närmast före 11 a § 2009:967.

[2] Senaste lydelse 2021:1173.

lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd,	lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd *samt strategiska förhållanden avseende sådana utländska direktinvesteringar som avses i lagen (2023:560) om granskning av utländska direktinvesteringar*,

5. allvarliga yttre hot mot samhällets infrastrukturer,
6. konflikter utomlands med konsekvenser för internationell säkerhet,
7. främmande underrättelseverksamhet mot svenska intressen,
8. främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik, eller
9. sådana företeelser som avses i 1–8, men som inte riktas mot Sverige eller rör svenska intressen, om det är nödvändigt för ett samarbete i underrättelsefrågor med andra länder och internationella organisationer som signalspaningsmyndigheten deltar i.

Om det är nödvändigt för försvarsunderrättelseverksamheten får signaler i elektronisk form inhämtas vid signalspaning även för att

1. följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet, samt
2. fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamhet enligt denna lag.

1 a §

Om det är nödvändigt för att utveckla förmågan att verka under höjd beredskap får signaler i elektronisk form även inhämtas vid övning.

2 §

Inhämtning som sker i tråd får endast avse signaler som förs över Sveriges gräns i tråd som ägs av en operatör.

Vid inhämtning enligt 1 och 1 a §§ av signaler i elektronisk form får signalspaningsmyndigheten vidta de tekniska åtgärder som är nödvändiga för att genomföra inhämtningen.

2 a §[3]

Inhämtning får inte avse signaler mellan en avsändare och mottagare som båda befinner sig i Sverige. Om sådana signaler inte kan avskiljas redan vid inhämtningen, ska upptagningen eller upptecknin gen förstöras så snart det står klart att sådana signaler har inhämtats. Kravet på förstöring gäller även i fråga om upptagningar och upptecknin gar som

[3] Senaste lydelse 2021:1173.

signalspaningsmyndigheten har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete.

Första stycket tillämpas inte i fråga om

1. signaler som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte innehåller personuppgifter, *eller*

2. signaler som sänds från eller till utländsk militär personal, utländska statsfartyg, statsluftfartyg eller militära fordon.

1. signaler som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte innehåller personuppgifter,

2. signaler som sänds från eller till utländsk militär personal, utländska statsfartyg, statsluftfartyg eller militära fordon, *eller*

3. signaler mellan en avsändare och en mottagare vid sådan övningsverksamhet som anges i 1 a §.

Första stycket och andra stycket 2 och 3 tillämpas även på signaler som lagras i Sverige.

2 b §

Bestämmelsen i 2 a § första stycket tillämpas inte i fråga om signaler i sådana brådskande situationer som innebär fara för människors liv eller hälsa eller för omfattande förstörelse av egendom.

Om sådana signaler som anges i 2 a § första stycket inte kan avskiljas redan vid inhämtningen, behöver upptagningen eller upptecknin gen inte förstöras om den innehåller

1. uppgifter om en brådskande situation, och

2. uppgifterna bedöms vara av avgörande betydelse för att skydda människors liv eller hälsa eller för att undvika omfattande förstörelse av egendom.

4 §[4]

I lagen (2000:130) om försvarsunderrättelseverksamhet finns bestämmelser om regeringens och myndigheters inriktning av sådan verksamhet. Inriktning av signalspaning får anges endast av

I lagen (2000:130) om försvarsunderrättelseverksamhet finns bestämmelser om regeringens och myndigheters inriktning av sådan verksamhet. Inriktning av signalspaning får anges endast av

[4] Senaste lydelse 2021:1173.

regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen *och* Nationella operativa avdelningen i Polismyndigheten.	regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen*,* Nationella operativa avdelningen i Polismyndigheten *och Inspektionen för strategiska produkter*.

Regeringen bestämmer inriktningen av sådan verksamhet som bedrivs enligt 1 § andra stycket 9 och tredje stycket.

	Regeringen och Försvarsmakten bestämmer inriktningen av sådan verksamhet som bedrivs enligt 1 a §.

En inriktning av signalspaningen får inte avse endast en viss fysisk person.

4 a §[5]

Signalspaningsmyndigheten ska ansöka om tillstånd hos Försvarsunderrättelsedomstolen för signalspaning enligt 1 §. En sådan ansökan ska innehålla uppgifter om	Signalspaningsmyndigheten ska ansöka om tillstånd hos Försvarsunderrättelsedomstolen för signalspaning enligt 1 och *1 a §§*. En sådan ansökan ska innehålla uppgifter om

1. det inhämtningsuppdrag som ansökan avser, med en närmare redogörelse för det behov som föranleder ansökan och uppgift om vilken inriktning uppdraget hänför sig till,

2. vilken eller vilka signalbärare avseende signaler i tråd som signalspaningsmyndigheten behöver ha tillgång till för att fullgöra uppdraget,	2. vilken eller vilka signalbärare avseende signaler i tråd som signalspaningsmyndigheten behöver ha tillgång till för att fullgöra uppdraget *samt en övergripande redovisning av övrig inhämtning*,

3. de sökbegrepp eller kategorier av sökbegrepp som är avsedda att användas vid inhämtningen,
4. vilken tid tillståndet ska gälla, och
5. de omständigheter i övrigt som myndigheten vill åberopa till stöd för sin ansökan.

5 a §[6]

I ett tillstånd ska anges

1. det inhämtningsuppdrag för vilket inhämtning får ske,
2. vilken eller vilka signalbärare avseende signaler i tråd som signalspaningsmyndigheten ska få tillgång till för att fullgöra uppdraget,
3. vilka sökbegrepp eller kategorier av sökbegrepp som får användas vid inhämtningen,
4. den tid som tillståndet avser, och

[5] Senaste lydelse 2009:967.
[6] Senaste lydelse 2009:967.

5. de villkor i övrigt som behövs för att begränsa intrånget i enskildas personliga integritet.

Ett tillstånd får ges för högst sex månader från dagen för beslutet och kan efter förnyad prövning förlängas med högst sex månader i taget.

Om det för fullgörande av inhämtningsuppdrag för vilket tillstånd *givits* uppstår behov av tillgång till ytterligare signalbärare *eller* användning av andra tillståndspliktiga sökbegrepp, ska särskilt tillstånd sökas. Vid ansökan och prövning gäller *4* och 5 §§ i tillämpliga delar. Ett sådant tillstånd ska ha samma varaktighet som tillståndet för det inhämtningsuppdrag *inom vilket tillgång till signalerna behövs eller sökbegreppen är avsedda att användas.*

Om det för fullgörande av inhämtningsuppdrag för vilket tillstånd *getts* uppstår behov av tillgång till ytterligare signalbärare, användning av andra tillståndspliktiga sökbegrepp *eller undantag enligt 2 b § första stycket*, ska särskilt tillstånd sökas. Vid ansökan och prövning gäller *4 a* och 5 §§ i tillämpliga delar. Ett sådant *särskilt* tillstånd ska *som längst* ha samma varaktighet som tillståndet för det inhämtningsuppdrag *som det särskilda tillståndet hänför sig till*.

7 §[7]

En upptagning eller uppteckning av uppgifter som har inhämtats enligt denna lag eller som signalspaningsmyndigheten har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete ska omgående förstöras om innehållet

1. har bedömts sakna betydelse för verksamhet som avses i 1 §,

1. har bedömts sakna betydelse för verksamhet som avses i 1 och *1 a §§*,

2. avser uppgifter för vilka tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen, eller som omfattas av efterforskningsförbudet i 3 kap. 5 § tryckfrihetsförordningen eller 2 kap. 5 § yttrandefrihetsgrundlagen,

3. omfattar uppgifter i sådana meddelanden mellan en person som är misstänkt för brott och hans eller hennes försvarare vilka skyddas enligt 27 kap. 22 § första stycket rättegångsbalken, eller

4. avser uppgifter lämnade under bikt eller enskild själavård, såvida det inte finns synnerliga skäl att behandla uppgifterna för syften som anges i 1 § andra stycket.

8 §[8]

Underrättelser med uppgifter som inhämtats enligt denna lag ska rapporteras till berörda myndigheter i enlighet med vad som föreskrivs i lagen (2000:130) om försvarsunderrättelseverksamhet. Om uppgifterna berör en viss fysisk person, får rapporteringen endast avse förhållanden som är av betydelse i de hänseenden som anges i 1 § den lagen.

[7] Senaste lydelse 2024:425.
[8] Senaste lydelse 2009:967.

	Uppgifter som inhämtats med stöd av 1 a § får inte resultera i underrättelser.

9 §[9]

I lagen (2000:130) om försvarsunderrättelseverksamhet finns bestämmelser om internationellt samarbete på försvarsunderrättelseområdet.

Signalspaningsmyndigheten får för den verksamhet som anges i 1 § tredje stycket, enligt regeringens närmare bestämmande, etablera och upprätthålla samarbete i signalspaningsfrågor med andra länder och internationella organisationer.	Signalspaningsmyndigheten får för den verksamhet som anges i 1 § tredje stycket och *1 a §*, enligt regeringens närmare bestämmande, etablera och upprätthålla samarbete i signalspaningsfrågor med andra länder och internationella organisationer.

10 a §[10]

Ett särskilt beslutandeorgan i kontrollmyndigheten är skyldigt att på begäran av en enskild kontrollera om hans eller hennes meddelanden har inhämtats i samband med signalspaning enligt denna lag och, om så är fallet, huruvida inhämtningen och behandlingen av inhämtade uppgifter har skett i enlighet med lag. Beslutandeorganet ska underrätta den enskilde om att kontrollen har utförts. Underrättelsen ska innehålla en motivering.	Ett särskilt beslutandeorgan i kontrollmyndigheten är skyldigt att på begäran av en enskild kontrollera om hans eller hennes meddelanden *eller lagrade uppgifter* har inhämtats i samband med signalspaning enligt denna lag och, om så är fallet, huruvida inhämtningen och behandlingen av inhämtade uppgifter har skett i enlighet med lag. Beslutandeorganet ska underrätta den enskilde om att kontrollen har utförts. Underrättelsen ska innehålla en motivering.

Beslutandeorganet får besluta att inhämtning avseende den som begärt kontrollen ska upphöra eller att upptagning eller uppteckning av inhämtade uppgifter ska förstöras, om det vid kontroll framkommer att inhämtningen inte är förenlig med tillstånd som lämnats enligt denna lag.

Ledamöterna i beslutandeorganet utses av regeringen för en bestämd tid. Ordföranden och vice ordföranden ska vara eller ha varit ordinarie domare eller ha motsvarande juridisk erfarenhet. Övriga ledamöter ska utses bland personer som föreslagits av partigrupperna i riksdagen.

[9] Senaste lydelse 2009:967.
[10] Senaste lydelse 2024:425.

12 b §

I lagen (2025:000) om signalspaning i försvarsunderrättelseverksamhet under krig eller krigsfara finns bestämmelser om signalspaning i försvarsunderrättelseverksamhet om Sverige är i krig eller i krigsfara eller det råder sådana extraordinära förhållanden som är föranledda av krig eller av krigsfara som Sverige har befunnit sig i.

Denna lag träder i kraft den 1 juni 2026.

1.3 Förslag till lag om ändring i lagen (2009:966) om Försvarsunderrättelsedomstol

Härigenom föreskrivs att 2, 6, 10 och 12 §§ lagen (2009:966) om Försvarsunderrättelsedomstol ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 §[1]	
Försvarsunderrättelsedomstolen består av en ordförande, en eller högst två vice ordförande samt minst två och högst *sex* särskilda ledamöter.	Försvarsunderrättelsedomstolen består av en ordförande, en eller högst två vice ordförande samt minst två och högst *åtta* särskilda ledamöter.
Ledamöterna ska vara svenska medborgare och får inte vara underåriga eller i konkurstillstånd eller ha förvaltare enligt 11 kap. 7 § föräldrabalken. Innan en ledamot börjar tjänstgöra i domstolen, ska han eller hon ha avlagt domared.	
I lagen (2010:1390) om utnämning av ordinarie domare finns bestämmelser om utnämning av ordförande i domstolen. Vice ordförande och särskilda ledamöter förordnas av regeringen för fyra år.	I lagen (2010:1390) om utnämning av ordinarie domare finns bestämmelser om utnämning av ordförande i domstolen. Vice ordförande och särskilda ledamöter förordnas av regeringen för *högst* fyra år *i sänder*.
6 §[2]	
Regeringen förordnar för minst fyra år i sänder personer som kan tjänstgöra som integritetsskydds-ombud. *Under fyraårsperioden får vid behov ytterligare personer förordnas för återstående del av perioden.*	Regeringen förordnar för *högst* fyra år i sänder personer som kan tjänstgöra som integritetsskydds-ombud.
Ett integritetsskyddsombud ska vara svensk medborgare och ska vara eller ha varit advokat eller ha varit ordinarie domare. Ett integritetsskyddsombud får inte vara i konkurstillstånd eller ha förvaltare enligt 11 kap. 7 § föräldrabalken.	
Regeringen ska inhämta förslag på lämpliga kandidater från Sveriges advokatsamfund och Domarnämnden.	
Ett integritetsskyddsombud får trots att regeringens förordnande har upphört slutföra pågående uppdrag.	

[1] Senaste lydelse 2010:1399.
[2] Ändringen innebär bl.a. att fjärde stycket tas bort.

10 §

Ordföranden får ensam på Försvarsunderrättelsedomstolens vägnar

1. företa förberedande åtgärder och besluta om avskrivning, *och*

2. pröva frågor enligt 5 a § tredje stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet om tillstånd i pågående och tillståndsprövade inhämtningsuppdrag, om prövningen är av enkel beskaffenhet och endast avser tillgång till signalbärare eller användning av sökbegrepp som inte är direkt hänförliga till viss fysisk person.

1. företa förberedande åtgärder och besluta om avskrivning,

2. pröva frågor enligt 5 a § tredje stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet om tillstånd i pågående och tillståndsprövade inhämtningsuppdrag, om prövningen är av enkel beskaffenhet och endast avser tillgång till signalbärare eller användning av sökbegrepp som inte är direkt hänförliga till *en* viss fysisk person, *och*

3. fatta beslut om ersättning till integritetsskyddsombud.

Ordföranden får förordna en lagfaren tjänsteman vid domstolen att ensam på domstolens vägnar vidta förberedande åtgärder.

12 §

När en ansökan om tillstånd till signalspaning har kommit in till domstolen, ska domstolen så snart som möjligt *utse ett integritetsskyddsombud i målet och* hålla ett sammanträde. Vid sammanträdet ska ansökande myndighet och integritetsskyddsombudet närvara. Domstolen får *förordna* att annan som kan lämna upplysningar av betydelse för prövningen får närvara vid sammanträdet.

När en ansökan om tillstånd till signalspaning har kommit in till domstolen, ska domstolen så snart som möjligt hålla ett sammanträde. Vid sammanträdet ska ansökande myndighet och *det integritetsskyddsombud som domstolen utser* närvara. Domstolen får *besluta* att *någon* annan som kan lämna upplysningar av betydelse för prövningen får närvara vid sammanträdet.

Om ärendet är så brådskande att ett dröjsmål allvarligt skulle riskera syftet med ansökan, får sammanträde hållas och beslut fattas utan att ett integritetsskyddsombud har varit närvarande eller annars fått tillfälle att yttra sig.

När ett beslut enligt 10 § första stycket 2 har fattats av ordföranden på domstolens vägnar ska det integritetsskyddsombud som varit närvarande vid prövningen av det inhämtningsuppdrag till vilket beslutet är hänförligt underrättas.

När ett beslut enligt andra stycket har fattats ska ett integritetsskyddsombud underrättas. När ett beslut enligt 10 § första stycket 2 har fattats av ordföranden på domstolens vägnar ska det integritetsskyddsombud som varit närvarande vid prövningen av det inhämtningsuppdrag till vilket beslutet är hänförligt underrättas. *Om integritetsskyddsombudets förordnande har upphört, får ett annat*

integritetsskyddsombud underrättas.

Denna lag träder i kraft den 1 juni 2026.

1.4 Förslag till lag om ändring i lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt

Härigenom föreskrivs i fråga om lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt

dels att 1 kap. 2 § och 2 kap. 9, 18 och 20 §§ ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 2 kap. 6 a och 6 b §§, och närmast före 2 kap. 6 a § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
2 §	
Denna lag gäller vid behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- *och utvecklingsverksamhet* samt informationssäkerhetsverksamhet.	Denna lag gäller vid behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- *, utvecklings-, och övnings-verksamhet* samt informations-säkerhetsverksamhet.
2 kap.	
	Övningsverksamhet
	6 a §
	Personuppgifter får behandlas i Försvarets radioanstalts övnings-verksamhet om det är nödvändigt för att bedriva sådan verksamhet som anges i 1 a § lagen (2008:717) om signalspaning i försvarsunder-rättelseverksamhet.
	6 b §
	Personuppgifter som behandlas med stöd av 6 a § får även behandlas om det är nödvändigt för att tillhandahålla information som behövs
	1. med anledning av samverkan med någon annan i fråga om övningsverksamhet, eller
	2. med anledning av samarbete om övningsverksamhet med andra länder eller internationella organisationer enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

9 §

Försvarets radioanstalt får behandla personuppgifter som utgör allmänt tillgänglig information om det är nödvändigt för den verksamhet som anges i 2, 5 och 7 §§.	Försvarets radioanstalt får behandla personuppgifter som utgör allmänt tillgänglig information om det är nödvändigt för den verksamhet som anges i 2, 5, *6 a* och 7 §§.

18 §

Hantering av information som innebär behandling av personuppgifter ska inte anses oförenlig med bestämmelserna i 1, 2, 5, 7, 9, 11–14 och 16 §§ i det skede av behandlingen då det inte har kunnat fastställas vilka personuppgifter som informationen innehåller.	Hantering av information som innebär behandling av personuppgifter ska inte anses oförenlig med bestämmelserna i 1, 2, 5, *6* a, 7, 9, 11–14 och 16 §§ i det skede av behandlingen då det inte har kunnat fastställas vilka personuppgifter som informationen innehåller.

20 §[1]

Personuppgifter som behandlas med stöd av denna lag får föras över till ett annat land eller en internationell organisation endast om det är nödvändigt för att Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet och	Personuppgifter som behandlas med stöd av denna lag får föras över till ett annat land eller en internationell organisation endast om det är nödvändigt för att Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet *eller övningssamarbetet* och

1. överföringen riktas till en utländsk underrättelse- eller säkerhetstjänst, eller ett underrättelse- eller säkerhetsorgan i en internationell organisation,
2. sekretess inte hindrar en överföring,
3. mottagaren garanterar tillräckligt skydd för personuppgifterna, och
4. överföringen inte innebär ett oproportionerligt intrång i den registrerades personliga integritet.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att överföring får ske även i andra fall än som anges i första stycket 1.

Regeringen får också besluta om sådan överföring i ett enskilt fall.

Denna lag träder i kraft den 1 juni 2026.

[1] Senaste lydelse 2024:426.

2 Ärendet och dess beredning

Den 14 juli 2022 beslutade regeringen att ge en särskild utredare i uppdrag att göra en översyn av lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (dir. 2022:120). Syftet med uppdraget var att säkerställa en modern och ändamålsenlig reglering som är anpassad efter den tekniska utvecklingen, omvärldsutvecklingen och de försvars- och säkerhetsmässiga behoven samt som beaktar skyddet för den personliga integriteten. En del av utredningsuppdraget var att analysera vilka åtgärder som bör vidtas för att ta om hand de brister som Europadomstolen i stor sammansättning (Grand Chamber) fann den 25 maj 2021 i sitt avgörande i målet Centrum för rättvisa mot Sverige (35252/08). En annan del av utredningsuppdraget var att analysera och bedöma dels vilka åtgärder som krävs för att Försvarets radioanstalt ska kunna bedriva en effektiv signalspaning oavsett säkerhetsläge, dels om fler myndigheter bör få inrikta signalspaning i försvarsunderrättelseverksamhet. Till utredaren knöts en parlamentarisk referensgrupp.

Utredningen, som antog namnet Utredningen om översyn av lagen om signalspaning i försvarsunderrättelseverksamhet, överlämnade i september 2023 sitt delbetänkande Signalspaning i försvarsunderrättelseverksamhet – frågor med anledning av Europadomstolens dom (SOU 2023:51). Förslagen i delbetänkandet har behandlats i regeringens proposition Signalspaning i försvarsunderrättelseverksamhet – åtgärder med anledning av Europadomstolens dom (prop. 2023/24:136, bet. 2023/24:FöU11, rskr. 2023/24:206).

I september 2024 överlämnade utredningen sitt slutbetänkande Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning (SOU 2024:59).

En sammanfattning av förslagen i slutbetänkandet finns i *bilaga 1*. Utredningens lagförslag finns i *bilaga 2*.

Slutbetänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 3*. Remissvaren finns tillgängliga på regeringens webbplats (regeringen.se) och i Försvarsdepartementet (Fö2024/01478).

Som ett led i den fortsatta beredningen av detta lagstiftningsärende har det utarbetats ett utkast till lagrådsremiss. I utkastet behandlas förslagen i slutbetänkandet. Det lämnas också kompletterande förslag.

3 Signalspaning – en översikt av verksamheten och regelverket

3.1 Vad är signalspaning?

Signalspaning är en metod för teknisk inhämtning av signaler i elektronisk form. Inhämtningen kan ske bland annat i etern och i tråd (kabel). Den inhämtade informationen bearbetas och analyseras vilket resulterar i underrättelser som rapporteras till berörda uppdragsgivare och myndigheter.

Möjligheten att använda signalspaning i försvarsunderrättelseverksamhet regleras framför allt i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet. Signalspaningsverksamheten är underkastad flera begränsningar, som att den bara får ske för vissa angivna syften och att dess inriktning endast får anges av vissa utpekade aktörer. All inhämtning av elektroniska signaler genom signalspaning kräver även tillstånd från Försvarsunderrättelsedomstolen. Därutöver har en särskild myndighet i uppgift att kontrollera att lagen om signalspaning i försvarsunderrättelseverksamhet följs.

3.2 Försvarets radioanstalts uppgifter

Försvarets radioanstalt är en civil myndighet under Försvarsdepartementet som bedriver signalspaning i försvarsunderrättelseverksamhet. Myndigheten har sedan bildandet 1942 bedrivit signalspaning mot eterburna signaler. Sedan 2009, när lagen om signalspaning i försvarsunderrättelseverksamhet trädde i kraft, bedriver myndigheten även signalspaning mot trådburna signaler.

Bestämmelser om Försvarets radioanstalts verksamhet finns förutom i lagen om signalspaning i försvarsunderrättelseverksamhet (fortsättningsvis signalspaningslagen) även bl.a. i lagen (2000:130) och förordningen (2000:131) om försvarsunderrättelseverksamhet, förordningen (2008:923) om signalspaning i försvarsunderrättelseverksamhet samt lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt (FRA-PuL) och förordningen (2021:1208) om behandling av personuppgifter vid Försvarets radioanstalt (FRA-PuF).

Försvarets radioanstalts uppgifter framgår av förordningen (2007:937) med instruktion för Försvarets radioanstalt. Enligt 1 § har Försvarets radioanstalt till uppgift att bedriva signalspaning enligt lagen om signalspaning i försvarsunderrättelseverksamhet och anslutande förordning. Av 2 § framgår att Försvarets radioanstalt särskilt ska följa förändringen av signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet, fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten samt utföra matematiska bedömningar av kryptosystem för totalförsvaret. Försvarets radioanstalt ska vidare upprätthålla kompetensen för de nationella behoven i fråga om kryptologi (2 a §) samt biträda andra myndigheter vid värdering, utveckling,

anskaffning och drift av signalspaningssystem (3 §). Försvarets radioanstalt ska också stödja Försvarsmakten genom att utveckla metodik och utbilda personal inom signalspaningsområdet (3 a §), stödja Försvarsmaktens deltagande i internationella insatser med kompetens, personal och materiel (3 b §), vidmakthålla och utveckla signalreferensbibliotek för Försvarsmaktens behov (3 c §) samt stödja Försvarsmakten i verksamhet som avser utveckling och vidmakthållande av Försvarsmaktens cyberförsvarsförmåga (3 e §). Försvarets radioanstalt får på uppdrag av Försvarets materielverk utföra prov och utveckling inom teleteknikområdet (3 d §).

Av 4 § i samma förordning framgår att Försvarets radioanstalt ska ha hög teknisk kompetens inom informationssäkerhetsområdet och att myndigheten, efter begäran, får stödja sådana statliga myndigheter och enskilda verksamhetsutövare som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. Försvarets radioanstalt ska särskilt kunna stödja insatser vid nationella kriser med it-inslag, medverka till identifieringen av inblandade aktörer vid it-relaterade hot mot samhällsviktiga system, genomföra it-säkerhetsanalyser och ge annat tekniskt stöd. Försvarets radioanstalt ska samverka med andra organisationer inom informationssäkerhetsområdet såväl inom som utom landet.

Sedan den 1 november 2024 är Nationellt cybersäkerhetscenter en del av Försvarets radioanstalt. Centret har till uppgift att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter (4 a §). Kompletterande bestämmelser om centrets uppgifter finns i förordningen (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt.

3.2.1 Försvarets radioanstalts försvarsunderrättelseverksamhet

Nuvarande reglering av försvarsunderrättelseverksamheten

Av 1 § lagen (2000:130) om försvarsunderrättelseverksamhet framgår att försvarsunderrättelseverksamhet ska bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. I verksamheten ingår att medverka i svenskt deltagande i internationellt säkerhetssamarbete. Försvarsunderrättelseverksamhet får endast avse utländska förhållanden. Av 1 § framgår vidare att regeringen bestämmer inriktningen för försvarsunderrättelseverksamheten och inom ramen för den inriktningen får de myndigheter som regeringen bestämmer ange en närmare inriktning av verksamheten. I signalspaningslagen finns särskilda bestämmelser om inriktning.

Försvarsunderrättelseverksamhet bedrivs enligt 2 § lagen om försvarsunderrättelseverksamhet genom inhämtning, bearbetning och analys av information. Processen resulterar i underrättelser som ska rapporteras till berörda myndigheter.

Försvarets radioanstalt är enligt 2 § förordningen om försvarsunderrättelseverksamhet en av de myndigheter som ska bedriva försvarsunderrättelseverksamhet.

Enligt 4 § första stycket lagen om försvarsunderrättelseverksamhet får det inom ramen för försvarsunderrättelseverksamheten inte vidtas åtgärder som syftar till att lösa uppgifter som enligt lagar eller andra föreskrifter ligger inom ramen för Polismyndighetens, Säkerhetspolisens och andra myndigheters brottsbekämpande och brottsförebyggande verksamheter. Enligt förarbetena är bestämmelsen inte avsedd att utgöra något hinder för till exempel signalspaning även när det gäller sådana förhållanden som är av relevans för det brottsbekämpande arbetet, eftersom sådan verksamhet inte bedrivs på sådant sätt att den kan störa andra myndigheters verksamhet och den inte heller syftar till att lösa en föreskriven uppgift för brottsbekämpande och brottsförebyggande verksamhet (prop. 2006/07:63 s. 48). Stöd får, enligt 4 § andra stycket lagen om försvars-underrättelseverksamhet, lämnas till andra myndigheters brotts-bekämpande och brottsförebyggande verksamhet, om det inte finns hinder enligt andra bestämmelser.

Av 1 § lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott framgår att uppgifter i underrättelser som Försvarets radioanstalt rapporterat till en annan myndighet enligt lagen om försvarsunderrättelseverksamhet inte får användas för att utreda brott. Enligt 2 § samma lag ska de brottsbekämpande myndigheterna se till att tillgången till sådana uppgifter som avses i 1 § begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter och det ska särskilt beaktas att uppgifterna inte får användas för att utreda brott.

Signalspaning i försvarsunderrättelseverksamhet

Som nämnts inledningsvis är signalspaning en form av teknisk inhämtning. Efter inhämtning bearbetar och analyserar Försvarets radioanstalt signalerna och rapporterar resultaten i form av underrättelser till uppdragsgivare och andra berörda myndigheter. De olika momenten i processen kräver olika typer av kompetenser, alltifrån dataanalys, språk och underrättelseanalys till kryptologi, telekommunikation och teknik. Verksamheten grundas alltid i uppdragsgivarnas inriktningar, såväl kortsiktiga som långsiktiga.

Signalspaningen tar i hög grad sikte på innehållet i kommunikationer och på information som på annat sätt hanteras i elektronisk form. Det kan till exempel röra sig om textmeddelanden, talad kommunikation eller dokument. Ett centralt inslag i verksamheten utgörs även av inhämtning och analys av trafikdata som härrör från så kallade kommunikations-händelser. Syftet är bland annat att fastställa vilka aktörer som kommunicerar med varandra och var dessa befinner sig. Andra delar av signalspaningen avser i stället att fastställa tekniska detaljer om framför allt radarsignaler från fartyg eller flygplan.

Med utgångspunkt i uppdragsgivarnas inriktningar av signalspaningen, inriktningarnas prioriteringar, tillgängliga resurser, accesser och övriga förmågor identifierar Försvarets radioanstalt vilka underrättelsebehov som det finns förutsättningar att uppfylla. Förutsättningarna påverkas av ett flertal faktorer, bland annat personella, kompetensmässiga och tekniska samt tillgången till relevanta språkkompetenser, kryptologisk expertis och teknisk utvecklingsverksamhet.

Försvarets radioanstalts försvarsunderrättelseverksamhet tar bland annat sikte på att upptäcka ännu okända hotaktörer, företeelser och uppgifter av relevans om dessa. Det kan exempelvis röra sig om uppgifter om nya utländska hot mot svenska säkerhetsintressen, samhällsviktiga funktioner eller svensk hemlig information som inte får röjas för främmande makt. Rapportering från Försvarets radioanstalt om nya hot uppmärksammar uppdragsgivare och andra berörda myndigheter på information och sakförhållanden av betydelse för deras egna verksamheter. Underrättelserna möjliggör till exempel för dem att vidta åtgärder för att reducera de hot som Försvarets radioanstalt rapporterat om eller att uppdatera underlag som ska ligga till grund för eget agerande av annat slag. Underrättelser från Försvarets radioanstalt används även som ingångsvärden till uppdragsgivarnas egen underrättelseverksamhet.

I signalspaningsverksamheten ingår även att kartlägga och följa upp redan kända företeelser och följa förändringar i dessa för att tidigt få kunskap om hotaktörers nya ambitioner, avsikter och förmågor. Signalspaningen är också ett centralt verktyg vid kartläggning i efterhand av händelser som oförutsett har inträffat. Genom sådan uppföljning kan ytterligare underrättelseinformation produceras som ger bättre förståelse för orsakerna bakom det inträffade. Det kan också ge kompletterande information om till exempel kvarvarande oupptäckta hot. Vid uppföljning av till exempel terrorattentat kan efterhandsanalys av trafikdata, och de kommunikationshändelser som föregick attentatet, ge möjlighet att identifiera bakomliggande aktörer och eventuella hotaktörer som ännu inte upptäckts och som planerar ytterligare attentat.

3.2.2 Försvarets radioanstalts utvecklingsverksamhet

För att kunna tillgodose uppdragsgivarnas underrättelsebehov behöver Försvarets radioanstalt ingående kunskap om signalmiljön för att på ett effektivt sätt kunna rikta inhämtningskapacitet mot adekvata delar av signalmiljön samt för att kunna urskilja, extrahera och tyda den relevanta informationen. För detta krävs expertkunskaper om såväl signalmiljöns strukturer som dess användning för kommunikation och informationshantering. Försvarets radioanstalt behöver bland annat kontinuerligt hålla sig uppdaterad om olika signalbärares och frekvensers relevans för myndighetens underrättelseproduktion. Försvarets radioanstalt bedriver därför en utvecklingsverksamhet för att etablera och upprätthålla en tillräckligt god förståelse av signalmiljön, samt tillräckligt god förmåga att kunna inhämta, bearbeta och analysera den information som förekommer i signalmiljön.

I signalspaningsverksamhetens inhämtnings- och bearbetningsprocesser behöver dagligen anpassningar och justeringar göras med anledning av förändringar i signalmiljön som påverkar förutsättningarna att inhämta, bearbeta och analysera i enlighet med uppdragsgivarnas inriktningar. Verksamheten är under ständig utveckling. Av omvärldens förändringar i kombination med telekommunikationsoperatörernas dynamiska utnyttjande av tillgängliga kommunikationsvägar samt den allt snabbare utvecklingstakten inom teknik och telekommunikationer följer att det för

signalspaningen aldrig finns några garantier att den information som inhämtas i dag även kommer att kunna inhämtas i morgon.

Den information som Försvarets radioanstalt strävar efter att finna och rapportera, i syfte att tillgodose uppdragsgivarnas underrättelsebehov, är därtill oftast känslig eller hemlig och därför skyddsvärd för den aktör som hanterar informationen. Informationen är oftast avsedd att hanteras konfidentiellt och därför försedd med någon form av åtkomstskydd för att förhindra obehörig åtkomst. Det krävs då aktuell och ingående kunskap dels om hur signaler förmedlas och hanteras i elektronisk form, dels om de mekanismer som används för att skydda informationen.

Utvecklingsverksamheten syftar enbart till att utveckla, etablera och vidmakthålla de förmågor som är nödvändiga för försvarsunderrättelseverksamheten.

3.3 Nuvarande reglering om signalspaning

3.3.1 Inriktning och ändamål för signalspaning

Signalspaning i försvarsunderrättelseverksamhet får, enligt 1 och 4 §§ signalspaningslagen, inriktas av regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten. Försvarets radioanstalt kan således inte initiera någon signalspaning utanför uppdragsgivarnas inriktningar. Endast regeringen kan inrikta Försvarets radioanstalts utvecklingsverksamhet och den verksamhet som bedrivs enligt 1 § andra stycket 9 signalspaningslagen. Av 4 § tredje stycket signalspaningslagen framgår att inriktning av signalspaning inte får avse endast en viss fysisk person.

Signalspaning får i enlighet med vad som anges i 1 § andra stycket signalspaningslagen endast bedrivas i syfte att kartlägga

1. yttre militära hot mot landet,
2. förutsättningar för svenskt deltagande i fredsfrämjande och humanitära internationella insatser eller hot mot säkerheten för svenska intressen vid genomförandet av sådana insatser,
3. strategiska förhållanden avseende internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen,
4. utveckling och spridning av massförstörelsevapen, krigsmateriel och produkter som avses i lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd,
5. allvarliga yttre hot mot samhällets infrastrukturer,
6. konflikter utomlands med konsekvenser för internationell säkerhet,
7. främmande underrättelseverksamhet mot svenska intressen,
8. främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik, eller
9. sådana företeelser som avses i 1–8, men som inte riktas mot Sverige eller rör svenska intressen, om det är nödvändigt för ett samarbete i underrättelsefrågor med andra länder och internationella organisationer som signalspaningsmyndigheten deltar i.

För Försvarets radioanstalts utvecklingsverksamhet anges i 1 § tredje stycket signalspaningslagen att om det är nödvändigt för försvars-underrättelseverksamheten får signaler i elektronisk form inhämtas vid signalspaning för att följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet samt för att fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamhet enligt signalspaningslagen.

3.3.2 Inhämtning av signaler

Inhämtning av signaler i tråd får, enligt 2 § signalspaningslagen, endast avse signaler som förs över Sveriges gräns i tråd som ägs av en operatör. Av 2 a § signalspaningslagen framgår att signaler mellan en avsändare och mottagare som båda befinner sig i Sverige inte får inhämtas. Förbudet omfattar dock, enligt andra stycket samma bestämmelse, inte signaler som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte innehåller personuppgifter, eller som sänds till eller från utländsk militär personal, utländska statsfartyg, statsluftfartyg eller militära fordon.

Inhämtning av signaler i tråd får enligt 3 § signalspaningslagen endast ske automatiserat och får endast avse signaler som identifierats med hjälp av sökbegrepp. Det framgår vidare att även vid annan automatiserad inhämtning ska sökbegrepp användas för identifiering av signaler. Sökbegrepp ska enligt samma bestämmelse utformas och användas med respekt för enskildas personliga integritet och så att signalspaningen medför ett så begränsat integritetsintrång som möjligt. För sökbegrepp som är direkt hänförliga till en viss fysisk person gäller därutöver att de endast får användas om det är av synnerlig vikt för verksamheten.

Sökbegreppen kan beskrivas som en representation av de aktörer, organisationer, plattformar eller tekniska system som signalspaningen behöver riktas mot. Sökbegreppen gör det inhämtningstekniskt möjligt för Försvarets radioanstalt att hitta och identifiera den relevanta informationen. En källa kan representeras av ett eller flera sökbegrepp. Ett enskilt sökbegrepp kan ofta hänföras till en viss kommunikationstjänst som källan använder sig av, till exempel en specifik mobiltelefonitjänst eller e-posttjänst. Utgångspunkten är att ju högre precision ett sökbegrepp har, desto snävare blir det samlade integritetsintrånget vid signalspaningen (jfr prop. 2006/07:63 s. 77).

3.3.3 Signalspaning kräver tillstånd

All inhämtning av signaler i elektronisk form vid signalspaning kräver tillstånd. Kravet på tillstånd gäller oavsett för vilket syfte som inhämtning sker och oberoende av vilken teknik som används. Det är Försvarsunderrättelsedomstolen som prövar frågor om tillstånd till signalspaning.

Försvarsunderrättelsedomstolens prövning av tillstånd

Bestämmelser om domstolen finns i lagen (2009:966) om Försvarsunderrättelsedomstol och i förordningen (2009:968) med instruktion för Försvarsunderrättelsedomstolen.

Försvarsunderrättelsedomstolen består av en ordförande, en eller högst två vice ordförande samt minst två och högst sex särskilda ledamöter. Ordföranden och vice ordförandena ska vara lagfarna med erfarenhet av tjänstgöring som domare. De särskilda ledamöterna ska ha särskild kunskap om förhållanden av betydelse för domstolens verksamhet. Ordföranden anställs av regeringen som ordinarie domare i domstolen. Vice ordförandena och de särskilda ledamöterna förordnas av regeringen för fyra år (2 och 3 §§ lagen om Försvarsunderrättelsedomstol).

Enligt 9 § lagen om Försvarsunderrättelsedomstolen är domstolen domför med ordföranden och två särskilda ledamöter.

Ordföranden får ensam på Försvarsunderrättelsedomstolens vägnar företa förberedande åtgärder och besluta om avskrivning. Ordföranden får också pröva frågor enligt 5 a § tredje stycket signalspaningslagen om tillstånd i pågående och tillståndsprövade inhämtningsuppdrag, om prövningen är av enkel beskaffenhet och endast avser tillgång till signalbärare eller användning av sökbegrepp som inte är direkt hänförliga till viss fysisk person (10 § första stycket lagen om Försvarsunderrättelsedomstol). Av 4 § följer att en vice ordförande träder i ordförandens ställe om ordföranden är förhindrad att tjänstgöra.

Vid domstolen finns även integritetsskyddsombud som på ett generellt plan ska bevaka enskildas integritetsintresse i domstolens mål. Ombudet har rätt att ta del av det som förekommer i målet och att yttra sig (5 § lagen om Försvarsunderrättelsedomstol). Regeringen förordnar för minst fyra år i sänder personer som kan tjänstgöra som integritetsskyddsombud. Under fyraårsperioden får vid behov ytterligare personer förordnas för återstående del av perioden. Ett integritetsskyddsombud ska vara svensk medborgare och ska vara eller ha varit advokat eller ha varit ordinarie domare. Ett integritetsskyddsombud får trots att regeringens förordnande har upphört slutföra pågående uppdrag (6 § första, andra och fjärde styckena lagen om Försvarsunderrättelsedomstol). Systemet med integritetsskyddsombud har utformats i huvudsak i enlighet med vad som gäller för offentliga ombud i ärenden om vissa hemliga tvångsmedel i allmän domstol (prop. 2008/09:201 s. 69 ff.).

Försvarets radioanstalts ansökan om signalspaning prövas vid ett sammanträde där Försvarets radioanstalt och ett integritetsskyddsombud närvarar. Domstolen ska enligt 12 § första stycket lagen om Försvarsunderrättelsedomstol när ansökan kommit in så snart som möjligt utse ett integritetsombud i målet och hålla sammanträde. Av paragrafens andra stycke framgår att om ärendet är så brådskande att ett dröjsmål allvarligt skulle riskera syftet med ansökan, får sammanträde hållas och beslut fattas utan att ett integritetsskyddsombud har varit närvarande eller annars fått tillfälle att yttra sig. Av förarbetena framgår att ombudet i sådana fall ska ha rätt att ta del av uppgifterna i efterhand (prop. 2008/09:201 s. 71).

Om ordföranden på domstolens vägnar fattat beslut i frågor enligt 5 a § tredje stycket signalspaningslagen ska det integritetsskyddsombud som

varit närvarande vid prövningen av det inhämtningsuppdrag till vilket beslutet är hänförligt underrättas (12 § tredje stycket lagen om Försvarsunderrättelsedomstol).

Ansökan och tillstånd

Försvarets radioanstalt ska enligt 4 a § signalspaningslagen ansöka om tillstånd för signalspaning hos Försvarsunderrättelsedomstolen. Ansökan ska bland annat innehålla uppgifter om det inhämtningsuppdrag som ansökan avser med en närmare redogörelse för det behov som föranleder ansökan och uppgift om vilken inriktning uppdraget hänför sig till, vilken eller vilka signalbärare avseende signaler i tråd som signalspaningsmyndigheten behöver ha tillgång till för att fullgöra uppdraget, de sökbegrepp eller kategorier av sökbegrepp som är avsedda att användas och vilken tid tillståndet ska gälla.

Tillstånd får enligt 5 § signalspaningslagen endast lämnas om uppdraget är förenligt med lagen om försvarsunderrättelseverksamhet och signalspaningslagen, syftet med inhämtningen inte kan tillgodoses på ett mindre ingripande sätt, uppdraget beräknas ge information vars värde är klart större än det integritetsintrång som inhämtning i enlighet med ansökan kan innebära, de sökbegrepp eller kategorier av sökbegrepp som är avsedda att användas är förenliga med 3 § signalspaningslagen samt ansökan inte avser endast en viss fysisk person.

Av 5 a § signalspaningslagen framgår vad tillståndet ska innehålla. I tillståndet ska anges bl.a. det inhämtningsuppdrag för vilket inhämtning får ske, vilken eller vilka signalbärare avseende signaler i tråd som signalspaningsmyndigheten ska få tillgång till för att fullgöra uppdraget, vilka sökbegrepp eller kategorier av sökbegrepp som får användas vid inhämtningen, den tid som tillståndet avser och de villkor i övrigt som behövs för att begränsa intrånget i enskildas personliga integritet. Ett tillstånd får ges för högst sex månader från dagen för beslutet och kan efter förnyad prövning förlängas med högst sex månader i taget. Av samma bestämmelse framgår att särskilt tillstånd ska sökas om det för fullgörande av inhämtningsuppdrag för vilket tillstånd givits uppstår behov av tillgång till ytterligare signalbärare eller användning av andra tillståndspliktiga sökbegrepp. Vid ansökan och prövning gäller 4 och 5 §§ signalspaningslagen i tillämpliga delar. Ett sådant tillstånd ska ha samma varaktighet som tillståndet för det inhämtningsuppdrag inom vilket tillgång till signalerna behövs eller sökbegreppen är avsedda att användas.

I 5 b § signalspaningslagen finns bestämmelser om brådskande förfarande. Om det kan befaras att inhämtande av Försvarsunderrättelsedomstolens tillstånd skulle medföra sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för något av de i 1 § signalspaningslagen angivna syftena, får tillstånd till signalspaningen ges av den befattningshavare vid signalspaningsmyndigheten som regeringen föreskriver. Ett sådant tillstånd ska utformas i enlighet med 5 a § signalspaningslagen. Om tillstånd har lämnats ska åtgärden genast anmälas skriftligen till Försvarsunderrättelsedomstolen. I anmälan ska skälen för åtgärden anges. Försvarsunderrättelsedomstolen ska skyndsamt pröva ärendet och, om den finner att det inte finns skäl för åtgärden, upphäva eller ändra beslutet. Om Försvarsunderrättelse-

domstolen ändrar ett brådskande beslut ska även sådan upptagning eller uppteckning av uppgifter som kan hänföras till ändringen omgående förstöras i den utsträckning upptagningen eller uppteckningen kan hänföras till ändringen. Om beslutet upphört att gälla innan domstolen har prövat ärendet, ska Försvarets radioanstalt anmäla åtgärden till kontrollmyndigheten Statens inspektion för försvarsunderrättelseverksamheten. Av 2 § förordningen om signalspaning i försvarsunderrättelseverksamhet framgår att Försvarets radioanstalts myndighetschef eller dennes ställföreträdare kan fatta beslut enligt 5 b § signalspaningslagen.

Försvarsunderrättelsedomstolens beslut i frågor som rör signalspaning, eller domstolens beslut i övrigt, kan inte överklagas.

3.3.4 Förstöringsskyldighet

Försvarets radioanstalt är under vissa omständigheter skyldig att omgående förstöra en upptagning eller uppteckning med visst innehåll.

Om Försvarets radioanstalt inhämtat signaler mellan mottagare och avsändare som båda befinner sig i Sverige ska enligt 2 a § signalspaningslagen upptagningen eller uppteckningen omgående förstöras så snart det kan klarläggas att sådana signaler inhämtats. Kravet på förstöring gäller även i fråga om upptagningar och uppteckningar som Försvarets radioanstalt har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete. Oavsett innehållet i signalerna får de inte hanteras i annan utsträckning än vad som krävs för att konstatera att förstöringsskyldighet föreligger (prop. 2008/09:201 s. 41).

Enligt 7 § signalspaningslagen ska upptagning eller uppteckning av uppgifter som inhämtats eller som Försvarets radioanstalt har fått från ett annat land eller en annan internationell organisation inom ramen för ett internationellt samarbete förstöras om innehållet

1. har bedömts sakna betydelse för verksamhet som avses i 1 § signalspaningslagen,
2. avser uppgifter för vilka tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen, eller som omfattas av efterforskningsförbudet i 3 kap. 5 § tryckfrihetsförordningen eller 2 kap. 5 § yttrandefrihetsgrundlagen,
3. omfattar uppgifter i sådana meddelanden mellan en person som är misstänkt för brott och hans eller hennes försvarare vilka skyddas enligt 27 kap. 22 § första stycket rättegångsbalken, eller
4. avser uppgifter lämnade under bikt eller enskild själavård, såvida det inte finns synnerliga skäl att behandla uppgifterna för syften som anges i 1 § andra stycket signalspaningslagen.

I fråga om den första punkten framgår det av förarbetena att det i automatisk och manuell inhämtning kan komma att finnas uppgifter om fysiska personer som saknar relevans för försvarsunderrättelse- och utvecklingsverksamheten. En upptagning eller uppteckning som innehåller både relevant och irrelevant information ska dock inte förstöras då den i vart fall till viss del har betydelse för verksamheten

(prop. 2006/07:63 s. 104–105). Däremot får inte överskottsinformation rörande enskilda som saknar relevans från försvarsunderrättelsesynpunkt rapporteras (samma prop. s. 108–109 och 140–141). I och med den lagändring som trädde i kraft den 1 juli 2024 gäller förstöringsskyldigheten enligt första punkten oavsett av om upptagningen eller upptecknigen innehåller personuppgifter eller inte. Någon förändring i fråga om hur material ska hanteras om det innehåller uppgifter som både är relevanta och saknar betydelse ur underrättelsesynpunkt är inte avsedd med ändringen (prop. 2023/24:136 s. 47).

Kravet på förstöring av uppgifter som omfattas av andra och tredje punkten är absolut. Någon annan bedömning av innehållet i upptagningen eller upptecknigen än vad som krävs för att konstatera om förstöringsskyldighet föreligger ska inte göras (jfr prop. 2006/07:63. s. 105–106 och 140). Förstöringsskyldigheten för uppgifter som omfattas av fjärde punkten är långtgående. Förstöringsskyldigheten skulle dock exempelvis kunna underlåtas om en religiös företrädare inom ramen för själavårdande samtal till exempel uppmanar till terrorism eller angrepp mot svenska förband i internationella insatser (prop. 2008/09:201 s. 114).

Om det vid en kontroll av kontrollmyndigheten framkommer att inhämtning inte är förenlig med det tillstånd som meddelats får myndigheten, enligt 10 § signalspaningslagen, besluta att viss inhämtning ska upphöra eller att upptagning eller upptecknig av inhämtade uppgifter ska förstöras. Det särskilda beslutandeorganet i kontrollmyndigheten som från och med den 1 januari 2025 prövar begäran om kontroll från enskild enligt 10 a § signalspaningslagen har en liknande möjlighet att besluta om att inhämtning ska upphöra eller att en upptagning eller upptecknig ska förstöras.

Av 5 § förordningen om signalspaning i försvarsunderrättelse-verksamhet framgår att förstöring av upptagningar eller upptecknigar enligt 7, 10 och 10 a §§ signalspaningslagen ska ske på ett sådant sätt att uppgifterna inte kan återskapas.

3.3.5 Rapportering

Underrättelser med uppgifter som inhämtats genom signalspaning i försvarsunderrättelseverksamhet ska enligt 8 § första meningen signalspaningslagen rapporteras till berörda myndigheter i enlighet med vad som föreskrivs i lagen om försvarsunderrättelseverksamhet. Rapporteringen till berörda myndigheter sker generellt sett utifrån aktuell situation. I normalfallet är rapporteringen skriftlig men även andra sätt kan vara godtagbara.

Om uppgifterna berör en viss fysisk person, får rapporteringen endast avse förhållanden som är av betydelse för försvarsunderrättelse-verksamheten (8 § andra meningen signalspaningslagen). Bestämmelsen innebär ett förbud mot rapportering av sådan överskottsinformation rörande enskilda som saknar relevans från försvarsunderrättelsesynpunkt (prop. 2006/07:63 s. 141).

3.3.6 Underrättelseskyldighet till enskilda

Om det vid signalspaning har använts sökbegrepp som är direkt hänförliga till en viss fysisk person ska denne enligt 11 a § signalspaningslagen underrättas om det. En underrättelse ska innehålla uppgift om när inhämtning har skett och syftet med inhämtningen. Underrättelsen ska lämnas så snart det kan ske utan men för försvarsunderrättelseverksamheten, men senast en månad efter att inhämtningsuppdraget som föranlett inhämtningen avslutats.

Av 11 b § signalspaningslagen framgår att underrättelse dock får skjutas upp om sekretess hindrar att underrättelsen lämnas. Om det på grund av sekretess inte har kunnat lämnas någon underrättelse inom ett år från att inhämtningsuppdraget avslutades, behöver någon underrättelse inte lämnas. Underrättelse ska inte lämnas om inhämtningen uteslutande avsett främmande makts förhållanden eller förhållanden mellan främmande stater.

3.3.7 Kontroll och tillsyn

Statens inspektion för försvarsunderrättelseverksamheten

Statens inspektion för försvarsunderrättelseverksamheten (Siun) ansvarar för kontrollen av försvarsunderrättelseverksamheten hos de myndigheter, däribland Försvarets radioanstalt, som bedriver sådan verksamhet. Siun är därutöver kontrollmyndighet enligt signalspaningslagen och har till uppgift att kontrollera att signalspaningslagen följs. Dessutom ska Siun granska sådan behandling av personuppgifter som utförs i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet med stöd av FRA-PuL. Bestämmelser som rör Siun och dess verksamhet finns i bland annat lagen om försvarsunderrättelseverksamhet och anslutande förordning, signalspaningslagen och förordningen (2009:969) med instruktion för Statens inspektion för försvarsunderrättelseverksamheten.

Av 10 § signalspaningslagen framgår att Siun ska ledas av en nämnd vars ledamöter utses av regeringen för en bestämd tid, minst fyra år, att ordföranden och vice ordföranden ska vara eller ha varit ordinarie domare och att övriga ledamöter ska utses bland personer som föreslagits av partigrupperna i riksdagen. Nämnden får ha högst sju ledamöter, vilket framgår av 8 § i nyss nämnda förordning.

Siuns kontroll av om signalspaningslagen följs ska enligt 10 § signalspaningslagen särskilt avse granskning av sökbegrepp enligt 3 §, förstöring av uppgifter enligt 7 § samt rapportering enligt 8 §. Om det vid en kontroll framkommer att inhämtningen inte är förenlig med det tillstånd som Försvarsunderrättelsedomstolen meddelat, får Siun besluta att viss inhämtning ska upphöra eller att upptagning eller uppteckning av inhämtade uppgifter ska förstöras.

Enligt 4 § förordningen med instruktion för Statens inspektion för försvarsunderrättelseverksamheten ska Siun i sin kontroll av försvarsunderrättelseverksamheten bland annat följa hur lagen och förordningen om försvarsunderrättelseverksamhet tillämpas, granska att försvarsunderrättelseverksamheten bedrivs i enlighet med den inriktning

som är bestämd och granska de verksamheter där teknisk och personbaserad inhämtning av underrättelser bedrivs med särskilda metoder.

Siun ska enligt 5 § samma förordning utöva sin kontroll genom inspektioner och andra undersökningar hos de myndigheter som bedriver försvarsunderrättelseverksamhet. Siun ska till myndigheten lämna de synpunkter och förslag till åtgärder som föranleds av granskningsverksamheten. Om det behövs ska Siun även lämna dessa synpunkter och förslag om åtgärder till regeringen. Av bestämmelsen framgår vidare att Siun senast 1 mars varje år ska lämna en rapport till regeringen om föregående års granskningsverksamhet.

Enligt 15 § förordningen med instruktion för Statens inspektion för försvarsunderrättelseverksamheten ska Siun, om nämnden uppmärksammar förhållanden som kan utgöra brott, anmäla det till Åklagarmyndigheten eller annan behörig myndighet. Om Siun uppmärksammar felaktigheter som kan medföra skadeståndsansvar för staten gentemot en fysisk eller en juridisk person, ska nämnden anmäla det till Justitiekanslern. Om Siun finner omständigheter som Integritetsskyddsmyndigheten bör uppmärksammas på, ska nämnden anmäla det till den myndigheten.

Utredningsskyldighet på begäran av en enskild

Enligt 10 a § signalspaningslagen kan en enskild begära kontroll av om hans eller hennes meddelanden har inhämtats i samband med signalspaning enligt signalspaningslagen och, om så är fallet, huruvida inhämtningen och behandlingen av inhämtade uppgifter har skett i enlighet med lag. Enligt tidigare lydelse av bestämmelsen var det Siun som utförde kontrollen.

Från och med den 1 januari 2025 är det i stället ett nytt särskilt beslutandeorgan inom Siun som utför kontroll enligt 10 a § signalspaningslagen. Av bestämmelsen framgår också att den underrättelse som lämnas till den enskilde ska innehålla en motivering.

I förarbetena anförs att en begäran kan framställas av alla, oavsett medborgarskap eller hemvist, och även av juridiska personer. De utredningsåtgärder som kan vidtas är beroende av vilken information som den enskilde kan tillhandahålla. Vilka uppgifter som kan lämnas utöver att kontrollen har utförts beror på vilken sekretess som gäller i det enskilda fallet. Enligt förarbetena bör den enskilde, om det kan konstateras att det inte förekommit någon signalspaning eller att signalspaning som förekommit varit lagenlig, endast få beskedet att inget otillbörligt har skett. Det fanns enligt förarbetena inte skäl för en annan ordning eftersom till exempel företrädare för främmande makt som varit föremål för lagenlig signalspaning i annat fall skulle kunna utnyttja utredningsskyldigheten för att kartlägga svensk underrättelseverksamhet. Om kontrollmyndigheten i stället kommer fram till att signalspaningen eller hanteringen av uppgifter har skett i strid med regelsystem, bör, enligt förarbetena, den enskilde i normalfallet upplysas om det och få del av de uppgifter som kan lämnas med hänsyn till gällande sekretess. Utöver information till den enskilde bör kontrollmyndigheten också anmäla sina iakttagelser och överlämna relevanta delar av det som har framkommit till den myndighet som

ansvarar för den fråga som är aktuell (prop. 2008/09:201 s. 92–93 och 115).

Inkoppling av signalbärare till Försvarets radioanstalt

Signalbärare är det medium som används för att överföra en eller flera signaler. Det finns en eller flera signalbärare i en tråd eller kabel, men signalbäraren är det minsta fysiska medium genom vilket signalerna kan överföras. För att det ska vara tekniskt möjligt att inhämta signaler i tråd är operatörer som äger tråd i vilka signaler förs över Sveriges gräns, enligt 9 kap. 30 § lagen (2022:482) om elektronisk kommunikation, skyldiga att överföra signalerna till samverkanspunkter.

Siun har enligt 12 § signalspaningslagen rådigheten över de signalbärare som trådägarna överför till samverkanspunkterna. En samverkanspunkt är en geografisk plats där trådägarna lämnar över signalerna till Siun. Siun ger i sin tur Försvarets radioanstalt tillgång till signalbärare endast i den utsträckning det följer av tillstånd enligt 5 a eller 5 b § signalspaningslagen.

Integritetsskyddsråd

Det ska enligt 11 § signalspaningslagen finnas ett integritetsskyddsråd vid Försvarets radioanstalt. Rådet har till uppgift att ha fortlöpande insyn i de åtgärder som vidtas för att säkerställa integritetsskyddet i signalspaningsverksamheten. Ledamöterna av rådet utses av regeringen för viss tid. Rådet ska rapportera sina iakttagelser till Försvarets radioanstalts ledning och, om rådet finner att det finns skäl för det, till Siun.

Integritetsskyddsmyndigheten

Integritetsskyddsmyndigheten är tillsynsmyndighet för den personuppgiftsbehandling som sker vid Försvarets radioanstalt. Siuns granskning av Försvarets radioanstalts behandling av personuppgifter utgör ett komplement till Integritetskyddsmyndighetens tillsyn.

Integritetsskyddsmyndigheten har enligt 6 kap. 3 § FRA-PuL för sin tillsyn rätt att bland annat få tillgång till de personuppgifter som behandlas, upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder samt tillträde till sådana lokaler som har anknytning till behandling av personuppgifter.

Integritetsskyddsmyndigheten har i enlighet med vad som närmare framgår av 6 kap. 4 och 5 §§ FRA-PuL vissa befogenheter i det förebyggande arbetet samt vissa korrigerande befogenheter som får användas om tillsynsmyndigheten konstaterar att Försvarets radioanstalt eller ett personuppgiftsbiträde behandlar personuppgifter i strid med lag eller annan författning eller annars inte fullgör sina skyldigheter.

3.3.8 Internationellt samarbete

Försvarets radioanstalt får, enligt regeringens närmare bestämmande, etablera och upprätthålla samarbete i underrättelsefrågor med andra länder och internationella organisationer, enligt 3 § lagen om försvars-

underrättelseverksamhet. Försvarets radioanstalt får också för sin utvecklingsverksamhet delta i internationellt samarbete, enligt vad som närmare framgår av 9 § signalspaningslagen.

Samarbete inom ramen för försvarsunderrättelseverksamheten får, enligt 3 § förordningen om försvarsunderrättelseverksamhet, endast ske under förutsättning att syftet med samarbetet är att tjäna den svenska statsledningen och det svenska totalförsvaret. För Försvarets radioanstalts utvecklingsverksamhet gäller att samarbete får ske endast om syftet med samarbetet är att tjäna den svenska statsledningen och den nationella säkerheten, enligt 6 § förordningen om signalspaning i försvars-underrättelseverksamhet. Av båda de nämnda bestämmelserna följer att de uppgifter som Försvarets radioanstalt lämnar till andra länder och internationella organisationer inte får vara till skada för svenska intressen.

Signalspaning får inte bedrivas för andra ändamål än de som anges i 1 § signalspaningslagen. Sedan den 1 januari 2022 får signalspaning enligt 1 § andra stycket 9 signalspaningslagen bedrivas för att kartlägga företeelser som inte riktas mot Sverige eller rör svenska intressen, om det är nödvändigt för ett samarbete i underrättelsefrågor med andra länder och internationella organisationer som Försvarets radioanstalt deltar i. För sådan signalspaning bestämmer regeringen inriktningen. Det krävs tillstånd för signalspaningen i likhet med annan signalspaning som Försvarets radioanstalt bedriver. I förarbetena anges att flertalet av ändamålen i signalspaningslagen är formulerade på ett sätt som ger uttryck för att företeelserna i fråga ska vara riktade mot Sverige eller röra svenska intressen (prop. 2020/21:224 s. 157). Även om samarbetande länders underrättelsebehov ofta sammanfaller på en övergripande nivå kan de enskilda behoven skilja sig åt i fråga om detaljerna. Ett sådant exempel är den internationella terrorismen som utgör ett hot som är påtagligt för många länder, men där ett visst land kan ha ett särskilt intresse för specifika terroristceller som bedöms utgöra ett hot mot det egna landet eller mot det egna landets intressen.

Av 4 § förordningen om försvarsunderrättelseverksamhet följer att Försvarets radioanstalt ska anmäla frågor om att etablera och upprätthålla internationellt samarbete till Regeringskansliet (Försvarsdepartementet). Försvarets radioanstalt ska även informera om viktiga frågor som uppkommer i samarbetet. Detsamma gäller för Försvarets radioanstalt beträffande internationellt samarbete avseende utvecklingsverksamheten enligt 7 § förordningen om signalspaning i försvarsunderrättelse-verksamhet.

Av 6 § första stycket förordningen om försvarsunderrättelseverksamhet följer att de myndigheter som bedriver försvarsunderrättelseverksamhet ska informera Siun om de principer som tillämpas för samarbete i underrättelsefrågor med andra länder och internationella organisationer samt lämna uppgift om med vilka länder och organisationer sådant samarbete sker. Försvarets radioanstalt ska sedan samarbetet etablerats informera inspektionen om omfattningen av samarbetet och, när det bedöms vara motiverat, om resultatet, erfarenheterna och den fortsatta inriktningen av samarbetet. Försvarets radioanstalt ska även i andra viktiga frågor som rör försvarsunderrättelseverksamhet lämna information till inspektionen. Försvarets radioanstalt ska vidare särskilt informera om innehållet i den instruktion och de föreskrifter som gäller för den eller de

enheter inom myndigheten som inhämtar underrättelser med särskilda metoder.

3.3.9 Försvarets radioanstalts personuppgiftsbehandling

Personuppgiftsbehandling i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet samt informationssäkerhetsverksamhet regleras i FRA-PuL och FRA-PuF. Lagen och förordningen trädde i kraft den 1 januari 2022. Även signalspaningslagen innehåller vissa bestämmelser om personuppgiftsbehandling, till exempel om användningen av sökbegrepp och förstöringsskyldighet.

Nedan lämnas en översiktlig redogörelse för delar av FRA-PuL och FRA-PuF. För en mer utförlig redogörelse av regelverket hänvisas till propositionen Behandling av personuppgifter vid Försvarsmakten och Försvarets radioanstalt (prop. 2020/21:224).

Översiktligt om regelverket

Enligt 2 kap. 1 § FRA-PuL får personuppgifter bara behandlas för särskilda, uttryckligt angivna och berättigade ändamål. Personuppgifter får inte behandlas för något ändamål som är oförenligt med det ändamål som de ursprungligen behandlades för.

Försvarets radioanstalt får behandla personuppgifter i sin försvarsunderrättelse- och utvecklingsverksamhet samt informationssäkerhetsverksamhet (2 kap. 2, 3, 5 och 7 §§ FRA-PuL). Det finns vidare möjlighet för Försvarets radioanstalt att i vissa särskilt angivna fall behandla uppgifter för ett annat ändamål än för det ändamål för vilket personuppgifterna har samlats in, så kallade sekundära ändamål (2 kap. 4, 6 och 8 §§ FRA-PuL).

Försvarets radioanstalt får enligt 2 kap. 9 § FRA-PuL behandla personuppgifter som utgör allmänt tillgänglig information om det är nödvändigt för den verksamhet som anges i 2, 5 och 7 §§ FRA-PuL. Försvarets radioanstalt får också behandla personuppgifter för vetenskapliga, statistiska eller historiska ändamål inom FRA-PuL:s tillämpningsområde (2 kap. 10 § FRA-PuL). Känsliga personuppgifter, som avslöjar bland annat ras, etniskt ursprung, politiska åsikter eller sexuell läggning får däremot inte behandlas. När personuppgifter behandlas får de dock kompletteras med sådana uppgifter, om det är absolut nödvändigt med hänsyn till ändamålen med behandlingen (2 kap. 13 §)

Information som Försvarets radioanstalt hanterar i försvarsunderrättelseverksamheten och informationssäkerhetsverksamheten kan vara krypterad eller avfattad på ett främmande språk. Innan informationen bearbetats saknas det förutsättningar att bedöma om den innehåller personuppgifter. Av 2 kap. 18 § FRA-PuL följer att Försvarets radioanstalts hantering av information som innebär behandling av personuppgifter inte ska anses oförenlig med bestämmelserna om tillåtlighet, grundläggande krav, känsliga personuppgifter, personnummer och samordningsnummer, i det skede av behandlingen då det ännu inte har

kunnat fastställas vilka personuppgifter som informationen innehåller. När det står klart att informationen innehåller personuppgifter, samt vilka personuppgifterna är, ska Försvarets radioanstalt behandla dem enligt lagen.

Enligt 2 kap. 19 § FRA-PuL får personuppgifter inte behandlas under längre tid än vad som behövs med hänsyn till ändamålen med behandlingen. Regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter eller i ett enskilt fall besluta om att personuppgifter får behandlas under endast viss tid eller fortsätta behandlas för arkivändamål av allmänt intresse eller för vetenskapliga, statistiska eller historiska ändamål.

Överföring av personuppgifter till en mottagare utomlands

Vid internationellt samarbete kan personuppgifter komma att överföras till ett annat land eller en internationell organisation. Förutsättningarna för att en överföring av personuppgifter till en mottagare utomlands ska var tillåten framgår av 2 kap. 20 § FRA-PuL och 2 kap. 1 § FRA-PuF. Enligt 2 kap. 20 § första stycket FRA-PuL får personuppgifter överföras till ett annat land eller en internationell organisation endast om det är nödvändigt för att Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet. Därutöver krävs att

1. överföringen riktas till en utländsk underrättelse- eller säkerhetstjänst, eller ett underrättelse- eller säkerhetsorgan i en internationell organisation,
2. sekretess inte hindrar en överföring,
3. mottagaren garanterar tillräckligt skydd för personuppgifterna, och
4. överföringen inte innebär ett oproportionerligt intrång i den registrerades personliga integritet.

Den första punkten innebär att överföringen riktas till en utländsk underrättelse- eller säkerhetstjänst, eller ett underrättelse- eller säkerhetsorgan i en internationell organisation. EU, FN och Nato har exempelvis denna typ av organ. Regeringen kan, enligt vad som framgår av andra och tredje styckena i 2 kap. 20 § FRA-PuL, genom föreskrift eller beslut i enskilda fall möjliggöra för att överföring av personuppgifter även kan ske till andra internationella aktörer. Det kan till exempel vid internationella militära insatser vara nödvändigt att överlämna underrättelser till en funktion i en annan stat som inte kan sägas vara en underrättelse- eller säkerhetstjänst.

Enligt den andra punkten får överföring endast ske om sekretess inte hindrar det. En sekretessprövning behöver således ske som en del i bedömningen om en överföring av personuppgifter ska ske (prop. 2020/21:224 s. 118–119).

Enligt den tredje punkten ska mottagaren garantera tillräckligt skydd för personuppgifterna. Enligt förarbetena är det Försvarets radioanstalt som, genom en sammanvägd bedömning, har till uppgift att bedöma om det mottagande landet eller organisationen erbjuder tillräckligt skydd. Personuppgifter bör få överföras om Försvarets radioanstalt tagit hänsyn till omständigheterna kring överföringen och dragit slutsatsen att

tillräckliga skyddsåtgärder för personuppgifterna föreligger. Som utgångspunkt bör lämpliga skyddsåtgärder anses föreligga om en mottagande stat är ansluten till dataskyddskonventionen eller annan internationell överenskommelse som innehåller bestämmelser om dataskydd och registrerades rättigheter. Därutöver bör Försvarets radioanstalt kunna beakta till exempel att den som kommer att behandla uppgifterna kommer att ha tystnadsplikt som omfattar de överförda uppgifterna och åtaganden från mottagarens sida att inte föra personuppgifterna vidare eller att inte använda personuppgifterna efter en viss tidpunkt (prop. 2020/21:224 s. 119).

Den fjärde punkten trädde i kraft den 1 juli 2024. Av bestämmelsen följer att den personliga integriteten ska beaktas vid överföring av personuppgifter till en mottagare utomlands. Bestämmelsen innebär att det ankommer på Försvarets radioanstalt att inför en sådan överföring av personuppgifter göra en proportionalitetsbedömning där det intrång i den registrerades personliga integritet som överföringen kan innebära ska vägas mot skälen för överföringen (prop. 2023/24:136 s. 48–49).

Av 2 kap. 1 § FRA-PuF framgår att Försvarets radioanstalt får föra över personuppgifter till en utländsk underrättelse- eller säkerhetstjänst, en utländsk organisation inom informationssäkerhetsområdet eller en internationell organisation, om överföringen tjänar den svenska statsledningen eller det svenska totalförsvaret. Det framgår vidare att överföringen av personuppgifter inte får vara till skada för svenska intressen.

Uppgiftssamlingar

En uppgiftssamling är, enligt definitionen i 1 kap. 5 § FRA-PuL, en samling med uppgifter som med hjälp av automatiserad behandling är gemensamt tillgängliga. Av 3 kap. 1 § FRA-PuL följer att personuppgifter får göras gemensamt tillgängliga och behandlas i uppgiftssamlingar om det behövs för något av de ändamål som anges i 2 kap. FRA-PuL. Regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive uppgiftssamling. Regeringen eller den myndighet som regeringen bestämmer får också besluta om uppgiftssamlingar i ett enskilt fall.

Skyldigheter som personuppgiftsansvarig

Försvarets radioanstalt ska, genom lämpliga tekniska och organisatoriska åtgärder, säkerställa att behandlingen av personuppgifter är författningsenlig och att de registrerades rättigheter skyddas. Tillgången till personuppgifter ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter. Försvarets radioanstalt ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska särskilt avse skydd mot obehörig eller otillåten behandling eller förstöring och mot förlust eller annan oavsiktlig skada (4 kap. 1–3 §§ FRA-PuL).

Försvarets radioanstalt ska enligt 4 kap. 4 § FRA-PuL utse ett eller flera dataskyddsombud. Ett dataskyddsombud har de uppgifter som närmare framgår av 4 kap. 5 § FRA-PuL. Bland annat ska dataskyddsombudet

självständigt kontrollera att Försvarets radioanstalt behandlar personuppgifter författningsenligt och på ett korrekt sätt och i övrigt fullgör sina skyldigheter. I 4 kap. 6–10 §§ FRA-PuL finns bestämmelser om personuppgiftsbiträden.

Enskildas rätt till information

Försvarets radioanstalt är skyldig att, utan avgift, en gång per kalenderår till den som begär det lämna skriftligt besked om huruvida personuppgifter som rör honom eller henne behandlas. Om sådana uppgifter behandlas ska sökanden få del av dem och skriftliga information om vilka personuppgifter om den sökande som behandlas, varifrån personuppgifterna kommer, ändamålen med behandlingen, mottagare eller kategorier av mottagare av personuppgifterna, även i annat land eller internationella organisationer, hur länge personuppgifterna får behandlas eller, om det inte är möjligt att ange, kriterierna för att fastställa det och rätten att begära rättelse, radering eller begränsning av behandlingen. Informationen ska lämnas inom en månad från det att ansökan gjordes. Om det finns särskilda skäl för det, får information dock lämnas senast fyra månader efter det att ansökan gjordes. Informationsskyldigheten gäller inte i den utsträckning sekretess hindrar att uppgifterna lämnas ut (5 kap. 2–4 §§ FRA-PuL).

4 Skyddet för den personliga integriteten

4.1 Regeringsformen

Enligt 2 kap. 6 § första stycket regeringsformen är var och en gentemot det allmänna skyddad mot bland annat husrannsakan och liknande intrång, undersökning av brev eller annan förtrolig försändelse samt hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Enligt andra stycket är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Fri- och rättigheter enligt 2 kap. 6 § regeringsformen kan begränsas endast genom lag. Riksdagen får avseende sådana fri- och rättigheter bemyndiga regeringen att meddela föreskrifter om när en lag ska träda i kraft och när delar av en lag ska börja eller upphöra att tillämpas (2 kap. 20 § regeringsformen). Begränsning av fri- och rättigheter får göras endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. En begränsning får inte gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar (2 kap. 21 § regeringsformen). För utländska medborgare som är bofasta i riket gäller att särskilda begränsningar i dessa rättigheter får göras genom lag (2 kap. 25 § regeringsformen).

4.2 Europakonventionen

Den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) gäller som lag i Sverige, se lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna. En lag eller annan föreskrift får enligt 2 kap. 19 § regeringsformen inte meddelas i strid med Sveriges åtaganden på grund av Europakonventionen.

Enligt artikel 8 i Europakonventionen har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. En offentlig myndighet får inte inskränka denna rätt annat än med stöd av lag och om det är nödvändigt i ett demokratiskt samhälle bland annat med hänsyn till statens säkerhet och den allmänna säkerheten. Lagen ska vara tillgänglig för den som berörs av åtgärden och den ska vara så preciserad att inskränkningarna är förutsebara. Vid åtgärder som begränsar skyddet i bl.a. art. 8.1 i Europakonventionen ska det göras en proportionalitetsbedömning där riskerna med en åtgärd vägs mot dess fördelar. Det innebär noggranna avvägningar mellan å ena sidan behovet av åtgärden samt åtgärdens förväntade effektivitet och nytta och å andra sidan vilka integritetsintrång som åtgärden kan förväntas medföra.

Av artikel 15 följer att under krig eller i annat allmänt nödläge som hotar nationens existens får en konventionsstat avvika från sina skyldigheter enligt konventionen. En stat får endast göra avvikelser i den utsträckning som det är oundgängligen nödvändigt med hänsyn till situationens krav och under förutsättning att dessa åtgärder inte strider mot dess övriga förpliktelser enligt den internationella rätten. Avvikelse får aldrig ske beträffande rätten till liv utom såvitt gäller dödande genom lagliga krigshandlingar (artikel 2). Vidare får avvikelse inte ske från förbudet mot tortyr och omänsklig eller förnedrande behandling eller bestraffning (artikel 3), förbudet mot slaveri och tvångsarbete (artikel 4) samt den straffrättsliga legalitetsprincipen och förbudet mot retroaktiv strafflagstillämpning (artikel 7). Om en stat gör avvikelser från konventionen enligt artikel 15 ska Europarådets generalsekreterare underrättas om de åtgärder som vidtagits och om skälen för dessa samt när åtgärderna upphört att gälla och konventionens bestämmelser åter blivit fullt tillämpliga.

4.3 Europarådets dataskyddskonvention

Sverige har ratificerat Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (ETS 108), den s.k. dataskyddskonventionen. Konventionen trädde i kraft den 1 oktober 1985 och kompletteras av ett antal av Europarådets ministerkommitté antagna icke-bindande rekommendationer. Dataskyddskonventionen gäller för Europarådets 46 medlemsstater, men det finns även andra länder som är parter till konventionen. Dataskyddskonventionen brukar ses som en precisering av artikel 8 i Europakonventionen och syftar till att säkerställa

respekten för grundläggande fri- och rättigheter såvitt avser behandling av personuppgifter (artikel 1 i dataskyddskonventionen).

Dataskyddskonventionen tar sikte på behandling av personuppgifter i automatiserade personregister och automatiserad personuppgifts-behandling i allmän och enskild verksamhet. Personuppgifterna ska enligt konventionen inhämtas och behandlas på ett korrekt sätt och de ska vara relevanta med hänsyn till ändamålet (artikel 5). Vissa kategorier av personuppgifter får inte behandlas genom automatiserad databehandling om inte den nationella lagstiftningen ger ett ändamålsenligt skydd. Till sådana kategorier hör personuppgifter som avslöjar ras, politisk tillhörighet, religiös tro eller övertygelse i övrigt, sexualliv samt uppgifter om att någon dömts för brott (artikel 6). Dataskyddskonventionen reglerar även enskildas rätt att veta att information lagras om honom eller henne och rätten att under vissa förutsättningar få informationen rättad (artikel 8). Inskränkningar av rättigheterna i konventionen är endast möjliga om de följer av nationell lag och är nödvändiga i ett demokratiskt samhälle för att skydda till exempel statens säkerhet (artikel 9). Enligt artikel 10, som även omfattar personuppgiftsbehandling som rör nationell säkerhet, åtar sig konventionsstaterna att införa lämpliga sanktioner och rättsmedel för överträdelser av sådana bestämmelser i nationell lag genom vilka de grundläggande principer för dataskydd som har angetts i konventionen har genomförts. Konventionen anger dock inte vilka krav som ställs på sådana sanktioner.

Europarådets ministerkommitté antog år 2001 ett tilläggsprotokoll till dataskyddskonventionen (ETS 181). Tilläggsprotokollet innehåller bestämmelser om tillsynsmyndigheter och överföring av personuppgifter till länder som inte är bundna av konventionen. Tilläggsprotokollet, som Sverige har ratificerat, trädde i kraft den 1 juli 2004. Av protokollet framgår bland annat att varje konventionsstat ska se till att en eller flera myndigheter ansvarar för att kontrollera att de åtgärder respekteras som inom dess nationella lagstiftning ger verkan åt konventionens principer.

Tilläggsprotokollet innehåller vidare bestämmelser som anger att konventionsstaterna ska säkerställa att överföring av personuppgifter till ett land som inte är konventionspart bara får ske om landet i fråga säkerställer en adekvat skyddsnivå för uppgifterna. Undantag från detta får emellertid göras bl.a. om överföringen tillåts av nationell lag som motiverats av ett viktigt allmänintresse.

Det grundläggande skyddet vid automatiserad behandling av personuppgifter inom EU regleras numera främst genom dataskyddsförordningen (Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning). Dataskyddskonventionen är dock alltjämt relevant, särskilt vid behandling av personuppgifter på områden som inte omfattas av EU:s kompetensområde, till exempel allmän säkerhet och försvar.

Efter en genomförd översyn av dataskyddskonventionen antog Europarådets medlemsstater den 18 maj 2018 ett ändringsprotokoll till konventionen (CETS 223). Ändringsprotokollet öppnades för undertecknande i oktober 2018 och träder som utgångspunkt i kraft när det

har ratificerats av samtliga parter till konventionen. Ikraftträdande sker också från fem år efter det att protokollet öppnades för undertecknande förutsatt att protokollet ratificerats av minst 38 parter. Sverige har undertecknat men inte ratificerat ändringsprotokollet, som per den 15 maj 2025 hade ratificerats av 33 stater.

Försvarets radioanstalts personuppgiftsbehandling regleras i bland annat lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt (se avsnitt 3.3.9).

4.4 EU-stadgan

Av Europeiska unionens stadga om de grundläggande rättigheterna, förkortad EU-stadgan, följer att var och en har rätt till respekt för sitt privatliv och familjeliv och sina kommunikationer (artikel 7). Av stadgan framgår även att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Sådana uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem. En oberoende myndighet ska kontrollera att dessa regler efterlevs (artikel 8). EU-stadgan är rättsligt bindande för medlemsstaterna vid tillämpning av unionsrätten. Stadgan är således inte tillämplig på nationell lagstiftning inom områden där EU inte har lagstiftningskompetens.

5 Signalspaning i krig och krigsfara

5.1 En översikt av den säkerhetspolitiska utvecklingen sedan signalspaningslagens tillkomst

I förarbetena till lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (signalspaningslagen) bedömdes ett enskilt militärt angrepp i alla dess former från en annan stat mot Sverige som osannolikt under en överskådlig tid, minst en tioårsperiod. Regeringen konstaterade då att de säkerhetspolitiska hoten var av en annan karaktär än under kalla kriget, och att hoten ofta är gränsöverskridande, icke-militära och inte sällan utgår från icke-statliga aktörer (prop. 2006/07:63 s. 16–17).

Sedan dess har den säkerhetspolitiska situationen stegvis försämrats, vilket regeringen bl.a. beskrivit i Försvarsbeslutet 2016–2020 (prop. 2014/15:109) och Försvarsbeslutet 2021–2025 (prop. 2020/21:30).

Regeringen fattade den 16 maj 2022 beslut om att Sverige ska ansöka om medlemskap i Nato och den 7 mars 2024 blev Sverige det 32:a medlemslandet i alliansen.

Som regeringen anfört i Försvarsbeslutet 2025–2030 (prop. 2024/25:34) har säkerhetsläget försämrats ytterligare. Ryssland och Kina utgör två exempel på stater som på olika sätt bidragit till detta.

Rysslands fullskaliga invasion av Ukraina har försämrat säkerhetsläget i Europa, Sverige och närområdet i grunden och för lång tid framåt, och ett väpnat angrepp mot Sverige eller våra allierade kan inte uteslutas (prop. 2024/25:34 s. 63). Det finns en bred och alltmer komplex hotbild mot Sverige och svenska intressen samt ökade risker för svensk säkerhet. Det är därför av största vikt att öka tempot i förstärkningen av det militära och civila försvarets förmåga.

Även Kina agerar i Sveriges närområde. Kina köper rysk energi och exporterar insatsvaror till Rysslands rustningsindustri. Kinas partnerskap med Ryssland och export av insatsvaror till rysk rustningsindustri möjliggör den ryska krigföringen i Ukraina. På så vis förstärker Kinas agerande det hot som Ryssland utgör mot det euroatlantiska området. Kina försöker skaffa sig tillgång till utländsk teknik genom strategiska uppköp och investeringar i digital och fysisk infrastruktur, vilket kan fylla såväl civila som militära syften. Vidare används studenter, gästforskare och forskningssamarbeten i väst på ett otillbörligt sätt för att inhämta information och kunskap. Även aktiviteter inom cyberområdet nyttjas för informationsinhämtning. Säkerhetspolisen har anfört att Kina bedriver underrättelse- och säkerhetshotande verksamhet i Sverige (se prop. 2024/25:34 s. 23).

5.2 Översiktligt om nationell reglering i krig

I Sverige har det sedan lång tid ansetts att man inte bör förlita sig på den s.k. konstitutionella nödrätten, dvs. grundsatsen att statsmakterna, när samhällets bestånd hotas, kan åsidosätta grundlag och ändå göra anspråk på att handla rättsenligt (SOU 2023:75 s. 81). Lagstiftaren har i stället valt att i fred utforma en rättslig reglering för kris- och krigssituationer i syfte att uppnå en så god författningsberedskap som möjligt. Utgångspunkten för regelverket är att Sverige ska utgöra en rättsstat även i krig. Regelverket ger rättsliga förutsättningar för samhället att verka enligt förenklade konstitutionella och förvaltningsrättsliga principer för att bland annat underlätta beslutsfattande. Det ger också förutsättningar för staten att kunna ingripa i enskilda individers fri- och rättigheter samt förfoga över resurser som finns i näringslivet för att på så sätt få tillgång till personella och materiella resurser som kan gynna de samlade försvars-ansträngningarna. Sammantaget syftar regelverket till att ge legala möjligheter till en betydande nationell kraftsamling för att försvara landet samt för att få samhället att fungera i laga former även under krigsförhållanden.

Regeringsformen

En omställning från freds- till krigssamhället måste vidtas snabbt för att få avsedd verkan. Likaså måste beslut inom den offentliga verksamheten många gånger kunna fattas och verkställas snabbare under krigsförhållanden än vad som normalt är fallet. Beslutsfattande och viktiga

samhällsinstitutioner måste också fungera under krig och krigsfara. I 15 kap. regeringsformen finns bestämmelser som syftar till att skapa en grund för legalt handlande även vid krig och krigsfara.

Begreppen krig och krigsfara är inte definierade i regeringsformen eller i dess förarbeten. Grundlagsberedningen anförde på 1970-talet att det inte var möjligt att vare sig i lag- eller motivtext närmare ange vilka slags handlingar eller händelser som ska anses innebära att krigstillstånd råder. Beredningen förutsatte dock att regeringsformens bestämmelser om krig alltid ska vara tillämpliga om riket är helt eller delvis ockuperat. Uppgiften att avgöra om krigstillstånd råder vilar enligt beredningen i första hand på regeringen (SOU 1972:15 s. 216 och 349). Enligt beredningen kan den svenska regeringens behörighet att sätta in Försvarsmakten för att möta ett angrepp inte få vara beroende av om angriparen uttryckligen förklarar krig eller betraktar angreppet som krig. Det måste vara regeringens sak att under parlamentariskt ansvar ta ställning till angreppets karaktär och bestämma försvarsinsatsernas omfattning därefter (SOU 1972:15 s. 189). Departementschefen instämde i beredningens uttalanden i denna del (prop. 1973:90 s. 446–447). I förarbetena till den reformerade regeringsformen som trädde i kraft 2011 återgav regeringen de tidigare förarbetsuttalandena om begreppen krig och krigsfara, och anförde att det även fortsättningsvis får ankomma på regeringen att under konstitutionellt ansvar tolka begreppet (prop. 2009/10:80 s. 204).

I 15 kap. 1–7 §§ regeringsformen finns bestämmelser som är av betydelse vid frågor om normgivning under krig och krigsfara. I 1 § regleras inkallande av riksdagen vid sådana omständigheter. Enligt 2 § ska en inom riksdagen utsedd krigsdelegation träda i riksdagens ställe, om riket är i krig eller krigsfara och om förhållandena kräver det. Krigsdelegationen har enligt 3 § samma befogenheter som riksdagen utom i vissa avseenden. Är riket i krig och kan regeringen till följd av detta inte fullgöra sina uppgifter, kan riksdagen (eller krigsdelegationen) enligt 4 § besluta om bildande av regering och om regeringens arbetsformer.

Regeringens befogenheter i krig och krigsfara regleras i 5 och 6 §§. Kan under krig varken riksdagen eller krigsdelegationen sammanträda, är regeringen enligt 5 § första stycket behörig att fullgöra deras uppgifter. Regeringens befogenheter begränsas dock till vad som behövs för att skydda riket och slutföra kriget. Enligt 5 § andra stycket undantas stiftande, ändring eller upphävande av grundlagarna, riksdagsordningen och lag om val till riksdagen från regeringens befogenheter.

Genom bestämmelsen i 6 § finns en möjlighet för riksdagen att i krigs- och kristider delegera normgivningskompetens till regeringen även i sådana ämnen där delegation annars är förbjuden. Den ger också stöd för beredskaps- och fullmaktslagarna. Paragrafen gäller inte bara under krig eller krigsfara, utan också om det råder sådana extraordinära förhållanden som är föranledda av krig eller av krigsfara som landet har befunnit sig i. Vad som är att anse som sådana extraordinära förhållanden har inte definierats i förarbetena till regeringsformen. Av förarbetena till 3 § lagen (1992:1403) om totalförsvar och höjd beredskap kan dock viss ledning hämtas. I nämnda bestämmelse används utomordentliga förhållanden som är föranledda av att det är krig utanför Sveriges gränser eller av att Sverige har varit i krig eller krigsfara. Det framgår av förarbetena att även om bestämmelserna – också enligt den dåvarande lydelsen av 15 kap. 6 §

regeringsformen – skiljer sig åt språkligt överensstämmer bestämmelserna i sak (prop. 1992/93:76 s. 46–47).

Riksdagens bemyndigande ska ges i lag och det ska i en sådan lag noga anges under vilka förutsättningar bemyndigandet får utnyttjas. Bemyndigandet medför inte rätt att stifta, ändra eller upphäva grundlag, riksdagsordningen eller lag om val till riksdagen.

I 7 § görs undantag från det särskilda förfarandet för rättighetsbegränsande lagstiftning om riket är i krig eller omedelbar krigsfara eller om krigsdelegationen i annat fall har trätt i riksdagens ställe.

Lagen om totalförsvar och höjd beredskap

I lagen (1992:1403) om totalförsvar och höjd beredskap definieras att totalförsvar är den verksamhet som behövs för att förbereda Sverige för krig och att verksamheten delas upp i dels militär verksamhet (militärt försvar), dels civil verksamhet (civilt försvar).

Av 1 § följer att beredskapen kan höjas för att stärka landets beredskapsförmåga och det finns två beredskapsnivåer; skärpt och högsta beredskap. Under högsta beredskap är totalförsvar all samhällsverksamhet som då ska bedrivas.

Är Sverige i krig råder högsta beredskap. Är Sverige i krigsfara eller råder det sådana utomordentliga förhållanden som är föranledda av att det är krig utanför Sveriges gränser eller av att Sverige har varit i krig eller krigsfara, får regeringen besluta om skärpt eller högsta beredskap. Beslut om höjd beredskap får avse en viss del av landet eller en viss verksamhet. Regeringen ska, när förhållandena inte längre råder, besluta att höjd beredskap inte längre ska gälla (3–5 §§).

Av 6 § framgår att beslut om höjd beredskap ska tillkännages på det sätt som regeringen bestämmer. Att beredskapen höjts till skärpt eller högsta beredskap ska tillkännages i enlighet med hur lagar och författningar kungörs samt i ljudradion och television. Om det råder högsta beredskap i hela landet, kan regeringen besluta att detta ska tillkännages även genom beredskapslarm. (9 § förordningen [2015:1053] om totalförsvar och höjd beredskap). Vid beredskapslarm tillämpas ett flertal lagar omedelbart, däribland förfogandelagen (1978:262) och lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. (13 § förordningen om totalförsvar och höjd beredskap).

Bestämmelsen i 3 § första stycket lagen om totalförsvar och höjd beredskap utgör en garanti för att ansträngningarna att försvara landet i ett krigsläge kommer i gång även om regeringen av någon anledning hindras att fatta beslut om beredskapshöjning. Som huvudregel bör man dock ha att räkna med att regeringen vid ett krigsutbrott på något sätt ger till känna att Sverige kommit i krig (prop. 1992/93:76 s. 46).

I förarbetena har begreppen i nuvarande 3 § till viss del definierats. Det anges att med att Sverige befinner sig i krigsfara avses att ett fientligt angrepp på landet bedöms vara förestående. Med utomordentliga förhållanden på grund av att det är krig utanför Sveriges gränser avses att det svenska samhället drabbas av kraftiga påkänningar och störningar på grund av ett krig som vi inte tar del i, till exempel att landet får ta emot stora strömmar av flyende eller att försörjningsläget blir ansträngt på grund

av avspärrning. Sådana utomordentliga förhållanden som är föranledda av att Sverige har varit i krig eller krigsfara, som motiverar beslut om beredskapshöjning, kan exempelvis vara att försörjningsläget är ansträngt, att viktiga samhällsfunktioner är utslagna på grund av krigshandlingar eller att det i landet finns stora skaror av utlänningar som söker skydd här. Vidare anfördes i förarbetena att högsta beredskap bör användas, förutom vid krig då den inträder automatiskt, när landet befinner sig i krigsfara, dvs. när risken för ett fientligt angrepp bedöms vara överhängande eller i andra situationer då samhällsfunktionerna utsätts för extrema påfrestningar, exempelvis efter ett krig där landet drabbats av omfattande förstörelse till följd av krigshandlingar (prop. 1992/93:76 s. 46–47).

Lagen om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m.

Lagen innehåller bestämmelser om organisation och verksamhet i kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara.

Lagens materiella regler i 5–37 §§ blir tillämpliga automatiskt om riket är i krig. Om krigsfara eller utomordentliga förhållanden som är föranledd av krig eller av krigsfara som riket har befunnit sig i råder kan regeringen föreskriva att 5–37 §§ ska tillämpas från en viss tidpunkt. I det fallet måste också föreskriften underställas riksdagen inom en månad från utfärdandet. Föreskriften upphör att gälla om den inte underställs i rätt tid eller om riksdagen inte godkänner den inom två månader. När bestämmelserna tillämpas gäller inte längre bestämmelser i andra lagar och författningar som avviker från det som anges i lagen (2 och 3 §§).

Bestämmelser om förvaltningsmyndigheterna finns i 11–16 §§. Regeringen får bland annat föreskriva att en myndighets uppgifter inte ska fullgöras, eller föras över till en annan myndighet eller en domstol samt att personalen som tjänstgör ska tjänstgöra i andra anställningar eller uppdrag hos det allmänna. Regeringen kan vidare överlåta sina befogenheter till bl.a. statliga förvaltningsmyndigheter.

I 17–28 §§ finns bestämmelser om domstolarnas organisation och verksamhet samt bestämmelser som innebär att processföringen kan förenklas eller förändras på olika sätt. Regeringen får bland annat föreskriva att en domstol ska ta över uppgifter som ankommer på en annan domstol av samma slag. Regeringen får också föreskriva att uppgifter som ankommer på en domstol, som inte är en allmän domstol eller allmän förvaltningsdomstol, inte ska fullgöras eller fullgöras av en annan domstol.

Förordningen om statliga myndigheters beredskap

Enligt förordningen (2022:524) om statliga myndigheters beredskap är alla statliga myndigheter skyldiga att beakta totalförsvarets krav i sin verksamhet. Myndigheterna ska också planera för att kunna fortsätta verksamheten så långt som möjligt även under höjd beredskap.

5.3 Grundläggande principer inom det svenska totalförsvaret

En grundläggande princip inom det svenska totalförsvaret är den s.k. ansvarsprincipen. Den innebär att strukturer som gäller i fred så långt som möjligt även ska upprätthållas vid höjd beredskap. Det som är väl inarbetat i vardagen har också förutsättningar att fungera under ansträngda förhållanden. I den svåra situation som uppstår när samhället ska hantera en allvarlig kris eller ytterst försvara sig mot ett väpnat angrepp behöver samhället därför så långt som möjligt undvika att ändra ledningsförhållanden, organisation och arbetssätt.

Likhetsprincipen är en tillämpning av ansvarsprincipen som innebär att en verksamhets organisering och lokalisering så långt som möjligt ska överensstämma i fred, kris och krig. Vissa avvikelser kan dock vara nödvändiga.

Närhetsprincipen innebär att kriser ska hanteras på lägsta möjliga nivå i samhället. Den ledningsnivå som närmast berörs av ett akut krisförlopp ska alltså normalt svara för ledningen av de åtgärder som krävs för att hantera krisen på ett effektivt sätt.

5.4 Försvarsunderrättelseverksamhet i ett allvarligt försämrat säkerhetsläge

Som framgår i avsnitt 5.1 har regeringen bedömt att ett väpnat angrepp mot Sverige eller våra allierade inte kan uteslutas. Det kan inte heller uteslutas att militära maktmedel eller hot om sådana kan komma att användas mot Sverige eller våra allierade. Militära operationer mot Sverige kan syfta till att besätta svenskt territorium för ryska militära syften och förneka tillgång till svenskt territorium för Natos samlade motåtgärder. En större konflikt kan inledas med ett angrepp på Sverige. Ett angrepp kan också syfta till att förhindra Sverige att lösa sina uppgifter som allierad.

Det övergripande målet för totalförsvaret ska vara att ha förmåga att försvara Sverige och vår befolkning mot väpnat angrepp, hävda vårt lands självständighet, suveränitet och territoriella integritet samt medverka till försvaret av allierade. Verksamhet inom totalförsvaret ska kunna bedrivas enskilt och tillsammans med andra, inom och utom landet och i enlighet med Sveriges åtaganden som medlem i Nato.

I enlighet med vad regeringen anförde i Försvarsbeslutet 2025–2030 (prop. 2024/25:34) är den svenska försvarsförmågan och möjligheterna för Sverige att föra en självständig utrikes-, säkerhets- och försvarspolitik beroende av en god förvarsunderrättelseförmåga. Försvarsunderrättelseverksamheten utgör en av flera viktiga delar av Sveriges samlade förmåga till säkerhetspolitisk omvärldsanalys. Den sammanvägda säkerhetspolitiska bedömningen som baseras på såväl försvarsunderrättelser som diplomatisk rapportering, information från Säkerhetspolisen med flera sker i Regeringskansliet. Försvarsunderrättelseverksamheten måste vara organiserad på sådant sätt att den kan arbeta uthålligt i hela konfliktskalan. Försvarsunderrättelseverksamheten ska redan i rådande säkerhetspolitiska

läge kunna hålla en hög beredskap, vilket ställer särskilda krav på uthållighet. Försvarsunderrättelseverksamhetens bedömningar ligger till grund för krigsförbandens förmågeutveckling och inriktning av Försvarsmaktens operativa verksamhet i fred, höjd beredskap och krig.

5.4.1 Signalspaning i krig och krigsfara

Försvarets radioanstalts signalspaningsverksamhet går ut på att inom ramen för gällande inriktningar upptäcka på förhand okända företeelser och uppgifter av relevans för dessa. Det kan exempelvis röra sig om uppgifter om nya hot mot svenska säkerhetsintressen, samhällsviktiga funktioner, eller underrättelsehot mot svensk känslig information som inte får hamna i främmande makts händer. Verksamheten innebär även att kartlägga redan kända företeelser och följa förändringar i dessa för att tidigt få kunskap om till exempel hotaktörers nya ambitioner, avsikter och förmågor. Försvarsunderrättelseverksamhet är också ett centralt verktyg vid kartläggning i efterhand av händelser som oförutsett inträffat, i syfte att finna förklaringar till det inträffade samt för att kartlägga eventuella ännu inte identifierade inslag i en inträffad händelse. Genom sådan uppföljning kan ytterligare underrättelseinformation produceras som dels ger bättre förståelse för orsakerna bakom det inträffade, dels ger kompletterande information om till exempel kvarvarande oupptäckta hot.

Försvarets radioanstalts signalspaning i försvarsunderrättelse-verksamhet är av stor betydelse för svensk utrikes-, säkerhets- och försvarspolitik i fredstid och kommer även vara av stor vikt för det fall Sverige skulle befinna sig i krig eller krigsfara. Det försämrade säkerhetspolitiska läget de senaste åren har bland annat inneburit att Försvarets radioanstalt fått en ökad mängd förfrågningar från sina uppdragsgivare. I händelse av krig eller krigsfara kommer det finnas ett än större behov av rapportering till regeringen och andra berörda myndigheter. Det får också anses sannolikt att det kommer finnas ett krav på en mer skyndsam rapportering. Även i tiden innan krig eller krigsfara råder finns det krav på ett gott informations- och underrättelseläge för att regeringen ska kunna agera förutseende, till exempel genom att fatta beslut om beredskapshöjningar och andra motåtgärder innan Sverige utsätts för ett angrepp.

Såväl tillståndsförfarandet, som utförs av Försvarsunder-rättelsedomstolen, som verkställigheten av tillstånd, som utförs av Statens inspektion av försvarsunderrättelseverksamheten (Siun) är enligt lagstiftningen centrala förutsättningar för att Försvarets radioanstalt ska kunna inhämta signaler i elektronisk form vid signalspaning. Om någon av dessa verksamheter inte skulle fungera i en krigssituation riskeras i förlängningen hela Försvarets radioanstalts signalspaningsverksamhet, vilket kan innebära betydande men för Sveriges förmåga att till exempel försvara sig mot främmande makt. Försvarets radioanstalts verksamhet omgärdas, i likhet med all försvarsunderrättelseverksamhet, av sträng sekretess. Mot bakgrund av detta är det i princip endast de organ som i fredstid utför uppgifter enligt signalspaningslagen som har förmåga att utföra dem också i krigstid. Det är en sårbarhet i krig och krigsfara, och skulle kunna innebära svårigheter i fråga om Försvarets radioanstalts

förmåga att effektivt och ändamålsenligt fullgöra sitt uppdrag rörande signalspaning i försvarsunderrättelseverksamhet.

Internationellt samarbete är av avgörande betydelse för svensk utrikes-, säkerhets- och försvarspolitik och i övrigt vid kartläggning av yttre hot mot landet. Betydelsen kommer inte att minska i händelse av krig eller krigsfara. Även inom ramen för det internationella samarbetet kan det komma att finnas behov av ett mer skyndsamt agerande och beslutsfattande. Vid överföring av personuppgifter till en mottagare utomlands ska Försvarets radioanstalt göra en bedömning av om en mottagare kan garantera tillräckligt skydd för uppgifterna. Den tid som denna prövning kan ta skulle under krigsförhållanden kunna komma att innebära svårigheter i fråga om möjligheten att bedriva en effektiv signalspaningsverksamhet under sådana förhållanden.

Om Sverige är i krig eller i krigsfara kan det bli aktuellt för Försvarets radioanstalt att göra andra prioriteringar mellan uppdragsgivarnas inriktningar. Den ordinarie fredstida lagstiftningen tillåter vidare inte andra än några få, särskilt angivna myndigheter att inrikta signalspaningsverksamheten. Det kan inte i fredstid fullt ut förutses var behoven av inriktningsrätt kan finnas i krigstid.

I händelse av krig eller krigsfara kan Sveriges suveränitet och territoriella integritet kränkas. Signaler i elektronisk form får – utom i vissa särskilda undantagsfall – inte inhämtas mellan en avsändare och en mottagare som båda befinner sig i Sverige. I händelse av krig eller krigsfara är det rimligt att anta att fiendestaten kan komma att bedriva fientlig verksamhet i Sverige som utgör hot mot Sveriges suveränitet och territoriella integritet med utgångspunkt även från icke militära plattformar och strukturer. Detta innebär att det finns en risk att förbudet innebär begränsningar för Försvarets radioanstalts möjligheter att bedriva en effektiv signalspaning under krigsförhållanden.

5.5 Reglering av signalspaning i försvarsunderrättelseverksamhet i krig och krigsfara

5.5.1 En ny lag som reglerar signalspaning i försvarsunderrättelseverksamhet i krig och krigsfara

Utkastets förslag: En särskild lag ska reglera vissa frågor om signalspaning i försvarsunderrättelseverksamhet om Sverige är i krig eller krigsfara.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: De flesta remissinstanser, däribland *Försvarets radioanstalt*, *Försvarsmakten*, *Integritetsskyddsmyndigheten* och *Polismyndigheten*, tillstyrker eller har inga invändningar mot förslaget. Integritetsskyddsmyndigheten konstaterar härvid att förslaget innebär ökade risker för den personliga integriteten, men bedömer att de är väl

avvägda ur integritetssynpunkt och får anses vara godtagbara med hänsyn till de tungt vägande intressen som redovisats.

Institutet för mänskliga rättigheter avstyrker att förslaget läggs fram på föreliggande beredningsunderlag eftersom det enligt institutet saknas överväganden om huruvida begränsningar av rättighetsskyddet i 2 kap. 6 § regeringsformen får göras så långtgående att de riskerar att utgöra vad som i internationell terminologi betraktas som en avvikelse. Institutet anser även att det saknas en tillräcklig proportionalitetsbedömning av förslagets inskränkningar i skyddet för den personliga integriteten, varför kompletteringar även behöver ske i den delen. *Föreningen för Digitala Fri- och Rättigheter* för fram liknande synpunkter.

Sveriges advokatsamfund instämmer i och för sig i utredningens bedömning att det föreligger ett behov av utökade möjligheter till signalspaning i situationer av krig eller krigsfara och finner även att det är angeläget att sådana regler finns för att bidra till skyddet av Sveriges säkerhet, territorium och suveränitet. Samfundet avstyrker däremot förslaget och anför att det saknas en djupare analys av hur detta förhåller sig till och uppfyller de grundläggande demokratiska och rättsstatliga principerna. Samfundet ställer även frågan om de ingrepp i enskildas fri- och rättigheter som förslaget innebär inte är alltför långtgående för att uppfylla kraven på proportionalitet.

Tjänstemännens centralorganisation (TCO) pekar på att i och med att lagen kan tillämpas i krigsfara kan den vara i kraft under lång tid, vilket inte framstår som proportionerligt. *Journalistförbundet* för fram en liknande synpunkt och avstyrker förslaget. Enligt förbundet framstår det i vart fall som oproportionerligt att lagen ska gälla redan under skärpt beredskap.

Skälen för utkastets förslag: Enligt utredningens bedömning är signalspaningslagstiftningen i stor utsträckning effektiv i både freds- och krigstid, men att lagstiftningen på vissa områden innebär att signalspaningsverksamheten inte kan bedrivas på det effektiva sätt som krävs under de särskilda förhållanden som gäller vid krig eller krigsfara. Det finns därför i viss utsträckning behov av en särreglering om Sverige är i krig eller krigsfara för att signalspaningen ska kunna utföras effektivt även under sådana förhållanden. För att skapa en ökad tydlighet och förståelse för regleringen bör en sådan särreglering införas i en ny lag. Det är vidare lämpligt att regleringen görs i en egen lag mot bakgrund av att det föreslås bestämmelser som innebär avsteg från såväl signalspaningslagen som lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt (FRA-PuL). Det är lämpligt och ändamålsenligt att i den föreslagna lagen använda samma terminologi och begrepp som används i signalspaningslagen och FRA-PuL. Därutöver bör i den föreslagna lagen hänvisning ske till signalspaningslagen i fråga om vilka myndigheter som är signalspaningsmyndighet respektive kontrollmyndighet.

I och med att den nya lagen ska tillämpas i såväl krig som krigsfara är det inte otänkbart, vilket *Journalistförbundet* och *TCO* påtalar, att den i vissa fall skulle kunna komma att gälla under en längre tidsperiod. Med hänsyn till lagens syfte och funktion är detta dock nödvändigt. Alternativet, dvs. att lagen inte skulle gälla under krigsfara eller viss beredskapsnivå, är varken ändamålsenligt eller försvarbart utifrån de

risker som en sådan ordning skulle kunna medföra. Frågan om tiden för lagens tillämpning behandlas vidare i följande avsnitt.

Att använda signalspaning innebär som utgångspunkt ett intrång i någon enskilds personliga integritet. Genom detta verktyg kan en enskilds uppgifter hämtas in för vidare bearbetning och analys. Det ligger i sakens natur att förfarandet sker i hemlighet och utan samtycke från den som berörs.

Enskilda tillförsäkras skydd mot godtyckliga ingrepp i sitt privat- och familjeliv från statens sida genom bl.a. 2 kap. 6 § regeringsformen och artikel 8 i Europakonventionen. I 2 kap. 6 § regeringsformen föreskrivs att var och en gentemot det allmänna är skyddad mot undersökning av brev och andra förtroliga försändelser samt mot hemlig avlyssning eller upptagning av telefonsamtal eller andra förtroliga meddelanden. Utöver detta är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

Paragrafens skydd för den personliga integriteten är inte absolut utan kan som tidigare nämnts begränsas genom lag. Detta förutsätter att begränsningen görs för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle, aldrig går utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den, inte sträcker sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar och inte görs enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning (2 kap. 20 § första stycket 2 och 21 § regeringsformen).

I artikel 8.1 i Europakonventionen anges att var och en har rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens. Inskränkningar i dessa rättigheter får endast göras med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt bl.a. med hänsyn till statens säkerhet och den allmänna säkerheten, till förebyggande av oordning och brott eller till skydd för andra personers fri- och rättigheter (artikel 8.2). Som redogjorts för tidigare föreskriver artikel 15 vidare att en konventionsstat under krig eller i annat allmänt nödläge som hotar nationens existens får avvika från sina skyldigheter enligt konventionen i vissa avseenden, bl.a. i förhållande till artikel 8.

Vid åtgärder som begränsar skyddet i 2 kap. 6 § regeringsformen och artikel 8.1 i Europakonventionen ska det göras en proportionalitetsbedömning där riskerna med en åtgärd vägs mot dess fördelar. Det innebär avvägningar mellan å ena sidan behovet av åtgärden samt åtgärdens förväntade effektivitet och nytta och å andra sidan vilka integritetsintrång som åtgärden kan förväntas medföra.

Till saken hör även att den svenska lagstiftningen om och tillämpningen av signalspaning i försvarsunderrättelseverksamhet nyligen har varit föremål för Europadomstolens prövning (*Centrum för rättvisa mot Sverige [GC]*). Domstolen kom då fram till att regelverket i huvudsak möter de krav som kan ställas i ett demokratiskt samhälle. De brister som Europadomstolen identifierade har därefter åtgärdats genom beslut om lagändringar i enlighet med förslag som lämnats i propositionen Signalspaning i försvarsunderrättelseverksamhet – åtgärder med anledning av Europadomstolens dom (prop. 2023/24:136, bet. 2023/24:FöU11, rskr. 2023/24:206).

Det huvudsakliga fokuset i krig eller krigsfara är den nationella säkerheten och att skydda civilbefolkningen, alltså enskilda. Den nya föreslagna lagen om signalspaning i krig och krigsfara innebär, som *Institutet för mänskliga rättigheter* och *Sveriges advokatsamfund* pekar på, bl.a. undantag från förbudet mot att inhämta inhemsk trafik om sådan inhämtning är av betydelse för att hantera yttre hot mot Sveriges säkerhet, ett förenklat tillståndsförfarande och att Försvarets radioanstalt ska ha rådigheten över signalbärare. Vidare ska kontroll och tillsyn av lagstiftningen ske i efterhand. Dessa avvikelser från den ordinarie lagstiftningen innebär alltså till viss del avsteg från åtgärder som är avsedda att skydda den personliga integriteten.

Signalspaningsverksamheten kommer under krigsförhållanden att utgöra en väsentlig del av Sveriges försvar. Syftet med förslaget är att möjliggöra att Försvarets radioanstalt även under sådana särskilda förhållanden som kan råda under krig och krigsfara kan utföra signalspaningsverksamheten på ett effektivt och ändamålsenligt sätt. Ett motsatt förhållande skulle kunna leda till betydande risker för Sveriges försvarsförmåga. Förslaget bedöms utifrån dessa aspekter som nödvändigt. Ytterst ska förslaget därmed bidra till att skydda Sveriges suveränitet, territoriella integritet och civilbefolkningen. Den ökade risk för den personliga integriteten som förslaget kan innebära måste alltså ses mot dessa mycket tungt vägande intressen. Som *Integritetsskydds-myndigheten* påpekar måste det härvid också beaktas att de situationer där förslaget blir tillämpligt sannolikt kommer inträffa i begränsad utsträckning.

Genom att det införs en särskild lag på området blir det även mer förutsebart och tydligt för enskilda när och i vilken omfattning signalspaning får användas under krigsförhållanden. För att tillgodose skyddet för enskildas personliga integritet ska det också finnas möjlighet att kontrollera efterlevnaden av lagen i efterhand, vilket motverkar oproportionerliga intrång i enskildas personliga integritet. Denna viktiga fråga behandlas vidare i redovisningen som följer.

Utredningen har genomfört en genomgång och belysning av relevant reglering ur såväl grundlags- som europarättsligt perspektiv samt vilka begränsningar som kan göras i förhållande till enskildas fri- och rättigheter under sådana särskilda förhållanden som kan råda i krig och krigsfara. Som beskrivs i följande avsnitt har utredningen också övervägt och lagt fram förslag till olika åtgärder som syftar till att ge skydd mot oproportionerliga intrång i enskildas personliga integritet. Som nämnts inledningsvis finns det redan i dag lagstiftning som medger att relativt långtgående åtgärder kan vidtas vid krig och krigsfara, vilket bl.a. kan avse att myndigheters eller vissa domstolars uppgifter inte ska fullgöras eller övertas av andra organ. Att förslaget under denna typ av förhållanden innebär en begränsning av Försvarsunderrättelsedomstolens och Siuns uppgifter är alltså något som i och för sig kan ske redan genom befintlig lagstiftning.

Mot denna bakgrund delas inte Institutet för mänskliga rättigheters och Sveriges advokatsamfunds uppfattning att det skulle krävas ytterligare analyser utifrån de aspekter som remissinstanserna nämner, eller att förslaget skulle innebära en alltför stor inskränkning av enskildas fri- och rättigheter som följer av regeringsformen eller folkrättsliga regelverk. Tvärtom tar förslaget hänsyn till skyddet för enskildas personliga integritet

på ett väl avvägt sätt i förhållande till de särskilda situationer då den föreslagna lagen kan komma att tillämpas. Sammanfattningsvis är de åtgärder som föreslås nödvändiga och proportionerliga för att uppnå syftet med förslaget. Det bedöms därmed att förslaget uppfyller kraven som följer av regeringsformen och artikel 8 i Europakonventionen. Det bör alltså genomföras.

5.5.2 Tidpunkt för tillämpning

Utkastets förslag: Lagen ska tillämpas utan särskilt beslut för det fall Sverige är i krig.

Regeringen får meddela föreskrifter om att bestämmelserna, helt eller delvis, ska tillämpas om Sverige är i krigsfara eller det råder sådana extraordinära förhållanden som är föranledda av krig eller av krigsfara som Sverige har befunnit sig i.

Regeringens föreskrift om att bestämmelserna ska tillämpas ska underställas riksdagen inom en månad från utfärdandet.

När förhållandena inte längre är sådana att lagen kan tillämpas, ska regeringen föreskriva att de särskilda beredskapsbestämmelserna i lagen inte längre ska tillämpas.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: En majoritet av remissinstanserna tillstyrker förslaget eller har inget att invända mot det.

Försvarshögskolan ställer sig positiv till förslaget men påpekar att i annan lagstiftning på området används främst begreppet ”utomordentliga förhållanden”, och inte ”extraordinära förhållanden”.

Centrum för rättvisa anser att tillämpningsområdet för lagen bör tydliggöras i syfte att säkerställa att lagen enbart kan tillämpas när förutsättningarna för att avvika från Europakonventionen är uppfyllda. *Tjänstemännens centralorganisation (TCO)* för fram en liknande synpunkt.

Skälen för utkastets förslag: Det finns fullmaktslagar på flera områden och de har i stor utsträckning utformats i fråga om dess tillämpning på liknande vis. Grund för bemyndigandena i fullmaktslagarna är 15 kap. 6 § regeringsformen. Riksdagen kan enligt bestämmelsen – om Sverige är i krig eller krigsfara eller det råder sådana extraordinära förhållanden som är föranledda av krig eller av krigsfara som riket har befunnit sig i – delegera normgivningskompetens till regeringen som genom förordning kan meddela föreskrifter i ett visst ämne som annars ska meddelas genom lag. Som *Försvarshögskolan* noterar förekommer i äldre fullmaktslagar hänvisning till utomordentliga förhållanden, vilket var den terminologi som tidigare användes i regeringsformen. Detta ändrades 2011 och det angavs då att ändringen bara var språklig (prop. 2009/10:80 s. 298). Samma begrepp bör användas även i den nya lagen.

Fullmaktslagar kan vara konstruerade så att de träder i tillämpning utan särskilt beslut i händelse av krig, medan det i andra situationer krävs att regeringen föreskriver att de ska tillämpas. I till exempel lagen om totalförsvar och höjd beredskap anges att högsta beredskap råder om Sverige är i krig. Om det råder krigsfara eller sådana utomordentliga

förhållanden som är föranledda av att det är krig utanför Sveriges gränser eller av att Sverige har varit i krig eller krigsfara, får regeringen besluta om skärpt eller högsta beredskap. Ett sådant beslut kan gälla i hela eller delar av landet.

I fråga om tillämpningen av den föreslagna lagen är det, i likhet med vad *Centrum för rättvisa* anför, lämpligt att den utformas på ett sätt som överensstämmer med annan lagstiftning som ska tillämpas i krig och krigsfara. Den föreslagna lagen ska därför tillämpas utan särskilt beslut om Sverige är i krig. Vid krigsfara eller om det råder extraordinära förhållanden som är föranledda av krig eller av krigsfara som Sverige har befunnit sig i ska lagen helt eller delvis tillämpas om regeringen föreskriver det. Det får, vilket uttryckts i tidigare förarbeten, anses vara en fördel att regeringen så långt som det är möjligt särskilt ska ta ställning till fullmaktslagens tillämpning (se t.ex. prop. 1987/88:6 s. 39). Det framstår inte som lämpligt att inom ramen för detta utkast närmare exemplifiera under vilka förhållanden eller i vilka situationer som den föreslagna lagen kan bli tillämplig. I avsnitt 5.2 redogörs för vad förarbetena till bl.a. regeringsformen anger beträffande begreppen krig och krigsfara samt extraordinära förhållanden på grund av krig eller krigsfara. Det kan utifrån förarbetena bl.a. konstateras att krig enligt regeringsformens mening alltid ska anses föreligga om riket är helt eller delvis ockuperat (SOU 1972:15 s. 216 och prop. 1973:90 s. 447). Vid sidan av ockupationsfallen kan många olika situationer och händelser rymmas under begreppen krig och krigsfara. Det behöver inte vara fråga om ett regelrätt militärt angrepp mot svenskt territorium eller en risk för detta (SOU 2023:75 s. 85). En aktion som är eller verkar vara ett terroristangrepp kan innebära att krig eller krigsfara ska anses råda, beroende på omständigheterna (SOU 2008:125 s. 518–519). Det har också antagits att krig eller krigsfara i regeringsformens mening i vissa fall skulle kunna anses råda om Sverige blir indraget i en väpnad konflikt utomlands (prop. 2009/10:80 s. 203–204). Att tolka begreppen krig och krigsfara i regeringsformens mening ankommer dock i första hand på regeringen, under konstitutionellt ansvar (SOU 1972:15 s. 216, prop. 1973:90 s. 446 och 447 samt prop. 2009/10:80 s. 204).

I avsnitt 5.5.1 görs bedömningen att förslaget om en ny lagstiftning som reglerar signalspaning i försvarsunderrättelseverksamhet i krig och krigsfara är förenlig med de krav som ställs upp i artikel 8 i Europakonventionen. De åtgärder som ska kunna vidtas enligt lagen är även beroende av vilken situation som Sverige befinner sig i. Som nyss beskrivits ska regeringen enligt förslaget få meddela föreskrifter om att bestämmelserna i lagen – helt eller delvis – ska tillämpas om Sverige är i krigsfara eller det råder sådana extraordinära förhållanden som är föranledda av krig eller av krigsfara som Sverige har befunnit sig i. En sådan ordning innebär att de olika former av åtgärder som lagen uppställer kan anpassas efter situationen som råder, vilket i sin tur begränsar riskerna för intrång i enskildas personliga integritet.

Som framgår av redogörelsen i avsnitt 4.2 föreskriver härutöver artikel 15 i Europakonventionen att en konventionsstat under krig eller i annat allmänt nödläge som hotar nationens existens får avvika från sina skyldigheter enligt konventionen i vissa avseenden. I artikeln föreskrivs även en underrättelseskyldighet i förhållande till Europarådets

generalsekreterare i sådana situationer, bl.a. om de åtgärder som vidtagits och om skälen för dessa. Konventionen gäller som lag i Sverige. Som utredningen har redogjort för är den aktuella konventionsbestämmelsen i regel tillämplig på exceptionella kris- eller nödsituationer som påverkar hela befolkningen och som utgör ett hot mot det organiserade livet i det samhälle som staten består av. Konventionsstaterna anses ha ett relativt stort, men inte obegränsat, utrymme att själva avgöra om den egna nationens existens hotas av ett allmänt nödläge. Konventionsstaternas tillämpning av artikel 15 kan vidare bli föremål för prövning av Europadomstolen. Mot bl.a. denna bakgrund finns det – till skillnad från vad Centrum för rättvisa och *TCO* anför – inte skäl att tydliggöra tillämpningsområdet för lagen ytterligare.

I likhet med vad som gäller enligt flera andra fullmaktslagar, och med hänsyn till den befogenhet som tillkommer regeringen, bör en föreskrift om att bestämmelser i lagen ska tillämpas underställas riksdagen för prövning inom en månad. Därigenom möjliggörs en parlamentarisk kontroll av de åtgärder som regeringen vidtar.

Den föreslagna lagen föreslås vidare innehålla bestämmelser om att regeringen ska förordna om att lagens bestämmelser inte längre ska tillämpas och att eventuella förordningar som meddelats med stöd av bemyndigande i lagen inte längre ska gälla när krig eller krigsfara inte längre råder. Lagen bör inte upphöra automatiskt eftersom det kan krävas en övergångsperiod för att övergå till normala förhållanden, till exempel för att Försvarsunderrättelsedomstolen och Siun ska kunna återgå till ordinarie verksamhet. Det är dock självklart av stor vikt att återgången kan ske så snabbt som möjligt. Motsvarande gäller enligt andra fullmaktslagar (se t.ex. 3 § förfogandelagen [1978:262], 3 § lagen [1988:97] om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. och 5 § lagen [1992:1403] om totalförsvar och höjd beredskap).

5.5.3 Inhämtningens omfattning

Utkastets förslag: Signaler mellan en avsändare och en mottagare som båda befinner sig i Sverige får inhämtas om sådan inhämtning är av betydelse för att hantera yttre hot mot Sveriges säkerhet.

Utredningens förslag överensstämmer i sak med utkastets men har en annan lagteknisk utformning.

Remissinstanserna: De flesta av remissinstanserna, däribland *Försvarshögskolan*, tillstyrker förslaget eller har inga synpunkter.

Tjänstemännens centralorganisation anför att om möjlighet till signalspaning avseende kommunikation inom Sverige ges kommer det att kraftigt påverka journalisters möjlighet att garantera källors anonymitet. *Journalistförbundet* avstyrker förslaget av samma skäl.

Skälen för utkastets förslag

Nuvarande reglering

Enligt 2 a § första stycket signalspaningslagen får inhämtning inte avse signaler mellan en avsändare och en mottagare som båda befinner sig i Sverige. Om sådana signaler inte kan avskiljas redan vid inhämtningen, ska upptagningen eller upptecknin gen förstöras så snart det står klart att sådana signaler har inhämtats. Kravet på förstöring gäller även i fråga om upptagningar och upptecknin gar som signalspaningsmyndigheten har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete. I andra stycket medges att inhämtning av inhemsk trafik får ske för dels signaler som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte innehåller personuppgifter, dels signaler som sänds från eller till utländsk militär personal, utländska statsfartyg, statsluftfartyg eller militära fordon.

Försvarets radioanstalts behov av inhämtning av inhemska signaler i vissa särskilda situationer

Försvarsunderrättelseverksamhet får enligt 1 § lagen (2000:130) om försvarsunderrättelseverksamhet endast avse utländska förhållanden. Det gäller även för signalspaning i försvarsunderrättelseverksamhet, och även i händelse av krig eller krigsfara.

I händelse av krig eller krigsfara kan fientlig verksamhet komma att ske på svenskt territorium. I fråga om signaler som sänds från eller till utländsk militär personal, utländska statsfartyg, statsluftfartyg eller militära fordon är den nuvarande lagstiftningen tillämpbar även i en krigssituation. Annan fientlig verksamhet på svenskt territorium omfattas dock inte. Det vill säga att om främmande makt bedriver fientlig verksamhet mot Sverige på svenskt territorium som inte omfattas av de situationer som anges ovan får inhämtning av sådana signaler inte ske. I händelse av krig eller krigsfara kan fienden komma att bedriva verksamhet i Sverige som utgör hot mot Sveriges suveränitet och territoriella integritet med utgångspunkt även från icke militära plattformar och strukturer. Sådan fientlig verksamhet kan ha sin utgångspunkt inom exempelvis politiska och diplomatiska, psykologiska och informationsmässiga, underrättelseinhämtande och krigsförberedande åtgärder. Begränsningar inom ovan i händelse av krig eller krigsfara utgör en uppenbar risk för hinder mot en effektiv signalspaning i fråga om att till exempel kartlägga främmande makts agerande, avsikt och svensk förmåga att upptäcka hot. Att det vid sidan av signalspaning i försvarsunderrättelseverksamhet kan förekomma polisiär användning av exempelvis hemliga tvångsmedel, eller att myndigheter genomför analyser av uppgifter från öppna källor, förtar inte denna risk. Detta inte minst med hänsyn till den gränsdragning som finns mellan försvarsunderrättelseverksamheten och den brottsutredande och brottsbekämpande verksamheten (prop. 2008/09:201 s. 41–42), vilket är en fråga som återkommer nedan.

Det kan härvid nämnas att det i norsk lagstiftning finns en möjlighet att använda inhämtningsmetoder mot personer i Norge i liknande situationer. Norska lov om Etterretningstjenesten reglerar den norska utrikesunderrättelsetjänstens verksamhet och trädde i kraft i juni 2020. Inhämtningsmetoder får som huvudregel inte användas mot personer i

Norge. Möjlighet till undantag finns dock om Norge är i krig, krig hotar eller Norges oberoende eller säkerhet är i fara. Under sådana förhållanden kan det beslutas att utrikesunderrättelsetjänsten – utan hinder av förbudet att använda inhämtningsmetoder mot personer i Norge – får inhämta uppgifter som är av betydelse för Försvarsmaktens förmåga att hantera fientlig militär verksamhet (§ 4–1 och § 4–2 första och andra stycken lov om Etterretningstjenesten).

Inhämtning av inhemsk trafik får ske om det är av betydelse för att hantera yttre hot mot Sveriges säkerhet

I händelse av krig eller krigsfara bör det finnas utrymme att under vissa särskilda förutsättningar inhämta inhemska signaler för att kunna hantera annan fientlig verksamhet på svenskt territorium, dvs. inhämtning av signaler som inte träffas av 2 a § andra stycket signalspaningslagen. Möjlighet att inhämta sådana signaler skulle kunna bidra till Sveriges förmåga att till exempel upptäcka hot och värna den territoriella integriteten. För att möjliggöra sådan inhämtning föreslås att det införs en bestämmelse om att signaler i elektronisk form som sänds mellan en mottagare och en avsändare i Sverige får inhämtas om inhämtning är av betydelse för att hantera yttre hot mot Sveriges säkerhet. Som föreslås i avsnitt 6.3 ska signalspaningslagen förtydligas på så sätt att signaler i elektronisk form ska få inhämtas vid signalspaning oavsett om signalerna är under förmedling eller är lagrade. Sådan inhämtning av inhemsk trafik som nu är aktuell får alltså även avse lagrade signaler.

Sedan signalspaningslagens tillkomst har en viktig utgångspunkt varit att regler om detta inte får strida mot det skydd för meddelarfriheten som gäller enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen. I förarbetena till lagen framhålls dock att även om signalspaningen inte riktas mot personer som är verksamma inom massmediaområdet kommer det inte att gå att helt undvika risken för att exempelvis ett meddelande mellan en journalist och en meddelare inhämtas. Denna problematik ansågs inte kunna lösas på annat sätt än genom en bestämmelse om en omgående förstöringsskyldighet (se prop. 2006/07:63 s. 105–106). Den aktuella förstöringsskyldigheten regleras i 7 § 2 signalspaningslagen. I den föreslagna lagen om signalspaning i krig eller krigsfara är nämnda regel inte undantagen. Det innebär att förstöringsskyldigheten ska vara tillämplig även i fråga om signalspaning i krig eller krigsfara.

Som *TCO* framför kan en inhämtning av inhemsk trafik visserligen innebära en viss utökad risk för att även uppgifter som omfattas av det s.k. källskyddet inhämtas. Genom förslagets utformning tillgodoses däremot, i likhet med nu gällande lagstiftning, anonymitetsskyddet och meddelarfriheten på ett sätt som får anses godtagbart med hänsyn till syftet med förslaget (jfr a. prop. s. 106 f.).

Vad beträffar uttrycket ”yttre hot” i förslaget klargörs att det är fråga om företeelser från främmande makt eller annan antagonistisk aktör. Utkastets förslag innebär således inte en möjlighet till allomfattande signalspaning av signaler som överförs i elektronisk form i Sverige. Uttrycket ”yttre hot” klargör också gränsen mot de brottsbekämpande och brottsutredande verksamheterna. Som nämnts syftar bestämmelsen om att inhemsk trafik inte får inhämtas bland annat till att tydliggöra gränsdragningen mellan

försvarsunderrättelseverksamheten och den brottsutredande och brottsbekämpande verksamheten. Gränsdragningen bör också vara gällande i händelse av krig eller krigsfara. Kartläggning av yttre hot mot landet är vidare enligt 1 § lagen om försvarsunderrättelseverksamhet en uppgift för försvarsunderrättelseverksamheten. Det innebär således också ett tydliggörande i fråga om att det är för försvarsunderrättelseverksamhet som inhämtningen får ske. Inte minst i förhållande till allmänheten är det av betydelse att lagstiftningen är transparent och tydlig i fråga om signalspaningens ramar och begränsningar.

Uttrycket ”Sveriges säkerhet” förekommer sedan tidigare i svensk författning, bland annat i brottsbalken, offentlighets- och sekretesslagen (2009:400) och säkerhetsskyddslagen (2018:585). Även det äldre uttrycket ”rikets säkerhet” förekommer. Det saknas en legaldefinition, men i tidigare förarbeten har det anförts att begreppet tar sikte på förhållanden av grundläggande betydelse för Sverige (se bl.a. prop. 2013/14:51 s. 36 och prop. 2017/18:89 s. 38 och 133).

I svensk författning förekommer också uttrycket ”nationell säkerhet”. Uttrycket används inom EU-rätten för att avgränsa dess tillämpningsområde i förhållande till medlemsstaterna. Så har uttrycket också använts i svensk lagstiftning, till exempel i fråga om när bestämmelser om personuppgiftsbehandling i vissa fall inte är tillämpliga (se t.ex. 1 kap. 4 § brottsdatalagen [2018:1177]). Regeringen har tidigare anfört att det i förlängningen ankommer på EU-domstolen att tolka begreppet (prop. 2017/18:232 s. 104).

I likhet med utredningen förordas i detta sammanhang uttrycket ”Sveriges säkerhet”. Det är ett etablerat uttryck som förekommer i annan lagstiftning och som, med hänsyn till att uttrycket ”nationell säkerhet” huvudsakligen används för att avgränsa tillämpningsområdet inom EU-rätten, framstår som mest lämpligt att använda. Med hänsyn till att Sveriges säkerhet förekommer också i annan lagstiftning är det inte lämpligt att närmare definiera begreppet, men i enlighet med tidigare förarbetsuttalanden tar det sikte på förhållanden av grundläggande betydelse för Sverige.

5.5.4 Det ska vara möjligt att tillåta ytterligare myndigheter att inrikta signalspaning i försvarsunderrättelseverksamhet

Utkastets förslag: Det ska finnas möjlighet för andra myndigheter än de som anges i lagen om signalspaning om försvarsunderrättelseverksamhet att inrikta signalspaningen.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: De flesta av remissinstanserna yttrar sig inte särskilt över förslaget. *Totalförsvarets forskningsinstitut* ställer sig tveksamt till de praktiska förutsättningarna att tillåta ytterligare myndigheter inrikta signalspaning i krig och krigsfara.

Skälen för utkastets förslag: Enligt 1 § lagen om försvarsunderrättelseverksamhet ska försvarsunderrättelseverksamhet bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för

kartläggning av yttre hot mot landet. Försvarsunderrättelseverksamhet får endast avse utländska förhållanden. Av bestämmelsen framgår vidare att regeringen ska bestämma försvarsunderrättelseverksamhetens inriktning och inom ramen för denna inriktning får de myndigheter som regeringen bestämmer ange en närmare inriktning av verksamheten. Regeringens beslut om vilka myndigheter som får inrikta försvarsunderrättelse-verksamheten omfattas av sekretess. I fråga om signalspaning i försvarsunderrättelseverksamhet framgår det emellertid av lag vilka myndigheter som får inrikta verksamheten. Enligt 1 och 4 §§ signalspaningslagen får signalspaning i försvarsunderrättelseverksamhet endast inriktas av regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten. I avsnitt 9.1 behandlas frågan om fler myndigheter ska ges rätt att inrikta signalspaning i försvarsunderrättelseverksamhet.

Den offentliga verksamheten kommer i händelse av krig eller krigsfara att behöva ställa om sin verksamhet på olika sätt. Det går inte att fullt ut förutse hur en krigssituation kan komma att utvecklas. En sådan situation kan också komma att påverka olika delar av landet i olika stor utsträckning. Det är därför inte möjligt att fullt ut förutse hur en omställning av den offentliga verksamheten kan komma att gestalta sig. I syfte att möjliggöra organisatoriska förändringar i den offentliga verksamheten har regeringen bland annat en vidsträckt möjlighet att föreskriva om överflyttning av uppgifter mellan myndigheter (2 och 11 §§ lagen om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m.). Det kan vidare inte heller uteslutas att det i krig eller krigsfara finns behov för andra myndigheter att inrikta signalspaning.

En effektiv signalspaning i denna del innebär bland annat att regeringens och myndigheters behov av underrättelser kan tillgodoses på ett tillfredställande sätt. Eftersom det inte kan fullt ut kan förutses om krig eller krigsfara kan komma att påverka inriktningsrätten, bör det finnas en beredskap i den nya lagen för att hantera den frågan. *Totalförsvarets forskningsinstituts* farhågor avseende de praktiska förutsättningarna kring en sådan ordning delas inte.

I utkastet föreslås att en särskild bestämmelse införs som ger regeringen möjlighet att i förordning föreskriva att ytterligare myndigheter får inrikta signalspaning i försvarsunderrättelseverksamhet. Genom en sådan föreskrift blir det, i likhet med den ordinarie lagstiftningen, offentligt vilka myndigheter som får inrikta signalspaningsverksamheten.

Det föreslås även att regeringen i enskilda fall ska få fatta beslut om ytterligare myndigheters inriktningsrätt. Förslaget överensstämmer i denna del med vad som gäller för annan inriktning av försvarsunderrättelseverksamhet enligt 1 § lagen om försvars-underrättelseverksamhet. Ett sådant beslut kommer med stor sannolikhet omfattas av sekretess. Det skulle således skilja sig från vad som annars gäller för signalspaning i försvarsunderrättelseverksamhet. Det kan i händelse av krig och krigsfara uppstå behov för regeringen att skyndsamt ge andra myndigheter inriktningsrätt. Vilka omständigheter det skulle kunna vara går inte att närmare exemplifiera, utan det får bedömas i varje enskilt fall. Det kan vidare inte bortses från att det under krigsförhållanden kan finnas skäl att i förhållande till bland annat främmande makt

hemlighålla om ytterligare myndigheter får inriktningsrätt. Som tidigare berörts kan en krigssituation inte fullt ut förutses. En lagstiftning som möjliggör en effektiv signalspaning i försvarsunderrättelseverksamheten måste därför ta hänsyn till att förhållandena snabbt kan förändras.

5.5.5 Ett särskilt tillståndsförfarande

Utkastets förslag: Tillstånd till signalspaning i försvarsunderrättelseverksamhet ska ges av den befattningshavare vid signalspaningsmyndigheten som regeringen föreskriver.

Beslut om tillstånd ska endast få ges om förutsättningarna för tillstånd i lagen om signalspaning i försvarsunderrättelseverksamhet är uppfyllda.

Tillstånd ska utformas enligt bestämmelserna i lagen om signalspaning i försvarsunderrättelseverksamhet.

Det ska på samma sätt som i den ordinarie lagstiftningen finnas möjlighet att fatta särskilt beslut om det tillkommer ytterligare tillståndspliktiga sökbegrepp eller behov av ytterligare signalbärare.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: En stor del av remissinstanserna tillstyrker förslaget eller yttrar sig inte särskilt över det.

Försvarshögskolan (FHS) för fram att det finns tungt vägande skäl för att under krig och krigsfara så långt möjligt upprätthålla kontrollsystem och skyddsmekanismer som säkerställer skydd för personlig integritet. FHS anser att det inte är tillräckligt visat eller motiverat varför avsteg från detta är nödvändigt utifrån den situation som därvid kan uppstå.

Föreningen för Digitala Fri- och Rättigheter anser att förslaget inte är förenligt med grundläggande rättsstatliga principer och att detta riskerar att leda till godtycke och missbruk av signalspaningsbefogenheterna. Enligt föreningen krävs en oberoende förhandsprövning av alla beslut om signalspaning för att säkerställa rättssäkerheten.

Skälen för utkastets förslag

Nuvarande reglering

All inhämtning av signaler i elektronisk form vid signalspaning kräver tillstånd. Kravet på tillstånd gäller oavsett för vilket syfte som inhämtning sker och oberoende av vilken teknik som används. Ansökan om tillstånd görs av Försvarets radioanstalt hos Försvarsunderrättelsedomstolen. Signalspaningslagen innehåller bestämmelser om vad en ansökan ska innehålla (4 a §), vilka förutsättningar som måste vara uppfyllda för att tillstånd ska få lämnas (5 §) och vad som ska anges i ett tillstånd (5 a §). Ett tillstånd får gälla i högst sex månader, och kan efter ny prövning förlängas med sex månader i taget.

Det finns även ett särskilt förfarande för tillstånd i brådskande fall (5 b § signalspaningslagen). I sådana brådskande fall kan den befattningshavare vid Försvarets radioanstalt som regeringen föreskriver fatta ett beslut som sedan anmäls till Försvarsunderrättelsedomstolen som i efterhand prövar åtgärden. Enligt 2 § förordningen (2008:923) om signalspaning i

försvarsunderrättelseverksamhet är det myndighetschefen vid Försvarets radioanstalt eller dennes ställföreträdare som kan fatta sådana beslut. Försvarsunderrättelsedomstolen kan upphäva eller ändra beslutet om den inte finner skäl för åtgärden. Försvarets radioanstalt ska om åtgärden upphört att gälla innan Försvarsunderrättelsedomstolen prövat ärendet anmäla åtgärden till Siun.

Försvarsunderrättelsedomstolen består av en ordförande, en eller högst två vice ordförande samt två eller högst sex särskilda ledamöter. Domstolen är beslutsför med ordförande och två särskilda ledamöter. I mål vid Försvarsunderrättelsedomstolen företräder ett integritetsombud enskildas integritetsintressen. Försvarets radioanstalts ansökan om signalspaning prövas vid ett sammanträde där rättens ledamöter, Försvarets radioanstalts företrädare och integritetsskyddsombudet närvarar.

Det bör även i krig finnas ett tillståndsförfarande

Ett tillståndsförfarande innebär ett säkerställande av att det intrång i den personliga integriteten som signalspaning kan innebära bara sker när viktiga intressen för det svenska samhället berörs. Det kan sägas ge vissa garantier för att signalspaning bedrivs inom ramen för de ändamål och förutsättningar i övrigt som gäller för verksamheten. Tillståndet utgör ramen för inhämtningsuppdraget och utgör också grunden för den kontroll som sker i efterhand.

Även i en krigssituation bör det finnas ett tillståndsförfarande. Tillståndsförfarandet bör utformas utifrån att det ska kunna ge ett skydd mot oproportionerliga intrång i den personliga integriteten samtidigt som det är anpassat för de särskilda förhållanden som råder i en sådan situation. Det måste finnas ett skyndsamt och effektivt förfarande utan risk för dröjsmål för att kunna tillgodose att Försvarets radioanstalt kan utföra sitt uppdrag effektivt och ändamålsenligt i händelse av krig eller krigsfara.

Tillståndsgivare

Försvarsunderrättelsedomstolen har till uppgift att pröva ansökningar om tillstånd till signalspaning. Domstolen är en specialdomstol och har ett uppdrag som är väsensskilt från andra domstolars verksamhet. Prövningen av ansökningarna bygger på mycket känslig information som det råder sträng sekretess för. Det ställer inte bara krav på de som deltar i prövningen, utan också på det fysiska skyddet och skyddet för de handlingar som Försvarsunderrättelsedomstolen hanterar. Om sekretessbelagd information skulle röjas, skulle det kunna få mycket betydande konsekvenser för det enskilda inhämtningsuppdraget men även t.ex. för Försvarets radioanstalts förmåga att bedriva inhämtning mot en viss företeelse.

När Försvarsunderrättelsedomstolen inrättades anfördes det i förarbetena att det inte finns någon annan domstol som kan anses ha den skyddsnivå eller den kompetens som krävs för att pröva ansökningar om tillstånd till signalspaning (prop. 2008/09:201 s. 46–47). Är Sverige i krig eller i krigsfara talar omständigheterna för att informationen är än mer känslig och än mer skyddsvärd, och således ställer än större krav på skyddsnivå. Om Försvarsunderrättelsedomstolen av någon anledning inte

skulle kunna fullgöra sitt uppdrag bedöms det inte finnas någon annan domstol eller annan myndighet som skulle kunna utöva domstolens uppgifter. Det innebär en risk för att prövningen av Försvarets radioanstalts ansökningar inte kan komma till stånd i en krigssituation, vilket i förlängningen skulle kunna innebära betydande men för bland annat Sveriges förmåga att skydda sig från hot mot främmande makt.

I brådskande fall kan Försvarets radioanstalt enligt 5 b § signalspaningslagen fatta beslut om tillstånd till signalspaning. Syftet med det brådskande förfarandet är att tillse att det finns en ordning som ger Försvarets radioanstalt en möjlighet att påbörja sin verksamhet i de fall en fördröjning skulle vara förknippad med allvarliga konsekvenser (prop. 2008/09:201 s. 62–63). Förfarandet är således tänkt att användas i undantagsfall. Om Försvarsunderrättelsedomstolen i en krigssituation är förhindrad att utföra sina uppgifter skulle det innebära en fördröjning av den efterföljande prövningen, som enligt 5 b § signalspaningslagen ska ske skyndsamt. Om åtgärden har upphört att gälla kommer någon prövning inte att ske, utan åtgärden ska i stället anmälas till Siun. Att använda det brådskande förfarandet i en krigssituation skulle bland annat riskera att ge sken av en domstolsprövning som kanske aldrig äger rum. Det gagnar inte allmänhetens förtroende för tillståndssystemet.

Försvarsunderrättelsedomstolens förutsättningar för att bedriva sin verksamhet är i allt väsentligt anpassade efter fredstida förhållanden. För att säkerställa domstolens förmåga att bedriva sin verksamhet i betryggande former även under krig och krigsfara skulle det krävas en rad kostsamma åtgärder i fråga om bland annat lokaler och personal. För att domstolen ska kunna garantera tillgång till nödvändig kompetens för att i alla hotnivåer kunna tillgodose lagstiftningens krav på en beslutsför sammansättning torde antalet särskilda ledamöter behöva utökas i en större omfattning samtidigt som det måste säkerställas att dessa kan prioritera domstolens verksamhet under krig och krigsfara. Det skulle innebära att ett stort antal personer skulle få insyn i den mycket känsliga verksamheten. Det framstår mot denna bakgrund inte som ett realistiskt alternativ att skapa sådan redundans kring domstolens verksamhet att risken för störningar vid krig eller krigsfara kan uteslutas.

Ett tillståndsförfarande med Försvarsunderrättelsedomstolen som tillståndsgivare kan leda till betydande men för Försvarets radioanstalts förmåga att bedriva en effektiv signalspaning i händelse av krig eller krigsfara, och därmed allvarligt försämra Sveriges möjligheter att hantera ett sådant läge. För att tillgodose Sveriges behov av en effektiv signalspaning bör tillståndsgivningen förenklas vid sådana svåra förhållanden. Det föreslås därför att den befattningshavare vid Försvarets radioanstalt som regeringen föreskriver ska få ge tillstånd till signalspaning i händelse av krig eller krigsfara. Till skillnad från *Försvarshögskolan* görs således bedömningen, med hänsyn till vad som nu har anförts, att det föreligger ett behov av en sådan ordning. *Föreningen för Digitala Fri- och Rättigheters* bedömning av följderna för ett sådant system delas inte heller. Som beskrivs i följande avsnitt (5.5.7) kommer även denna form av signalspaning att vara föremål för kontrollåtgärder.

Utkastets förslag kan sägas innebära ett avsteg från den så kallade ansvarsprincipen som innebär att den som har ansvar för en verksamhet i fred även ska ha det vid höjd beredskap. Den föreslagna förändringen av

tillståndsförfarandet bedöms oundgängligen nödvändig för att Försvarets radioanstalt ska kunna bedriva en effektiv och ändamålsenlig signalspaning i försvarsunderrättelseverksamhet i händelse av krig eller krigsfara. Förutsättningarna för att lämna tillstånd till signalspaning som anges i 5 § lagen om signalspaning i försvarsunderrättelseverksamhet ska gälla även i sådana tillståndsförfaranden som omfattas av förslaget. Med hänsyn till det ovan sagda bedöms den föreslagna förändringen vara förenlig med artikel 8 i Europakonventionen. Det finns alltså starkt vägande skäl för att göra avsteg från ansvarsprincipen i denna del.

Tillståndsprövning, utformning och tidsbegränsning

Den nya lagen är tänkt att särreglera vissa frågor. I övrigt ska signalspaningslagen och annan lagstiftning som är tillämplig på Försvarets radioanstalts signalspaningsverksamhet tillämpas också i krig eller krigsfara. Det innebär bl.a. att bestämmelserna om för vilka ändamål som signalspaning får bedrivas, om hur sökbegrepp ska utformas och att inriktning inte får avse en viss fysisk person är tillämpliga. En tillståndsprövning under krigsförhållanden ska alltså i likhet med det ordinarie förfarandet omfatta en prövning av detta. Även i övrigt ska bestämmelser om förutsättningarna för tillstånd enligt 5 § signalspaningslagen tillämpas i en krigssituation. Utkastets förslag innebär således ingen förändring i fråga om i vilka fall och under vilka förutsättningar som signaler i elektronisk form får inhämtas.

Beslut vid signalspaning i krig och krigsfara ska vidare utformas i enlighet med bestämmelserna i 5 a § signalspaningslagen. Det bidrar bland annat till möjligheten att utföra efterhandskontroll av signalspaningsverksamheten.

Det bör också finnas utrymme att ge särskilt tillstånd om det uppstår behov av tillgång till ytterligare signalbärare eller användning av andra tillståndspliktiga sökbegrepp i likhet med vad som gäller enligt 5 a § tredje stycket signalspaningslagen.

Det är lämpligt att tillstånd även i krigstid får beviljas för högst sex månader med möjlighet till förlängning med sex månader åt gången.

I likhet med vad som gäller enligt 13 § signalspaningslagen och 16 § lagen (2009:966) om Försvarsunderrättelsedomstol bör beslut enligt den föreslagna lagen inte kunna överklagas.

5.5.6 Försvarets radioanstalt ska ha rådigheten över signalbärare

Utkastets förslag: Försvarets radioanstalt ska ha rådigheten över signalbärarna.

Tillgången till signalbärare ska begränsas till vad som följer av tillståndet.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: De flesta remissinstanser tillstyrker förslaget eller invänder inte mot det.

Försvarshögskolan ifrågasätter om det finns tillräckliga skäl för förslaget eftersom det främst verkar motiveras av effektivitetsskäl. Även

Föreningen för Digitala Fri- och Rättigheter ifrågasätter förslaget utifrån ett rättssäkerhetsperspektiv.

Skälen för utkastets förslag

Nuvarande reglering

Signalbärare är det medium som används för att överföra en eller flera signaler i tråd. Det finns en eller flera signalbärare i en tråd eller kabel, men signalbäraren är det minsta fysiska medium genom vilket signalerna kan överföras. För att det ska vara tekniskt möjligt att inhämta signaler i tråd är operatörer som äger tråd i vilka signaler förs över Sveriges gräns, enligt 9 kap. 30 § lagen (2022:482) om elektronisk kommunikation, skyldiga att överföra signalerna till samverkanspunkter. Siun har enligt 12 § signalspaningslagen rådigheten över de signalbärare som trådägarna överför till samverkanspunkterna. En samverkanspunkt är en geografisk plats där trådägarna lämnar över signalerna till Siun. Siun ger i sin tur Försvarets radioanstalt tillgång till signalbärare endast i den utsträckning det följer av tillstånd enligt 5 a eller 5 b § signalspaningslagen. Enligt 7 § andra stycket förordningen (2009:969) med instruktion för Statens inspektion för försvarsunderrättelseverksamheten får verkställighetsåtgärder vidtas av den anställde vid Siun som nämnden som leder Siun bestämmer.

Regleringen i denna del tillkom i samband med de lagändringar som följde på den politiska överenskommelsen hösten 2008. Den ursprungliga lydelsen av signalspaningslagen innebar att Försvarets radioanstalt hade tillgång till signalerna vid samverkanspunkterna. Regeringen påpekade i förarbetena att den ursprungliga regleringen inte innebar att Försvarets radioanstalt hade rätt eller möjlighet att ta del av innehållet i all den trafik som överförs till samverkanspunkterna. Regeringen föreslog emellertid – bland annat för att säkerställa att den tekniska tillgången begränsas till sådan trafik som är relevant – det nuvarande systemet som innebär dels att tillståndsprövningen omfattar tillgången till signalbärare, dels att Siun har rådigheten över signalbärarna (prop. 2008/09:201 s. 33–40).

Rådigheten över signalbärare i krigstid

Signalspaning i krig och krigsfara kan förväntas innebära större och mer skyndsamma behov av rapportering till såväl regeringen som till andra berörda myndigheter. För att tillgodose en effektiv signalspaning under sådana förhållanden måste Försvarets radioanstalt ha möjlighet att inhämta elektroniska signaler genom signalspaning utan risk för fördröjningar.

Tillgång till signalbärare är en förutsättning för inhämtning av signaler i tråd. Fördröjningar i fråga om verkställigheten av tillstånd skulle kunna påverka Försvarets radioanstalts möjligheter att inhämta sådana signaler negativt. Nämnden som leder Siun bestämmer vilka anställda i Siun som får vidta verkställighetsåtgärder. Det skulle krävas en personalmässig redundans hos Siun, som är en liten myndighet, för att säkerställa att verkställigheten kan ske på ett sådant sätt som är nödvändigt för att Försvarets radioanstalts möjligheter att inhämta signaler i tråd inte skulle påverkas negativt. Det skulle bl.a. innebära att fler personer skulle få insyn i den mycket känsliga verksamheten. Siun skulle även behöva vidta ett

antal övriga åtgärder för att åstadkomma aktuellt säkerställande. Därtill finns det – i händelse av att Siun inte skulle kunna utföra sitt uppdrag i denna del – inte någon annan som kan utföra det. I förarbetena ansågs det till exempel direkt olämpligt att operatörerna skulle anförtros ansvaret för verkställigheten (prop. 2008/09:201 s. 38). I krigstid får det anses vara av än större vikt att uppgifter som rör försvarsunderrättelseverksamheten inte röjs.

Om verkställigheten inte kan ske eller den riskerar att fördröjas skulle det kunna innebära negativa konsekvenser för till exempel Sveriges förmåga att försvara sig mot ett angrepp från främmande makt. Försvarets radioanstalt bör därför ha rådigheten över signalbärarna i krig och, om regeringen föreskriver om det, vid krigsfara.

Till skillnad från *Försvarshögskolan* görs alltså bedömningen att den avvikelse som görs i förhållande till den ordinarie regleringen är nödvändig för att Försvarets radioanstalt ska kunna bedriva en effektiv signalspaning i krigstid. Det kan påpekas att bestämmelsen ska tillämpas i krig utan särskilt beslut, men att det i övrigt krävs att regeringen föreskriver att bestämmelsen ska tillämpas, i enlighet med vad som beskrivits ovan. Det måste således göras en bedömning utifrån rådande situation om rådigheten ska överflyttas.

Föreningen för Digitala Fri- och Rättigheters farhågor delas inte i sammanhanget. Försvarets radioanstalt ska inte i krig eller krigsfara ha rätt eller möjlighet att ta del av innehållet i all den trafik som överförs till samverkanspunkterna. Inhämtningen ska bl.a. föregås av en tillståndsprövning. För att tydliggöra att tillgången ska begränsas till vad som följer av tillstånd föreslås att en bestämmelse om detta införs i den nya lagen.

5.5.7 Kontroll och tillsyn

Utkastets förslag: Efterhandskontroll och kontroll på begäran av en enskild enligt lagen om signalspaning i försvarsunderrättelseverksamhet ska inte utföras om Sverige är i krig eller, om regeringen föreskriver om det, vid krigsfara. Detsamma bör gälla för övriga uppgifter som Statens inspektion för försvarsunderrättelseverksamheten har i fråga om Försvarets radioanstalts verksamhet.

Integritetsskyddsrådet ska inte utföra någon uppgift enligt lagen om signalspaning i försvarsunderrättelseverksamhet.

Efterhandskontroll och kontroll på begäran av en enskild ska utföras när krig eller krigsfara inte längre råder.

Försvarets radioanstalt ska ha en skyldighet att vidta åtgärder för att underlätta kontroll i efterhand.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: De flesta remissinstanser, däribland *Integritetsskyddsmyndigheten*, tillstyrker eller har inga invändningar mot förslaget.

Sveriges advokatsamfund avstyrker förslaget och anser att det saknas en analys av hur det ska kunna garanteras att en efterhandskontroll avseende genomförd signalspaning och dess konsekvenser ska kunna genomföras på ett effektivt sätt. Enligt advokatsamfundet är utredningens förslag till

möjligheter till kontroll i efterhand inte tillräckligt tydliga eller uttömmande, vilket är en problematik som även *Försvarshögskolan* och *Föreningen för Digitala Fri- och Rättigheter* pekar på. Försvarshögskolan för också fram att det bör utredas ytterligare hur lagen kan utformas för att säkerställa någon form av ändamålsenlig process gällande tillstånd, kontroll och tillsyn även under krig och krigsfara. Högskolan poängterar att förslagen främst fokuserar på effektivitet, vilket gör att balansen mellan detta och skyddet för den personliga integriteten blir ytterst ojämn.

Försvarsmakten för fram att även myndigheten har behov av att under krig och krigsfara vara undantagen från sådan kontroll av myndighetens försvarsunderrättelseverksamhet och militära säkerhetstjänst som utförs av Statens inspektion för försvarsunderrättelseverksamheten. Försvarsmakten anser även att det bör övervägas om samtliga myndigheter som bedriver försvarsunderrättelseverksamhet ska vara undantagna kontrollen. *Statens inspektion för försvarsunderrättelseverksamheten* (Siun) uppmärksammar samma fråga. Siun anmärker även att utredningen inte har föreslagit alla nödvändiga författningsändringar som krävs för att Försvarets radioanstalt helt ska vara undantagen från inspektionens kontroll i aktuella situationer.

Riksarkivet lyfter frågan om beslutandeorganet i kontrollmyndigheten i sin efterhandskontroll enligt den föreslagna lagen även kan beakta andra behov i sin bedömning. Enligt myndighetens uppfattning kan en krigssituation innebära särskilda behov av att dokumentation finns exempelvis för utredningar av händelser.

Skälen för utkastets förslag

Nuvarande reglering

Siun är ansvarig för kontrollen av försvarsunderrättelseverksamheten enligt lagen om försvarsunderrättelseverksamhet och av Försvarets radioanstalts signalspaningsverksamhet enligt signalspaningslagen.

Av förordningen med instruktion för Statens inspektion för försvarsunderrättelseverksamheten framgår att Siun bland annat ska följa hur lagen om försvarsunderrättelseverksamhet och anslutande förordning tillämpas, granska att försvarsunderrättelseverksamheten bedrivs i enlighet med den inriktning som är bestämd samt granska de verksamheter där teknisk och personbaserad inhämtning av underrättelser bedrivs med särskilda metoder. Därutöver ska Siun granska behandling av personuppgifter som utförs i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet. Siuns uppgift att kontrollera försvarsunderrättelseverksamheten enligt lagen om försvars-underrättelseverksamhet gäller för samtliga myndigheter som bedriver sådan verksamhet.

Av 10 § signalspaningslagen följer att Siun ska kontrollera att Försvarets radioanstalt följer signalspaningslagen. Kontrollen ska särskilt avse granskning av sökbegrepp, förstöring av uppgifter och rapportering.

Försvarets radioanstalt ska till Siun redovisa sådana sökbegrepp som enligt 3 § signalspaningslagen är direkt hänförliga till fysisk person och som används i signalspaningsverksamheten.

Enligt 10 a § signalspaningslagen ska ett särskilt beslutandeorgan i Siun på begäran av en enskild kontrollera om hans eller hennes meddelanden

inhämtats genom signalspaning och, om så är fallet, om inhämtningen och behandlingen av inhämtade uppgifter har skett i enlighet med lag.

Enligt 11 § signalspaningslagen ska det vidare inom Försvarets radioanstalt finnas ett råd med uppgift att utöva fortlöpande insyn i de åtgärder som vidtas för att säkerställa integritetsskyddet i signalspaningsverksamheten. Rådets ledamöter utses av regeringen för viss tid.

Kontroll av signalspaning i krig och krigsfara

Försvarets underrättelsenämnd, som inrättades år 1976, ansvarade tidigare för kontrollen av försvarsunderrättelseverksamheten. I de två första instruktionerna för Försvarets underrättelsenämnd fanns en bestämmelse om att underrättelsenämndens verksamhet upphör vid krig och, om regeringen bestämmer det, vid krigsfara (10 § förordningen [1976:498] med instruktion för försvarets underrättelsenämnd och 14 § förordningen [1988:552] med instruktion för Försvarets underrättelsenämnd). Någon motsvarande bestämmelse fördes inte in i den instruktion som trädde i kraft den 1 januari 2008 (jfr förordningen [2007:852] med instruktion för Försvarets underrättelsenämnd). Någon bestämmelse med sådan innebörd finns heller inte i förordningen med instruktion för Statens inspektion för försvarsunderrättelseverksamheten.

Siun får i sin kontrollverksamhet ta del av mycket känslig information, vilket ställer krav på bland annat skyddet av lokaler och hantering av handlingar. Siuns kontrollverksamhet består bland annat av inspektioner på plats hos de myndigheter som bedriver försvarsunderrättelseverksamhet. För att på begäran av enskild kontrollera om han eller hon har varit föremål för signalspaning görs slagningar i Försvarets radioanstalts system. Såväl den nämnd som leder Siun, som det särskilda beslutandeorganet, består av bland annat ledamöter som ska utses av regeringen efter förslag från riksdagspartierna. Sammanträdena kan inte hållas på distans.

För att kontrollen ska kunna utföras på ett ändamålsenligt sätt är Siun i behov av fysisk tillgång till Försvarets radioanstalt, såväl i fråga om lokaler, som it-system och personal. Siun behöver således i stor utsträckning befinna sig i Försvarets radioanstalts lokaler för att kunna utföra sitt uppdrag, till exempel genom att göra sökningar i Försvarets radioanstalts system. Krig eller krigsfara kommer med hög sannolikhet att innebära att det kommer finnas mycket begränsade möjligheter för Siun att ha fysisk tillgång till Försvarets radioanstalt. Det finns bl.a. mot den bakgrunden betydande svårigheter för Siun att utföra sin kontrollverksamhet under krigsförhållanden. Det skulle också kunna uppstå betydande svårigheter i fråga om att samla en beslutsför nämnd. Svårigheterna finns därmed såväl vid informationsinsamling som i beslutsfattandet. Det går därför inte att lösa genom att till exempel föreskriva om en annan sammansättning i nämnden. Instruktionerna för föregångaren till Siun, Försvarets underrättelsenämnd, ger vid handen att den tidigare avsikten varit att någon kontroll av försvarsunderrättelseverksamheten inte ska utföras i krig.

Det föreslås att kontroll enligt 10 och 10 a §§ signalspaningslagen inte ska utföras i krig och, om regeringen föreskriver om det, inte heller vid krigsfara.

Kontrollen som utförs enligt både lagen om försvarsunderrättelseverksamhet och signalspaningslagen innebär ett skydd för den personliga integriteten. Det får anses vara av särskild vikt i en verksamhet som i stor utsträckning omgärdas av sträng sekretess. Att efterhandskontrollen inte ska utföras under krigsförhållanden kan således anses som en försvagning av detta skydd, vilket är en aspekt som bl.a. *Försvarshögskolan* lyfter fram. Detta innebär bland annat även att det inte kommer finnas möjlighet för kontrollmyndigheten, eller det särskilda beslutandeorganet inom den myndigheten, att besluta om att viss inhämtning ska upphöra. I stort syftar alla förslag, och så även detta, till att möjliggöra att Försvarets radioanstalt även under sådana förhållanden kan utföra signalspaningsverksamheten på ett effektivt och ändamålsenligt sätt. Därigenom kan myndigheten bland annat bidra till att skydda den territoriella integriteten och civilbefolkningen. Förslaget om att efterhandskontrollen inte ska utföras är nödvändigt för att kunna säkerställa att Försvarets radioanstalt kan utföra sina uppdrag i krig eller krigsfara.

Förslaget kan anses innebära ett avsteg från den så kallade ansvarsprincipen som innebär att den som har ansvar för en verksamhet i fred även ska ha det vid höjd beredskap. Förslaget är även i denna del nödvändigt för att kunna tillförsäkra att Försvarets radioanstalt kan fortsätta att bedriva sin verksamhet effektivt och ändamålsenligt i händelse av krig eller krigsfara.

Siun tar upp frågan om utredningen även har avsett att myndighetens kontroll respektive granskning av Försvarets radioanstalts verksamhet enligt lagen om försvarsunderrättelseverksamhet (2000:130) och lagen om behandling av personuppgifter vid Försvarets radioanstalt (2021:1172) inte ska utföras. En sådan ordning är i och för sig tänkbar med hänsyn till syftet med förslaget. Utredningen har dock inte lämnat förslag till ändringar av Siuns övriga kontroll- och granskningsansvar. Det finns inte heller underlag för att inom ramen för detta lagstiftningsärende överväga en ordning där även andra myndigheter undantas från Siuns kontrollverksamhet under krig och krigsfara, vilket *Försvarsmakten* föreslår.

Integritetsskyddsrådet

Integritetsskyddsrådet är i behov av tillgång till Försvarets radioanstalts lokaler, it-system och personal för att kunna utföra sitt uppdrag. Rådet består av ledamöter som utses av regeringen. Ledamöterna är externa i förhållande till Försvarets radioanstalt och har således ingen annan koppling dit. De kan ha sin dygnsvila på olika platser i Sverige. Som tidigare konstaterats kommer krig eller krigsfara med hög sannolikhet att innebära att det kommer finnas mycket begränsade möjligheter för inte anställda att ha fysisk tillgång till Försvarets radioanstalt. Även för Integritetsskyddsrådet finns det betydande svårigheter att, med hänsyn till avsaknaden av möjlighet till fysisk tillgång till Försvarets radioanstalt, utföra den insyn som följer av 11 § signalspaningslagen i händelse av krig eller krigsfara. Det kan även med hänsyn till att krig eller krigsfara kan medföra svårigheter att resa inom landet finnas betydande utmaningar för rådet att utföra sin insyn eftersom Integritetsskyddsrådets verksamhet, i likhet med kontroll- och tillsynsverksamheterna, inte kan utföras på

distans. Det föreslås därför att rådet inte ska utföra några uppgifter i krig eller, om regeringen föreskriver det, vid krigsfara.

Kontroll när krig eller krigsfara inte längre råder

Efterlevnaden av den föreslagna lagen bör i stället kontrolleras särskilt när krigsförhållanden inte längre råder. Det finns då bättre förutsättningar att genomföra kontroll. Att sådan efterhandskontroll sker kan ge allmänheten förtroende för att eventuella brister och felaktigheter uppmärksammas och innebär i förlängningen också ett skydd för den personliga integriteten.

Det bör vidare vara möjligt för en enskild att, efter det att krig eller krigsfara inte längre råder, begära kontroll av om hans eller hennes meddelanden eller lagrade uppgifter inhämtats vid signalspaning enligt den nya lagen.

Krigsförhållanden kan råda under lång tid, och kontroll kan komma att ske långt efter att åtgärden utförts. För att underlätta kontrollen bör därför Försvarets radioanstalt ha en skyldighet att vidta åtgärder som kan underlätta den efterföljande kontrollen, till exempel genom att föra särskilda register eller annan form av dokumentation som gör det lättare att följa vidtagna åtgärder.

Till skillnad från *Sveriges advokatsamfund* och *Föreningen för Digitala Fri- och Rättigheter* anses utredningens förslag till efterhandskontroll, när krig eller krigsfara inte längre råder, vara tillräckligt tydligt utformat. I detta sammanhang måste också syftet med förslaget återigen betonas, nämligen att möjliggöra att Försvarets radioanstalt även under sådana särskilda förhållen som kan råda under krig och krigsfara kan utföra signalspaningsverksamheten på ett effektivt och ändamålsenligt sätt, vilket har stor betydelse för skyddet av Sverige. En nedgång i förmågan skulle följaktligen kunna leda till betydande konsekvenser för landets försvarsförmåga, vilket understryker förslagets nödvändighet. Den ökade risk för den personliga integriteten som förslaget kan innebära måste ses mot dessa tungt vägande intressen. När det gäller intresseavvägningen mellan skyddet av Sverige å ena sidan och skyddet för enskildas personliga integritet å den andra framstår förslaget som både angeläget, behövligt och väl avvägt. Sammanfattningsvis bedöms förslaget som nödvändigt och proportionerligt för att dess syfte ska uppnås. Det bör alltså genomföras.

Några andra klargöranden eller analyser av det slag som advokatsamfundet, *Försvarshögskolan* och *Riksarkivet* efterfrågar är inte behövliga.

5.5.8 Mottagarens skydd för personuppgifter vid överföring till en utländsk mottagare

Utkastets förslag: Det ska vara möjligt att göra undantag från att mottagaren ska garantera tillräckligt skydd för uppgifterna vid överföring till en mottagare utomlands.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för utkastets förslag: Utbyte av underrättelser och samarbete om metodik och teknik är centrala inslag i försvarsunderrättelse-

verksamhet och i Försvarets radioanstalts signalspaningsverksamhet. De internationella samarbetena är nödvändiga eftersom inget land på egen hand kan inhämta ett fullständigt underrättelseunderlag till stöd för den bedrivna utrikes-, säkerhets- och försvarspolitiken, eller för kartläggningen av yttre hot mot landet. Förtroendefulla och effektiva samarbeten med motsvarande organisationer i utlandet är en förutsättning för att Försvarets radioanstalt på ett fullgott sätt ska kunna tillgodose det underrättelsebehov som finns hos regeringen och övriga inriktande myndigheter.

Försvarets radioanstalt får, enligt regeringens närmare bestämmande, etablera och upprätthålla samarbete i underrättelsefrågor med andra länder och internationella organisationer, enligt 3 § lagen om försvarsunderrättelseverksamhet. Försvarets radioanstalt får också för sin utvecklingsverksamhet delta i internationellt samarbete, enligt vad som närmare framgår av 9 § signalspaningslagen. Samarbete inom ramen för försvarsunderrättelseverksamheten får, enligt 3 § förordningen om försvarsunderrättelseverksamhet, endast ske under förutsättning att syftet med samarbetet är att tjäna den svenska statsledningen och det svenska totalförsvaret. För Försvarets radioanstalts utvecklingsverksamhet gäller att samarbete får ske endast om syftet med samarbetet är att tjäna den svenska statsledningen och den nationella säkerheten, enligt 6 § förordningen om signalspaning i försvarsunderrättelseverksamhet. Av båda de nämnda bestämmelserna följer att de uppgifter som Försvarets radioanstalt lämnar till andra länder och internationella organisationer inte får vara till skada för svenska intressen.

Vid internationella samarbeten kan personuppgifter komma att överföras till en mottagare utomlands. Enligt 2 kap. 20 § första stycket FRA-PuL får personuppgifter överföras till ett annat land eller en internationell organisation endast om det är nödvändigt för att Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet. Därutöver krävs att överföringen riktas till en utländsk underrättelse- eller säkerhetstjänst, eller ett underrättelse- eller säkerhetsorgan i en internationell organisation, att sekretess inte hindrar en överföring, och att mottagaren garanterar tillräckligt skydd för personuppgifterna. Det sistnämnda kravet gäller också som huvudregel enligt dataskyddskonventionens tilläggsprotokoll (ETS 181). Därutöver ska den personliga integriteten beaktas. Enligt 2 kap. 20 § andra och tredje styckena FRA-PuL kan regeringen, genom föreskrift eller beslut i enskilda fall, möjliggöra överföring av personuppgifter även i förhållande till andra internationella aktörer. Ett sådant behov kan till exempel uppkomma inom ramen för en internationell insats där mottagaren av Försvarets radioanstalts underrättelser är ett organ i en annan stats väpnade styrkor som inte kan sägas vara ett underrättelse- eller säkerhetsorgan (prop. 2020/21:224 s. 118).

Internationella samarbeten är än mer i krigstid av mycket stor betydelse för Försvarets radioanstalts försvarsunderrättelseverksamhet. Sådana förhållanden innebär att det kommer att ställas större krav på Försvarets radioanstalts förmåga att kunna agera skyndsamt. Vid överföring av personuppgifter till en mottagare utomlands ska Försvarets radioanstalt göra en sammanvägd bedömning av om det mottagande landet eller

organisationen erbjuder tillräckligt skydd för personuppgifterna innan en överföring får ske. Av förarbetena framgår bland annat att Försvarets radioanstalt ska bedöma alla omständigheter kring överföringen och komma till slutsatsen att skyddsåtgärderna är tillräckliga. Om en mottagande stat är ansluten till dataskyddskonventionen eller en annan internationell överenskommelse som innehåller bestämmelser om dataskydd och registrerades rättigheter kan lämpliga skyddsåtgärder som utgångspunkt anses föreligga (prop. 2020/21:224 s. 224).

I händelse av krig eller krigsfara finns det en risk för att den tid som denna bedömning tar i vissa fall kan komma att påverka Försvarets radioanstalts möjligheter att bedriva ett effektivt internationellt samarbete negativt, vilket i förlängningen kan innebära att Försvarets radioanstalt inte får information som myndigheten är i behov av. Det bör finnas en möjlighet att överföra personuppgifter även om Försvarets radioanstalt inte kunnat förvissa sig om skyddet för de överförda personuppgifterna hos mottagaren. Det ska därför vara möjligt för regeringen att meddela föreskrifter eller i ett enskilt fall fatta beslut om undantag från kravet om att mottagaren ska garantera tillräckligt skydd för uppgifterna. Med hänsyn till att den föreslagna bestämmelsen ska gälla i krig eller krigsfara görs bedömningen att den är motiverad av ett sådant viktigt allmänintresse som avses i dataskyddskonventionens tilläggsprotokoll (ETS 181).

Det kan i sammanhanget påpekas att det inte föreslås någon ändring i fråga om den proportionalitetsbedömning som Försvarets radioanstalt enligt 2 kap. 20 § första stycket 4 FRA-PuL ska göra vid överföring av personuppgifter till en mottagare utomlands. En sådan proportionalitets-bedömning ska alltså utföras också i de fall när undantag görs från kravet på att mottagaren ska garantera tillräckligt skydd för uppgifterna. Med hänsyn till detta, och mot bakgrund av de tungt vägande intressen som motiverar förslaget, bedöms detta vara såväl nödvändigt som proportionerligt i förhållande till de eventuella risker för den personliga integriteten som kan uppstå.

5.5.9 Tillsyn av personuppgiftsbehandling

Utkastets förslag: Tillsyn enligt lagen om behandling av personuppgifter vid Försvarets radioanstalt ska inte utföras.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: De flesta remissinstanser, däribland *Integritetsskyddsmyndigheten*, tillstyrker eller har inga invändningar mot förslaget.

Föreningen för Digitala Fri- och Rättigheter påtalar att förslaget innebär att viktiga kontrollfunktioner sätts ur spel just när behovet av rättssäkerhetsgarantier är som störst.

Skälen för utkastets förslag: Integritetsskyddsmyndigheten är tillsynsmyndighet för den personuppgiftsbehandling som sker vid Försvarets radioanstalt. Siuns granskning av Försvarets radioanstalts behandling av personuppgifter utgör ett komplement till Integritetskyddsmyndighetens tillsyn.

Integritetsskyddsmyndigheten har för sin tillsyn rätt att bland annat få tillgång till de personuppgifter som behandlas, upplysningar om och dokumentation av behandlingen av personuppgifter och säkerhets- och skyddsåtgärder samt tillträde till sådana lokaler som har anknytning till behandling av personuppgifter. Integritetsskyddsmyndigheten har vissa befogenheter i det förebyggande arbetet samt vissa korrigerande befogenheter som får användas om tillsynsmyndigheten konstaterar att Försvarets radioanstalt eller ett personuppgiftsbiträde behandlar personuppgifter i strid med lag eller annan författning eller annars inte fullgör sina skyldigheter (6 kap. 3–5 §§ FRA-PuL).

Tillsynen av personuppgiftsbehandling vid Försvarets radioanstalt kräver, i likhet med kontrollverksamheten, bland annat fysisk tillgång till Försvarets radioanstalts lokaler, it-system och personal. Krigsförhållanden kommer med hög sannolikhet att innebära att det kommer att finnas mycket begränsade möjligheter för Integritetsskyddsmyndigheten att ha fysisk tillgång till Försvarets radioanstalt. Utan sådan tillgång kan tillsyn av personuppgiftsbehandlingen inte utföras. Det har ovan konstaterats att Siuns kontroll av Försvarets radioanstalts verksamhet bland annat till följd av detta svårligen kan utföras i krigstid. Mot denna bakgrund bör det inte utföras någon tillsyn av personuppgiftsbehandlingen vid Försvarets radioanstalt i krig eller, om regeringen föreskriver det, vid krigsfara.

Ansvarsprincipen innebär, som tidigare nämnts, att den som har ansvar för en verksamhet i fred även ska ha det vid höjd beredskap. Likhetsprincipen är en tillämpning av ansvarsprincipen som innebär att en verksamhets organisering och lokalisering så långt som möjligt ska överensstämma i fred, kris och krig. Vissa avvikelser kan dock vara nödvändiga. Utkastets förslag kan anses innebära ett avsteg från principerna. Det är dock inte fråga om att låta någon annan myndighet överta Integritetsskyddsmyndighetens tillsynsverksamhet, utan förslaget innebär att sådan verksamhet inte ska ske i krigsförhållanden. Ett sådant avsteg från principerna är nödvändigt för att Försvarets radioanstalt ska ha möjlighet att bedriva en effektiv och ändamålsenlig signalspaning i försvarsunderrättelseverksamhet i sådana särskilt allvarliga förhållanden som krig eller krigsfara innebär.

Integritetsskyddsmyndigheten ska – när krigsförhållanden inte längre råder – åter utöva tillsyn över Försvarets radioanstalts personuppgiftsbehandling. Någon särskild reglering för detta krävs inte eftersom FRA-PuL är tillämpbar på den personuppgiftsbehandling som sker inom ramen för den signalspaning som bedrivs enligt den nya lagen. När regeringen förordnat om att bestämmelserna i den föreslagna lagen inte längre ska tillämpas, kan således tillsyn utövas av den personuppgiftsbehandling som skett för signalspaning som bedrivits enligt den nya lagen. *Föreningen för Digitala Fri- och Rättigheters* oro för förslagets följder delas därför inte.

5.5.10 Enskildas rätt till information

Utkastets förslag: Det ska vara möjligt att skjuta upp lämnandet av information till en enskild till efter att krigsförhållanden upphört.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: Majoriteten av remissinstanserna yttrar sig inte särskilt över förslaget. *Föreningen för Digitala Fri- och Rättigheter* för fram att förslaget kan bryta mot rätten till insyn och transparens enligt dataskyddsförordningen och kan påverka enskildas möjlighet att hävda och försvara sina rättigheter.

Skälen för utkastets förslag: En enskild har efter ansökan rätt till viss personrelaterad information enligt 5 kap. 2 § FRA-PuL. Av bestämmelsen framgår att information ska lämnas inom en månad från ansökan. Om det finns särskilda skäl får informationen dock lämnas senast fyra månader efter ansökan. Enligt 5 kap. 3 § FRA-PuL gäller inte informationsskyldigheten i den utsträckning som sekretess hindrar det.

Enligt artikel 8 i dataskyddskonventionen har var och en vissa rättigheter, däribland rätt till information om huruvida personuppgifter avseende honom eller henne behandlas. Av artikel 9 följer att avvikelse från rättigheterna i artikel 8 får föreskrivas i lag, om avvikelsen är nödvändig i ett demokratiskt samhälle för att skydda till exempel statens säkerhet.

Det huvudsakliga fokuset i händelse av krig eller krigsfara kommer att vara det militära försvaret, samtidigt som de viktigaste samhällsfunktionerna behöver säkerställas och civilbefolkningen skyddas. En effektiv signalspaning i krigstid kräver att Försvarets radioanstalt har möjlighet att fullt ut fokusera på sin kärnverksamhet. Det innebär bland annat att de personella resurser som Försvarets radioanstalt disponerar över måste användas på ett ändamålsenligt sätt. Arbetet med att lämna information till en enskild i händelse av krig eller krigsfara riskerar att ta värdefulla resurser i anspråk vid myndigheten.

Det måste finnas utrymme för Försvarets radioanstalt att använda sina resurser på bästa sätt i krigstid. För tillgodose detta föreslås att 5 kap. 2 § FRA-PuL inte ska tillämpas i krig eller, om regeringen föreskriver det, vid krigsfara. Förslaget bedöms lämpligt och nödvändigt för att möjliggöra att Försvarets radioanstalt kan bedriva en effektiv och ändamålsenlig signalspaning i händelse av krig eller krigsfara. Sett till de mycket speciella och samtidigt avgränsade omständigheter som krävs för att den föreslagna bestämmelsen ska bli tillämplig bedöms förslaget även vara proportionerligt ur ett integritetsskyddsperspektiv och förenligt med dataskyddskonventionen. När krig eller krigsfara inte längre råder ska bestämmelserna i 5 kap. 2 § FRA-PuL åter tillämpas. *Föreningen för Digitala Fri- och Rättigheters* bedömning av förslagets konsekvenser delas inte.

6 Inhämtning av signaler i elektronisk form – ett förtydligande i lag

6.1 Teknik- och telekommunikationsutvecklingens betydelse för tidigare lagstiftning

Lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (signalspaningslagen) tillkom mot bakgrund av den teknik- och telekommunikationsutveckling som skedde under 1990-talet och tidiga 2000-talet och som innebar att fler signaler tillkom och att signalerna i allt större omfattning överfördes i tråd (kabel). Innan signalspaningslagen trädde i kraft var Försvarets radioanstalts inhämtning begränsad till trådlös kommunikation, till exempel radio- och satellitkommunikation. I förarbetena till signalspaningslagen beskrev regeringen att eftersom en dominerande och växande del av elektronisk kommunikation skedde via tråd eller kabel hade signalspaningens möjligheter att inhämta relevanta underrättelser radikalt reducerats, vilket hade minskat den tillgängliga mängden underrättelser. Detta kunde på sikt medföra allvarliga men för underrättelseproduktionen till stöd för Sveriges utrikes-, säkerhets-, och försvarspolitik (prop. 2006/07:63 s. 57).

Regeringen framförde i nämnda förarbeten att det framstod som ett mycket angeläget intresse att signalspaningsmyndigheten även i framtiden skulle kunna bedriva en ändamålsenlig verksamhet. En avgörande förutsättning är dock att signalspaningen kan genomföras oavsett med vilken teknik signalerna förmedlas. Regeringen ansåg därför att signaler i elektronisk form skulle få inhämtas, även då signalerna befinner sig i tråd (prop. 2006/07:63 s. 69). Av förarbetena framgår att lagregleringen av signalspaning i försvarsunderrättelseverksamhet ska vara teknikneutral på så sätt att signalerna rättsligt sett bör behandlas lika oavsett hur och från vilket medium kommunikationen inhämtas (prop. 2006/07:63 s. 70). Möjligheten att inhämta signaler i elektronisk form är inte knuten till var signalerna befinner sig, utan är teknikneutral. Därmed kan inhämtning ske oavsett om signalerna befinner sig i etern eller i kabel (dvs. är trådburen) eller någon annanstans (prop. 2006/07:63 s. 137).

6.2 Teknik- och telekommunikationsutveckling sedan signalspaningslagens tillkomst

Det är över 15 år sedan signalspaningslagen trädde i kraft. Den tekniska utvecklingen av signalmiljön har varit snabb och omfattande sedan dess och är fortsatt under ständig förändring. Det rör sig bland annat om allmän digitalisering, dynamiken och föränderligheten i var och hur information överförs och tillgängliggörs, den alltmer utbredda användningen av kryptering samt utvecklingen rörande generell informationssäkerhet.

Det har under de senare åren blivit allt vanligare att lagra information i så kallade molntjänster. Lagring av data kan därigenom ske på internetservrar i stället för att lagras direkt på användarens utrustning.

Förändringen i omvärldsläget med ökad regionalisering av internet har som en direkt följd påverkat signalmiljön på motsvarande sätt. Ett exempel på detta är enskilda länder som avsiktligt vidtar tekniska åtgärder för att begränsa kommunikation till och från det egna landet via internet.

Det finns flera anledningar till att kryptering används i allt större utsträckning. En högre grad av informationshantering har ökat behovet av att skydda information eller kommunikation från obehöriga, men även för att upprätthålla informationens integritet. Den teknologiska utvecklingen har gjort det möjligt att använda sig av kryptering för att möta dessa behov. Sammantaget har detta lett till en större tillgänglighet av avancerad kryptering, ofta utan användarens kännedom, i produkter och tjänster på marknaden avseende kommunikation och hantering av data.

Nya teknologier ger bland annat nya möjligheter för anslutning av än fler typer av uppkopplad utrustning och än större fokus på integritet och kryptering. De tjänster som ofta förknippas med dessa nya lösningar är tillämpningar inom det som kallas ”sakernas internet” (eng. internet of things), där föremål kopplas upp och kommunicerar via internet. Det kan till exempel röra sensorer, mätare och liknande i kontroll- och säkerhetssystem i både kontors-, industri- och offentlig miljö, fjärrstyrda robotar och avancerade tillämpningar för artificiell intelligens.

6.3 Ett förtydligande i lag av att signaler i elektronisk form får inhämtas oavsett var de befinner sig

Utkastets förslag: Det ska framgå av lagen om signalspaning i försvarsunderrättelseverksamhet att

– signaler i elektronisk form vid signalspaning får inhämtas oavsett om signalerna är under förmedling eller är lagrade,

– signalspaningsmyndigheten får vidta de tekniska åtgärder som är nödvändiga för att genomföra inhämtning av signaler i elektronisk form,

– förbudet mot att inhämta signaler som sänds mellan en avsändare och en mottagare som båda befinner sig i Sverige också gäller för signaler som lagras i Sverige, och

– kontroll på begäran av enskild även ska avse lagrade uppgifter som har inhämtats i samband med signalspaning enligt lagen.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: De flesta remissinstanser tillstyrker eller har inga synpunkter på förslaget, däribland *Försvarets radioanstalt*.

Sveriges advokatsamfund avstyrker förslaget och menar att det saknas en bedömning av såväl hur gamla data som får inhämtas som vilka andra begränsningar som ska gälla för lagrade signaler jämte vilka konsekvenser inhämtning av lagrade signaler kan få för den personliga integriteten och allmänhetens tillit till myndigheterna. Advokatsamfundet anser dock att en möjlighet att inhämta även lagrade signaler i stort sett är mindre betänkligt. Även *Journalistförbundet* avstyrker förslaget och ifrågasätter om detta kan anses utgöra ett förtydligande av lagen. Förbundet efterlyser även en

riskanalys i förhållande till förstöringsskyldigheten kopplad till källskyddet.

Integritetsskyddsmyndigheten anser att det saknas en integritetsanalys av förslaget. *Föreningen för Digitala Fri- och Rättigheter* för fram liknande synpunkter. *Statens inspektion för försvarsunderrättelseverksamheteten* (Siun) noterar å sin sida att myndigheten enbart har mandat och möjlighet att genomföra kontroll av tekniska åtgärder inom ramen för laglighetsgranskning. Siun framhåller vidare att förslaget måste ses som en vidare utredningsskyldighet gällande den kontroll som sker på begäran av enskild enligt lagen och efterlyser ett förtydligande i frågan.

Skälen för utkastets förslag

Gällande ordning

Försvarets radioanstalt får – om förutsättningarna för det är uppfyllda enligt lagen (2000:130) om försvarsunderrättelseverksamhet och signalspaningslagen – inhämta signaler i elektronisk form vid signalspaning. Uttrycket signaler i elektronisk form beskriver föremålet för inhämtningen. Regeringen anförde i propositionen En anpassad försvarsunderrättelseverksamhet att fokus bör vara på vad som får inhämtas, snarare än i vilket system signalerna överförs. Med signaler i elektronisk form avses alla former av signaler som överförs bland annat med hjälp av elektromagnetiska vågor. (prop. 2006/07:63 s. 70–71). I författningskommentaren angav regeringen vidare att möjligheten att inhämta signaler i elektronisk form inte är knuten till var signalerna befinner sig. Därmed kan inhämtning ske oavsett om signalerna befinner sig i etern eller i kabel (dvs. är trådburen) eller någon annanstans (prop. 2006/07:63 s. 137). Det kan exempelvis vara fråga om signaler som överförs via satellit eller signaler som är lagrade i nätverksansluten utrustning, i såväl mjuk- som hårdvara. Det senare, vilket Försvarsberedningen beskrivit som nätverksinhämtning, syftar till att kartlägga och få åtkomst till information i informationssystem, datorer eller nätverk av dessa (Ds 2019:8 s. 253). All digital information utgörs således av signaler i elektronisk form.

Försvarets radioanstalt har inhämtat lagrade signaler inom ramen för tillståndsprövade inhämtningsuppdrag. Siun har granskat denna inhämtning.

Internationell utblick

Nedan redogörs för bestämmelser i Finlands, Norges och Storbritanniens lagstiftningar om inhämtning av information som är lagrad i exempelvis datasystem och annan nätverksansluten utrustning. Gemensamt för lagstiftningarna är att de – i jämförelse med signalspaningslagen – är förhållandevis nya.

I Finland regleras Försvarsmaktens underrättelseverksamhet i bland annat lagen om militär underrättelseverksamhet (2019/590). Lagen, som trädde i kraft 2019, innehåller bland annat bestämmelser om ett flertal olika metoder som under olika förutsättningar får tillämpas i sådan verksamhet. En av dessa benämns som underrättelseinhämtning i utländska datasystem (62 §) och innebär att information inhämtas med

datatekniska metoder från ett datasystem utanför Finland. Av förarbetena framgår att bestämmelsen är teknikneutral på sådant sätt att underrättelseinhämtningen kan riktas inte bara mot datorer utan också mot andra motsvarande tekniska anordningar. Underrättelseinhämtningen kan också inbegripa inhämtande av information om en funktion i en anordnings programvara, lagrad information eller identifierings-uppgifterna i en anordning samt avlyssning, upptagning eller annan behandling av ett meddelande som inte är avsett för utomstående (RP 203/2017 rd s. 279). Enligt 63 § nämnda lag fattas beslut om underrättelseinhämtning i utländska datasystem av huvudstabens underrättelsechef.

Norska lov om Etterretningstjenesten, som trädde i kraft år 2020, innehåller bestämmelser om Etterretningstjeneste (ET) som är Norges utrikesunderrättelsetjänst. Lagen innehåller bland annat bestämmelser om vilka inhämtningsmetoder som ET får använda, däribland ”midtpunktinnhenting” (§ 6–9) och ”endepunktinnhenting” (§ 6–10). ”Midtpunktinnhenting” innebär att ET kan inhämta elektronisk kommunikation i transit och kartlägga kommunikationsinfrastruktur. ”Endepunktinnhenting” innebär att ET kan observera och inhämta elektronisk information från icke-öppna datasystem eller liknande system eller tjänster. Med andra ord sker inhämtning av informationen vid ”endepunktinnhenting” inte när informationen överförs utan där information lagras. Av förarbetena till lagen framgår att bestämmelsen är en precisering och kodifiering av gällande metodanvändning (prop. 80 L s. 81). Om det finns anledning att tro att information som inhämtas med ”endepunktinnhenting” kommer att omfatta information som inte är avsedd att kommuniceras, får inhämtning enligt bestämmelsens andra stycket ske endast om det är absolut nödvändigt. Beslut om att använda ”endepunktinnhenting” fattas av chefen för ET och får inte ges för längre tid än nödvändigt, dock längst för ett år gången (§ 6–12). Av § 6–8 följer att ET får inhämta information genom att använda tekniska sensorer eller andra tekniska metoder än de som anges i bland annat § 6–10. Enligt § 6–11 får ET vidta de förberedande åtgärder som är nödvändiga för att använda metoderna som anges i kapitel 6 i nämnda lag, bland annat kringgå faktiska och tekniska hinder, installera, genomsöka eller tillägna sig teknisk utrustning och programvara samt ta kontroll över, ändra eller använda elektronisk eller annan teknisk utrustning.

I Storbritannien regleras tillståndsprocesser för olika former av inhämtningsmetoder som underrättelse- och säkerhetstjänsterna samt brottsbekämpande myndigheter får använda sig av i Investigatory Powers Act 2016 (IPA). I IPA, som antogs 2016, finns bland annat bestämmelser om en metod som benämns ”equipment interference”. Metoden finns dels som s.k. ”targeted equipment interference”, dels som s.k. ”bulk equipment interference”. Det senare fallet får endast användas av underrättelse- och säkerhetstjänster, och tar sikte på utländska förhållanden. För ”bulk equipment interference” krävs tillstånd (eng. warrant) av en Secretary of State och därefter krävs också godkännande av tillståndet från en Judicial Commissioner, som är eller har varit domare (178 och 179 IPA). Med ”equipment” avses, enligt Section 135 och 198 IPA, ”equipment producing electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment”. Av Equipment

Interference Code of Practice, som kompletterar bestämmelserna i IPA, framgår vidare att "'equipment' for these purposes is not limited to equipment which is switched on and/ or is emitting signals but also includes equipment which is capable of producing such emissions" (Equipment Interference Code of Practice, Home Office, Mars 2018, s. 6).

Folkrättsliga aspekter

Signalspaning i försvarsunderrättelseverksamhet sker bl.a. i cyberrymden. Det råder internationell samsyn om att folkrätten, inklusive FN-stadgan, är tillämplig i cyberrymden. Frågor om hur folkrätten ska tillämpas i olika avseenden diskuteras fortsatt, bl.a. i FN-sammanhang. Sverige publicerade i juli 2022 en nationell position om folkrättens tillämplighet i cyberrymden och i november 2024 publicerades en EU-deklaration om samma fråga, som bl.a. behandlar frågor om cyberaktiviteter på andra staters territorium. I den nationella positionen anges bl.a. att Sverige inte ser behov av några nya folkrättsliga regler på cyberområdet. Liknande ställningstaganden görs även i EU:s deklaration. Flera andra stater har också publicerat denna typ av nationella positioner om folkrättens tillämplighet i cyberrymden.

Underrättelseinhämtning med cybermetoder är inte underkastad ett generellt folkrättsligt förbud. Detta synsätt har bl.a. stöd i Sveriges och andra staters positionspapper om cyber och folkrätt samt i litteratur (se den av NATO Cooperative Cyber Defence Centre of Excellence upprättade webbsidan cyberlaw.ccdcoe.org och Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, andra upplagan, 2017, s. 168–174).

Signalspaning i försvarsunderrättelseverksamhet är en form av underrättelseinhämtning som får bedrivas för särskilt angivna ändamål och enligt särskilt tillstånd (se avsnitt 3.2 och 3.3). Lagstiftningen har anpassats i enlighet med Europadomstolens dom i målet Centrum för rättvisa mot Sverige (se avsnitt 5.5.1). Lagstiftningen och de förslag som lämnas i detta utkast till lagrådsremiss bedöms uppfylla gällande folkrätt.

Ett tydliggörande i lag bör göras om att inhämtning av signaler i elektronisk form får ske oavsett om de är under förmedling eller är lagrade

Teknik- och telekommunikationsutvecklingen, och med den en signalmiljö under ständig förändring, har varit mycket omfattande sedan signalspaningslagens tillkomst. Internets omfattning vad gäller överföringshastigheter och trafikmängder samt dynamiken och föränderligheten i var och hur information överförs och tillgängliggörs från en stund till en annan för med sig att det blir svårare för signalspaningsverksamheten att hitta relevant information i den signalmiljö som Försvarets radioanstalt kan nå. Information som Försvarets radioanstalt är i behov av för att kunna svara på de inriktande myndigheternas underrättelsebehov. Därutöver tillkommer den alltmer utbredda användningen av kryptering i kommunikationstjänster.

Signalspaningslagstiftningen är som tidigare nämnts teknikneutral, även om det finns vissa särskilda bestämmelser för inhämtning i tråd av signaler i elektronisk form. Signalspaningslagstiftningen kan utifrån dess teknikneutralitet i viss utsträckning anses vara rustad för att möta den

accelererande teknik- och telekommunikationsutvecklingen. Av förarbetena till signalspaningslagen följer, som nämnts ovan, att inhämtning får ske oavsett var signalerna befinner sig. Försvarets radioanstalt har inhämtat lagrade signaler i elektronisk form, vilket har granskats av Siun. Det bedöms inte finnas någon risk för att ett förtydligande av lagen på föreslaget sätt kan leda till tillämpningssvårigheter av de slag som *Sveriges advokatsamfund* lyfter. Som anförts tidigare utgörs all digital information av signaler i elektronisk form. Vad som är avgörande är att inhämtningen måste följa det tillstånd som getts och i övrigt uppfylla förutsättningarna som uppställs i signalspaningslagen. Som advokatsamfundet även för fram skulle en annan ordning kunna medföra gränsdragningsproblematik eftersom en signal som förmedlas för att därefter mottas i praktiken omedelbart skulle kunna övergå till att bli lagrad. Att uppställa uttryckliga begränsningar avseende längden på signalernas lagringstid, alltså åldern på de lagrade signaler som inhämtas, är inte lämpligt och skulle kunna leda till praktiska svårigheter.

Integritetsskyddsmyndigheten efterfrågar en integritetsanalys av förslaget, eftersom detta enligt myndigheten innebär en utvidgning av möjligheten att inhämta information i förhållande till vad som var avsikten vid lagens tillkomst. Även *Föreningen för Digitala Fri- och Rättigheter* har efterlyst ytterligare analyser av förslaget. Det är av stor betydelse för allmänhetens förtroende för signalspaning i försvarsunderrättelseverksamhet att verksamhetens omfattning är klar och tydlig. Som framgått ovan finns det i bland annat Finlands, Norges och Storbritanniens lagstiftningar särskilda bestämmelser om inhämtning av exempelvis information som är lagrad i datasystem och annan nätverksansluten utrustning. Det bör därför tydliggöras i signalspaningslagen att inhämtning av signaler i elektronisk form får ske oavsett om signalerna är under förmedling eller är lagrade. Mot bakgrund av vad som har anförts ovan gällande signalspaningslagens förarbeten och hur lagstiftningen har tillämpats innebär förslaget, i likhet med utredningens bedömning, ett förtydligande om att inhämtningen inte är beroende av var signalerna befinner sig och är ett klargörande av rättsläget. Till skillnad från *Journalistförbundet* anses också att förfarandet ryms inom den befintliga definitionen av signalspaning. Det rör sig alltså inte om någon egentlig förändring, utan tvärtom har lagstiftningen redan tillämpats på detta sätt. Förslaget säkerställer också att signalspaningslagstiftningen kan möta den alltmer accelererande teknik- och telekommunikationsutvecklingen som innebär både nya utmaningar och möjligheter, bland annat i fråga om den alltmer utbredda användningen av kryptering. Förslaget innebär således att Försvarets radioanstalt fortsatt kan bedriva en effektiv och ändamålsenlig signalspaningsverksamhet. Som framgår nedan föreslås även vissa följdändringar i signalspaningslagen för att tillse att förslaget inte innebär en försämring för enskildas integritetsskyddsintressen. Det är bl.a. mot den bakgrunden – och med hänsyn till att förslaget endast utgör ett förtydligande av befintlig lag och ett klargörande av rättsläget – inte behövligt med några ytterligare analyser ur ett integritetsskyddsperspektiv än de som utredningen har lagt fram.

Vad beträffar frågan om förslaget kan komma att ha någon inverkan på uppgifter som omfattas av det s.k. källskyddet har en liknande fråga

behandlats i avsnitt 5.5.3. Det kan också konstateras att förslaget inte har någon påverkan på den förstöringsskyldighet som regleras i 7 § 2 signalspaningslagen. Anonymitetsskyddet och meddelarfriheten kommer alltså även fortsättningsvis att vara tillgodosett genom lagstiftningen, på samma sätt som tidigare.

Ett tydliggörande i lag bör göras om att signalspaningsmyndigheten får vidta nödvändiga tekniska åtgärder för att genomföra inhämtningen av signaler i elektronisk form

För att genomföra inhämtning av signaler i elektronisk form kan tekniska åtgärder behöva vidtas. Vilken typ av åtgärder som krävs är beroende av vilka företeelser som signalspaningen riktas mot, den tekniska utvecklingen och signalmiljön. Vid exempelvis inhämtning av lagrade uppgifter kan Försvarets radioanstalt behöva utnyttja tekniska sårbarheter, förbiseenden och av leverantören inbyggda åtkomstmöjligheter i nätverksansluten utrustning. Flera olika typer av tekniska åtgärder kan behöva vidtas mot en eller flera nätverksanslutna utrustningar. Vidare kan åtgärderna behöva ske över tid. När det gäller inhämtning av signaler som inte är lagrade kan det exempelvis röra sig om tekniska åtgärder som vidtas för att ta om hand signalerna från samverkanspunkterna eller för att etablera en satellitinhämtningsmiljö. Det är dock självfallet så att de tekniska åtgärder som vidtas omfattas av den efterhandskontroll som utförs av Siun, och någon ändring avseende denna kontrollverksamhet är alltså inte avsedd. Det bör förtydligas i signalspaningslagen att signalspaningsmyndigheten (Försvarets radioanstalt) får vidta de tekniska åtgärder som är nödvändiga för att genomföra inhämtning av signaler i elektronisk form.

Tydliggörande följdändringar

Enligt 2 a § signalspaningslagen får inhämtning inte avse signaler mellan en avsändare och en mottagare som båda befinner sig i Sverige. Med hänsyn till det förtydligande om lagrade uppgifter som föreslås finns det en risk för att 2 a § signalspaningslagen i sin nuvarande ordalydelse inte omfattar sådana signaler. Det är inte avsikten med förslaget. Försvarets radioanstalt tillämpar i dag bestämmelsen på sådant sätt att lagrade uppgifter i Sverige endast kan bli föremål för inhämtning om undantagen i andra stycket är tillämpliga. Det bedöms i likhet med utredningen att Försvarets radioanstalts tillämpning av bestämmelsen framstår som rimlig och lämplig. Bestämmelsen har ett tydligt integritetsskyddande syfte. Med hänsyn till detta och till vikten av att eventuella oklarheter kring dess tillämpning klargörs bör det därför framgå att inhämtningsförbudet även gäller signaler som är lagrade i Sverige. Detsamma bör även gälla förstöringsskyldigheten om sådana signaler inte kan avskiljas vid inhämtningen. Enbart den omständigheten att signalerna är lagrade i Sverige innebär dock inte per automatik att inhämtningsförbudet aktualiseras, utan detta förutsätter som huvudregel att avsändaren och mottagaren båda befinner sig här. Vidare bör det förtydligas att undantagen i andra stycket omfattar all inhämtning. Det är av vikt både i fråga om inhämtning som riktas mot militär personal m.m. och övningsverksamhet (se förslag i avsnitt 7.3) att inhämtning kan ske för

lagrade signaler. I fråga om signaler som utväxlas autonomt mellan tekniska system, och som inte innehåller personuppgifter, är dock sådana signaler till sin natur alltid under förmedling.

Det föreslagna förtydligandet om lagrade uppgifter ska inte heller innebära någon förändring i fråga om den kontroll som regleras i 10 a § signalspaningslagen. Av bestämmelsen följer att kontrollen ska avse om den enskildes meddelanden inhämtats i samband med signalspaning enligt signalspaningslagen. För att förslaget om förtydligande i 1 § signalspaningslagen inte ska innebära en försämring för den enskilde bör det i lagen anges att kontrollen ska avse hans eller hennes meddelanden eller lagrade uppgifter. Sådana lagrade uppgifter kan vara meddelanden som skickats eller tagits emot av den enskilde, men också andra lagrade uppgifter hos den enskilde omfattas. Det bör i likhet med vad som tidigare uttalats vara fråga om uppgifter som inhämtats från den enskilde och som genom urvalsprocessen med sökbegrepp blivit tillgänglig för Försvarets radioanstalt för vidare bearbetning och analys (jfr prop. 2008/09:201 s. 92). I enlighet med vad som tidigare uttalats är de utredningsåtgärder som kan vidtas avhängiga vilken information den enskilde kan tillhandahålla (a. prop. s. 92–93).

7 Signalspaning i övningsverksamhet

7.1 Behov av signalspaning i övningsverksamhet

Utkastets bedömning: Försvarets radioanstalt bör få inhämta signaler i elektronisk form vid signalspaning till stöd för övningsverksamhet som sker i syfte att utveckla totalförsvarsförmågan.

Utredningens bedömning överensstämmer med utkastets.

Remissinstanserna: *Försvarets radioanstalt* instämmer i utredningens bedömning. Övriga remissinstanser yttrar sig inte särskilt i frågan.

Skälen för utkastets bedömning: Det säkerhetspolitiska läget har försämrats de senaste åren och Sverige är sedan mars 2024 medlem i Nato (se avsnitt 5.1). Det försämrade säkerhetspolitiska läget har bland annat inneburit en utökad nationell övningsverksamhet för Försvarsmakten. Även övningsverksamheten tillsammans med internationella samarbetspartners har ökat med anledning av det försämrade omvärldsläget och Sveriges medlemskap i Nato. Ett försämrat säkerhetspolitiskt läge innebär också större behov av övningsverksamhet inom totalförsvaret. Utbildning och övning utgör viktiga verktyg för att bygga reell totalförsvarsförmåga.

Försvarets radioanstalt ska enligt senare regleringsbrev för myndigheten stärka myndighetens förmåga att verka vid svåra påfrestningar och under höjd beredskap. Beredskapsplanering vid Försvarets radioanstalt inom totalförsvaret innefattar planering, förberedelser och övningar i syfte att Försvarets radioanstalt ska kunna klara av omställningen till krigsorganisation och kunna verka när krigsförhållanden råder i Sverige.

Eftersom det inte går att förutse hur sådana förhållanden kan komma att gestalta sig innebär det således förberedelser för något som i dag är okänt.

Det är av stor vikt att Försvarets radioanstalt har möjlighet att öva i den skarpa signalmiljön för att kunna utveckla myndighetens förmåga att verka under höjd beredskap. All inhämtning av signaler i elektronisk form vid signalspaning kräver stöd i lag. Försvarets radioanstalt får inte inhämta signaler i elektronisk form genom signalspaning för några andra ändamål än dem som anges i 1 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (signalspaningslagen). Signalspaning till stöd för svensk övningsverksamhet inom ramen för utveckling av totalförsvarsförmågan saknas som ett ändamål i nämnda bestämmelse. Detta innebär att Försvarets radioanstalt inte kan delta med signalspaning i övningar som bedrivs i den skarpa signalmiljön. Det saknas alltså enligt nuvarande reglering möjlighet för Försvarets radioanstalt att delta med signalspaning i övningsverksamhet.

Signalspaning inom ramen för övningsverksamhet innebär att rikta inhämtningen mot de aktörer eller förband som i övningen representerar främmande makt. Det föreligger ofta naturliga beröringspunkter mellan övningsscenarier och verkligheten. En övning ska ytterst bidra till att utveckla de övandes förmåga att lösa sina uppgifter i ett verkligt skeende. Utgångspunkten för ett övningsscenario kan till exempel vara skydd av ett verkligt område, en anläggning eller en annan resurs av betydelse för det svenska militära försvaret eller totalförsvaret.

Det försämrade säkerhetspolitiska läget innebär att det finns allt större behov av att stärka och utveckla totalförsvarsförmågan. Genom övning med signalspaning i skarp signalmiljö skulle Försvarets radioanstalt enskilt och tillsammans med Försvarsmakten kunna utveckla och förbereda verksamheten inför beredskapshöjning, krig och krigsfara på ett sätt som inte är möjligt enligt den nuvarande reglering. Förberedelser och övningar krävs för att effektivt agera i det system i vilket den egna verksamheten utgör ett delsystem eller ett enskilt verktyg.

Med mer övningsverksamhet och aktivitet inom Försvarsmakten och totalförsvaret ökar vidare exponeringen av den skyddsvärda verksamheten. Signalspaning inom ramen för övningsverksamhet kan således också syfta till att minska risken för att svenska militära förbandsenheter identifieras av främmande makts underrättelsetjänst. Vid sådan verksamhet ska Försvarets radioanstalt rikta signalspaning mot enheterna för att verifiera deras modus och egen radiosignalering. Det kan till exempel handla om att svenska förbandsenheter ska kunna förflytta sig geografiskt utan att bli upptäckta och lägesbestämda när de kommunicerar.

Det finns mot bakgrund av det försämrade säkerhetsläget och de ökade behoven av övningsverksamhet inom såväl det militära försvaret som i totalförsvaret behov av att Försvarets radioanstalt kan delta med signalspaning i övningar. Vid sådan övningsverksamhet ges Försvarets radioanstalt och Försvarsmakten möjlighet att utveckla och förstärka sin förmåga att samverka inför beredskapshöjning och i krig och krigsfara. I likhet med vad utredningen anfört bedöms övningsverksamheten i första hand kunna vara till stor nytta för att myndigheterna ska kunna verka tillsammans under sådana förhållanden. Sådan övningsverksamhet kan också vara till stor nytta för att effektivisera och utveckla Försvarets radioanstalts egen förmåga att bedriva sin verksamhet. Övnings-

verksamheten kan därutöver även vara till nytta för att stärka och utveckla totalförsvarsförmågan hos andra i totalförsvaret. Signaler i elektronisk form bör således få inhämtas vid signalspaning också inom ramen för övningsverksamhet.

Eftersom övningsverksamhet innebär att förbereda sig för framtida, okända skeenden är det svårt att fullt ut förutse hur olika övningsscenarion kan komma att se ut. Lagstiftningen måste därför kunna ge Försvarets radioanstalt tillräckliga möjligheter att bedriva en effektiv och ändamålsenlig övningsverksamhet för att totalförsvarsförmågan i sin tur ska kunna utvecklas.

7.2 Ett nytt ändamål för signalspaning i övningsverksamhet

Utkastets förslag: En ny bestämmelse som möjliggör inhämtning av signaler i elektronisk form vid signalspaning i övningsverksamhet införs i lagen om signalspaning i försvarsunderrättelseverksamhet.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: En majoritet av remissinstanserna, däribland *Försvarets radioanstalt*, *Försvarsmakten*, *Integritetsskyddsmyndigheten, Justitiekanslern* och *Polismyndigheten*, tillstyrker eller har inga synpunkter på förslaget.

Sveriges advokatsamfund avstyrker förslaget och anför att det saknas en bedömning av vilka särskilda begränsningar som bör kunna gälla för inhämtningen för att åtgärderna inte i onödan ska inkräkta på den personliga integriteten. Advokatsamfundet ser inte heller hur en övning ska kunna ge sådan information vars värde är klart större än det integritetsintrång som inhämtningen kan innebära. Enligt advokatsamfundet borde särskilda signalutväxlingar kunna ordnas som kan bli föremål för övningsverksamheten, vilket skulle undvika onödiga integritetsintrång.

Tjänstemännens centralorganisation (TCO) avstyrker förslaget om att övning ska kunna ske i den skarpa signalmiljön eftersom det inte kan uteslutas att uppgifter som omfattas av källskydd kan inhämtas och därefter hanteras av myndigheter i andra länder. *Journalistförbundet* framför synpunkter av liknande slag och avstyrker förslaget. Förbundet pekar på att det inte kan uteslutas att övningsverksamheten kan resultera i större inhämtningar av uppgifter vilket leder till att intrång i den personliga integriteten kan bli omfattande. Förbundet anser även att förslaget innebär en begränsning av fri- och rättigheter enligt regeringsformen men att det saknas en proportionalitetsbedömning av detta.

Skälen för utkastets förslag

Nuvarande reglering

Enligt 1 § lagen (2000:130) om försvarsunderrättelseverksamhet ska försvarsunderrättelseverksamhet bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot

mot landet. Försvarsunderrättelseverksamhet får endast avse utländska förhållanden. Signalspaningslagen innehåller i sin tur begränsningar för signalspaningsverksamheten. Av 1 § andra stycket signalspaningslagen framgår att signalspaning i försvarsunderrättelseverksamhet endast får ske i syfte att kartlägga de företeelser som anges i bestämmelsen. Av 1 § tredje stycket signalspaningslagen följer att signalspaning också får ske för Försvarets radioanstalts utvecklingsverksamhet.

En ny ändamålsbestämmelse för signalspaning i övningsverksamhet

Det finns behov av att Försvarets radioanstalt kan bedriva signalspaning i övningsverksamhet. Som konstateras ovan omfattas inhämtning av signaler i elektronisk form i övningsverksamhet inte av det nuvarande regelverket. För att signalspaning i övningsverksamhet ska få bedrivas krävs således att det införs ett nytt lagstöd som kan möjliggöra detta. Det bör därför införas en ny särskild ändamålsbestämmelse som innebär att Försvarets radioanstalt får inhämta signaler i elektronisk form vid signalspaning i övningsverksamhet.

Förslaget innebär att Försvarets radioanstalt får delta med signalspaning i övningar i den skarpa signalmiljön. Genom övning med signalspaning i den miljön kan Försvarets radioanstalt enskilt och tillsammans med Försvarsmakten utveckla och förbereda verksamheten inför beredskapshöjning, krig och krigsfara på ett sätt som inte är möjligt enligt den nuvarande regleringen. I första hand är det fråga om gemensam övningsverksamhet tillsammans med Försvarsmakten. Men Försvarets radioanstalt kan även komma att bedriva övningsverksamhet på egen hand. I ett större totalförsvarssammanhang skulle det också kunna förekomma att andra myndigheter deltar i övningarna. Det kan röra sig om nationell övningsverksamhet, men också internationell. Övningsverksamheten ska ge deltagarna möjlighet att öva på uppgifter som de kan komma att möta i ett verkligt scenario. Den ska bidra till att deltagarna får utveckla sina förmågor att lösa problem och utmaningar som de kan möta i exempelvis en situation då Sverige är i krig eller i krigsfara. I detta sammanhang är det avgörande att kunna hantera signalmiljön i vilken signalspaningen ska kunna verka i vid krigsfara eller krig. Syftet med övningsverksamheten är således att utveckla förmågan hos myndigheterna och i förlängningen Sverige att verka inför och under höjd beredskap. Signaler i elektronisk form ska enligt förslaget få inhämtas vid övning, om det är nödvändigt för att utveckla förmåga att verka under höjd beredskap.

Intrång i den personliga integriteten

Övningsverksamheten innebär att förbereda sig för något som är okänt. Signalspaning i övningsverksamhet är därför avsedd att bedrivas i verklighetsnära, om än fiktiva, scenarier. Det innebär bland annat att Försvarets radioanstalt vid övningar kommer att verka i och kartlägga den skarpa signalmiljön, vilket, till skillnad från vad *Sveriges advokatsamfund* anser, bedöms vara mest ändamålsenligt. Signalspaning i övnings-verksamhet kommer troligen i huvudsak att avse inhämtning av signaler i elektronisk form som överförs i etern. Vid sådan inhämtning inhämtas färre signaler än vad som är fallet vid inhämtning av signaler i tråd. Övningsscenarierna kommer dock att påverka inhämtningsbehoven vid

respektive tillfällen, till exempel kan de komma att skilja sig åt vid en mindre, lokal övning i jämförelse med en större internationell övning med många deltagare. Det kan dock, i likhet med vad som gäller vid signalspaning i försvarsunderrättelse- och utvecklingsverksamhet, inte uteslutas att en upptagning eller uppteckning som innehåller uppgifter som saknar relevans inhämtas. Som Sveriges advokatsamfund påpekar finns det alltså en risk för intrång i den personliga integriteten för enskilda som inte deltar i övningen. För den enskilde som deltar i övningen, till exempel i egenskap av figurant som agerar som främmande makt, måste dock intrånget i den personliga integriteten anses vara obefintligt.

Journalistförbundet och *TCO* har påpekat att om signalspaning tillåts i de fall som nu är aktuella skulle det kunna medföra en risk för att uppgifter som omfattas av källskydd inhämtas för att därefter hanteras av utländska myndigheter.

För att en sådan inskränkning i den personliga integriteten som förslaget riskerar att medföra ska kunna godtas, måste detta stå i proportion till dess syfte. För att signalspaning i övningsverksamhet ska anses vara acceptabel är det alltså viktigt att verksamheten omgärdas av rättssäkerhetsgarantier och har ett tydligt tillämpningsområde.

Som beskrivits inledningsvis i detta kapitel finns det ett tydligt och angeläget behov för Försvarets radioanstalt att bedriva signalspaning i övningsverksamhet, bland annat för att effektivisera och utveckla den egna förmågan men även för att stärka och utveckla totalförsvarsförmågan hos andra i totalförsvaret. Något mindre ingripande alternativ för att uppnå syftet med förslaget bedöms inte heller finnas. Det finns därtill ett flertal mekanismer i bland annat signalspaningslagen som syftar till att värna enskildas integritetsskyddsintressen. Det innebär exempelvis att den signalspaning som bedrivs inom ramen för övningsverksamhet ska föregås av en inriktning (se avsnitt 7.4) och av tillståndsprövning av Försvarsunderrättelsedomstolen (se avsnitt 7.5). Det föreslås också att Försvarets radioanstalt ska ha en förstöringsskyldighet avseende upptagningar och uppteckningar som inhämtas inom ramen för övningsverksamheten (se avsnitt 7.6). Även den förstöringsskyldighet som föreligger enligt 2 a och 7 §§ signalspaningslagen ska vara tillämplig vid signalspaning i övningsverksamhet. Verksamheten ska också omfattas av Statens inspektion för försvarsunderrättelseverksamhetens (Siun) efterhandskontroll. Samma rättssäkerhetsgarantier ska alltså vara tillämpliga vid signalspaning i övningsverksamhet. Som beskrivs nedan ska även samma villkor som ska vara uppfyllda vid överföring av personuppgifter till en mottagare utomlands i försvarsunderrättelse- och säkerhetssamarbetet även vara uppfyllda vid sådan överföring som sker inom ramen för internationellt samarbete i övningsverksamheten. Regleringen innebär alltså ett ändamålsenligt skydd för den typen av uppgifter som Journalistförbundet och TCO syftar på. Sveriges advokatsamfunds och Journalistförbundets farhågor kring tillämpningen av det nya regelverket delas därför inte heller.

Som Journalistförbundet påpekar leder förslaget i och för sig till att fler uppgifter kan omfattas av inhämtning genom signalspaning vilket alltså kan innebära en risk för intrång i enskildas grundläggande fri- och rättigheter som skyddas enligt 2 kap. 6 § regeringsformen och artikel 8 i Europakonventionen. Den regleringen beskriver utredningen i avsnitt 4 i

betänkandet. Utredningen har även redogjort för nödvändigheten av förslaget och utformat detta på ett sätt som ska främja skyddet för enskildas personliga integritet. Flera av dessa åtgärder har nyss redovisats. Journalistförbundets beskrivning av att det saknas en proportionalitetsbedömning av förslaget delas därför inte. Förslaget bedöms tillhandahålla ett tillräckligt skydd för enskildas personliga integritet.

7.3 Inhämtning av inhemska signaler

Utkastets förslag: Signaler i elektronisk form som sänds mellan en avsändare och en mottagare som båda befinner sig i Sverige och signaler som lagras i Sverige får inhämtas vid signalspaning i övningsverksamhet.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna yttrar sig inte särskilt över förslaget i denna del.

Skälen för utkastets förslag: Det är avgörande för förmågeuppbyggnad att dels kunna hantera den skarpa signalmiljön i vilken signalspaning ska kunna verka i vid krig eller krigsfara, dels kunna ha möjlighet att öva i den skarpa signalmiljön. Grunden för målsökning och inhämtning av exempelvis signaltekniska uppgifter och adresseringsuppgifter vid övningsverksamhet är att kartlägga signalmiljön i vilken övningen bedrivs. Med utgångspunkt från det kan sedan målsökning och inhämtning mot avsändare och mottagare inom övningen genomföras.

Av naturliga skäl kommer nationell övningsverksamhet för det militära försvaret, eller i ett större totalförsvarssammanhang, bedrivas i Sverige. De inslag i övningsverksamheten som står i fokus för signalspaningen är signaler i elektronisk form, dvs. inslag i övningen som innefattar användning av tekniska system för kommunikation och informationshantering från övningsdeltagarnas sida. Både avsändare och mottagare kommer i dessa sammanhang troligen befinna sig i Sverige. För att signalspaning i övningsverksamhet fullt ut ska kunna bidra till att utveckla totalförsvarsförmågan är det av vikt att övning kan ske under så realistiska former som möjligt. Med andra ord att signaler i elektronisk form kan inhämtas vid signalspaning mellan deltagarna i övningen. Nationell övningsverksamhet i en skarp signalmiljö förutsätter alltså att signaler kan inhämtas mellan en avsändare och en mottagare som båda befinner sig i Sverige. Enligt nuvarande reglering är sådan inhämtning inte tillåten.

Enligt 2 a § första stycket signalspaningslagen får inhämtning inte avse signaler mellan en avsändare och mottagare som båda befinner sig i Sverige. Om sådana signaler inte kan avskiljas redan vid inhämtningen, ska upptagningen eller uppteckningen förstöras så snart det står klart att sådana signaler har inhämtats. Detsamma gäller i fråga om upptagningar och uppteckningar som Försvarets radioanstalt har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete. Från förbudet att inhämta inhemska signaler finns två undantag i paragrafens andra stycke. Undantag gäller dels för signaler som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte

innehåller personuppgifter, dels för signaler som sänds från eller till utländsk militär personal, utländska statsfartyg, statsluftfartyg eller militära fordon. I avsnitt 6.3 föreslås att förbudet att inhämta signaler mellan en avsändare och mottagare som båda befinner sig i Sverige och undantaget från förbudet för utländsk militär personal m.m. ska omfatta också signaler som lagras i Sverige.

I förarbetena anförde regeringen att förbudet mot inhämtning av signaler mellan en avsändare och mottagare som båda befinner sig i Sverige, liksom de begränsningar i övrigt som lagen uppställer, endast gäller vid signalspaning som sker utan samtycke (prop. 2008/09:201 s. 42). Det skulle således i och för sig vara möjligt att inhämta inhemsk trafik i övningsverksamheten med stöd av samtycke från avsändare och mottagare. Det är dock inte en lämplig ordning bland annat med hänsyn till att det inte garanteras att det aldrig inhämtas uppgifter som saknar relevans för övningsverksamheten (jfr prop. 2006/07:63 s. 104–105). Om ett system med samtycke skulle användas i övningsverksamhet skulle det också ställa stora krav på särskild dokumentation för att möjliggöra efterföljande granskning. Det riskerar att leda till en administrativt tung börda för Försvarets radioanstalt och för övriga som deltar i övningen. Det är en lämpligare och mer ändamålsenligt att ha ett särskilt undantag i lag. En lagreglering i denna fråga innebär också att signalspaningslagstiftningens omfattning blir tillgänglig för allmänheten.

För att möjliggöra en ändamålsenlig signalspaning i övningsverksamhet föreslås att Försvarets radioanstalt vid sådan verksamhet ska tillåtas att inhämta signaler i elektronisk form som sänds mellan en avsändare och mottagare som båda befinner sig i Sverige. Detsamma föreslås ska gälla för signaler som lagras i Sverige (se avsnitt 6.3). Signalerna kan sändas från eller till såväl fysiska personer som fartyg, luftfartyg och fordon. Beroende på övningssammanhang kan det vara fråga om både militära och civila avsändare och mottagare. Signalspaning i övningsverksamhet kan användas vid både nationella och internationella övningar. Även internationella avsändare och mottagare på svenskt territorium bör därför omfattas av undantaget. Det kan därutöver även vara fråga om signaler som sänds till, från eller utväxlas autonomt mellan tekniska system. Det föreslagna undantaget vid signalspaning i övningsverksamhet omfattar således också sådan inhämtning som anges i 2 a § andra stycket 1 och 2 signalspaningslagen.

Om signaler inhämtas som inte omfattas av undantaget ska upptagningen eller uppteckningen, i enlighet med vad som gäller enligt 2 a § första stycket signalspaningslagen, förstöras så snart det står klart att sådana signaler har inhämtats. Samma förstöringsskyldighet ska gälla i fråga om upptagning eller uppteckning som Försvarets radioanstalt får inom ramen för internationellt samarbete i övningsverksamheten. Försvarets radioanstalts förstöringsskyldighet behandlas vidare i avsnitt 7.6.

7.4 Inriktning av signalspaning i övningsverksamhet

Utkastets förslag: Regeringen och Försvarsmakten får ansvar att inrikta signalspaning i övningsverksamhet.

Regeringen ska ensam ansvara för inriktning av övningsverksamhet vid internationellt samarbete.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för utkastets förslag: Det är regeringen som enligt 1 § lagen om försvarsunderrättelseverksamhet bestämmer försvarsunderrättelseverksamhetens inriktning. Signalspaning i försvarsunderrättelseverksamhet får enligt 1 § första stycket och 4 § första stycket signalspaningslagen inriktas av regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten. Det följer av 3 § lagen om försvarsunderrättelseverksamhet att Försvarets radioanstalt, enligt regeringens närmare bestämmande, får etablera och upprätthålla samarbete i underrättelsefrågor med andra länder och internationella organisationer. Detsamma gäller för Försvarets radioanstalts internationella samarbete inom utvecklingsverksamheten enligt 9 § andra stycket signalspaningslagen.

Det är självklart att regeringen, liksom vad som gäller för övrig signalspaning, ska inrikta signalspaning i övningsverksamhet. Frågan är om någon annan myndighet också bör få inriktningsrätt i denna del.

Övningsverksamheten ska i förlängning bidra till att utveckla och stärka förmågan för Försvarets radioanstalt att verka under höjd beredskap. I vissa avseenden finns det likheter med Försvarets radioanstalts utvecklingsverksamhet, som regeringen ensam inriktar. I förarbetena anfördes att det mot bakgrund av att utvecklingsverksamheten syftar till att tillgodose Försvarets radioanstalts eget behov av att följa den tekniska utvecklingen inte fanns anledning att ge andra myndigheter möjlighet att inrikta den (prop. 2006/07:63 s. 79). Övningsverksamheten ska dock inte endast kunna användas för att utveckla Försvarets radioanstalts egen verksamhet, utan också kunna bidra till utvecklingen av totalförsvarsförmågan hos andra myndigheter. Det är huvudsakligen genom övningar tillsammans med Försvarsmakten som sådant utvecklingsarbete är avsett att bedrivas. Sett till detta är det lämpligt att också Försvarsmakten får inrikta signalspaning i övningsverksamhet. En sådan inriktningsrätt för Försvarsmakten bedöms möjliggöra effektiva övningar i den skarpa signalmiljön. Det finns inte behov av att tillåta ytterligare myndigheter att inrikta signalspaning i övningsverksamhet.

I avsnitt 7.8 nedan föreslås att Försvarets radioanstalt vid signalspaning i övningsverksamhet ska få samarbeta med andra länder och internationella organisationer. Regeringen bör ensam ansvara för inriktning av övningsverksamhet vid internationellt samarbete. Det överensstämmer med att det endast är regeringen som får inrikta Försvarets radioanstalts internationella samarbete i försvarsunderrättelse- och utvecklingsverksamhet. I tidigare förarbeten har det motiverats med

det internationella samarbetets tydliga utrikes-, säkerhets- och försvarspolitiska aspekter samt att det är efter regeringens närmare bestämmande som sådant samarbete får ske (prop. 2020/21:224 s. 158). Samma skäl gör sig gällande även i fråga om internationellt samarbete i övningsverksamheten. Det bör således ankomma på regeringen att ensam inrikta verksamheten i den delen. Någon särskild reglering i denna fråga är inte nödvändig, eftersom ett sådant samarbete endast ska få ske efter regeringens närmare bestämmande (se avsnitt 7.8).

7.5 Tillstånd för signalspaning vid övningsverksamhet

Utkastets förslag: Det ska krävas tillstånd för att signaler i elektronisk form ska få inhämtas vid signalspaning i övningsverksamhet.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för utkastets förslag: Det krävs tillstånd av Försvarsunderrättelsedomstolen för att Försvarets radioanstalt ska få inhämta signaler i elektronisk form vid signalspaning. Bestämmelser om vad en ansökan till Försvarsunderrättelsedomstolen ska innehålla och vad domstolen ska pröva framgår av 4 a och 5 §§ signalspaningslagen. I 5 b § signalspaningslagen finns bestämmelser om tillståndsprövningen i brådskande fall. Tillståndsprövningen innebär en form av förhandskontroll. Bland annat ska användning av sökbegrepp eller kategorier av sökbegrepp prövas av domstolen. Domstolsprövningen utgör således ett skydd mot otillbörliga intrång i den personliga integriteten för enskilda. Tillstånden utgör också en grund för den efterhandskontroll som Siun utför enligt 10 § signalspaningslagen.

Även signalspaning i övningsverksamhet ska föregås av tillstånd av Försvarsunderrättelsedomstolen. Med hänsyn till att övningsverksamheten kommer att föregås av planering bedöms det inte finnas behov av en möjlighet att fatta brådskande beslut enligt 5 b § signalspaningslagen. Det finns därför inte skäl att göra några ändringar i nämnda paragraf.

Förslaget i fråga om signalspaning i övningsverksamhet innebär ingen skillnad i fråga om vad en ansökan ska innehålla eller vad Försvarsunderrättelsedomstolen ska pröva (prop. 2008/09:201 s. 56–59 och 111–112). Det ankommer på Försvarets radioanstalt att utifrån de behov som finns inom ramen för övningsverksamheten formulera en ansökan till Försvarsunderrättelsedomstolen i enlighet med vad som krävs enligt signalspaningslagen.

7.6 Förstöringsskyldighet

Utkastets förslag: En upptagning eller uppteckning som innehåller uppgifter som saknar relevans för övningsverksamheten ska omgående förstöras.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: De flesta av remissinstanserna yttrar sig inte specifikt över förslaget. *Statens inspektion för försvarsunderrättelseverksamheten* (Siun) framhåller att förstöringsskyldigheten innebär att det kommer finnas en begränsad tid för granskning av det inhämtade materialet. Siun anser att ytterligare åtgärder måste övervägas för att säkerställa att det finns tillräckligt med tid för kontrollen.

Skälen för utkastets förslag

Nuvarande reglering

Som nämnts tidigare innehåller 2 a § signalspaningslagen en förstöringsskyldighet vid inhämtning av inhemska signaler. Ytterligare bestämmelser om Försvarets radioanstalts förstöringsskyldighet finns i 7 § signalspaningslagen. Av 7 § 1 signalspaningslagen framgår att en upptagning eller uppteckning omgående ska förstöras om innehållet har bedömts sakna betydelse för verksamhet som avses i 1 § signalspaningslagen. Enligt 7 § 2–4 signalspaningslagen ska en upptagning eller uppteckning också förstöras om innehållet

- avser uppgifter för vilka tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen, eller som omfattas av efterforskningsförbudet i 3 kap. 5 § tryckfrihetsförordningen eller 2 kap. 5 § yttrandefrihetsgrundlagen,
- omfattar uppgifter i sådana meddelanden mellan en person som är misstänkt för brott och hans eller hennes försvarare vilka skyddas enligt 27 kap. 22 § första stycket rättegångsbalken, eller
- avser uppgifter lämnade under bikt eller enskild själavård, såvida det inte finns synnerliga skäl att behandla uppgifterna för syften som anges i 1 § andra stycket signalspaningslagen.

Kravet på förstöring gäller även i fråga om upptagningar och uppteckningar som Försvarets radioanstalt har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete.

Därutöver kan Siun vid efterhandskontroll enligt 10 § signalspaningslagen besluta att en upptagning eller uppteckning under vissa omständigheter ska förstöras. Enligt 10 a § signalspaningslagen har det särskilda beslutandeorganet som utför kontroll på begäran av enskild en motsvarande befogenhet. Av 5 § förordningen (2008:923) om signalspaning i försvarsunderrättelseverksamhet framgår att förstöring av upptagningar eller uppteckningar enligt 7, 10 och 10 a §§ signalspaningslagen ska ske på ett sådant sätt att uppgifterna inte kan återskapas.

Förstöring av upptagning eller uppteckning som inhämtas vid signalspaning i övningsverksamhet

Det föreslås att Försvarets radioanstalt ska få inhämta signaler i elektronisk form vid signalspaning i övningsverksamhet. Enligt 3 § signalspaningslagen ska inhämtning av signaler i tråd ske automatiserat. Sådan inhämtning får endast avse signaler som identifierats genom sökbegrepp. Även vid annan automatiserad inhämtning ska sökbegrepp användas för identifiering av signaler. Genom användningen av sökbegrepp sker ett urval av vilka signaler som inhämtas. Urvalsprocessen syftar till att få fram uppgifter som är relevanta, vilket innebär ett visst integritetsskydd. Det kan dock konstateras att det inte finns någon absolut garanti för att det ändå inte kan förekomma uppgifter som saknar relevans i det material som inhämtas.

Det kan inte heller i fråga om signalspaning i övningsverksamhet uteslutas att det kan förekomma uppgifter som saknar relevans för övningsverksamhetens behov. Eftersom uppgifterna inte behövs för övningsverksamheten saknas det skäl att hantera dem. Prövningen av uppgifternas relevans för övningsverksamheten bör ske löpande. Så snart det kan konstateras att en upptagning eller uppteckning innehåller uppgifter som saknar betydelse för övningsverksamheten ska de förstöras.

Övningsverksamheten ska inte resultera i några underrättelser (se avsnitt 7.7). Det innebär att relevansen av de inhämtade uppgifterna upphör när övningen avslutats och de slutsatser och erfarenheter som övningen lett till har summerats. Det saknas efter denna tidpunkt skäl att hantera uppgifterna vidare och de bör således omgående förstöras. Det kan med hänsyn till övningens omfattning variera vilken tid som är nödvändig för att sammanställa erfarenheter och slutsatser från den. Det går därför inte att uttala sig om någon exakt tidpunkt för när en sådan sammanställning ska vara färdigställd. Det bör dock ankomma på Försvarets radioanstalt att så snart som det är möjligt efter övningens avslutande dokumentera erfarenheter och slutsatser så att inhämtade uppgifter kan förstöras.

För att tillgodose att en upptagning eller uppteckning som inhämtas inom ramen för övningsverksamheten förstörs i enligt med vad som anges ovan föreslås att 7 § 1 signalspaningslagen ändras på sådant sätt att övningsverksamheten också omfattas av bestämmelsen.

Övriga bestämmelser som reglerar Försvarets radioanstalts förstöringsskyldighet är såsom bestämmelserna är utformade tillämpbara även på signalspaning i övningsverksamhet.

I fråga om kontroll av Försvarets radioanstalts förstöring kan det konstateras att Siun, enligt 10 § signalspaningslagen, särskilt ska kontrollera bland annat förstöring av uppgifter. Det innebär i detta fall att Siun har till uppgift att kontrollera att Försvarets radioanstalt inte bevarar och hanterar upptagningar eller uppteckningar som innehåller uppgifter som saknar relevans för övningsverksamheten. Eftersom förstöring av uppgifter ska ske i anslutning till övningens slut och summering av slutsatserna och erfarenheterna kring denna så kan detta innebära, vilket *Siun* framhåller, beroende av övningens beskaffenhet finnas en begränsad tidsperiod då inspektionen kan genomföra efterhandskontroll av det material som inhämtats. Siun bör dock vid behov kunna koordinera sina inspektioner och granskningar med övningsverksamheten för att på så sätt

ges möjlighet att granska materialet innan förstöring sker. I annat fall får som nyss nämnts kontrollen bl.a. avse att förstöring av uppgifter sker på ett korrekt sätt.

7.7 Övningar får inte resultera i underrättelser

Utkastets förslag: Uppgifter som inhämtats vid signalspaning i övningsverksamhet får inte resultera i underrättelser.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för utkastets förslag: Av 2 § lagen om försvarsunderrättelseverksamhet framgår att försvarsunderrättelseverksamhet ska fullgöras genom inhämtning, bearbetning och analys av information. Underrättelser ska rapporteras till berörda myndigheter. Enligt 8 § första meningen signalspaningslagen ska Försvarets radioanstalt rapportera underrättelser med uppgifter som inhämtats enligt signalspaningslagen till berörda myndigheter i enlighet med vad som föreskrivs i lagen om försvarsunderrättelseverksamhet. Av 8 § andra meningen signalspaningslagen följer att om uppgifterna berör en viss fysisk person, får rapporteringen endast avse förhållanden som är av betydelse i de hänseenden som anges i 1 § lagen om försvarsunderrättelseverksamhet.

Signalspaning i övningsverksamhet syftar till att stärka och utveckla Försvarets radioanstalts och andra myndigheters förmåga att verka under höjd beredskap. För att åstadkomma ett effektivt och ändamålsenligt utvecklingsarbete behöver resultaten av en övning bland annat analyseras och följas upp. En övning kan således komma att resultera i olika former av dokumenterade erfarenheter och slutsatser som, vid behov, kan delas med andra myndigheter. Sådan dokumentation är dock inte att anse som underrättelser som ska rapporteras enligt lagen om försvarsunderrättelseverksamhet. Övningsverksamheten bör därmed inte omfattas av 8 § första meningen signalspaningslagen. För att tydliggöra detta föreslås att det införs ett nytt andra stycke som förtydligar att uppgifter som inhämtas vid signalspaning i övningsverksamhet inte får resultera i underrättelser.

7.8 Internationellt samarbete

Utkastets förslag: Försvarets radioanstalt får vid signalspaning i övningsverksamhet samarbeta med andra länder och internationella organisationer.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för utkastets förslag: Enligt 3 § lagen om försvarsunderrättelseverksamhet får den eller de myndigheter som bedriver försvarsunderrättelseverksamhet, efter regeringens närmare bestämmande, etablera och upprätthålla samarbete i underrättelsefrågor med andra länder och internationella organisationer. De myndigheter som

bedriver försvarsunderrättelseverksamhet får samarbeta i underrättelsefrågor med andra länder och internationella organisationer endast under förutsättning att syftet med samarbetet är att tjäna den svenska statsledningen och det svenska totalförsvaret. De uppgifter som myndigheterna lämnar till andra länder och internationella organisationer får inte vara till skada för svenska intressen (3 § förordningen [2000:131] om försvarsunderrättelseverksamhet).

En motsvarande reglering finns för internationellt samarbete i fråga om Försvarets radioanstalts utvecklingsverksamhet enligt 9 § andra stycket signalspaningslagen och 6 § förordningen om försvarsunderrättelseverksamhet.

Försvarets radioanstalts deltagande i internationellt samarbete inom myndighetens försvarsunderrättelse- och utvecklingsverksamhet utgör en integrerad och viktig del i myndighetens arbete. Inget land kan på egen hand inhämta ett fullständigt underrättelseunderlag till stöd för den bedrivna utrikes-, säkerhets- och försvarspolitiken, eller för kartläggningen av yttre hot mot landet. Utbyte av underrättelser och samarbete om metodik och teknik är centrala inslag i försvarsunderrättelseverksamhet, och inte minst i Försvarets radioanstalts signalspaningsverksamhet. Internationella samarbeten kan åstadkomma en utökad geografisk räckvidd för Försvarets radioanstalts signalspaning, och motsvarande för en samarbetspart. Förtroendefulla samarbeten bidrar också påtagligt till möjligheterna att möta den dynamiska och accelererande teknik- och telekommunikationsutveckling som fortlöpande ställer signalspaningen inför nya utmaningar och som inget land ensamt förmår möta. Förtroendefulla och effektiva samarbeten med motsvarande organisationer i utlandet är en förutsättning för att Försvarets radioanstalt på ett fullgott sätt ska kunna tillgodose det underrättelsebehov som finns hos regeringen och övriga inriktande myndigheter. Försvarets radioanstalts internationella samarbeten inom försvarsunderrättelse- och utvecklingsverksamhet är således av avgörande betydelse för svensk utrikes-, säkerhets- och försvarspolitik och i övrigt vid kartläggning av yttre hot mot landet.

Det finns även inom ramen för övningsverksamheten behov av att samarbeta med andra länder och internationella organisationer, till exempel med utländska signalspaningsfunktioner vid internationella övningar. Sådana samarbeten kan bidra till att utveckla och stärka totalförsvarsförmågan hos Försvarets radioanstalt. Mot bakgrund av att Försvarets radioanstalt, efter regeringens närmande bestämmande, får bedriva internationella samarbeten inom försvarsunderrättelse- och utvecklingsverksamheten framstår det som lämpligt att sådana samarbeten också får ske inom ramen för övningsverksamheten. Det bör därför i signalspaningslagen införas en bestämmelse som möjliggör internationellt samarbete, vilken bör få motsvarande innehåll som bestämmelserna som reglerar internationellt samarbete i försvarsunderrättelse- och utvecklingsverksamheten. Frågan om inriktning av sådan verksamhet berörs i avsnitt 7.4.

Överföring av personuppgifter till en mottagare utomlands behandlas i avsnitt 7.12 nedan.

7.9 Ändamål för personuppgiftsbehandling i övningsverksamhet

Utkastets förslag: Personuppgifter får behandlas i Försvarets radioanstalts övningsverksamhet om det är nödvändigt för att bedriva sådan övningsverksamhet som anges i lagen om signalspaning i försvarsunderrättelseverksamhet.

Personuppgifter som behandlas i Försvarets radioanstalts övningsverksamhet får myndigheten även behandla om det är nödvändigt för att tillhandahålla information som behövs

1. med anledning av samverkan med annan i fråga om övningsverksamhet, eller
2. med anledning av samarbete om övningsverksamhet med andra länder eller internationella organisationer enligt lagen om signalspaning i försvarsunderrättelseverksamhet.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: De flesta remissinstanser, däribland *Integritetsskyddsmyndigheten*, tillstyrker eller har inga synpunkter på förslaget.

Föreningen för Digitala Fri- och Rättigheter anser bl.a. att en personuppgiftsbehandling av det aktuella slaget inte är inte acceptabel, och att användningen av riktiga personuppgifter i övningssyfte skapar onödiga integritetsrisker som inte kan motiveras i relation till behovet. Föreningen påpekar även att behandlingen inte vore nödvändig om övningar i stället kan utföras med anonymiserade uppgifter eller syntetisk data.

Skälen för utkastets förslag

Nuvarande reglering

Upptagningar och uppteckningar som Försvarets radioanstalt inhämtar vid signalspaning innehåller inte sällan personuppgifter. Detsamma kan antas i fråga om den inhämtning vid signalspaning som sker inom ramen för övningsverksamheten. Den huvudsakliga regleringen av Försvarets radioanstalts personuppgiftsbehandling finns i lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt (FRA-PuL) och förordningen (2021:1208) om behandling av personuppgifter vid Försvarets radioanstalt.

Försvarets radioanstalt får behandla personuppgifter bara för särskilda, uttryckligt angivna och berättigade ändamål. Personuppgifter får inte behandlas för något ändamål som är oförenligt med det ändamål för vilket personuppgifterna ursprungligen behandlades (2 kap. 1 § FRA-PuL). Regeringen uttalade i förarbetena att med att ändamålen ska vara särskilda innebär att de måste vara tillräckligt specificerade för att ge ledning för bedömningen av vilka uppgifter som är adekvata och relevanta för den aktuella behandlingen och för att det ska kunna avgöras att inte fler uppgifter än nödvändigt behandlas. Något hinder mot att ange flera parallella ändamål för behandlingen finns inte. Regeringen anförde vidare att ändamålen ska anges uttryckligen redan när personuppgifterna samlas in. Att ändamålen ska vara berättigade innebär att det ska finnas en

koppling till myndighetens reglerade verksamhet som utgör den rättsliga grunden. Personuppgifter får således inte behandlas för ett ändamål som inte är berättigat i förhållande till verksamheten. Det ska finnas ett särskilt, uttryckligt angivet och berättigat ändamål för behandlingen inte bara vid insamlingen, utan även för varje åtgärd som vidtas med de insamlade uppgifterna (prop. 2020/21:224 s. 65–66). Försvarets radioanstalt får behandla personuppgifter i sin försvarsunderrättelse- och utvecklingsverksamhet samt informationssäkerhetsverksamhet (2 kap. 2, 3, 5 och 7 §§ FRA-PuL).

Det finns vidare möjlighet för Försvarets radioanstalt att i vissa särskilt angivna fall behandla uppgifter för ett annat ändamål än för det ändamål för vilket personuppgifterna har samlats in, så kallade sekundära ändamål (2 kap. 4, 6 och 8 §§ FRA-PuL). I förarbetena anges att en sådan ordning skapar en ökad tydlighet och innebär ett stärkt integritetsskydd. Försvarets radioanstalts verksamhetsansvar är av sådan tydligt avgränsad omfattning att ett införande av sekundära ändamål är lämpligt när det gäller behandling av personuppgifter i myndighetens försvarsunderrättelse- och utvecklingsverksamhet samt informationssäkerhetsverksamhet (prop. 2020/21:224 s. 66). Därutöver gäller den generella så kallade finalitetsprincipen (prop. 2020/21:224 s. 80, 82 och 84). Principen innebär att fortsatt behandling inte får ske för något ändamål som är oförenligt med det ändamål för vilket personuppgifterna ursprungligen behandlades och kommer till uttryck i 2 kap. 1 § andra stycket FRA-PuL (prop. 2020/21:224 s. 213).

Behandling av personuppgifter i övningsverksamheten

Det föreslås att Försvarets radioanstalt ska få bedriva signalspaning i övningsverksamhet. Som anförts i tidigare avsnitt är bedömningen även att det är mest ändamålsenligt att övningarna kan ske i den skarpa signalmiljön. Det bör därför införas en ändamålsbestämmelse som ger uttryck för att Försvarets radioanstalt får behandla personuppgifter om det är nödvändigt för att bedriva övningsverksamheten.

Behandling av personuppgifter för sekundära ändamål

Från integritetssynpunkt är det en fördel att så långt som möjligt precisera i vilka fall personuppgiftsbehandling får ske för annat ändamål än det ändamål enligt vilket uppgifterna har samlats in (prop. 2020/21:224 s. 81).

Signalspaning i övningsverksamhet syftar till att stärka och utveckla totalförsvarsförmågan. Försvarets radioanstalts verksamhet i denna del kommer att innebära att det finns behov av att samverka med nationella och internationella myndigheter och internationella organisationer. Personuppgifter som behandlas i Försvarets radioanstalts övnings-verksamhet bör därför även få behandlas om det är nödvändigt för att tillhandahålla information som behövs i samverkan med annan avseende övningsverksamhet eller med anledning av samarbete om övnings-verksamhet med andra länder och internationella organisationer enligt signalspaningslagen.

7.10 Behandling av allmänt tillgänglig information

Utkastets förslag: Försvarets radioanstalt får behandla personuppgifter som utgör allmänt tillgänglig information om det är nödvändigt för de ändamål som anges för övningsverksamheten.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för utkastets förslag: Av 2 kap. 9 § FRA-PuL framgår att Försvarets radioanstalt får behandla personuppgifter som utgör allmänt tillgänglig information om det är nödvändigt för den verksamhet som anges i 2 kap. 2, 5 och 7 §§ FRA-PuL.

I förarbetena uttalades att Försvarets radioanstalt för att bedriva en effektiv försvarsunderrättelseverksamhet har behov av god tillgång till allmänt tillgänglig information. Den information som inhämtats genom särskilda metoder kan därigenom på ett bättre sätt sättas i sitt sammanhang. Det är framför allt fråga om personuppgifter som kan påträffas vid sökning på internet eller vid sökningar i öppna databaser. Databaser med publikt tillgänglig information anskaffas och läggs upp som referensdatabaser hos myndigheten där den kan göra sökningar. I försvarsunderrättelseverksamheten kan ett syfte med att behandla personuppgifter i referensdatabaser vara att identifiera vem som använder en adressuppgift av intresse. Försvarets radioanstalt har vidare behov av att behandla personuppgifter i sådana databaser för att kunna filtrera bort signaler i sådana fall där både sändare och mottagare befinner sig i Sverige, till exempel genom att bedöma vilka IP-adresser som avser datorer i Sverige. Det kan även inom utvecklingsverksamheten vara nödvändigt att behandla personuppgifter som utgör allmänt tillgänglig information, bland annat vid kartläggning av signalmiljön (prop. 2020/21:224 s. 84–85).

Bedömningen är att det också i övningsverksamheten kan uppstå behov av att behandla personuppgifter som utgör allmän information, exempelvis i syfte att filtrera bort signaler. I enlighet med vad som anfördes i förarbetena kan behandlingen av allmänt tillgänglig information bidra till att minska omfattningen av sådan inhämtning som inte är tillåten enligt signalspaningslagen (prop. 2020/21:224 s. 85). Det föreslås därför att Försvarets radioanstalt ska få behandla personuppgifter som utgör allmänt tillgänglig information om det är nödvändigt för de ändamål som anges för övningsverksamheten. Signalspaning i övningsverksamhet föreslås alltså omfattas av 2 kap. 9 § FRA-PuL.

7.11 Behandling av personuppgifter i vissa fall

Utkastets förslag: Bestämmelsen i lagen om personuppgiftsbehandling vid Försvarets radioanstalt om behandling av personuppgifter i vissa fall ska också omfatta Försvarets radioanstalts signalspaning i övningsverksamhet.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för utkastets förslag: Försvarets radioanstalts inhämtning av signaler i tråd ska ske automatiserat och sökbegrepp ska användas för att identifiera signalerna. Även vid annan inhämtning ska sökbegrepp användas (3 § signalspaningslagen). Personuppgifter behandlas redan när informationen i tillståndsgivna signalbärare genomgår urval med hjälp av sökbegrepp. Personuppgiftsbehandling sker således även för information som inte inhämtas, och många av de personuppgifter som behandlas automatiskt blir dessutom aldrig föremål för manuell granskning (prop. 2020/21:224 s. 95). Information som Försvarets radioanstalt hanterar i försvarsunderrättelseverksamheten och informationssäkerhetsverksamheten kan därutöver vara krypterad eller på ett främmande språk. Innan informationen bearbetats saknas det förutsättningar att bedöma om den innehåller personuppgifter (prop. 2020/21:224 s. 222).

Av 2 kap. 18 § FRA-PuL följer att Försvarets radioanstalts hantering av information som innebär behandling av personuppgifter inte ska anses oförenlig med bestämmelserna om tillåtlighet, grundläggande krav, känsliga personuppgifter, personnummer och samordningsnummer, i det skede av behandlingen då det ännu inte har kunnat fastställas vilka personuppgifter som informationen innehåller. När det står klart att informationen innehåller personuppgifter, samt vilka personuppgifterna är, ska Försvarets radioanstalt behandla dem enligt övriga bestämmelser (prop. 2020/21:224 s. 222).

Inhämtning av signaler i elektronisk form vid signalspaning i övningsverksamhet ska ske på samma sätt som annan inhämtning. Det kan förekomma att den information som Försvarets radioanstalt hanterar i övningsverksamheten är sådan att den måste bearbetas innan det går att bedöma om den innehåller personuppgifter. Det föreslås därför att 2 kap. 18 § FRA-PuL också ska omfatta Försvarets radioanstalts övningsverksamhet.

7.12 Överföring av personuppgifter till en mottagare utomlands

Utkastets förslag: Bestämmelser om överföring av personuppgifter till en mottagare utomlands ska tillämpas vid sådan överföring som sker inom ramen för internationellt övningssamarbete.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: De flesta remissinstanser, däribland *Integritetsskyddsmyndigheten*, tillstyrker eller har inga invändningar mot förslaget.

Institutet för mänskliga rättigheter hänvisar till vad institutet i sitt remissvar till utredningens delbetänkande anfört beträffande den personliga integriteten och överföring av personuppgifter till annat land eller en internationell organisation. Institutet anser att samma brister som då gjordes gällande är aktuella beträffande överföring av personuppgifter till ett annat land eller en internationell organisation inom ramen för övningsverksamhet.

Skälen för utkastets förslag: I avsnitt 7.8 föreslås att Försvarets radioanstalt vid signalspaning som sker inom ramen för övningsverksamhet ska få bedriva internationellt samarbete. Vid sådant internationellt samarbete kan personuppgifter komma att överföras till ett annat land eller en internationell organisation. I fråga om Försvarets radioanstalts internationella försvarsunderrättelse- och säkerhetssamarbete regleras förutsättningarna för sådan överföring i 2 kap. 20 § FRA-PuL och 2 kap. 1 § FRA-PuF.

Enligt 2 kap. 20 § första stycket FRA-PuL får personuppgifter överföras till ett annat land eller en internationell organisation endast om det är nödvändigt för att Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet. Därutöver krävs enligt 2 kap. 20 § första stycket 1 FRA-PuL att överföringen riktas till en utländsk underrättelse- eller säkerhetstjänst, eller ett underrättelse- eller säkerhetsorgan i en internationell organisation. EU, FN och Nato har exempelvis denna typ av organ. Regeringen kan, enligt vad som framgår av 2 kap. 20 § andra och tredje styckena FRA-PuL, genom föreskrift eller beslut i enskilda fall möjliggöra för att överföring av personuppgifter även kan ske till andra internationella aktörer. Det kan till exempel vid internationella militära insatser vara nödvändigt att överlämna underrättelser till en funktion i en annan stat som inte kan sägas vara en underrättelse- eller säkerhetstjänst.

Enligt 2 kap. 20 § första stycket 2 FRA-PuL ska sekretess inte hindra en överföring. En sekretessprövning behöver således ske som en del i bedömningen om en överföring av personuppgifter ska ske.

Enligt den tredje punkten ska mottagaren garantera tillräckligt skydd för personuppgifterna. Enligt förarbetena är det Försvarets radioanstalt som, genom en sammanvägd bedömning, har till uppgift att bedöma om det mottagande landet eller organisationen erbjuder tillräckligt skydd. Personuppgifter bör få överföras om Försvarets radioanstalt tagit hänsyn till omständigheterna kring överföringen och dragit slutsatsen att tillräckliga skyddsåtgärder för personuppgifterna föreligger. Som utgångspunkt bör lämpliga skyddsåtgärder anses föreligga om en mottagande stat är ansluten till dataskyddskonventionen eller annan internationell överenskommelse som innehåller bestämmelser om dataskydd och registrerades rättigheter. Därutöver bör Försvarets radioanstalt kunna beakta till exempel att den som kommer att behandla uppgifterna kommer att ha tystnadsplikt som omfattar de överförda uppgifterna och åtaganden från mottagarens sida att inte föra personuppgifterna vidare eller att inte använda personuppgifterna efter en viss tidpunkt (prop. 2020/21:224 s. 119).

Enligt 2 kap. 20 § första stycket 4 FRA-PuL ska slutligen den personliga integriteten beaktas vid överföring av personuppgifter till en mottagare utomlands.

De krav som gör sig gällande vid överföring av personuppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet gör sig också gällande vid sådan överföring som kan komma att ske inom ramen för internationellt samarbete inom ramen för övningsverksamheten. För att tillgodose att samma villkor tillämpas också vid sådan överföring bör 2 kap. 20 § FRA-PuL ändras på sådant sätt så att internationellt övningssamarbete också omfattas av bestämmelsen.

Förslaget innebär att samma villkor som ska vara uppfyllda vid överföring av personuppgifter till en mottagare utomlands i försvarsunderrättelse- och säkerhetssamarbetet även ska vara uppfyllda vid sådan överföring som sker inom ramen för internationellt samarbete i övningsverksamheten. Det innebär bland annat Försvarets radioanstalt ska göra en bedömning av om mottagaren garanterar tillräckligt skydd för uppgifterna och en proportionalitetsbedömning innan personuppgifterna får överföras. I bedömningarna får omständigheterna i det enskilda fallet beaktas. Sett i ljuset av förslaget i fråga om förstöringsskyldighet (se avsnitt 7.6) bör åtaganden från mottagaren om dennes hantering av personuppgifterna få betydelse i Försvarets radioanstalts bedömning av om mottagaren garanterar tillräckligt skydd för uppgifterna. Det kan till exempel vara fråga om åtaganden om att förstöra eller inte använda personuppgifterna efter en viss tidpunkt Det ska här även framhållas att underrättelsesamarbete bygger på ett ömsesidigt förtroende. En motpart som missbrukar förtroendet kommer inte längre att få ta del av information.

De önskemål om förtydliganden samt synpunkter som *Institutet för mänskliga rättigheter* framför i denna del har närmast bäring på redan gällande lagstiftning och är inte föremål för detta lagstiftningsärende. Det kan även påpekas att regeringen tidigare har bedömt att lagstiftningen i FRA-PuL tillgodoser den brist som Europadomstolen identifierat i detta sammanhang (prop. 2020/21:224 s. 119 och prop. 2023/24:136 s. 33).

8 Inhämtning av inhemsk trafik i vissa brådskande situationer och en anpassad ändamålsbestämmelse

8.1 Förbudet mot att inhämta inhemsk trafik

Av 2 a § första stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (signalspaningslagen) framgår att signaler som sänds mellan en avsändare och en mottagare som båda befinner sig i Sverige inte får inhämtas. Om sådana signaler inte kan avskiljas redan vid inhämtningen, ska upptagningen eller uppteckningen förstöras så snart det står klart att sådana signaler har inhämtats. Kravet på förstöring gäller även i fråga om upptagningar och uppteckningar som signalspaningsmyndigheten har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete. Av paragrafens andra stycke framgår att första stycket inte tillämpas i fråga om dels signaler som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte innehåller personuppgifter, dels signaler som sänds från eller till utländsk militär personal, utländska statsfartyg, statsluftfartyg eller militära fordon.

Bestämmelsen har sin bakgrund i den politiska överenskommelsen som träffades mellan de i regeringen ingående partierna hösten 2008. Enligt en av punkterna i överenskommelsen skulle det i lagen tydliggöras att

Försvarets radioanstalt inte får signalspana mot trafik med både avsändare och mottagare i Sverige.

I det förslag till bestämmelse som lämnades i promemorian Förslag till ändring av signalspaningslagen (Ds 2009:1) fanns inte några undantag från förbudet mot att inhämta inhemsk trafik. Flera remissinstanser var kritiska till det absoluta förbudet, bland annat ifrågasatte Justitiekanslern om förbudet inte innebar att man någon gång tappar bort högst väsentliga försvarsunderrättelser och om inte en ventil för synnerligen angelägna fall borde övervägas (prop. 2008/09:201 s. 40). Regeringen föreslog i propositionen ett undantag i fråga om signaler mellan sändare och mottagare på utländska statsfartyg, statsluftfartyg eller militära fordon. Riksdagen beslutade därefter i enlighet med regeringens förslag (bet. 2009/10:FöU3, rskr. 2009/10:3).

Efter senare lagändringar, som trädde i kraft den 1 januari 2022, omfattar inte förbudet signaler som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte innehåller personuppgifter och inte heller signaler som sänds från eller till utländsk militär personal (prop. 2020/21:224, bet. 2021/22:FöU2, rskr. 2021/22:45).

8.2 Finns det behov av ytterligare undantag från förbudet mot att inhämta inhemsk trafik?

Förbudet och förstöringsskyldigheten i 2 a § första stycket signalspaningslagen gäller som huvudregel oavsett för vilken företeelse inhämtningen sker och oavsett vilka uppgifter som en inhämtad upptagning eller uppteckning innehåller. Det innebär att om signalspaning bedrivs mot avsändare och mottagare som befinner sig utanför Sverige måste inhämtningen avbrytas och inhämtade uppgifter förstöras om både avsändaren och mottagaren skulle förflytta sig in i Sverige. Denna ordning riskerar att få allvarliga konsekvenser i vissa brådskande situationer när ett utländskt förhållande sträcker sig in i Sverige och hotar liv, hälsa eller egendom. Utredningen exemplifierar detta enligt följande.

- Vid signalspaning upptäcker Försvarets radioanstalt att internationella terrorister, som befinner sig utanför Sverige, inom kort planerar ett terrorattentat i Sverige. Under tiden som inhämtningsuppdraget pågår förflyttar sig terroristerna över Öresundsbron och in i Sverige. Enligt den nuvarande lagstiftningen ska inhämtningen av signaler dem emellan avbrytas och de uppgifter som eventuellt inhämtats när avsändare och mottagare befinner sig i Sverige förstöras. Regelverket gäller således oavsett vilka uppgifter som framkommer och oavsett hur allvarlig eller brådskande situationen är, dvs. även om enskilda människors liv eller hälsa är i fara.
- Försvarets radioanstalt finner vid analys av en inhämtad upptagning eller uppteckning konkret information om att ett terrorattentat ska ske inom kort. Det visar sig dock vid en vidare analys att avsändare och mottagare befann sig i Sverige när upptagningen eller uppteckningen inhämtades. Försvarets radioanstalt ska då förstöra upptagningen eller uppteckningen, och får inte rapportera uppgifterna vidare. Förstöringsskyldigheten gäller alltså även om Försvarets radioanstalt

skulle ha uppgifter som skulle kunna vara av avgörande betydelse för att skydda människors liv eller hälsa.

- Efter en oförutsedd inträffad händelse i Sverige råder en akut situation där nationella resurser måste konsolideras för att säkerställa att det inte finns några kvarvarande hot från exempelvis internationella terrorister. Om en avsändare eller en mottagare befinner sig utanför Sverige kan Försvarets radioanstalt inhämta signaler som kan ge information om kvarvarande oupptäckta yttre hot och som kan skydda människors liv eller hälsa. Om en avsändare och en mottagare båda befinner sig i Sverige saknar dock Försvarets radioanstalt, enligt nuvarande lagstiftning, möjlighet att bidra med sådan information.

I den typ av situationer som exemplifierats ovan innebär förbudet, som Justitiekanslern framhöll inom ramen för det tidigare lagstiftningsärendet, att det finns en risk för att uppgifter som kan ha ett mycket betydande underrättelsevärde inte kan inhämtas eller att de måste förstöras. Det finns som en följd av detta en uppenbar risk för enskilda människors liv eller hälsa eller för omfattande förstörelse av egendom. Försvarets radioanstalts myndighetschef riskerar dessutom att ställas inför mycket svåra moraliska och etiska dilemman. Ställt på sin spets handlar det i en sådan situation om att antingen följa signalspaningslagstiftningen och då riskera människors liv eller att agera i strid med lagen. En annan aspekt som det inte går att bortse från är hur allmänhetens förtroende för statens förmåga att skydda befolkningen skulle påverkas om det skulle bli känt att till exempel ett terroristattentat hade kunnat förhindras och människoliv räddas om signalspaningen hade fått fortsätta eller om rapportering hade fått ske av uppgifter som faktiskt fanns tillgängliga för Försvarets radioanstalt.

8.3 Inhämtning av inhemsk trafik i vissa brådskande situationer som innebär fara för människors liv eller hälsa eller för omfattande förstörelse av egendom

Utkastets förslag: Förbudet mot inhämtning av inhemsk trafik i lagen om signalspaning i försvarsunderrättelseverksamhet ska inte tillämpas i fråga om signaler i sådana brådskande situationer som innebär fara för människors liv eller hälsa eller för omfattande förstörelse av egendom.

En tillämpning av undantaget ska kräva ett särskilt tillstånd.

Ett sådant särskilt tillstånd ska kunna ges kortare varaktighet än det tillstånd för det inhämtningsuppdrag som det särskilda tillståndet hänför sig till.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: De flesta remissinstanser tillstyrker eller har inga synpunkter på utredningens förslag, däribland *Försvarets radioanstalt*, *Fortifikationsverket, Integritetsskyddsmyndigheten* och *Åklagarmyndigheten*.

Journalistförbundet avstyrker förslaget.

Försvarsunderrättelsedomstolen lyfter ett antal frågeställningar beträffande utredningens förslag, bl.a. i fråga om efterhandskontroll. *Statens inspektion för försvarsunderrättelseverksamheten* efterfrågar ett klargörande om inspektionens efterhandskontroll även omfattar lagligheten av tillstånd som meddelats av befattningshavare vid Försvarets radioanstalt.

Polismyndigheten, Försvarsunderrättelsedomstolen och Försvarets radioanstalt väcker frågan om uttrycket strategiska förhållanden i ändamålsbestämmelsen i signalspaningslagen behöver ses över för att regelverket ska fungera mer ändamålsenligt.

Skälen för utkastets förslag

Inhämtning av inhemsk trafik bör kunna ske i vissa brådskande situationer som hotar liv, hälsa eller egendom

Som beskrivits i avsnitt 3.2.1 får försvarsunderrättelseverksamhet enligt 1 § lagen (2000:130) om försvarsunderrättelseverksamhet endast avse utländska förhållanden. Det gäller också den signalspaning som bedrivs för försvarsunderrättelseändamål. Huvudregeln enligt 2 a § första stycket signalspaningslagen är vidare att inhämtning inte får avse signaler mellan en avsändare och mottagare som båda befinner sig i Sverige. Redan när bestämmelsen infördes var den försedd med vissa undantag, nämligen för signaler mellan sändare och mottagare på utländska statsfartyg, statsluftfartyg eller militära fordon. Dessa undantag från inhämtningsförbudet tillkom för att skapa förutsättningar för att Försvarets radioanstalt ska kunna bedriva en effektiv och ändamålsenlig försvarsunderrättelseverksamhet (jfr prop. 2008/09:201 s. 42). Undantagen utökades därefter år 2022 till att bl.a. även avse signaler som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte innehåller personuppgifter. Det finns starka skäl för att införa ytterligare ett undantag, nämligen för sådana brådskande situationer som innebär fara för människors liv eller hälsa eller för omfattande förstörelse av egendom. I avsnitt 8.2 beskrivs några exempel på sådana situationer. Det rör sig om situationer där bestämmelser om nödvärn och nöd aktualiseras (se 24 kap. brottsbalken). Sådana situationer kan uppstå i två olika typfall. I det ena fallet kommer informationen om en sådan situation från en av Försvarets radioanstalts inriktande myndigheter. I dagsläget får inte den myndighet som har informationen inrikta signalspaning i syfte att erhålla information för att kunna avvärja situationen, om både avsändare och mottagare finns i Sverige. I det andra fallet är det Försvarets radioanstalt som identifierar situationen genom information som finns i redan inhämtat material. I dagsläget får den informationen inte föras vidare till brottsbekämpande myndigheter utan måste förstöras, och kan således inte användas för att avvärja situationen.

I likhet med utredningens slutsats är bedömningen att det är en brist i den nuvarande regleringen att det saknas möjlighet till undantag från förbudet mot inhämtning av inhemsk trafik i brådskande situationer som innebär fara för människors liv eller hälsa eller för omfattande förstörelse av egendom uppstår. Det finns i sådana situationer en uppenbar risk för att uppgifter som kan vara av avgörande betydelse för att kunna förhindra

allvarlig brottslighet och att skydda enskilda människors liv eller hälsa och egendom mot omfattande förstörelse går förlorade.

Det torde vara ovanligt att den typ av brådskande situationer som innebär fara för människors liv eller hälsa eller för omfattande förstörelse av egendom uppstår. Detta innebär dock inte att det inte finns ett behov av att möjliggöra att inhämtning kan ske om sådana situationer skulle inträffa. Sett i ljuset av de allvarliga konsekvenser ett inhämtningsförbud kan få i dessa fall bör även inhemsk trafik kunna inhämtas i sådana situationer.

I likhet med utredningens uppfattning kan det inte heller anses acceptabelt att en enskild beslutsfattare ska behöva ställas inför den typ av etiska och moraliska dilemman som beskrivits ovan. Vidare bör den konstitutionella nödrätten som utgångspunkt inte användas för ett undantag från 2 a § signalspaningslagen. Denna nödrätt kan beskrivas som grundsatsen att statsmakterna, när samhällets bestånd hotas, kan åsidosätta grundlag och ändå göra anspråk på att handla rättsenligt (SOU 2023:75 s. 81). Statsmakterna har i princip tagit avstånd från denna nödrätt (prop. 1973:90 s. 444). Ett visst begränsat utrymme för en sedvanerättsligt grundad konstitutionell nödrätt anses visserligen finnas, något som har kommit till tydligast uttryck i samband med terroristaktioner. Det är dock oklart hur långt den konstitutionella nödrätt som anses finnas sträcker sig (SOU 2023:75 s. 83 och prop. 2005/06:111 s. 41). Regeringen har i förarbetena till lagen (2006:343) om Försvarsmaktens stöd till polisen vid terrorismbekämpning ansett att en reglering av möjligheterna att i vissa fall sätta in militära förband med våldsbefogenheter för att ingripa mot terroristhandlingar inte bör ta sin utgångspunkt i vad som kan anses gälla enligt den konstitutionella nödrätten (prop. 2005/06:111 s. 40). I likhet med utredningen kan det inte anses lämpligt eller ändamålsenligt att en beslutsfattare ska förlita sig på nödrätten i brottsbalken i sådana situationer. Det bör därför finnas en ventil från förbudet mot att inhämta inhemsk trafik som kan tillämpas i vissa brådskande situationer som hotar liv, hälsa eller egendom. Det sker lämpligast genom att ett särskilt undantag införs i signalspaningslagen.

Ett nytt undantag för inhämtning av inhemsk trafik i vissa brådskande situationer som hotar liv, hälsa eller egendom

Som framkommit i det föregående måste Försvarets radioanstalt upphöra med signalspaningen och inhämtade uppgifter måste förstöras om det framkommer att såväl avsändare som mottagare befinner sig i Sverige. Detsamma gäller om de förflyttar sig så att de båda befinner sig i Sverige. Som också angetts ovan är bedömningen att detta riskerar få allvarliga konsekvenser eftersom det hindrar inhemsk signalspaning även i sådana brådskande situationer som innebär fara för människors liv eller hälsa eller för omfattande förstörelse av egendom.

Förbudet mot att inhämta inhemsk trafik har bl.a. införts för att tydliggöra gränsdragningen mellan försvarsunderrättelseverksamheten och den brottsutredande och brottsbekämpande verksamheten (jfr prop. 2008/09:201 s. 42). I linje med detta är de brottsbekämpande myndigheterna förbjudna att använda de uppgifter som Försvarets radioanstalt rapporterar för att utreda brott (se lagen [2019:547] om förbud mot användning av vissa uppgifter för att utreda brott). Något hinder mot

att använda uppgifterna för att förebygga, förhindra och upptäcka brott finns däremot inte (prop. 2018/19:96 s. 28). Ett syfte med 2 a § första stycket signalspaningslagen är vidare att tydliggöra att försvarsunderrättelseverksamheten är inriktad mot utländska förhållanden. Begränsningen till utländska förhållanden i 1 § lagen (2000:130) om försvarsunderrättelseverksamhet hindrar dock inte att försvarsunderrättelseverksamheten kan avse även vissa företeelser inom landet. Det är inte avgörande var den relevanta verksamheten bedrivs. I tidigare förarbeten har som exempel på när utländska förhållanden måste anses sträcka sig innanför landets gränser angetts att en organisation med verksamhet som utgör ett hot mot landet har sitt ursprung i ett annat land men verkar genom representanter i Sverige eller genom att på annat sätt utnyttja resurser i Sverige. Det handlar då om att följa upp utländska förhållandens koppling till Sverige för att kunna bedöma hotbilden mot landet. Enligt vad regeringen då framhöll är mandatet för de myndigheter som bedriver försvarsunderrättelseverksamhet begränsat till just underrättelseverksamhet och alla åtgärder som syftar till att hantera de hot av kriminell karaktär som kan identifieras inom landet är förbehållna de brottsbekämpande myndigheterna (prop. 2006/07:63 s. 43). Som framkommit ovan finns det inget som hindrar att de brottsbekämpande myndigheterna använder sig av uppgifter som de fått från signalspaning, med undantag för att sådana uppgifter inte får användas i förundersökningsverksamheten. Tvärt om är syftet med att Nationella operativa avdelningen i Polismyndigheten och Säkerhetspolisen får inrikta signalspaning och att inhämtning får ske avseende internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen att bidra till förutsättningarna för brottsbekämpande myndigheter att kunna lösa sina uppgifter och avvärja allvarliga hot mot Sverige.

Med utgångspunkt i detta och med hänsyn till i vilka typer av situationer som behovet av inhämtning kan uppstå i är bedömningen, i enlighet med flertalet remissinstanser, däribland *Försvarets radioanstalt* och *Integritetsskyddsmyndigheten*, men till skillnad från *Journalistförbundet*, att utredningens förslag bör genomföras. Därför föreslås att inhemsk trafik ska få inhämtas i sådana brådskande situationer som innebär fara för människors liv eller hälsa. Fara för omfattande förstörelse av egendom bör också omfattas. Omfattande förstörelse av egendom kan, även om det inte direkt innebär att människor dör eller skadas, i förlängningen komma att få stora konsekvenser för samhället och för enskilda människors liv eller hälsa. Så kan vara fallet när hotet riktas mot fastigheter innehållande samhällsviktiga funktioner, men också bostadsfastigheter. Ytterligare exempel är sådan egendom som kan anses utgöra kritisk infrastruktur, till exempel broförbindelser eller ledningar för vattenförsörjning. Om fara för omfattande förstörelse av egendom inte skulle omfattas är bedömningen att undantagets tillämpningsområde riskerar att bli för alltför begränsat. Det kan inte heller bortses från att det finns en risk för att liknande svåra moraliska och etiska dilemman som tidigare beskrivits kan uppstå om endast fara för människors liv eller hälsa omfattas.

Bedömningen av om det rör sig om en sådan brådskande situation som innebär fara för människors liv eller hälsa eller för omfattande förstörelse av egendom får göras utifrån de uppgifter som Försvarets radioanstalt har

tillgång till i varje enskilt fall. Det innebär att Försvarets radioanstalt i stor utsträckning kommer att vara beroende av de uppgifter som lämnas av den inriktande myndigheten i det enskilda fallet. Rapportering av underrättelser enligt det nya undantaget bör ske enligt de gällande bestämmelserna i 8 § signalspaningslagen (se avsnitt 3.3.5) och får anpassas efter den situation som råder i det enskilda fallet.

I sammanhanget ska framhållas att polisiära myndigheter har tillgång till flera verkningsfulla verktyg för att genomföra sitt uppdrag. Ett sådant exempel är hemliga tvångsmedel som kan användas i olika skeden av det brottsbekämpande arbetet, både för att förebygga, förhindra eller upptäcka allvarlig brottslig verksamhet i underrättelseverksamhet (så kallade preventiva tvångsmedel) och för att utreda brott i en förundersökning. Till dessa hemliga tvångsmedel hör bl.a. hemlig avlyssning och övervakning av elektronisk kommunikation och hemlig kameraövervakning, vilka regleras i 27 kap. rättegångsbalken, men även hemlig dataavläsning enligt lagen (2020:62) om hemlig dataavläsning. Vidare bedrivs underrättelseverksamhet av bland annat Polismyndigheten och Säkerhetspolisen som innebär insamling, bearbetning och analys av information som senare kan ha betydelse för att förhindra eller för att utreda brott. Även i sådan verksamhet finns det vissa möjligheter att använda tvångsmedel vilket regleras i flera lagar, bland annat i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen), lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) och lagen om hemlig dataavläsning.

Användandet av dessa tvångsmedel omgärdas av ett omfattande regelverk, och signalspaning bör inte kunna användas för att kringgå detta regelverk. Det aktuella förslaget bedöms inte medföra någon sådan risk. För det första får signalspaning endast bedrivas inom ramen för försvarsunderrättelseverksamhet i enlighet med vad som föreskrivs i lagen om försvarsunderrättelseverksamhet. Till detta kommer att undantaget från förbudet mot inhämtning av inhemsk trafik är mycket begränsat i och med att det endast avser brådskande situationer som därtill innebär fara för människors liv eller hälsa eller för omfattande förstörelse av egendom. Som tidigare framhållits får vidare uppgifter från signalspaning inte användas i förundersökning. Det ska även understrykas att även all användning av signalspaning omgärdas av ett omfattande regelverk.

Polismyndigheten, Försvarsunderrättelsedomstolen och Försvarets radioanstalt har med anledning av utredningens förslag framfört synpunkter på begränsningen i ändamålsbestämmelsen i signalspaningslagen till kartläggning av strategiska förhållanden när det gäller internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen. Den frågan behandlas i avsnitt 8.5.

En särskild tillståndsprövning bör gälla för inhämtning av inhemsk trafik i vissa brådskande situationer

Vid all inhämtning av signaler i elektronisk form krävs tillstånd från Försvarsunderrättelsedomstolen eller i brådskande fall från myndighets-

chefen vid Försvarets radioanstalt eller dennes ställföreträdare (4 a–5 b §§ signalspaningslagen och 2 § förordningen [2008:923] om signalspaning i försvarsunderrättelseverksamhet). Sett till den typ av situationer som förslaget ska kunna tillämpas för bör det krävas en särskild tillståndsprövning för att tillämpa det föreslagna undantaget.

Behovet av att inhämta signaler mellan en avsändare och en mottagare som båda befinner sig i Sverige kommer torde vanligen uppstå i ett pågående redan tillståndsprövat inhämtningsuppdrag, vilket kan illustreras genom de tre exempel som redogjorts för i avsnitt 8.2. Det framstår inte som lämpligt eller ändamålsenligt att i de situationer där tillstånd finns behöva göra en ny ansökan eftersom det innebär att det kan löpa parallella tillstånd rörande samma inhämtningsuppdrag. Utgångspunkten bör i stället vara att ett särskilt tillstånd ska sökas om behov av att tillämpa det föreslagna undantaget uppstår. Det föreslås därför att en bestämmelse med sådan innebörd införs. En liknande möjlighet finns vid behov av ytterligare signalbärare och tillkommande sökbegrepp enligt 5 a § tredje stycket signalspaningslagen. Det framstår som lämpligt att reglera möjligheten till särskilt tillstånd beträffande det föreslagna undantaget i samma bestämmelse.

Som Försvarsunderrättelsedomstolen för fram anger 5 § signalspaningslagen att tillstånd till signalspaning endast får lämnas om syftet med inhämtningen inte kan tillgodoses på ett mindre ingripande sätt. Enligt förarbetena till den bestämmelsen anges bl.a. att när underrättelsebehovet är framställt av en annan svensk underrättelsemyndighet bör utgångspunkten vara att den myndigheten har uttömt praktiska möjligheter att på annat sätt få informationen (prop. 2008/09:201 s. 111). Enligt 5 a § tredje stycket gäller bestämmelsen i 5 § i tillämpliga delar vid ansökan och prövning. Huruvida ett underrättelsebehov i en sådan brådskande situation som förslaget aktualiserar skulle kunna tillgodoses genom olika former av straffprocessuella tvångsmedel, i stället för genom signalspaning, är en fråga som får bedömas från fall till fall. Någon bestämmelse som särskilt reglerar detta förhållande är inte behövlig. Som angetts ovan bör dock utgångspunkten vara att möjligheten att inhämta uppgifter med stöd av regelverket om försvarsunderrättelseverksamhet inte får användas för att kringgå regelverket om straffprocessuella tvångsmedel.

Om behov skulle uppstå av att tillämpa undantaget utan att det finns ett tillståndsprövat inhämtningsuppdrag, får ansökan göras i enlighet med 4 a § signalspaningslagen.

Ett tillstånd till signalspaning får ges för högst sex månader åt gången och kan efter förnyad prövning förlängas med högst sex månader i taget (5 a § andra stycket signalspaningslagen). Att det är fråga om en brådskande situation som hotar liv, hälsa eller egendom bör få genomslag i fråga om tillståndens längd. Det bör endast vara aktuellt med tillstånd som gäller för en mycket begränsad tidsperiod, någon eller allra högst några dagar. Det innebär att om den brådskande situationen fortgår måste en ny ansökan således göras och skälen för inhämtningen övervägas, om inhämtning med stöd av det föreslagna undantaget fortsatt ska kunna ske. Tillstånd efter en särskild ansökan i ett redan tillståndsprövat uppdrag bör således ges kortare varaktighet än ursprungstillståndet. Det kan även i fråga om behov av ytterligare signalbärare och tillkommande sökbegrepp

finnas behov av en möjlighet att ge tillstånd med kortare varaktighet än ursprungstillståndet. Det föreslås därför att signalspaningslagen ändras för att möjliggöra detta.

Tillstånd till inhämtning vid signalspaning ska enligt huvudregeln meddelas av Försvarsunderrättelsedomstolen. Med hänsyn till de nu aktuella ärendenas brådskande natur kommer det dock ofta vara fråga om tillstånd som meddelas av Försvarets radioanstalts myndighetschef eller dennes ställföreträdare enligt 5 b § signalspaningslagen och 2 § förordningen om signalspaning i försvarsunderrättelseverksamhet. Sådana beslut ska genast anmälas till Försvarsunderrättelsedomstolen, som skyndsamt ska pröva ärendet. Domstolen kan, om den finner att det inte finns skäl för åtgärden, upphäva eller ändra beslutet. Om ett brådskande beslut har upphört att gälla innan domstolen har prövat ärendet, ska Försvarets radioanstalt anmäla åtgärden till Statens inspektion för försvarsunderrättelseverksamheten (Siun). Givet bedömningen att tillstånden i fråga kommer avse en mycket begränsad tidsperiod, någon eller allra högst några dagar, kommer domstolen typiskt sett inte ha möjlighet att pröva ärendet. Siun kommer dock i efterhand granska Försvarets radioanstalts hantering.

För en effektiv efterhandskontroll är det av vikt att Försvarets radioanstalt underrättar Siun vid tillämpning av den föreslagna bestämmelsen om inhämtning av inhemsk trafik i vissa brådskande situationer. Ett sådant förfarande kan lämpligen regleras i förordning.

När det gäller beslut som har fattats av Försvarets radioanstalts myndighetschef eller dennes ställföreträdare, och som upphört att gälla innan domstolen har haft möjlighet att pröva ärendet, lyfter Försvarsunderrättelsedomstolen och *Siun* frågan om inspektionens kontroll även omfattar tillståndets lagenlighet och proportionalitet. I förarbetena till 5 b § signalspaningslagen framgår att en anmälan till Siun enligt bestämmelsens andra stycke bör generera någon form av närmare kontroll av åtgärdens lagenlighet (prop. 2008/09:201 s. 64). Någon ändring av gällande ordning i detta avseende är inte avsedd.

8.4 Undantag från förstöringsskyldigheten

Utkastets förslag: Om signaler mellan en avsändare och en mottagare som båda befinner sig i Sverige inte kan avskiljas redan vid inhämtningen, behöver upptagningen eller uppteckningen inte förstöras om den innehåller

1. uppgifter om en brådskande situation, och
2. uppgifterna bedöms vara av avgörande betydelse för att skydda människors liv eller hälsa eller för att undvika omfattande förstörelse av egendom.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: *Försvarsunderrättelsedomstolen* har inte några invändningar mot förslaget. Övriga remissinstanser yttrar sig inte särskilt i denna del.

Skälen för utkastets förslag

Ett undantag från förstöringsskyldigheten bör införas för vissa upptagningar och uppteckningar

Försvarets radioanstalt vidtar olika åtgärder för att tillgodose att inhemsk trafik inte inhämtas. I vissa fall är det trots detta inte möjligt att bedöma vilka signaler som kan innefatta trafik mellan en avsändare och en mottagare som båda befinner sig i Sverige. Om sådana signaler inte kan avskiljas redan vid inhämtningen ska därför upptagningen eller uppteckningen, enligt 2 a § första stycket signalspaningslagen, förstöras så snart det står klart att signaler som omfattas av förbudet har inhämtats.

Som tidigare har beskrivits är förstöringsskyldigheten i 2 a § första stycket signalspaningslagen absolut när det inte rör sig om sådana uppgifter som anges i 2 a § andra stycket. Det innebär att en upptagning eller uppteckning ska förstöras oavsett vilka uppgifter som framkommer i det inhämtade materialet. Det innebär i sin tur exempelvis att Försvarets radioanstalt, trots att det rör sig om uppgifter om ett utländskt förhållande, inte till berörda myndigheter får rapportera konkreta uppgifter om ett nära förestående terroristbrott i Sverige eller mot svenskar utomlands om avsändaren och mottagaren båda befann sig i Sverige när signalerna inhämtades. Det finns alltså ingen möjlighet i en sådan situation för brottsbekämpande myndigheter att få kännedom om uppgifter som kan vara av avgörande betydelse i fråga om Sveriges förmåga att förhindra allvarlig brottslighet och att skydda enskilda människors liv eller hälsa samt egendom mot omfattande förstörelse. Det kan i enlighet med vad som konstaterats ovan inte anses acceptabelt att en enskild befattningshavare vid Försvarets radioanstalt i en sådan situation ska ställas inför valet att förstöra uppgifter i enlighet med lag, med vetskap om att människors liv riskeras, eller att rapportera uppgifterna till brottsbekämpande myndigheter med de konsekvenser som kan följa på att han eller hon agerat i strid med lag. Det bör därför finnas en möjlighet till undantag från förstöringsskyldigheten i 2 a § första stycket signalspaningslagen i vissa brådskande situationer där liv, hälsa eller egendom är i fara. Det sker lämpligast genom att ett särskilt undantag införs i signalspaningslagen.

Om det är fråga om uppgifter som är av avgörande betydelse för att skydda människors liv eller hälsa eller för att undvika omfattande förstörelse av egendom bör uppgifter således få bevaras och rapporteras, i stället för att förstöras. Detta bör gälla under förutsättning att upptagningen eller uppteckningen inte ska förstöras enligt någon annan bestämmelse. Det måste också vara uppgifter som fått inhämtas enligt bestämmelser i lagen om försvarsunderrättelseverksamhet och signalspaningslagen, bland annat ska det vara fråga om ett utländskt förhållande. Det är alltså fråga om ett undantag från förstöringsskyldigheten för underrättelser som är av avgörande betydelse i fråga om att förhindra sådan allvarlig brottslighet och som hade fått rapporteras om avsändaren eller mottagaren befunnit sig utanför Sverige när signalerna inhämtades. Det bör också vara fråga om en brådskande situation.

Till skillnad från vid inhämtning, där Försvarets radioanstalt får information från en av de inriktande myndigheterna, är det i denna typ av situationer Försvarets radioanstalt som vid bearbetning och analys av inhämtade upptagningar och uppteckningar uppmärksammar uppgifter.

Det är således Försvarets radioanstalt som har att göra en bedömning av det tillgängliga materialet samt dess brådskande natur och betydelse för att förhindra den allvarliga brottsligheten. Ett undantag bör utformas utifrån detta. Det föreslås därför att Försvarets radioanstalt ska få göra undantag från förstöringsskyldigheten om upptagningen eller uppteckningen innehåller uppgifter om en brådskande situation och uppgifterna bedöms vara av avgörande betydelse för att skydda människors liv eller hälsa eller för att undvika omfattande förstörelse av egendom.

På motsvarande sätt som vid tillämpning av den föreslagna bestämmelsen om inhämtning av inhemsk trafik i vissa brådskande situationer är det för en effektiv efterhandskontroll av vikt att Försvarets radioanstalt även underrättar Siun vid tillämpning av den föreslagna bestämmelsen om undantag från förstöringsskyldigheten. Detta kan lämpligen regleras i förordning.

Försvarets radioanstalts rapportering av underrättelser till berörda myndigheter får, enligt vad som anges i avsnitt 8.3, anpassas efter den situation som råder i det enskilda fallet.

8.5 En anpassad ändamålsbestämmelse

Utkastets förslag: Ändamålsbestämmelsen i signalspaningslagen avseende kartläggning av internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen ska inte längre begränsas till kartläggning av strategiska förhållanden.

Utredningen har inte lagt fram något förslag i detta avseende.

Remissinstanserna: *Försvarsunderrättelsedomstolen* anser att det för att uppnå syftet med förslaget om en bestämmelse som medger inhämtning av inhemsk trafik i vissa nödliknande situationer framstår som nödvändigt att ändamålsbestämmelsen i signalspaningslagen justeras och att uttrycket strategiska förhållanden tas bort eller omformuleras. Även *Polismyndigheten* och *Försvarets radioanstalt* väcker frågan om uttrycket behöver ses över för att regelverket ska fungera mer ändamålsenligt.

Skälen för utkastets förslag

Nuvarande reglering

Av 1 § andra stycket 3 signalspaningslagen framgår att signalspaning får bedrivas i syfte att kartlägga strategiska förhållanden avseende internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen. Begränsningen till kartläggning av strategiska förhållanden framgick inte av signalspaningslagen i dess ursprungliga lydelse, men ansågs följa av att försvarsunderrättelseverksamheten i första hand är inriktad på att ge sådan strategisk information som regeringen och olika myndigheter behöver för planering, beslut och andra åtgärder (prop. 2006/07:63 s. 40).

Bestämmelsen i 1 § andra stycket 3 signalspaningslagen fick sin nuvarande utformning 2009. Regeringen angav då att signalspaningens uppgift i förhållande till internationell terrorism eller annan grov

gränsöverskridande brottslighet av så allvarlig karaktär att den kan hota väsentliga nationella intressen är att kartlägga den utifrån ett utrikes- och säkerhetsperspektiv medan sådan underrättelseverksamhet som behövs för att operativt bekämpa brottsligheten är primärt ett polisiärt ansvar (prop. 2008/09:201 s. 109).

I samband med att Säkerhetspolisen och Rikskriminalpolisen (numera Nationella operativa avdelningen i Polismyndigheten) år 2013 åter gavs rätt att inrikta signalspaning i försvarsunderrättelseverksamhet konstaterade regeringen i förarbetena att signalspaning utgör en viktig källa för att ge dessa organ underrättelser om utländska förhållanden (prop. 2011/12:179 s. 14–16).

Ändamålsbestämmelsen som rör internationell terrorism och annan grov gränsöverskridande brottslighet bör inte längre begränsas till sådan kartläggning som enbart avser strategiska förhållanden

En grundläggande förutsättning för det undantag som föreslås i avsnitt 8.3 är att det är fråga om försvarsunderrättelseverksamhet enligt 1 § lagen om försvarsunderrättelseverksamhet. Det ska alltså bl.a. vara ett utländskt förhållande, dvs. verksamheter eller företeelser som har sin utgångspunkt i utlandet (prop. 2006/07:63 s. 43). Den typ av situationer som utredningen beskrivit kan härröra från internationell terrorism, men även från annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen. Därtill måste det finnas en inriktning från regeringen eller annan inriktande myndighet och inhämtningen måste avse kartläggning av någon av företeelserna i 1 § andra stycket signalspaningslagen. Enligt nuvarande regelverk ska det vara fråga om kartläggning av strategiska förhållanden avseende internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen. Utredningen har i detta hänseende anfört att även om det också kan finnas operativa inslag, måste det – med hänsyn till nämnda bestämmelse – alltid vara fråga om kartläggning av strategiska förhållanden.

Försvarsunderrättelsedomstolen och *Polismyndigheten* har i det sammanhanget framfört att begreppet strategiska förhållanden bör ses över för att uppnå syftet med förslaget, nämligen att med hjälp av signalspaning kunna stödja Säkerhetspolisen och Polismyndigheten med uppgifter i brådskande fall. *Försvarets radioanstalt* är av en liknande uppfattning.

Uttrycket strategiska förhållanden i den aktuella ändamålsbestämmelsen har införts i syfte att ytterligare tydliggöra gränsdragningen mellan försvarsunderrättelseverksamhet och polisiär brottsbekämpande verksamhet. I förarbetena framhålls att försvarsunderrättelseverksamheten rent generellt syftar till att ge underlag på en övergripande nivå, inte att kartlägga verksamheten i operativt brottsbekämpande syfte (jfr prop. 2006/07:63 s. 137 och prop. 2008/09:201 s. 29).

Samtidigt står klart att all inhämtning i kartläggande syfte består av inhämtning avseende konkreta företeelser, t.ex. i form av terroristnätverks planer och åtgärder för att utföra dåd i Sverige. Den nuvarande begränsningen av inriktningsmöjligheten när det gäller internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen till kartläggning av just strategiska förhållanden riskerar att i allt för stor utsträckning begränsa Försvarets

radioanstalts möjlighet att inhämta och till berörda myndigheter förmedla konkreta uppgifter. Detta riskerar i förlängningen leda till att uppgifter om utländska företeelser som utgör internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen inte kommer brottsbekämpande myndigheter till handa och därmed inte kan användas för att hindra sådan brottlighet. Det är dessutom förenat med svåra avvägningar att avgöra vilka konkreta uppgifter som är av relevans för strategiska förhållanden, och som därför får inhämtas och rapporteras, och vilka som är av så pass stor operativ betydelse för polisiära myndigheter, att de inte anses avse strategiska förhållanden och därmed inte får inhämtas och vidareförmedlas. Detta talar för att begränsningen till kartläggning av strategiska förhållanden bör tas bort. Det ska dock framhållas att signalspaning alltjämt ska bedrivas i försvarsunderrättelseverksamhet och därmed endast får bedrivas avseende utländska förhållanden samt även fortsatt bör avse kartläggning.

Problematiken med nuvarande begränsning till strategiska förhållanden när det gäller förslaget om att signalspaning i vissa brådskande fall ska få avse inhemsk trafik har lyfts av såväl Försvarsunderrättelsedomstolen som Polismyndigheten och Försvarets radioanstalt. De exempel som redogjorts för i avsnitt 8.2, och som alltså illustrerar nödvändigheten av en särskild reglering för vissa brådskande situationer, rör främst akuta situationer med ageranden i form av internationell terrorism eller annan grov gränsöverskridande brottslighet. För att den föreslagna bestämmelsen om vissa brådskande situationer ska ge avsedd effekt måste signalspaningen kunna ske på en mer preciserad och konkret nivå för att kunna bidra till att avvärja hotet i fråga. Utredningens förslag till reglering i fråga om signalspaning för vissa brådskande situationer tydliggör därmed den begränsning som uttrycket strategiska förhållanden innebär för att kunna uppnå förslagets önskvärda effekt.

En sådan ordning som nu beskrivits är inte rimlig och riskerar att direkt motverka förslaget till undantag från inhämtning av inhemsk trafik i brådskande situationer när liv, hälsa eller egendom är i fara.

Den aktuella problematiken gör sig dock även gällande i andra situationer. Säkerhetspolisen och Polismyndigheten har ingen möjlighet att självständigt bedriva polisiär verksamhet i utlandet och är, liksom påpekats i tidigare förarbeten, vid sidan av signalspaning i huvudsak hänvisade till internationella samarbeten för att på så sätt inhämta närmare information om utländska förhållanden och företeelser (jfr prop. 2011/12:179 s. 14–16). En sådan inhämtning är dock naturligtvis begränsad i olika avseenden, så som möjligheten att kunna påverka urvalet av information eller kontrollera uppgifternas tillförlitlighet. Mer preciserade underlag genom signalspaning skulle alltså kunna utgöra en värdefull resurs för att underlätta Säkerhetspolisens och Polismyndighetens förebyggande arbete mot terrorism och annan allvarlig brottslighet med internationella kopplingar in i Sverige.

Som Försvarsunderrättelsedomstolen även påpekar är signalspaning i syfte att kartlägga främmande underrättelseverksamhet mot svenska intressen, vilket regleras i 1 § andra stycket 7 signalspaningslagen, inte begränsad till att avse endast strategiska förhållanden. Som domstolen konstaterar innebär detta att möjligheten till signalspaning och underrättelserapportering är mer begränsad när det exempelvis gäller

Säkerhetspolisens kontraterrorismverksamhet jämfört med samma myndighets kontraspionageverksamhet. Detta framstår vare sig som konsekvent eller ändamålsenligt.

En fråga som uppkommer i sammanhanget, och som också identifierats av Försvarsunderrättelsedomstolen, är hur en ändring av den aktuella ändamålsbestämmelsen i signalspaningslagen förhåller sig till de slutsatser som dragits i tidigare förarbeten till lagen, enligt vad som beskrivits ovan. Signalspaningslagstiftningen har sedan dess tillkomst kommit att förtydligas i vissa avseenden som har bäring på den polisiära användningen av uppgifter från signalspaning i försvarsunderrättelse-verksamhet. Utöver att Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten getts inriktningsrätt har det bland annat införts reglering som möjliggör att dessa organ får ta emot underrättelser med inhämtade uppgifter från Försvarets radioanstalt, även om det pågår en förundersökning. Regleringen är tydligt avgränsad i förhållande till Säkerhetspolisens och Polismyndighetens brottsutredande verksamhet då den uppställer ett förbud mot att använda underrättelseuppgifterna i en förundersökning. Det finns däremot inte något hinder mot att använda uppgifterna för att förebygga, förhindra och upptäcka brott (prop. 2018/19:96 s. 27–28). Ett sådant förfarande som nu beskrivits måste dock rimligtvis inbegripa någon form av operativt inslag, vilket alltså även nu gällande reglering möjliggör i viss begränsad utsträckning. Enbart det förhållandet att signalspaning i försvarsunderrättelseverksamhet skulle ske på en mer preciserad nivå i stället för övergripande sådan – beträffande samma typ av yttre hot som tidigare och med oförändrade förutsättningar av hur uppgifterna kan användas – kan inte innebära något principiellt avsteg i sammanhanget. Det står vidare klart att både Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten har ett stort behov av uppgifter som kan tillhandahållas genom signalspaning, exempelvis för att kartlägga terroristnätverk eller andra kriminella grupperingar som ägnar sig åt allvarlig gränsöverskridande brottslighet och som hotar väsentliga nationella säkerhetsintressen. Med hänsyn till den slags brottslighet som uppgifterna kan gälla finns det även en risk för att den nuvarande avgränsningen i ändamålsbestämmelsen i signalspaningslagen om strategiska förhållanden avseende internationell terrorism och annan grov brottslighet som kan hota väsentliga nationella intressen kan leda till allvarliga konsekvenser och utgöra ett väsentligt hinder för staten att fullgöra dess grundläggande uppgifter, så som att värna Sveriges och allmänhetens säkerhet. Detta kan i sin tur påverka tilltron till staten och myndigheterna på ett negativt sätt.

Sammanfattningsvis finns det övertygande skäl för att justera den aktuella ändamålsbestämmelsen på så sätt att begreppet strategiska förhållanden tas bort. Detta innebär bland annat att kartläggningen kan ske på en mer preciserad nivå och att Försvarets radioanstalts underrättelser exempelvis kan innefatta information som är tidskritisk och individspecifik. Justeringen medför däremot inte något ändrat synsätt i fråga om den gränsdragning som även fortsatt ska gälla mellan försvarsunderrättelseverksamheten och den brottsbekämpande verksamheten, vilket utvecklas närmare i följande avsnitt.

8.6 Gränsdragningen mellan försvarsunderrättelseverksamhet och brottsbekämpande verksamhet

Utkastets bedömning: Förslagen om en bestämmelse som medger inhämtning av inhemsk trafik i vissa brådskande situationer och en reviderad ändamålsbestämmelse påverkar inte den grundläggande gränsdragning som finns mellan försvarsunderrättelseverksamhet och brottsbekämpande verksamhet.

Utredningens bedömning överensstämmer med utkastets.

Remissinstanserna: *Försvarsunderrättelsedomstolen* efterfrågar förtydliganden eller exemplifieringar hur uppgifterna kan användas för att förhindra brott i sådana akuta situationer som förslaget om att tillåta inhämtning av inhemsk trafik under vissa premisser avser.

Skälen för utkastets bedömning: Försvarsunderrättelseverksamhetens förhållande till den brottsbekämpande verksamheten regleras närmare i 4 § lagen om försvarsunderrättelseverksamhet. Enligt paragrafen får det inom försvarsunderrättelseverksamheten inte vidtas åtgärder som syftar till att lösa uppgifter som enligt lagar eller andra föreskrifter ligger inom ramen för Polismyndighetens, Säkerhetspolisens och andra myndigheters brottsbekämpande och brottsförebyggande verksamhet. Om det inte finns hinder enligt andra bestämmelser, får dock de myndigheter som bedriver försvarsunderrättelseverksamhet lämna stöd till andra myndigheters brottsbekämpande och brottsförebyggande verksamhet. De åtgärder som inte får vidtas i försvarsunderrättelseverksamheten är, enligt vad som anges i förarbetena till bestämmelsen, konkreta åtgärder i den brottsförebyggande och brottsbekämpande verksamheten med det direkta syftet att lösa uppgifter som föreskrivs för denna verksamhet. Det handlar om sådana åtgärder som, om de vidtogs av andra myndigheter, skulle kunna störa utövandet av den brottsbekämpande eller brottsförebyggande verksamheten. Begränsningen träffar endast sådana åtgärder för inhämtning av information som tar sig mer konkreta uttryck än t.ex. inhämtning av signaler i elektronisk form vid signalspaning (prop. 1999/2000:25 s. 20 och prop. 2006/07:63 s. 135 f.). En grundläggande princip som följer av andra regler, och som därför inte har ansetts behöva anges uttryckligen i signalspaningslagen, är dock att försvarsunderrättelseverksamheten inte får innefatta förfarande i samband med förundersökning, vissa arbetsmetoder som är förbehållna polismän och användning av straffprocessuella tvångsmedel (prop. 2006/07:63 s. 41 och 135). I samband med att Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten gavs rätt att inrikta signalspaning i försvarsunderrättelseverksamhet påpekades i förarbetena att detta inte innebar någon ändring i fråga om gränsdragningen mellan försvarsunderrättelseverksamhet och brottsbekämpande verksamhet (prop. 2011/12:179 s. 22). Enligt 1 § lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott får uppgifter i underrättelser som Försvarets radioanstalt rapporterat till en annan myndighet i enlighet med lagen om försvarsunderrättelseverksamhet inte användas för att utreda brott. Sådana uppgifter får alltså inte användas i

förundersökning. Regleringen hindrar dock inte att uppgifterna i övrigt används inom den brottsbekämpande verksamheten, i vilken bl.a. ingår att upptäcka och förhindra brott. Eftersom förbudet inte påverkas av förslaget upprätthålls den grundläggande gränsdragningen mellan försvarsunderrättelseverksamheten och den brottsbekämpande verksamheten (jfr prop. 2018/19:96 s. 18).

Försvarsunderrättelsedomstolen efterfrågar förtydliganden eller exemplifieringar hur uppgifterna kan användas för att förhindra brott i sådana akuta situationer som förslaget om att tillåta inhämtning av inhemsk trafik under vissa premisser avser. Aktuella förslag – såväl i nu nämnda avseende, som förslaget om en ändrad ändamålsbestämmelse – är inte avsett att förändra gränsdragningen mellan försvarsunderrättelseverksamheten och den brottsbekämpande verksamheten. Försvarets radioanstalt ska inte heller fortsättningsvis vara en brottsbekämpande myndighet. Myndighetens uppgift ska även fortsatt vara att inhämta och rapportera uppgifter till berörda myndigheter i enlighet med 8 § signalspaningslagen. Det är sedan upp till de brottsbekämpande myndigheterna att bedöma vilka åtgärder som kan vidtas med anledning av de uppgifter som Försvarets radioanstalt rapporterar, med beaktande av lagen om förbud mot användning av vissa uppgifter för att utreda brott. Uppgifterna kan således inte användas i en förundersökning, medan inget hindrar att de i övrigt används för andra syften än att utreda brott, t.ex. användning för att förebygga, förhindra och upptäcka brottslig verksamhet. Det finns inte heller något hinder mot att uppgifterna används inom underrättelseverksamheten för att få fram ytterligare uppgifter som i sin tur kan användas för att utreda brott (prop. 2018/19:96 s. 22 f.). Några ytterligare förtydliganden eller exemplifieringar är inte behövliga.

8.7 Den personliga integriteten

Utkastets bedömning: Det eventuella intrång i den personliga integriteten som förslagen innebär, är proportionerligt.

Utredningens bedömning överensstämmer med utkastets.

Remissinstanserna: *Tjänstemännens centralorganisation (TCO)* och *Journalistförbundet* bedömer att förslaget om en bestämmelse som medger inhämtning av inhemsk trafik i vissa brådskande situationer riskerar att kraftigt påverka journalisters möjlighet att garantera källors anonymitet. Enligt Journalistförbundet är det positivt att det grundlagsreglerade källskyddet värnas genom att kravet på att förstöra uppgifter som omfattas av källskydd upprätthålls.

Skälen för utkastets bedömning: Förslaget till en ny bestämmelse i signalspaningslagen innebär att inhämtning ska få ske mellan en avsändare och en mottagare som båda befinner sig i Sverige i vissa brådskande situationer som innebär fara för människors liv eller hälsa eller för omfattande förstörelse av egendom. Enligt förslaget ska det också finnas en möjlighet till undantag från förstöringsskyldigheten i 2 a § första stycket signalspaningslagen i vissa brådskande situationer där liv, hälsa eller egendom är i fara.

Inhämtning enligt förslaget förutsätter även fortsatt att det är fråga om ett utländskt förhållande, att inriktning finns från en inriktande myndighet, att inhämtningen sker i syfte att kartlägga någon av de särskilt angivna företeelserna i signalspaningslagen och att det finns tillstånd. Det är således fråga om inhämtning som ur ett integritetskyddsperspektiv skulle kunna anses godtagbar om exempelvis avsändaren, men inte mottagaren, befann sig i Sverige. Syftet med de föreslagna bestämmelserna är att möjliggöra att allvarlig brottslighet som innebär fara för människors liv eller hälsa eller för omfattande förstörelse av egendom kan förhindras. Förslaget om en ny bestämmelse om undantag från förstörings-skyldigheten innebär inte heller att signaler kan inhämtas i större utsträckning. Det innebär däremot att redan inhämtade uppgifter, som annars hade förstörts, kan rapporteras i vissa brådskande situationer. Mot bakgrund av detta bedöms att det intrång som aktuella förslag kan komma att innebära för den personliga integriteten för avsändaren och mottagaren är begränsat och får anses vara proportionerligt sett till syftet med bestämmelserna.

Beträffande förslaget om ändring i den berörda ändamålsbestämmelsen i signalspaningslagen innebär detta å sin sida att signalspaning bör få ske för att på en mer konkret nivå kartlägga terrorism och vissa former av grov internationell brottslighet. Det rör sig dock om samma typ av brottslighet som omfattas av nu gällande ändamålsbestämmelse. Den absoluta huvuddelen av den brottslighet som polisiära myndigheter bl.a. har att förhindra är alltså inte av sådant slag som omfattas av ändamåls-bestämmelsen, utan det rör sig om brott av allvarligare beskaffenhet och som är av internationell karaktär. Det är i samtliga fall fråga om utländska förhållanden som sträcker sig in i landet. Syftet med förslaget är att möjliggöra att sådan allvarlig brottslighet kan förhindras. Det rör sig härvid om inhämtning som i relativt stor utsträckning redan kan ske enligt nu gällande regelverk. Skillnaden är att förslaget till ett reviderat ändamål, som inte är avgränsat till att endast avse strategiska förhållanden, medger inhämtning på ett mer preciserat sätt, och att Försvarets radioanstalts underrättelser exempelvis kan innefatta information som är tidskritisk och individspecifik. Samtidigt bedöms en mer preciserad inhämtning leda att färre irrelevanta uppgifter inhämtas, vilket är till gagn för den personliga integriteten. Med hänsyn till detta och till att ändamålet är avgränsat till att endast avse internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen bedöms sammantaget att det integritetsintrång för enskilda som förslaget kan anses innebära är av begränsat slag.

Det finns dock, som vid all signalspaning, en viss risk för att upptagningar eller uppteckningar som saknar relevans för inhämtnings-uppdraget inhämtas. Det finns därför skäl att påminna om signalspanings-lagens bestämmelser om bland annat förstöring och rapportering, vilka syftar till att värna enskildas integritetsintressen. Bestämmelserna innebär exempelvis att om en upptagning eller uppteckning inhämtas mellan en avsändare och mottagare som inte är av relevans ur försvarsunderrättelse-synpunkt ska den förstöras (7 § 1 signalspaningslagen). Förstörings-skyldigheten i 7 § 2 och 3 signalspaningslagen är absolut. Detta innebär att skyldigheten enligt dessa bestämmelser gäller utan hinder av förslaget om en ny bestämmelse som möjliggör inhämtning av inhemsk trafik vid

vissa brådskande situationer, vilket också *Journalistförbundet* noterar. Enligt *Tjänstemännens centralorganisation (TCO)* riskerar förslaget om att kunna inhämta inhemsk trafik i vissa brådskande situationer, trots förstöringskravet, att kraftigt påverka journalisters möjlighet att garantera källors anonymitet. Journalistförbundet framför en liknande synpunkt. Anonymitetsskyddet och meddelarfriheten kommer även fortsättningsvis att vara tillgodosett genom lagstiftningen, på samma sätt som tidigare.

Vidare gäller att om uppgifter som rapporteras till berörda myndigheter berör en viss fysisk person, får rapporteringen endast avse förhållanden som är av betydelse i försvarsunderrättelsesynpunkt (8 § signalspaningslagen). Slutligen kan nämnas att Siun har i uppgift att kontrollera att Försvarets radioanstalt följer signalspaningslagen (10 § signalspaningslagen). Siun ska särskilt granska användningen av sökbegrepp, förstöring och rapportering. En enskild kan enligt 10 a § signalspaningslagen begära kontroll av om hans eller hennes meddelanden har inhämtats och, om så skett, huruvida inhämtningen varit lagenlig.

Sammantaget innebär det att de mekanismer i signalspaningslagen som syftar till att skydda den personliga integriteten är tillämpbara också vid tillämpningen av de regler som föreslås. Därtill utövar Säkerhets- och integritetsskyddsnämnden tillsyn över Säkerhetspolisens och Polismyndighetens tillämpning av lagen om förbud mot användning av vissa uppgifter för att utreda brott (1 § tredje stycket lagen [2007:980] om tillsyn över viss brottsbekämpande verksamhet).

Syftet med förslagen är bl.a. att möjliggöra att allvarlig brottslighet som innebär fara för människors liv eller hälsa eller för omfattande förstörelse av egendom kan förhindras. Förslagen kan således åstadkomma ett skydd för den personliga integriteten för dem som kan komma att utsättas för sådan allvarlig brottslighet. Som framgår av redogörelsen i avsnitt 8.3 och 8.5 är förslagen motiverade av tungt vägande intressen, och utifrån dessa nödvändiga. Något mindre ingripande alternativ bedöms inte heller finnas. Med hänsyn till detta, och till de skyddsmekanismer som finns i signalspaningslagen, är det intrång i den personliga integriteten som förslagen skulle kunna innebära vid inhämtning av signaler i elektronisk form proportionerligt.

9 Inriktning av signalspaning i försvarsunderrättelseverksamhet

9.1 Inspektionen för strategiska produkter ges rätt att inrikta signalspaning i försvarsunderrättelseverksamhet

Utkastets förslag: Inspektionen för strategiska produkter får inrikta signalspaning i försvarsunderrättelseverksamhet.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: De flesta remissinstanserna, däribland *Inspektionen för strategiska produkter*, tillstyrker förslaget eller har inga synpunkter på det.

Försvarets radioanstalt är av uppfattningen att ingen ytterligare myndighet bör ges rätt att inrikta signalspaning i försvarsunderrättelseverksamhet och avstyrker förslaget. Försvarets radioanstalt anför vidare att om någon ytterligare myndighet ska få inriktningsrätt kan det ifrågasättas om inte Tullverket vore ett mer lämpligt val. Myndigheten framför också att förslaget kommer att leda till undanträngningseffekter i förhållande till redan befintliga inriktande myndigheter. Även *Säkerhetspolisen* avstyrker förslaget och anför att det finns en konkret risk för att detta kommer att leda till undanträngningseffekter. Säkerhetspolisen påpekar även att om inriktningsrätt ges till en myndighet som i övrigt har begränsade möjligheter till egen underrättelseinhämtning riskerar det att leda till en inkomplett underrättelsebild. *Försvarsmakten* pekar också på riskerna för undanträngningseffekter och anser att en undanträngning av myndighetens underrättelsebehov till förmån för en tillkommande inriktande myndighet inte kan accepteras.

Försvarets materielverk och *Totalförsvarets forskningsinstitut* anser att båda myndigheterna bör få inriktningsrätt. *Tullverket* och *Myndigheten för psykologiskt försvar* för å sin sida fram att respektive myndighet bör få sådan rätt. Myndigheten för psykologiskt försvar anser därtill att det saknas tillräckligt underlag för regeringens beslut i frågan.

Skälen för utkastets förslag

Nuvarande reglering

Regeringen bestämmer inriktningen för försvarsunderrättelseverksamheten. Inom ramen för den inriktningen får de myndigheter som regeringen bestämmer ange närmare inriktning av verksamheten (1 § andra stycket lagen [2000:130] om försvarsunderrättelseverksamhet). Signalspaning i försvarsunderrättelseverksamhet får dock endast ske i de fall regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten närmare har bestämt inriktningen av signalspaningen. I fråga om Försvarets radioanstalts utvecklingsverksamhet och internationella samarbete är det endast regeringen som får inrikta signalspaningen (1 § första stycket och 4 §

första och andra styckena lagen [2008:717] om signalspaning i försvarsunderrättelseverksamhet [signalspaningslagen]).

En fortsatt restriktiv hållning i fråga om ifall ytterligare myndigheter ska ges rätt att inrikta signalspaning i försvarsunderrättelseverksamhet

Enligt den ursprungliga lydelsen av 1 § signalspaningslagen fick signalspaning i försvarsunderrättelseverksamhet ske i de fall regeringen eller, enligt regeringens bestämmande, en myndighet närmare bestämt inriktningen för signalspaningen. Bestämmelsen överensstämde således tidigare med vad som gäller för annan försvarsunderrättelseverksamhet. Den politiska överenskommelsen mellan partierna i regeringen hösten 2008 innebar att det endast var regeringen, Regeringskansliet och Försvarsmakten som skulle få inrikta signalspaning i försvarsunderrättelseverksamhet (prop. 2008/09:201 s. 31–32). Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten (tidigare Rikskriminalpolisen) har därefter getts rätt att inrikta signalspaning i försvarsunderrättelseverksamhet (prop. 2011/12:179, bet. 2012/13:JuU7, rskr. 2012/13:61). Frågan om vilka myndigheter som ska få inrikta signalspaning i försvarsunderrättelseverksamhet har således präglats av en mycket restriktiv hållning i princip sedan signalspaningslagens tillkomst.

Signalspaning i försvarsunderrättelseverksamhet är en mycket känslig verksamhet som omgärdas av stark sekretess. Många uppgifter är kvalificerat hemliga. Signalspaning är vidare en inhämtningsmetod som medför intrång i den personliga integriteten. En central utgångspunkt mot bakgrund av detta är att det måste finnas ett reellt behov av signalunderrättelser hos en myndighet som ska inrikta signalspaning i försvarsunderrättelseverksamhet. Behovet ska inte kunna tillgodoses på något annat mindre ingripande sätt, exempelvis inhämtning genom andra källor eller genom att myndigheten i egenskap av berörd myndighet får ta del av underrättelser från Försvarets radioanstalt enligt 8 § signalspaningslagen. Signaler i elektronisk form får vidare endast inhämtas om Försvarsunderrättelsedomstolen lämnar tillstånd. En förutsättning för tillstånd är bland annat att syftet med inhämtningen inte kan tillgodoses på ett mindre ingripande sätt. Andra, mindre ingripande åtgärder måste alltså vara uteslutna för att signalspaning ska få användas.

Det finns med hänsyn till den mycket känsliga verksamhet som Försvarets radioanstalt bedriver skäl att fortsatt tillämpa en restriktiv hållning i fråga om antalet inriktande myndigheter. Ju fler inriktande myndigheter, desto större spridning riskerar inhämtade uppgifter att få. Detta gäller såväl för uppgifter som har bäring på Sveriges säkerhet, som för uppgifter som rör den personliga integriteten.

Försvarets radioanstalts signalspaningsverksamhet är vidare en begränsad resurs. Med fler inriktande myndigheter kan Försvarets radioanstalt behöva göra prioriteringar mellan olika uppdrag och uppdragsgivare, i en än högre utsträckning än vad som redan sker. Som *Säkerhetspolisen* och *Försvarsmakten* pekar på är en konsekvens som kan följa på fler inriktande myndigheter alltså olika former av undanträngningseffekter som kan komma att drabba de i dag inriktande myndigheterna negativt. Även detta talar för en fortsatt restriktiv hållning i fråga om att ge fler myndigheter inriktningsrätt.

Vidare delas utredningens bedömning att av de myndigheter som utredningen undersökt och som uttryckt behov av att inrikta signalspaning i försvarsunderrättelseverksamhet, är Inspektionen för strategiska produkter (ISP) den myndighet som bör övervägas i fråga om att få sådan inriktningsrätt. Till skillnad från vad *Myndigheten för psykologiskt försvar* anför anses det finnas ett tillräckligt underlag för att göra en bedömning i denna fråga.

Inspektionen för strategiska produkters uppgifter

ISP är förvaltningsmyndighet för ärenden och tillsyn enligt lagen (1992:1300) om krigsmateriel samt lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd. Myndigheten är vidare nationell myndighet med de uppgifter som följer av lagen (1994:118) om inspektioner enligt Förenta nationernas konvention om förbud mot kemiska vapen och anslutande förordning (1997:121). ISP ska hantera riktade sanktioner enligt de förordningar om sanktioner som beslutas av Europeiska unionen, efter beslut av regeringen med anledning av sådana förordningar eller enligt föreskrifter som regeringen beslutar med stöd av lagen (1996:95) om vissa internationella sanktioner.

Sedan den 1 december 2023 är ISP granskningsmyndighet enligt lagen (2023:560) om granskning av utländska direktinvesteringar. ISP ska enligt lagen granska utländska direktinvesteringar och kan, om det är nödvändigt, förbjuda dem. ISP är också Sveriges kontaktpunkt enligt Europaparlamentets och rådets förordning (EU) 2019/452 av den 19 mars 2019 om upprättande av en ram för granskning av utländska direktinvesteringar i unionen.

Lagen om granskning av utländska direktinvesteringar

Lagen om granskning av utländska direktinvesteringar blir tillämplig vid investeringar i skyddsvärd verksamhet. Vad som avses med skyddsvärd verksamhet och utländsk direktinvestering definieras i lagen.

Den som har för avsikt att investera i skyddsvärd verksamhet har en skyldighet att anmäla till granskningsmyndigheten om någon av förutsättningarna i 7, 9 eller 10 §§ är uppfyllda. En granskning av en investering kan även inledas på granskningsmyndighetens initiativ.

Granskningsmyndigheten ska inom viss tid besluta om att antingen lämna en anmälan utan åtgärd eller inleda en granskning av investeringen (14 §). Enligt 15 § ska granskningsmyndigheten, om en granskning inleds, därefter fatta beslut om att antingen förbjuda eller godkänna investeringen. För att en investering som omfattas av anmälningsskyldigheten ska få genomföras krävs antingen att anmälan om investeringen har lämnats utan åtgärd eller att investeringen har godkänts vid en granskning (16 §).

En investering ska förbjudas om det är nödvändigt för att förebygga skadlig inverkan på Sveriges säkerhet eller på allmän ordning eller allmän säkerhet i Sverige (20 §).

Granskningsmyndigheten får, enligt 29 §, i samband med sin granskning eller sin kontroll av efterlevnaden av meddelade villkor begära information från kommuner, regioner och statliga myndigheter. Enligt 30 § ska granskningsmyndigheten vid sin granskning samverka med de

statliga myndigheter som regeringen bestämmer. Regeringen har i 7 § förordningen (2023:624) om granskning av utländska direktinvesteringar angett vilka myndigheter det är.

Inspektionen för strategiska produkter bör ges inriktningsrätt

Riksdagen påpekade i ett tillkännagivande till regeringen i mars 2018 att signalspaning bedrivs i syfte att kartlägga utveckling och spridning av massförstörelsevapen, krigsmateriel och produkter med dubbla användningsområden, men att ISP inte har rätt att inrikta signalspaning för att uppnå detta syfte. Regeringen bör därför se över möjligheten att ge ISP rätt att inrikta signalspaning från Försvarets radioanstalt (rskr. 2017/18:178, bet. 2017/18:FöU5).

ISP har ett operativt inriktat samarbete på handläggarnivå inom gruppen för ickespridning och exportkontroll (ISEK). Samarbetet sker genom regelbundna möten mellan ISP och Försvarets radioanstalt, Försvarsmakten genom Militära underrättelse- och säkerhetstjänsten, Säkerhetspolisen, Totalförsvarets forskningsinstitut och Tullverket (skr. 2022/23:114 s. 96). I likhet med utredningens bedömning bör ISP genom detta samarbete till stor del kunna få sitt underrättelsebehov på området tillgodosett. Även *Försvarets radioanstalt* och *Säkerhetspolisen* har framfört att ISP:s underrättelsebehov kan tillgodoses på annat sätt.

ISP har dock fler uppgifter. ISP har enligt lagen om granskning av utländska direktinvesteringar till uppgift att efter anmälan eller på eget initiativ granska utländska direktinvesteringar i skyddsvärd verksamhet. Lagen syftar till att hindra utländska direktinvesteringar i svensk skyddsvärd verksamhet som kan inverka skadligt på Sveriges säkerhet eller på allmän ordning eller allmän säkerhet i Sverige. Uppgiften att granska utländska direktinvesteringar fyller en viktig funktion för att bland annat behålla Sveriges oberoende och skydda Sveriges säkerhet. Det är en uppgift som inte direkt kan sägas ha någon motsvarighet i de nuvarande inriktande myndigheternas inriktningar till Försvarets radioanstalt. Dessa omständigheter talar för att ISP ska ges rätt att inrikta signalspaning i försvarsunderrättelseverksamhet.

ISP har i sin granskning enligt lagen om granskning av utländska direktinvesteringar vissa särskilda tidsfrister att förhålla sig till både i fråga om att fatta beslut om att inleda en granskning och att fatta beslut om att förbjuda eller godkänna en investering. Detta skiljer sig från Försvarets radioanstalts signalspaningsverksamhet i det avseendet att verksamheten bedrivs med långa ledtider i syfte att upptäcka ännu okända hotaktörer, företeelser och uppgifter av relevans om dessa. Med hänsyn till de tidsfrister som ISP har att tillämpa skulle detta kunna innebära att signalspaning är en mindre väl lämpad metod för att tillgodose ISP:s underrättelsebehov för ärendehanteringen. Det framstår därför som att signalspaning i försvarsunderrättelseverksamhet är mer lämpad för att kartlägga strategiska förhållanden än för ett enskilt ärende.

I fråga om ISP:s ärendehantering måste också beaktas att Försvarets radioanstalts rapportering är underrättelseinformation. Det bör således inte vara möjligt att använda informationen som underlag för beslut i ett enskilt ärende. I jämförelse är brottsbekämpande myndigheter förbjudna att använda uppgifter från Försvarets radioanstalt i en förundersökning (1 §

lagen [2019:547] om förbud mot användning av vissa uppgifter för att utreda brott). Detta talar också emot signalspaning i försvarsunderrättelseverksamhet som metod för att tillgodose ISP:s underrättelsebehov i ett enskilt ärende.

Det finns alltså ett antal omständigheter som visserligen talar emot att ge ISP inriktningsrätt. De är huvudsakligen hänförliga till att ISP i sitt arbete med ickespridning och exportkontroll till stor del bör kunna få sitt underrättelsebehov tillgodosett på annat sätt, och till ISP:s eventuella användning av uppgifter från Försvarets radioanstalt i sin prövning av enskilda ärenden enligt lagen om granskning av utländska direktinvesteringar. Något annat har dock inte framkommit än att signalspaning i försvarsunderrättelseverksamhet bör kunna användas för strategisk kartläggning kring företeelser som kan vara av betydelse för ISP:s granskning av utländska direktinvesteringar. ISP:s uppgift på detta område fyller mycket viktiga funktioner för att bland annat skydda Sveriges säkerhet. Uppgiften är relativt ny och dess betydelse kan förväntas öka över tid. Inte minst med hänsyn till det allvarliga säkerhetspolitiska läge som Sverige befinner sig i är det av vikt att ISP ges ytterligare verktyg för denna uppgift. Utredningen har därtill gjort bedömningen att en fördjupad dialog med Försvarets radioanstalt inte skulle tillgodose ISP:s behov på detta område i tillräcklig utsträckning. Det har inte framkommit tillräckliga skäl att frångå utredningens slutsats i denna del. Efter en sammantagen bedömning är slutsatsen, till skillnad från Försvarets radioanstalts och Säkerhetspolisens, att ISP bör få inrikta signalspaning i försvarsunderrättelseverksamhet.

Vad Försvarets radioanstalt, *Försvarsmakten* och Säkerhetspolisen har anfört om risken för undanträngningseffekter, om ytterligare myndigheter ges inriktningsrätt, måste samtidigt beaktas i sammanhanget. Förslaget om att ge ISP inriktningsrätt bedöms dock vara av sådant avgränsat slag att några betydande undanträngningseffekter inte bör uppkomma. Detta särskilt eftersom det nya ändamålet för signalspaning som föreslås införas avgränsas till kartläggning av strategiska förhållanden avseende aktuella utländska direktinvesteringar. Det rör sig alltså om signalspaning som syftar till att tillhandahålla underlag på en mer övergripande nivå. Denna fråga behandlas närmare i nästföljande avsnitt.

9.2 Ett nytt ändamål för signalspaning införs

Utkastets förslag: Signalspaning i försvarsunderrättelseverksamhet ska få bedrivas för att kartlägga strategiska förhållanden avseende sådana utländska direktinvesteringar som avses i lagen om granskning av utländska direktinvesteringar.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: Endast *Försvarets radioanstalt* och *Inspektionen för strategiska produkter* yttrar sig särskilt i denna del och tillstyrker förslaget.

Skälen för utkastets förslag: Enligt 1 § lagen om försvarsunderrättelseverksamhet får försvarsunderrättelseverksamhet bedrivas i syfte att stödja svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för att

kartlägga yttre hot mot landet. Verksamheten får därutöver vidare endast avse utländska förhållanden. Signalspaning i försvarsunderrättelseverksamhet får endast bedrivas för att kartlägga de särskilda företeelser som anges i 1 § andra stycket signalspaningslagen. För att det ska vara möjligt för Försvarets radioanstalt att bedriva signalspaning efter inriktning från ISP (avsnitt 9.1) och för ISP:s underrättelsebehov måste det således finns något eller några företeelser i nämnda bestämmelse som signalspaning får bedrivas för.

ISP:s uppgifter i fråga utveckling och spridning av massförstörelsevapen, krigsmateriel och produkter med dubbla användningsområden omfattas av 1 § andra stycket 4 signalspaningslagen. Det finns dock ingen ändamålsbestämmelse som fullt ut kan tillämpas för granskning av utländska direktinvesteringar. En sådan bestämmelse måste därför införas om signalspaning i försvarsunderrättelseverksamhet ska kunna användas för att tillgodose ISP:s underrättelsebehov i den delen.

I likhet med utredningen görs bedömningen att signalspaning i försvarsunderrättelseverksamhet i förhållande till lagen om granskning av utländska direktinvesteringar är bäst lämpad för kartläggning av företeelser om strategiska förhållanden av betydelse för ISP:s granskningsverksamhet. Signalspaningens uppgift skulle i sådana fall vara att kartlägga företeelser på en strategisk nivå för att ge ett övergripande underlag. För sin bedömning i ett enskilt ärende är ISP emellertid i behov av information från andra källor. Förslaget är även tydligt motiverat utifrån dess betydelse för Sveriges säkerhet och bedöms vara acceptabelt i förhållande till den risk för ökat integritetsintrång som förslaget kan medföra. Det föreslås därför att signalspaning i försvarsunderrättelseverksamhet ska få användas för att kartlägga strategiska förhållanden avseende sådana utländska direktinvesteringar som avses i lagen om granskning av utländska direktinvesteringar.

10 Övriga förslag

10.1 En övergripande redovisning av övrig inhämtning ska ingå i ansökan

Utkastets förslag: I ansökan om tillstånd för signalspaning ska, utöver vilken eller vilka signalbärare avseende signaler i tråd som signalspaningsmyndigheten behöver ha tillgång till för att fullgöra uppdraget, en övergripande redovisning av övrig inhämtning anges.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: *Sveriges advokatsamfund* efterlyser ett förtydligande om att signalspaningsmyndigheten vid ansökan ska åläggas att presentera en analys och bedömning av de hot, risker och skador som kan uppkomma vid signalspaningen och vid överföring av uppgifter utomlands. Övriga remissinstanser yttrar sig inte särskilt över förslaget.

Skälen för utkastets förslag: All inhämtning av signaler i elektronisk form kräver tillstånd av Försvarsunderrättelsedomstolen. Ansökan om

tillstånd för signalspaning ska göras av Försvarets radioanstalt. I 4 a § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (signalspaningslagen) finns bestämmelser om vad en ansökan ska innehålla. Av 5 § signalspaningslagen framgår kriterierna för att tillstånd ska få lämnas.

Vid prövningen av en ansökan ska domstolen bland annat ta ställning till om uppdraget beräknas ge information vars värde är klart större än det integritetsintrång som inhämtning i enlighet med ansökan kan innebära (5 § 3 signalspaningslagen). Detta förutsätter att domstolen på ett övergripande plan får information om all den inhämtning som kan komma att bli aktuell under tillståndets giltighetstid. Enligt 4 a § 2 signalspaningslagen är redovisningen av själva inhämtningen emellertid begränsad till inhämtning i tråd. I enlighet med utredningens förslag bör det uttryckligen framgå av lagtexten att annan inhämtning ska redovisas på ett övergripande plan i ansökan.

Den fråga som *Sveriges advokatsamfund* väcker är inte föremål för aktuellt lagstiftningsärende, vilket advokatsamfundet även noterar. Därtill uppfyller nuvarande reglering de ändamål som advokatsamfundet efterfrågar. Förslaget medför också att förutsättningarna för den proportionalitetsbedömning som Försvarsunderrättelsedomstolen ska göra efter en ansökan om tillstånd ytterligare stärks.

10.2 Ett förtydligande av tillämplig bestämmelse

Utkastets förslag: Av 5 a § lagen om signalspaning i försvarsunderrättelseverksamhet ska det framgå att vid utformningen av ansökan enligt bestämmelsen gäller 4 a § nämnda lag i tillämpliga delar.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna uttalar sig inte särskilt över förslaget.

Skälen för utkastets förslag: I 5 a § tredje stycket signalspaningslagen finns en möjlighet för Försvarets radioanstalt att ansöka om ett särskilt tillstånd inom ramen för ett redan tillståndsprövat inhämtningsuppdrag om det uppstår behov av tillgång till ytterligare signalbärare eller användning av andra tillståndspliktiga sökbegrepp. Av bestämmelsen framgår att vid utformningen av ansökan och vid prövningen av den gäller 4 och 5 §§ signalspaningslagen i tillämpliga delar. Hänvisningen till 4 § framstår som felaktig då nämnda paragraf innehåller bestämmelser om inriktning. Hänvisning torde rätteligen göras till 4 a § signalspaningslagen, som reglerar vad en ansökan ska innehålla. I författningskommentaren till 5 a § signalspaningslagen anges även att 4 a § signalspaningslagen ska gälla i tillämpliga delar (prop. 2008/09:201 s. 112). Det föreslås därför att bestämmelsen ändras på sådant sätt att hänvisning görs till 4 a § signalspaningslagen.

10.3 Underrättelseskyldigheten till enskilda upphävs

Utkastets förslag: Bestämmelsen om underrättelseskyldighet till enskilda i lagen om signalspaning i försvarsunderrättelseverksamhet upphävs.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: *Försvarets radioanstalt* tillstyrker förslaget och anser att det finns skäl att upphäva även andra bestämmelser.

Föreningen för Digitala Fri- och Rättigheter för fram att förslaget kan bryta mot rätten till insyn och transparens enligt dataskyddsförordningen och kan påverka enskildas möjlighet att hävda och försvara sina rättigheter.

Skälen för utkastets förslag

Nuvarande reglering

Om det vid signalspaning har använts sökbegrepp som är direkt hänförliga till en viss fysisk person ska personen underrättas om detta. En underrättelse ska lämnas så snart det kan ske utan men för försvarsunderrättelseverksamheten, dock senast en månad efter att det inhämtningsuppdrag som föranlett inhämtningen avslutades. En underrättelse får dock skjutas upp om sekretess hindrar att underrättelse lämnas. Har det på grund av sekretess inte kunnat lämnas någon underrättelse inom ett år från det att inhämtningsuppdraget avslutades, behöver någon underrättelse inte lämnas. Underrättelse ska inte heller lämnas om inhämtningen uteslutande avser främmande makts förhållanden eller förhållanden mellan främmande makter (11 a och 11 b §§ signalspaningslagen).

Underrättelseskyldigheten aktualiseras i de situationer då det vid signalspaning har använts sökbegrepp som är direkt hänförliga till en fysisk person. Syftet med bestämmelsen är att denna person ska få möjlighet att bedöma vilket integritetsintrång som han eller hon har varit föremål för och att reagera mot vad han eller hon kan anse vara en rättsstridig åtgärd. Införandet av en underrättelseskyldighet var en av punkterna i den politiska överenskommelsen som träffades mellan regeringspartierna i september 2008 (prop. 2008/09:201 s. 86).

Signalspaningskommitténs syn på underrättelseskyldigheten i signalspaningslagen

Signalspaningskommittén tillsattes av regeringen i februari 2009 för att tillgodose vad riksdagen anfört i samband med slutbehandlingen av propositionen En anpassad försvarsunderrättelseverksamhet (prop. 2006/07:63) om att en kommitté skulle följa Försvarets radioanstalt från ett integritetsskyddsperspektiv (bet. 2007/08:FöU15 och rskr. 2007/08:266). Signalspaningskommittén redovisade sitt uppdrag i betänkandet Uppföljning av signalspaningslagen (SOU 2011:13).

I fråga om underrättelseskyldigheten i signalspaningslagen ansåg Signalspaningskommittén att den inte var ändamålsenlig. Enligt kommittén får underrättelseskyldigheten inte någon praktisk funktion som

rättssäkerhetsgaranti eller som ett skydd för enskildas integritet, eftersom verksamheten vid Försvarets radioanstalt är omgärdad av omfattande sekretess. Signalspaningskommittén konstaterade också att någon underrättelse vid utgången av 2010 inte hade lämnats, och att det finns anledning att tro att någon underrättelse aldrig kommer att lämnas. Ett viktigare instrument enligt kommittén är den kontroll på begäran av enskild som ska utföras enligt 10 a § signalspaningslagen (SOU 2011:13 s. 77–78).

Europadomstolens syn på underrättelseskyldigheten i signalspaningslagen

Den europeiska domstolen för de mänskliga rättigheterna i stor sammansättning (Europadomstolen) prövade i målet Centrum för rättvisa mot Sverige [GC] regleringen om och tillämpningen av signalspaningslagen. I avgörandet uttalade sig domstolen bland annat om underrättelseskyldigheten.

Europadomstolen konstaterade i domen att i tidigare praxis har efterföljande notifieringar till enskilda i fråga om hemliga tvångsmedel ansetts vara en relevant faktor vid bedömningen av hur effektiva rättsmedlen är. Sådana notifieringar har dock inte ansetts nödvändiga om de nationella rättsmedlen är tillgängliga för alla, dvs. tillgången till rättsmedlen är oberoende av om en enskild underrättats eller inte (p. 271). Inom ramen för signalspaning kan ett rättsmedel som inte är beroende av notifiering till enskild vara ett effektiv sådant och, beroende på omständigheterna, till och med erbjuda bättre garantier för ett korrekt förfarande, än ett system som baseras på notifiering. Europadomstolen konstaterade att såväl sekretess som att det kan vara svårt att identifiera var enskilda utanför statens eget territorium befinner sig kan medföra att notifiering till enskilda vid signalspaning saknar eller får mycket liten praktisk effekt (p. 272).

Europadomstolen konstaterade att på grund av sekretess har någon underrättelse enligt signalspaningslagen aldrig skickats till någon enskild (p. 354). Domstolen konstaterade också att även om det skulle vara tekniskt möjligt att genomföra en sådan underrättelse, skulle det kunna få oförutsebara och långtgående konsekvenser (p. 355). Med hänvisning till tidigare uttalanden konstaterade Europadomstolen att även ett rättsmedel som inte bygger på notifiering kan anses vara effektivt sådant. Europadomstolen godtog således den svenska ordningen, men betonade samtidigt att avsaknaden av en fungerande notifieringsmekanism måste vägas mot effektiviteten av de rättsmedel som finns tillgängliga för den enskilde (p. 355).

Underrättelseskyldigheten bör upphävas

Försvarets radioanstalt har sedan bestämmelsen infördes, på grund av sekretess, aldrig lämnat någon underrättelse till en enskild enligt 11 a § signalspaningslagen. I likhet med utredningen är det svårt att se att någon underrättelse enligt bestämmelserna i signalspaningslagen kommer att lämnas i framtiden. Underrättelseskyldigheten fyller således inte någon praktisk funktion som rättssäkerhetsgaranti eller som ett skydd för enskildas integritet. Som Europadomstolen anförde i sitt avgörande i målet

Centrum för rättvisa mot Sverige, är en sådan underrättelseskyldighet inte nödvändig för att en enskild ska anses ha tillgång till ett effektivt rättsmedel, så länge rättsmedlen är tillgängliga för envar. Den utredningsskyldighet som erbjuds en enskild enligt 10 a § signalspaningslagen är tillgänglig för såväl fysiska som juridiska personer och oberoende av hemvist eller medborgarskap. Det finns således inga begränsningar i fråga om vem som kan begära kontroll enligt bestämmelsen. Kontroll enligt 10 a § signalspaningslagen innebär en granskningsmöjlighet från ett fristående och självständigt organ. Organet kan få tillgång till material som den enskilde på grund av sekretess inte kan ta del av. Det finns därigenom större möjligheter att bedöma och åtgärda eventuella integritetsintrång och därmed goda förutsättningar att tillvarata den enskildes intressen. Med hänsyn även till att ett nytt särskilt beslutandeorgan från och med den 1 januari 2025 har i uppgift att pröva begäran får enskilda anses ha tillgång till ett effektivt rättsmedel. Därför delas inte *Föreningen för Digitala Fri- och Rättigheters* farhågor i sammanhanget. Det kan även tilläggas att regeringen föreslog utredningsskyldigheten i 10 a § signalspaningslagen mot bakgrund av att en underrättelseskyldighet, med hänsyn till bland annat sekretess, bedömdes som otillräcklig för att enskilda ska kunna tillvarata sin rätt (prop. 2008/09:201 s. 91–92).

Avslutningsvis delas, till skillnad från *Försvarets radioanstalt*, utredningens bedömning att det saknas skäl att föreslå att bestämmelser om den enskildes rätt till personrelaterad information 5 kap. 2 § lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt ska upphävas.

10.4 Försvarsunderrättelsedomstolen

Försvarsunderrättelsedomstolen prövar frågor om tillstånd till signalspaning i försvarsunderrättelseverksamhet. Bestämmelser om domstolen finns i lagen (2009:966) om Försvarsunderrättelsedomstol och i förordningen (2009:968) med instruktion för Försvarsunderrättelse-domstolen.

10.4.1 Antalet särskilda ledamöter och förordnandetid för vice ordförande och de särskilda ledamöterna

Utkastets förslag: Antalet särskilda ledamöter utökas till högst åtta stycken.

Vice ordförande och särskilda ledamöter förordnas av regeringen för högst fyra år i sänder.

Utredningens förslag överensstämmer delvis med utkastets. Utredningen föreslår inte att antalet särskilda ledamöter utökas.

Remissinstanserna: *Försvarsunderrättelsedomstolen* anser att det högsta antalet särskilda ledamöter vid domstolen bör utökas till tio stycken. Övriga remissinstanser uttalar sig inte särskilt om förslaget.

Skälen för utkastets förslag: En närmare redogörelse för regleringen kring Försvarsunderrättelsedomstolens sammansättning finns i avsnitt 3.3.3. Domstolen består av en ordförande, en eller högst två vice ordförande samt minst två och högst sex särskilda ledamöter. Det är endast ordföranden som är fast anställd i Försvarsunderrättelsedomstolen. Vice ordförande och de särskilda ledamöterna utför uppdraget som ett sidouppdrag. Förordnandetiden för dessa om fyra år bestämdes med hänsyn till att det, inte minst ur sekretessynpunkt, bedömdes finns behov av att få kontinuitet i domstolens verksamhet (prop. 2008/09:201 s. 68–69).

Eftersom Försvarets radioanstalt endast får bedriva signalspaning efter tillstånd av Försvarsunderrättelsedomstolen är det viktigt att det finns ledamöter tillgängliga som kan pröva Försvarets radioanstalts ansökningar. Det är med hänsyn till de mål Försvarsunderrättelse-domstolen prövar ett begränsat antal personer i Sverige som kan vara aktuella för uppdraget som särskild ledamot. För att säkerställa att Försvarsunderrättelsedomstolen också fortsättningsvis kan utföra sitt uppdrag på ett ändamålsenligt och effektivt sätt finns det därför skäl att överväga om åtgärder bör vidtas för att trygga domstolens tillgång till ledamöter.

Ett alternativ som skulle kunna övervägas är att utöka antalet ledamöter, vilket *Försvarsunderrättelsedomstolen* föreslår. Enligt domstolen kan det uppstå behov av en större krets särskilda ledamöter i ett förändrat omvärldsläge, som inte är så allvarligt att den föreslagna lagen om signalspaning i krig eller krigsfara ska tillämpas. Det kan t.ex. vara fråga om fredstida kriser som gör det svårt för de särskilda ledamöterna att ta sig till domstolen eller prioritera domstolens verksamhet. Att utöka möjligheten att förordna fler särskilda ledamöter skulle medföra ett större handlingsutrymme för att snabbt anpassa verksamheten efter nya förhållanden. Hänsyn måste dock härvid tas till att den verksamhet som Försvarsunderrättelsedomstolen bedriver innehåller hemliga och känsliga uppgifter. Fler personer än nödvändigt bör inte få insyn i verksamheten. Vid en samlad bedömning är slutsatsen att antalet ledamöter bör utökas, men att antalet lämpligen bör bestämmas till högst åtta stycken.

En flexibel förordnandetid är också en åtgärd som kan skapa än bättre förutsättningar för Försvarsunderrättelsedomstolens verksamhet. Särskilt i sådana fall där en vice ordförande eller särskild ledamot ska förordnas på nytt och på grund av till exempel ålder eller stundande pensionsavgång har önskemål om en kortare förordnandetid skulle en kortare tid än fyra år kunna övervägas. En mer flexibel förordnandetid skulle då möjliggöra en bibehållen kontinuitet i domstolen om alternativet i stället är att den tidigare förordnade ledamoten avstår från ett nytt förordnande.

Det föreslås därför att förordnandetiden för vice ordförande och särskilda ledamöter ändras från fyra år till högst fyra år. Behovet av kontinuitet, inte minst av sekretesskäl, bör alltjämt vara av stor vikt vid bestämmande av tiden för förordnandet. Utgångspunkten bör därför fortsatt vara att vice ordförande och särskilda ledamöter, i likhet med nuvarande reglering, förordnas för fyra år. Förslaget innebär dock att det finns möjlighet att ta hänsyn till en ledamots behov i det enskilda fallet och i vissa särskilda fall förordna för en kortare tid. Så skulle till exempel kunna vara fallet om en tidigare ledamot ska förordnas på nytt och på

grund av till exempel ålder eller stundande pensionsavgång själv har önskemål om en kortare förordnandetid. I dylika situationer bör det ur sekretessynpunkt vara godtagbart att förordna ledamoten för en kortare period än fyra år.

10.4.2 Förordna och utse integritetsskyddsombud

Utkastets förslag: Integritetsskyddsombud förordnas av regeringen för högst fyra år i sänder.

Bestämmelsen om att förordna ytterligare integritetskyddsombud inom tidsperioden upphävs.

Bestämmelsen om när ett integritetskyddsombud ska utses ändras för att bättre motsvara förutsättningarna för Försvarsunderrättelse-domstolens verksamhet.

Utredningens förslag överensstämmer med utkastets.
Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för utkastets förslag

Förordnande av integritetsskyddsombud

I avsnitt 3.3.3 finns en redogörelse av integritetsombuden vid Försvarsunderrättelsedomstolen och den reglering som är relevant i sammanhanget. Ombuden förordnas alltså för minst fyra år i sänder, och vid behov får under fyraårsperioden ytterligare personer förordnas för återstående del av denna. Systemet med integritetsskyddsombud har utformats enligt systemet med offentligt ombud i ärenden om vissa hemliga tvångsmedel i allmän domstol (prop. 2008/09:201 s. 69–71). En bestämmelse om förordnande av offentliga ombud i sådana ärenden finns i 27 kap. 27 § rättegångsbalken. Av förarbetena till bestämmelsen framgår att systemet har utformats för att de offentliga ombuden ska vara oavhängiga. Utformningen av bestämmelsen följde på att Lagrådet riktade kritik mot lagrådsremissens förslag i denna del, och syftade till att tydliggöra att regeringen inte fritt kan entlediga ett offentligt ombud. Genom att regeringen förordnar dem som ska tjänstgöra som offentligt ombud för en viss period och under denna period kan förordna ytterligare personer för återstående del av perioden så ansåg regeringen att någon särskild föreskrift som gav regeringen möjligt att entlediga ett offentligt ombud inte behövdes (prop. 2002/03:74 s. 25–26).

Det har framkommit att integritetsskyddsombuden förordnas av regeringen för fyra år i sänder, oavsett när i tiden de förordnas. Det förekommer således inte att integritetsskyddsombud förordnas för återstående del av en fyraårsperiod, utan tillkommande ombud förordnas för en egen fyraårsperiod. Det framstår inte som att ordningen på något sätt hindrar integritetsskyddsombudets oberoende. Det saknas därför behov av att särskilt reglera förordnandet av tillkommande integritetsskyddsombud. Bestämmelsen i 6 § första stycket andra meningen lagen om Försvarsunderrättelsedomstol bör därför upphävas.

Förordnandetiden föreslås också ändras så att den överensstämmer med vad utredningen föreslår i fråga om domstolens ledamöter. Även i fråga

om förordnandetiden för integritetsskyddsombud bör dock fortsatt utgångspunkten vara att förordnande sker för fyra år.

Utse integritetsskyddsombud

Av 12 § första stycket lagen om Försvarsunderrättelsedomstol följer att domstolen ska utse ett integritetsskyddsombud i målet så snart som möjligt efter att ansökan kommit in. Försvarets radioanstalt meddelar alltid domstolen innan en ansökan skickas in. Kansliet påbörjar då inbokning av integritetsskyddsombud och särskilda ledamöter till sammanträdet. Integritetsskyddsombudet förordnas sedan formellt i målet i samband med sammanträdet, vilket antecknas i akten. Några särskilda handläggningsåtgärder, såvitt gäller integritetsskyddsombudet, vidtas inte i samband med att ansökan inkommer till domstolen. Bestämmelsen i 12 § första stycket kan dock enligt ordalydelsen tolkas som att det formella förordnandet ska ske redan i samband med att ansökan kommer in, även om integritetsskyddsombudet i praktiken redan har utsetts i samband med inbokningen till sammanträdet.

Det framgår inte av förarbetena till bestämmelsen varför lagstiftaren valt nämnda tidpunkt för att utse integritetsskyddsombud. Som konstaterats ovan har dock systemet med integritetsskyddsombud utformats enligt bestämmelserna om offentligt ombud i ärenden om vissa hemliga tvångsmedel i allmän domstol. Det kan konstateras att 12 § första stycket lagen om Försvarsunderrättelsedomstol har likheter med 27 kap. 28 § rättegångsbalken som reglerar allmän domstols handläggning i ärenden om vissa hemliga tvångsmedel. Av förarbeten till bestämmelsen i rättegångsbalken följer att bestämmelsen utformats efter Lagrådets synpunkter. Utformningen av bestämmelsen tar sikte på att tillgodose att det finns ett förordnat offentligt ombud också i sådana brådskande förfaranden där sammanträde äger rum utan att ett offentligt ombud är närvarande (prop. 2002/03:74 s. 27 och 102).

En möjlighet att i brådskande situationer hålla sammanträde utan att ett integritetsskyddsombud närvarar finns i 12 § andra stycket lagen om Försvarsunderrättelsedomstol. Ett integritetsskyddsombud ska i sådana fall ha rätt att ta del av handlingar i efterhand (prop. 2008/09:201 s. 71). En skillnad mellan de olika systemen är att det inte går att överklaga Försvarunderrättelsedomstolens domar och beslut. Ett offentligt ombud har således en tillkommande uppgift som integritetsskyddsombudet saknar och det är naturligtvis nödvändigt att det offentliga ombudet förordnas och får del av handlingarna innan överklagandetiden löper ut. Integritetsskyddsombudet ska emellertid, om ombudet uppmärksammar missförhållanden, påtala det för Riksdagens ombudsmän och Justitiekanslern (prop. 2008/09:201 s. 71). Detta är dock till skillnad från ett överklagande inte begränsat i tid.

Försvarsunderrättelsedomstolen hanterar i sin verksamhet i princip uteslutande känsliga och hemliga uppgifter. Inga handlingar skickas av säkerhetsskyddsskäl ut inför sammanträdena. Det framstår därför som såväl lämpligt som ändamålsenligt att utse integritetsskyddsombuden i samband med sammanträdet, i stället för så snart som möjligt efter att ansökan kommit in. Såvitt kan bedömas påverkar inte handläggning i denna del integritetsskyddsombudens möjlighet att bevaka enskildas

integritetsintresse i målet. Bestämmelsen om när ett integritetsskyddsombud utses i målet bör därför förtydligas så att den bättre motsvarar Försvarsunderrättelsedomstolens faktiska handläggning i denna del.

Bestämmelsen i 12 § tredje stycket lagen om Försvarsunderrättelsedomstol bör vidare utformas på sådant sätt, att den möjliggör att det finns ett utsett integritetsskyddsombud som kan ta del av handlingar inom ramen för det brådskande förfarandet i 12 § andra stycket samma lag. Även om det inte finns några tidsfrister att beakta ligger det i sakens natur att så sker i nära anslutning till sammanträdet.

10.4.3 Underrättelse till integritetsskyddsombud efter beslut från ordföranden

Utkastets förslag: Om förordnandet för ett integritetsskyddsombud upphört ska ett annat integritetsskyddsombud kunna underrättas om ordförandens beslut i fråga om tillgång till signalbärare eller användning av sökbegrepp i pågående och tillståndsprövade inhämtningsuppdrag.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för utkastets förslag: Enligt 5 a § tredje stycket signalspaningslagen ska särskilt tillstånd sökas om det för fullgörande av inhämtningsuppdrag för vilket tillstånd givits uppstår behov av tillgång till ytterligare signalbärare eller användning av andra tillståndspliktiga sökbegrepp. Ordföranden i Försvarsunderrättelsedomstolen får på domstolens vägnar fatta beslut om tillstånd i pågående och tillståndsprövade inhämtningsuppdrag, om prövningen är av enkel beskaffenhet och endast avser tillgång till signalbärare eller användning av sökbegrepp som inte är direkt hänförliga till viss fysisk person, enligt 10 § första stycket 2 lagen om Försvarsunderrättelsedomstol. Enligt 12 § tredje stycket samma lag ska vid sådana beslut det integritetsskyddsombud som närvarade vid prövningen av den ursprungliga ansökan till vilken beslutet är hänförlig underrättas. Om domstolen i andra fall prövar frågor om tillstånd i pågående och tillståndsprövade inhämtningsuppdrag ska sammanträde hållas (13 §).

Integritetsskyddsombud ska säkerhetsprövas (3 kap. 1 § säkerhetsskyddslagen [2018:585]). Säkerhetsprövningen ska följas upp under den tid som deltagandet i den säkerhetskänsliga verksamheten pågår och bland annat ska registerkontroll göras, varvid uppgifter löpande ska hämtas under den tid deltagandet i den säkerhetskänsliga verksamheten pågår (3 kap. 3 och 14 §§ samma lag).

När integritetsskyddsombudets förordnande upphör avslutas normalt säkerhetsprövningen och den kontinuerliga registerkontrollen. Det innebär att ombudet inte längre kan ta del av säkerhetsskyddsklassificerade uppgifter. För det fall integritetsskyddsombudets uppdrag har upphört framstår det av säkerhetsskyddsskäl som olämpligt att han eller hon underrättas enligt 12 § tredje stycket lagen om Försvarsunderrättelsedomstol.

En ansökan om tillstånd till ytterligare signalbärare eller sökbegrepp kan ske under tillståndsperioden om högst sex månader. Bestämmelsen om underrättelse till integritetsskyddsombudet kan således komma att tillämpas under hela tillståndsperioden. För att möjliggöra att ett integritetsskyddsombud kan ta del av säkerhetsskyddsklassificerade uppgifter efter att förordnandet upphört skulle säkerhetsprövningen behöva fortgå även efter det att förordnandet upphört. Detta skulle i sådant fall behöva ske i fråga om samtliga integritetsombud efter att deras förordnande upphör, eftersom det inte är möjligt att i förväg veta om det kommer uppstå behov av underrättelse enligt 12 § tredje stycket lagen om Försvarsunderrättelsedomstol. Det framstår inte som en lämplig ordning. Det finns därför skäl att överväga om bestämmelsen om vilket integritetsskyddsombud som ska underrättas bör ändras.

I syfte att begränsa spridningen av hemligt och känsligt material torde det i regel vara lämpligast att det ombud som närvarade vid prövningen av den ursprungliga ansökan underrättas. Om ett integritetsskyddsombuds förordnande har upphört bör det emellertid vara lämpligare ur sekretess- och säkerhetsskyddsynpunkt att ett annat, förordnat integritetsskyddsombud underrättas.

Frågan är om integritetsskyddsombudets uppgift att bevaka enskildas intressen påverkas av en ändring av bestämmelsen.

Integritetsskyddsombudets uppgift är att bevaka enskildas integritetsintresse i mål vid domstolen. Uppdraget handlar om att bevaka enskildas intressen i allmänhet. Integritetsskyddsombudet företräder alltså inte någon särskild person (prop. 2008/09:201 s. 118). Eftersom uppdraget inte är knutet till en viss person kan det argumenteras för att det inte är nödvändigt att underrätta samma ombud som närvarade vid den ursprungliga ansökan. Det finns inte heller någon motsvarande bestämmelse om vilket integritetsskyddsombud som ska närvara vid prövning av frågor om tillstånd i pågående och tillståndsprövade inhämtningsuppdrag som sker vid sammanträde. I förarbetena anges att det inte finns något hinder mot att samma integritetsskyddsombud anlitas i flera mål som har samband med varandra, till exempel vid en begäran om att tillstånd ska avse tillgång till ytterligare signalbärare eller användning av andra sökbegrepp (prop. 2008/09:201 s. 120).

Vid prövningen vid ett sammanträde kan dock omständigheterna till viss del anses skilja sig åt eftersom integritetsskyddsombudet då har rätt att yttra sig. Vid underrättelse enligt 12 § tredje stycket lagen om Försvarsunderrättelsedomstol får integritetsskyddsombudet i stället ta del av handlingarna i efterhand. Det får integritetsskyddsombudet också göra när domstolen prövat en ansökan vid ett sammanträde utan att ett integritetsskyddsombud närvarat eller yttrat sig, enligt 12 § andra stycket lagen om Försvarsunderrättelsedomstol. I det sistnämnda fallet har i tidigare förarbeten uttalats att för det fall integritetsskyddsombudet uppmärksammar missförhållanden är det en naturlig följd av uppdraget att han eller hon påtalar det för Riksdagens ombudsmän eller Justitiekanslern (prop. 2008/09:201 s. 71). Motsvarande torde anses vara gällande för det fall ett ombud efter underrättelse uppmärksammar missförhållanden. Omständigheten att integritetsskyddsombudet tar del av handlingarna i efterhand utgör inte ett hinder mot ombudets möjligheter att utföra sitt uppdrag.

Den nuvarande regleringen framstår av säkerhetsskyddsskäl inte som lämplig. Det bör vid underrättelse enligt 12 § tredje stycket lagen om Försvarsunderrättelsedomstol då ett integritetsskyddsombuds förordnande upphört vara möjligt att underrätta ett annat integritetsskyddsombud än det som närvarade vid den ursprungliga prövningen. Ett annat ombud bedöms ha fullgoda möjligheter att bevaka enskildas integritetsintresse även om han eller hon inte närvarade vid prövningen av den ursprungliga ansökan. Det föreslås därför att bestämmelsen ändras på så sätt att den möjliggör underrättelse till ett annat förordnat integritetsskyddsombud när förordnandet upphört för det integritetsskyddsombud som närvarade vid prövningen av den ursprungliga ansökan.

10.4.4 Deltagande i verksamheten efter att integritetsskyddsombudets förordnande upphört

Utkastets förslag: Bestämmelsen om att integritetsskyddsombudet efter att förordnandet upphört får slutföra pågående uppdrag upphävs.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna uttalar sig inte särskilt över förslaget.

Skälen för utkastets förslag: Ett integritetsskyddsombud får, trots att förordnandet upphört, slutföra pågående uppdrag (6 § fjärde stycket lagen om Försvarsunderrättelsedomstol). Systemet med integritetsskyddsombud är som tidigare nämnts utformat efter systemet för offentliga ombud som företräder enskildas integritetsintresse i ärenden om vissa hemliga tvångsmedel, och en liknande regel finns i 27 kap. 27 § fjärde stycket rättegångsbalken.

I den verksamhet som Försvarsunderrättelsedomstolen bedriver behandlas uteslutande hemliga och känsliga uppgifter. Bestämmelsen om att ett integritetsskyddsombud får slutföra pågående uppdrag trots att förordnandet har upphört är därför av säkerhetsskyddsskäl problematisk, eftersom bland annat den kontinuerliga registerkontrollen då har upphört.

Som tidigare angetts utser Försvarsunderrättelsedomstolen integritetsskyddsombud för målet i samband med sammanträdet. Utifrån detta kan det inte uppstå någon period mellan det att ombudet utses och att ansökan prövas där det kan uppstå behov för ett ombud vars förordnande upphört att slutföra sitt uppdrag. Såvitt framkommit uppstår det inte heller behov av att tillämpa bestämmelsen med hänsyn till sammanträdenas längd eller liknande. Det är endast vid underrättelse enligt 12 § tredje stycket lagen om Försvarsunderrättelsedomstol som det kan finnas behov av att tillämpa bestämmelsen. Eftersom det föreslås en ändring av den bestämmelsen finns det inte heller vid sådan underrättelse anledning att tillämpa bestämmelsen.

Tillämpningen av bestämmelsen om att integritetsskyddsombudet får slutföra pågående uppdrag trots att regeringens förordnande har upphört framstår som olämplig av säkerhetsskyddsskäl. Såvitt framkommit fyller inte bestämmelsen någon praktisk funktion eftersom någon situation där bestämmelsen kan behöva tillämpas inte kan uppstå. Bestämmelsen bör därför upphävas. Mot bakgrund av att regeringen förordnar integritetsskyddsombuden för viss tid, och således inte utan godtagbara skäl kan

entlediga ett integritetsskyddsombud under pågående förordnande, bedöms förslaget inte påverka integritetsskyddsombudets oberoende.

10.4.5 Beslut om ersättning till integritetsskyddsombud

Utkastets förslag: Ordföranden får ensam fatta beslut om ersättning till integritetsskyddsombud.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna har inte några synpunkter på förslaget.

Skälen för utkastets förslag: Ett integritetsskyddsombud har rätt till ersättning. Enligt 7 § lagen om Försvarsunderrättelsedomstol ska i fråga om ersättning till integritetsskyddsombud 21 kap. 10 § första och andra styckena rättegångsbalken tillämpas. Av författningskommentaren till bestämmelsen framgår att ombudet ska yrka ersättning för varje enskilt mål och att det är rätten som fattar beslut om ersättning.

Enligt 10 § första stycket lagen om Försvarsunderrättelsedomstol får ordföranden ensam vidta vissa åtgärder. Bestämmelsen anger, enligt förarbetena, i vilken utsträckning som den som tjänstgör som ordförande får vidta vissa åtgärder. Om ordföranden är förhindrad att tjänstgöra, inträder en vice ordförande i ordförandens ställe (4 §).

Det har framkommit att det med hänsyn till den verksamhet som domstolen bedriver varken är praktiskt eller lämpligt att rätten fattar beslut om ersättning. Ordföranden bör därför ensam på domstolens vägnar få fatta beslut om ersättning till integritetsskyddsombuden och det föreslås att en bestämmelse med sådan innebörd införs i 10 § första stycket lagen om Försvarsunderrättelsedomstol. Det har inte framkommit att det är nödvändigt för att bedöma skäligheten av integritetsskyddsombudets yrkade ersättning att det är den som tjänstgjort som ordförande vid rättens prövning som också fattar beslut om ersättningen. För att underlätta en effektiv och ändamålsenlig hantering av integritetsskyddsombudens ersättningsanspråk bör det därför inte uppställas något krav på att det är den som tjänstgjort som ordförande vid rättens prövning av ett enskilt mål som också ska fatta beslut om integritetsskyddsombudets ersättning i målet. I normalfallet torde det dock vara ordföranden i Försvarsunderrättelsedomstolen som deltar i rättens prövning av ansökan om tillstånd och vid ett senare tillfälle fattar beslut om ersättning till det integritetsskyddsombud som närvarat vid sammanträdet.

11 Ikraftträdande- och övergångsbestämmelser

Utkastets förslag: De föreslagna ändringarna ska träda i kraft den 1 juni 2026.

Utkastets bedömning: Det finns inte behov av några särskilda övergångsbestämmelser.

Utredningens förslag och bedömning överensstämmer delvis med utkastets. Utredningen föreslår ett annat datum för ikraftträdande.

Remissinstanserna: *Försvarets radioanstalt* instämmer i utredningens förslag och bedömning. Övriga remissinstanser yttrar sig inte i denna del.

Skälen för utkastets förslag och bedömning: Med hänsyn bland annat till det rådande säkerhetspolitiska läget är det angeläget att den nya lagen och övriga lagändringar kan träda i kraft så snart som möjligt. De bör lämpligen träda i kraft den 1 juni 2026.

Förslagen bedöms inte medföra några behov av övergångsbestämmelser.

12 Konsekvenser

Utkastets bedömning: De kostnadsökningar som förslagen kan medföra för berörda myndigheter kan finansieras inom befintliga ekonomiska ramar. Förslagen medför inga ökade kostnader för det allmänna i övrigt eller för enskilda.

De konsekvenser som förslagen kan medföra för den personliga integriteten är proportionerliga.

Utredningens bedömning överensstämmer med utkastets.

Remissinstanserna: *Sveriges advokatsamfund* anser att utredningen inte har gjort tillräckliga analyser kring integritets-, cyber-, informations- och rättssäkerhetsfrågor. *Föreningen för Digitala Fri- och Rättigheter* för fram liknande synpunkter och ifrågasätter förslagens proportionalitet samt efterlyser en jämförelse med andra EU-länders lagstiftning.

Centrum för rättvisa anför att eftersom det föreslås ytterligare utvidgningar av Försvarets radioanstalts verksamhet bör Sverige skyndsamt åtgärda de kvarstående brister i lagstiftningen på området som Europadomstolen identifierade i målet Centrum för rättvisa mot Sverige. *Tjänstemännens centralorganisation (TCO)* för fram liknande synpunkter.

Polismyndigheten framhåller att det är av stor vikt att förslaget om att Inspektionen för strategiska produkter ska få inrikta signalspaning i försvarsunderrättelseverksamhet inte medför sådana befarade undanträngningseffekter som kan riskera att påverka Polismyndigheten negativt. *Säkerhetspolisen* pekar på att det finns en konkret risk för undanträngningseffekter i och med att Försvarets radioanstalt inte föreslås få några utökade anslag för den utvidgade inriktningsrätten.

Försvarsmakten för fram en liknande synpunkt och föreslår att Försvarets radioanstalt tillförs medel för att detta ska undvikas. Även *Försvarets radioanstalt* pekar på risken för undanträngningseffekter, som inte är av tillfällig karaktär. Det anförs även att flera av utredningens förslag förutsätter att myndighetens verksamhet utvecklas och behöver byggas upp i vissa delar, vilket kommer innebära kostnadsökningar.

Statens inspektion för försvarsunderrättelseverksamheten framhåller att för det fall förslagen innebär ändrade förutsättningar för inspektionens kontroll måste ytterligare resurser tillföras myndigheten.

Skälen för utkastets bedömning

Konsekvenser för Försvarets radioanstalt

Förslaget om en ny lag om signalspaning i försvarsunderrättelseverksamhet i krig och krigsfara bedöms inte komma att medföra några kostnadsökningar som inte ryms inom ramen för befintlig ekonomisk ram.

I fråga om förslaget om signalspaning i övningsverksamhet är det en ny verksamhet för Försvarets radioanstalt. Eftersom det är en ny verksamhet, som i stor utsträckning kommer bedrivas i samverkan med Försvarsmakten, finns det vissa osäkerhetsfaktorer i fråga om i vilken omfattning som verksamheten i vart fall inledningsvis kommer att bedrivas. De kostnader som förslagen i denna del kan komma att medföra bör kunna rymmas inom Försvarets radioanstalts befintliga ekonomiska ramar.

Förslaget om att Inspektionen för strategiska produkter (ISP) ska få inrikta signalspaning i försvarsunderrättelseverksamhet innebär att ytterligare en myndighet ges rätt att inrikta sådan verksamhet. Mot bakgrund av att Försvarets radioanstalts signalspaningsverksamhet är en begränsad resurs kommer en ytterligare inriktande myndighet att innebära att Försvarets radioanstalt, i vart fall inledningsvis, framför allt kommer att behöva göra prioriteringar mellan de inriktande myndigheterna. Den främsta konsekvensen består av undanträngningseffekter, vilket riskerar att drabba de myndigheter som i dag får inrikta sådan verksamhet negativt. Även om en ytterligare inriktande myndighet skulle innebära en viss utökning av verksamheten bör de kostnadsökningar som förslaget kan medföra kunna finansieras inom Försvarets radioanstalts befintliga ekonomiska ramar.

Förslagen i övrigt syftar i stor utsträckning till att den lagstiftning som reglerar Försvarets radioanstalts signalspaningsverksamhet ska blir mer modern och ändamålsenlig. Övriga förslag som lämnas bedöms inte medföra några kostnadsökningar för Försvarets radioanstalt.

Konsekvenser för Försvarsunderrättelsedomstolen

Förslaget om att Försvarets radioanstalt ska få bedriva signalspaning i övningsverksamhet kan komma att innebära en viss ökning av antalet ansökningar till domstolen. Även förslaget om en ny inriktande myndighet skulle kunna innebära en viss ökning av antalet ansökningar. De eventuella kostnadsökningar som detta kan innebära bör kunna finansieras inom myndighetens befintliga ekonomiska ramar.

Förslagen i övrigt, bland annat i fråga om ändringar i lagen (2009:966) om Försvarsunderrättelsedomstol, bedöms inte medföra några kostnadsökningar för Försvarsunderrättelsedomstolen.

Konsekvenser för Statens inspektion för försvarsunderrättelseverksamheten

Det föreslås att upptagningar eller uppteckningar som inhämtats vid signalspaning i övningsverksamhet ska förstöras så snart de inte längre är av relevans för övningsverksamheten. För att genomföra efterhandskontrollen i den delen på ett ändamålsenligt sätt kan den behöva genomföras på ett annat sätt än efterhandskontrollen annars genomförs. De kostnadsökningar som förslagen kan komma att medföra för Statens inspektion för försvarsunderrättelseverksamheten bör kunna rymmas inom ramen för myndighetens befintliga ekonomiska ramar.

Konsekvenser för andra myndigheter

De kostnadsökningar som förslaget om att ISP ska få inrikta signalspaning i försvarsunderrättelseverksamhet kan komma att innebära för ISP bör kunna rymmas inom myndighetens befintliga ekonomiska ramar.

För de myndigheter som i dag inriktar signalspaning i försvarsunderrättelseverksamhet – regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten – bedöms förslaget, som nämns ovan, framför allt medföra undanträngningseffekter. Eventuella kostnadsökningar som detta skulle kunna medföra bedöms rymmas inom myndigheternas befintliga ekonomiska ramar.

Förslaget om ett undantag från förbudet mot inhämtning av inhemsk trafik i vissa brådskande situationer bedöms i viss utsträckning kunna förbättra Säkerhetspolisens och Polismyndighetens förmåga att identifiera och motverka hot mot Sveriges säkerhet, bl.a. i form av brottslig verksamhet som innefattar terrorbrott. Samma resonemang kan anläggas gällande förslaget om en anpassad ändamålsbestämmelse i signalspaningslagstiftningen.

Förslagen bedöms inte medföra några kostnadsökningar för andra statliga myndigheter.

Konsekvenser för enskilda

I anslutning till vissa av förslagen behandlas vilka konsekvenser för den personliga integriteten som förslagen bedöms få. Det gäller för förslagen om signalspaning i krig och krigsfara (avsnitt 5), signalspaning i övningsverksamhet (avsnitt 7), inhämtning av inhemsk trafik i vissa brådskande situationer och undantag från förstöringsskyldigheten i sådana situationer samt en anpassad ändamålsbestämmelse (avsnitt 8), upphävande av bestämmelser om underrättelseskyldigheten (avsnitt 10.3) samt ändringar avseende integritetsskyddsombuden (avsnitt 10.4.2–10.4.4). De konsekvenser för enskildas personliga integritet som förslagen kan medföra är proportionerliga sett till syftena med förslagen, vilka bland annat är att skydda civilbefolkningen i händelse av krig och krigsfara och att i brådskande situationer skydda enskilda människors liv och hälsa.

Därutöver lämnas förslag om att signaler i elektronisk form ska få inhämtas oavsett var de befinner sig. Förslaget innebär ett förtydligande i lag. Förslaget bidrar till att tydliggöra inhämtningens omfattning. Det lämnas också förslag om följdändringar som syftar till att tillgodose att förtydligandet inte leder till ett försämrat skydd för den personliga integriteten. Det föreslås också att en ny inriktande myndighet ska få rätt att inrikta signalspaning i försvarsunderrättelseverksamhet och att det införs en ny ändamålsbestämmelse. Förslagen innebär att inhämtningen får ske för att kartlägga en ytterligare företeelse, vilket skulle kunna innebära en viss ökad inhämtning. För de övriga förslag som lämnas gäller, i likhet med all annan inhämtning, att de bestämmelser i signalspaningslagstiftningen som syftar till att värna enskildas integritetsskyddsintressen och skydda enskilda från otillbörliga intrång i den personliga integriteten ska tillämpas. Sammantaget bedöms att de konsekvenser som förslagen i dessa delar kan medföra för enskilda är proportionerliga. Det anses även, till skillnad från *Sveriges advokatsamfund* och *Föreningen för Digitala Fri- och Rättigheter*, att utredningen har beaktat relevanta frågor om personlig integritet och rättssäkerhet samt cyber- och informationssäkerhetsfrågor på ett väl avvägt sätt. Det kan i detta sammanhang framhållas att Försvarets radioanstalt i sin verksamhet har att beakta tillämpliga bestämmelser om bl.a. sekretess, säkerhetsskydd och dataskydd vid sin behandling av uppgifter. Myndigheten har mycket goda förutsättningar att upprätthålla de krav som ställs enligt sådana regelverk. Några vidare jämförelser med andra länders regelverk än de som utredningen har redovisat är inte heller behövliga.

Beträffande frågan om de brister i den svenska lagstiftningen om och tillämpningen av signalspaning i försvarsunderrättelseverksamhet som Europadomstolen har identifierat genom sitt avgörande i målet Centrum för rättvisa mot Sverige [GC] har dessa behandlats i propositionen Signalspaning i försvarsunderrättelseverksamhet – åtgärder med anledning av Europadomstolens dom (prop. 2023/24:136). Till skillnad från vad *Centrum för rättvisa* och *TCO* anför bedöms identifierade brister ha tagits om hand genom de författningsändringar som skett med anledning av den propositionen. Några ytterligare folkrättsliga avvägningar utöver de som har gjorts är inte heller behövliga utifrån de nu aktuella förslagens beskaffenhet.

Ingenting har framkommit som tyder på kostnadsökningar för de trådägande operatörerna som en följd av förslaget om en ytterligare inriktande myndighet eller av någon av de andra förslagen. Förslagen i övrigt medför inte heller några ekonomiska konsekvenser för enskilda.

Övriga konsekvenser

Förslagen bedöms inte påverka
- den kommunala självstyrelsen,
- sysselsättning och offentlig service i olika delar av landet,
- små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags,
- jämställdheten mellan kvinnor och män, eller
- möjligheten att nå de integritetspolitiska målen.

Förslagen bedöms inte heller i övrigt medföra några konsekvenser av betydelse.

13 Författningskommentar

13.1 Förslaget till lag om signalspaning i försvarsunderrättelseverksamhet i krig eller krigsfara

Lagens tillämpning

1 § Om Sverige är i krig ska 5–14 §§ tillämpas.

I paragrafen anges att de särskilda beredskapsbestämmelserna ska tillämpas automatiskt om Sverige kommer i krig. Övervägandena finns i avsnitt 5.5.2.

I 5–14 §§ finns särskilda bestämmelser som innebär att regelverket för signalspaning i försvarsunderrättelseverksamhet anpassas för att möta behoven under krig. Dessa beredskapsbestämmelser ska tillämpas om Sverige kommer i krig.

Bestämmelserna i lagen ska tillämpas automatiskt om Sverige kommer i krig. Det utgör en garanti för att reglerna sätts i funktion vid ett krigsutbrott, även om regeringen av någon anledning skulle vara förhindrad att förklara att krigstillstånd har inträtt. Huvudregeln är dock att regeringen ger till känna att Sverige är i krig.

Det har i förarbetena till regeringsformen uttalats att det inte är möjligt att i vare sig lag- eller motivtext närmare ange vilka slags handlingar eller händelser som ska anses innebära att krigstillstånd råder. Krig ska dock alltid anses föreligga om landet är helt eller delvis ockuperat (se prop. 1973:90 s. 373 och 446 f. samt prop. 2009/10:80 s. 204).

2 § Om Sverige är i krigsfara eller om det råder sådana extraordinära förhållanden som är föranledda av krig eller av krigsfara som Sverige har befunnit sig i, får regeringen meddela föreskrifter om att 5–14 §§ helt eller delvis ska tillämpas från den tidpunkt som regeringen bestämmer.

En sådan föreskrift ska underställas riksdagen inom en månad från utfärdandet. Föreskriften upphör att gälla, om den inte underställs riksdagen i rätt tid eller om riksdagen inte godkänner den inom två månader från det att den underställdes.

I paragrafen anges förutsättningarna för att tillämpa lagens beredskapsbestämmelser i andra situationer än krig och att sådana föreskrifter ska underställas riksdagen inom viss tid. Övervägandena finns i avsnitt 5.5.2.

Av *första stycket* framgår att regeringen får föreskriva att 5–14 §§ ska tillämpas om Sverige är i krigsfara eller om det råder extraordinära förhållanden. Dessa situationer överensstämmer med riksdagens möjlighet att delegera normgivningskompetens till regeringen enligt 15 kap. 6 § regeringsformen. Regeringen kan, utifrån de förhållanden som råder, välja

om 5–14 §§ ska tillämpas i sin helhet eller endast delar därav. Regeringen har att, utifrån sitt konstitutionella ansvar, pröva om situationen kräver en viss åtgärd.

Av *andra stycket* framgår att föreskrifter som meddelats med stöd av första stycket ska underställas riksdagen inom en månad från utfärdandet. Om så inte sker, eller om riksdagen inte godkänner föreskriften inom två månader från underställningen, så upphör föreskriften att gälla.

3 § Under den tid som 5–14 §§ tillämpas gäller dessa bestämmelser, eller föreskrifter som meddelats med stöd av dem, i stället för avvikande bestämmelser i någon annan lag eller författning.

Regeringen ska föreskriva att bestämmelserna i 5–14 §§ inte ska tillämpas, när det inte längre råder sådana förhållanden som avses i 1 § eller 2 § första stycket.

I *första stycket* anges att lagens beredskapsbestämmelser och föreskrifter som har meddelats med stöd av bemyndigandena i lagen har företräde i den mån de avviker från bestämmelser i någon annan lag eller föreskrift. Sådana bestämmelser finns i första hand i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet och i lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt.

Av *andra stycket* framgår att regeringen ska förordna om att lagens beredskapsbestämmelser inte längre ska tillämpas när Sverige inte längre är i krig eller när den krigsfara eller de extraordinära förhållanden som har föranlett att regeringen aktiverat bestämmelser i lagen har upphört. Bestämmelsen innebär således att beredskapsbestämmelserna inte automatiskt upphör att gälla.

Övervägandena finns i avsnitt 5.5.1 och 5.5.2.

4 § Med signalspaningsmyndighet och kontrollmyndighet i denna lag avses de myndigheter som anges i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Av paragrafen följer att signalspaningsmyndigheten och kontrollmyndigheten i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet också är signalspaningsmyndighet och kontrollmyndighet i denna lag. Övervägandena finns i avsnitt 5.5.1.

Signalspaningens omfattning

5 § Bestämmelsen i 2 a § första stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, om att inhämtning inte får avse signaler mellan en avsändare och mottagare som båda befinner sig i Sverige, ska inte tillämpas om sådan inhämtning är av betydelse för att hantera yttre hot mot Sveriges säkerhet.

I paragrafen anges ett undantag från 2 a § första stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet. Övervägandena finns i avsnitt 5.5.3.

Paragrafen innebär att signaler som sänds mellan en avsändare och en mottagare som båda befinner sig i Sverige får inhämtas, om sådan inhämtning är av betydelse för att hantera yttre hot mot Sveriges säkerhet. Bestämmelsen är avsedd att tillämpas i fråga om fientlig verksamhet som tar sin utgångspunkt från icke militära plattformar och strukturer. Sådan

fientlig verksamhet kan ha sin utgångspunkt inom exempelvis politiska och diplomatiska, psykologiska och informationsmässiga, underrättelseinhämtande och krigsförberedande åtgärder.

Med uttrycket ”yttre hot” avses att det är fråga om företeelser från främmande makt eller annan antagonistisk aktör.

Uttrycket ”Sveriges säkerhet” tar, i enlighet med vad som uttalas i propositionerna Förstärkt skydd mot främmande makts underrättelseverksamhet (prop. 2013/14:51) och Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag (prop. 2017/18:89), sikte på förhållanden av grundläggande betydelse för Sverige. Uttrycket kan enligt tidigare förarbetsuttalanden sammanfattas som skyddet för Sveriges oberoende – i betydelsen självständighet och suveränitet – och bestånd. Det innefattar en rätt till okränkta landsgränser, ett bevarande av det svenska självstyret och det demokratiska statsskicket samt av nationens grundläggande funktionalitet. Uttrycket tar således inte enbart sikte på skyddet av det fysiska territoriet. Det avser också hävdandet av Sveriges suveränitet, vilket innebär att Sverige ska kunna bruka sin exklusiva frihet under det folkrättsliga regelverket, för att på det egna territoriet självständigt utöva statens funktioner, såväl vad avser statens inre som yttre förbindelser. Vad som är av betydelse för Sveriges säkerhet kan förändras över tid, bland annat i takt med samhällsutvecklingen. Tidigare var begreppet starkt förknippat med Försvarsmaktens verksamhet, eftersom det främsta hotet mot rikets säkerhet ansågs vara ett militärt angrepp. I dag är samhället och hotbilden mer komplex och föränderlig, vilket i sin tur har fört med sig att uppgifter hänförliga till förhållanden inom andra samhällssektorer kan vara av betydelse för Sveriges säkerhet (se prop. 2013/14:51 s. 36).

Inriktning

6 § Regeringen får meddela föreskrifter om att någon annan myndighet än de som anges i 4 § första stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet får inrikta signalspaning i försvarsunderrättelseverksamhet.

Regeringen får också besluta om detta i ett enskilt fall.

I paragrafen regleras inriktning av signalspaning i försvarsunderrättelseverksamhet i krig och krigsfara. Övervägandena finns i avsnitt 5.5.4.

Av paragrafen framgår att regeringen genom föreskrift i förordning eller i ett enskilt fall kan besluta om att ytterligare myndigheter får inrikta signalspaning i försvarsunderrättelseverksamhet. Paragrafen innebär att andra myndigheter än de som anges i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet kan ges rätt att inrikta denna signalspaning. Det ankommer på regeringen att i det enskilda fallet avgöra om situationen är sådan att ytterligare myndigheter bör få inrikta sådan verksamhet. Det ankommer också på regeringen att avgöra om ytterligare myndigheters inriktningsrätt ska anges i förordning eller i ett beslut. Ett beslut kommer med stor sannolikhet att omfattas av sekretess till skillnad från en förordning. Beroende på förhållandena i den vid tillfället rådande

situationen kan det finnas skäl att för exempelvis främmande makt inte röja om andra myndigheter ges inriktningsrätt.

Tillstånd

7 § Tillstånd till signalspaning enligt 1 och 1 a §§ lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet får ges av den befattningshavare vid signalspaningsmyndigheten som regeringen föreskriver.

Tillstånd enligt första stycket får endast lämnas om förutsättningarna för tillstånd enligt 5 § lagen om signalspaning i försvarsunderrättelseverksamhet är uppfyllda.

Paragrafen innehåller bestämmelser om tillståndsförfarandet. Övervägandena finns i avsnitt 5.5.5.

Av *första stycket* följer att tillstånd får ges av den befattningshavare vid Försvarets radioanstalt som regeringen föreskriver. Det ankommer således på regeringen att i förordning anvisa vilken eller vilka befattningshavare som ska ha rätt att fatta beslut om signalspaning i försvarsunderrättelseverksamhet. För att möjliggöra en effektiv och ändamålsenlig signalspaning i försvarsunderrättelseverksamhet under de särskilda förhållande som råder bör det i vart fall finnas fler än två befattningshavare som kan fatta beslut. Om bestämmelsen tillämpas innebär den alltså att Försvarsunderrättelsedomstolen inte ska pröva ansökningar om tillstånd.

I *andra stycket* anges att bestämmelserna om under vilka förutsättningar som tillstånd får lämnas i 5 § lagen om signalspaning i försvarsunderrättelseverksamhet ska vara uppfyllda för att tillstånd ska få lämnas. Det är således samma krav som ska tillämpas under krigsförhållanden som i fredstid.

8 § Tillstånd enligt 7 § ska utformas enligt 5 a § första och andra styckena lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Om det för fullgörande av inhämtningsuppdrag för vilket tillstånd getts uppstår behov av tillgång till ytterligare signalbärare eller användning av andra tillståndspliktiga sökbegrepp, gäller 5 a § tredje stycket lagen om signalspaning i försvarsunderrättelseverksamhet i tillämpliga delar.

Paragrafen innehåller bestämmelser om tillståndsförfarandet. Övervägandena finns i avsnitt 5.5.5.

Av *första stycket* följer att tillstånd ska utformas i enlighet med bestämmelserna i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Av *andra stycket* framgår att bestämmelser i lagen om signalspaning i försvarsunderrättelseverksamhet ska tillämpas i tillämpliga delar om det uppstår behov av ytterligare signalbärare eller tillståndspliktiga sökbegrepp i ett pågående inhämtningsuppdrag.

Rådighet över signalbärare

9 § Signalspaningsmyndigheten ska ha rådigheten över signalbärare innehållande sådana signaler som överförs i enlighet med bestämmelser som avses i 12 § första stycket lagen (2008:717) om signalspaning i försvarsunderrättelse-verksamhet.

Signalspaningsmyndigheten ska begränsa sin tillgång till signalbärare till vad som följer av tillstånd enligt 7 §.

I paragrafen regleras rådigheten över signalbärare. Övervägandena finns i avsnitt 5.5.6.

Första stycket innebär att om bestämmelsen tillämpas på grund av att Sverige är i krig eller för att regeringen enligt 2 § första stycket meddelat föreskrifter om att den ska tillämpas, ska Försvarets radioanstalt ha rådigheten över signalbärarna. Bestämmelsen innebär alltså att kontrollmyndigheten inte ska ha rådigheten över signalbärare.

Av *andra stycket* följer att Försvarets radioanstalt ska begränsa sin tillgång till signalbärarna så att myndigheten endast har tillgång till de signalbärare som följer av tillstånd enligt 7 §.

Överföring av personuppgifter till en mottagare utomlands

10 § Regeringen får meddela föreskrifter eller i ett enskilt fall besluta att personuppgifter som behandlas enligt lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt får överföras till ett annat land eller en internationell organisation även om förutsättningarna i 2 kap. 20 § första stycket 3 den lagen inte är uppfyllda.

I paragrafen ges möjlighet att göra undantag från ett av de villkor som uppställs för att en överföring av personuppgifter till ett annat land eller en internationell organisation ska vara tillåten. Övervägandena finns i avsnitt 5.5.8.

Enligt 2 kap. 20 § första stycket 3 lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt ska mottagaren garantera tillräckligt skydd för personuppgifterna. Det är Försvarets radioanstalt som ska göra en sammanvägd bedömning av om det mottagande landet eller organisationen erbjuder tillräckligt skydd för personuppgifterna innan en överföring får ske. Försvarets radioanstalt ska bedöma alla omständigheter kring överföringen och komma till slutsatsen att skyddsåtgärderna är tillräckliga. Om en mottagande stat är ansluten till dataskydds-konventionen eller en annan internationell överenskommelse som innehåller bestämmelser om dataskydd och registrerades rättigheter kan lämpliga skyddsåtgärder som utgångspunkt anses föreligga (se prop. 2020/21:224 s. 224).

Av paragrafen framgår att regeringen kan meddela föreskrifter eller i ett enskilt fall besluta om att personuppgifter får överföras till en mottagare utomlands även om Försvarets radioanstalt inte gjort en bedömning av mottagarens skydd av personuppgifterna. Behov av föreskrift eller beslut kan exempelvis uppstå i en akut situation där det saknas tidsmässigt utrymme för Försvarets radioanstalt att göra en sådan bedömning, men där det för Försvarets radioanstalts möjligheter att bedriva ett effektivt internationellt signalspaningssamarbete är av stor vikt att person-uppgifterna överförs.

Villkoren för överföring av personuppgifter till en mottagare utomlands enligt 2 kap. 20 § lagen om behandling av personuppgifter vid Försvarets radioanstalt ska i övrigt vara uppfyllda för att sådan överföring ska vara tillåten.

Enskilds rätt till information

11 § Bestämmelserna om Försvarets radioanstalts skyldighet att lämna information till en enskild enligt 5 kap. 2 § lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt ska inte tillämpas.

Paragrafen innehåller undantag från en enskilds rätt till viss personrelaterad information enligt 5 kap. 2 § lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt. Av paragrafen följer att Försvarets radioanstalt inte behöver lämna sådan information till en enskild. Övervägandena finns i avsnitt 5.5.10.

Kontroll och tillsyn

12 § Bestämmelserna om kontroll enligt 10 § första och andra styckena och 10 a § första och andra styckena lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska inte tillämpas.

I paragrafen anges att bestämmelserna om kontroll enligt 10 § första och andra styckena och 10 a § första och andra styckena lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet inte ska tillämpas. Av paragrafen följer således att sådan kontroll inte ska utföras om bestämmelsen aktiveras. Övervägandena finns i avsnitt 5.5.7.

13 § Integritetskyddsrådets uppgifter enligt 11 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska inte utföras.

I paragrafen anges att Integritetsskyddsrådet inte ska utföra de uppgifter som anges i 11 § lagen om signalspaning i försvarsunderrättelseverksamhet. Övervägandena finns i avsnitt 5.5.7.

14 § Tillsyn enligt lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt ska inte utföras.

I paragrafen anges att tillsyn av Försvarets radioanstalts behandling av personuppgifter enligt lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt inte ska utföras. När krigsförhållanden inte längre råder kan bestämmelserna om tillsyn i lagen om behandling av personuppgifter vid Försvarets radioanstalt tillämpas på sådan personuppgiftsbehandling som skett när sådan förhållanden rådde. Övervägandena finns i avsnitt 5.5.9.

15 § När det inte längre råder sådana förhållanden som anges i 1 § eller 2 § första stycket, ska kontrollmyndigheten kontrollera att denna lag har följts.

Vid sådan kontroll ska 10 § första och andra styckena lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet tillämpas.

Paragrafen innehåller bestämmelser om efterhandskontroll när krig eller krigsfara inte längre råder. Övervägandena finns i avsnitt 5.5.7.

Bestämmelsen innebär att kontrollmyndigheten ska kontrollera att lagen har följts när krig, krigsfara eller extraordinära förhållanden inte längre råder. När sådan kontroll utförs ska bestämmelserna i 10 § första och andra styckena lagen (2008:717) om signalspaning i försvarsunderrättelse-

verksamhet tillämpas. Det innebär att kontrollmyndigheten särskilt ska granska användningen av sökbegrepp, förstöring och rapportering. Kontrollmyndigheten kan också besluta om att upptagning eller uppteckning ska förstöras, om inhämtningen inte är förenlig med tillstånd som meddelats enligt lagen.

16 § När det inte längre råder sådana förhållanden som anges i 1 § eller 2 § första stycket, ska det särskilda beslutandeorganet i kontrollmyndigheten tillämpa bestämmelserna i 10 a § första och andra styckena lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet på meddelanden och lagrade uppgifter som inhämtats i samband med signalspaning enligt denna lag och på tillstånd som lämnats enligt denna lag.

Paragrafen reglerar utredningsskyldighet på begäran av enskild när krig eller krigsfara inte längre råder. Övervägandena finns i avsnitt 5.5.7.

Av paragrafen följer att det särskilda beslutandeorganet ska tillämpa bestämmelserna i 10 a § första och andra styckena lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet på meddelanden och lagrade uppgifter (se avsnitt 6.3) som inhämtats i samband med signalspaning enligt de särskilda beredskapsbestämmelserna och på tillstånd som lämnats enligt de särskilda beredskapsbestämmelserna. Det innebär att det särskilda beslutandeorganet ska kontrollera om den enskildes meddelanden eller lagrade uppgifter har inhämtats vid signalspaning och, om så är fallet, huruvida inhämtningen och behandlingen av inhämtade uppgifter har skett i enlighet med lag. I enlighet med 10 a § första stycket lagen om signalspaning i försvarsunderrättelseverksamhet ska den enskilde underrättas om att kontrollen har utförts. Det särskilda beslutandeorganet kan också besluta om att inhämtning avseende den som begärt kontrollen ska upphöra eller att upptagning eller uppteckning av inhämtade uppgifter ska förstöras, om det vid kontroll framkommer att inhämtningen inte är förenlig med det tillstånd som lämnats.

17 § Signalspaningsmyndigheten ska vidta de åtgärder som är nödvändiga för att underlätta kontroll enligt 15 och 16 §§.

Paragrafen reglerar Försvarets radioanstalts skyldighet att vidta åtgärder som kan underlätta kontrollen enligt 15 och 16 §§. Övervägandena finns i avsnitt 5.5.7.

Sådana åtgärder kan till exempel vara att föra särskilda register eller annan form av dokumentation. Syftet med bestämmelsen är att möjliggöra att kontrollmyndigheten och det särskilda beslutandeorganet när krigsförhållanden inte längre råder i efterhand kan följa och därigenom kontrollera de åtgärder som Försvarets radioanstalt vidtagit under sådana förhållanden.

Övriga bestämmelser

18 § Beslut enligt denna lag får inte överklagas.

Beslut enligt lagen får, i likhet med vad som gäller enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet och lagen (2009:966) om Försvarsunderrättelsedomstol, inte överklagas. Övervägandena finns i avsnitt 5.5.5.

13.2 Förslaget till lag om ändring i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet

1 § I försvarsunderrättelseverksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet får den myndighet som regeringen bestämmer (signalspaningsmyndigheten) inhämta signaler i elektronisk form vid signalspaning, *oavsett om signalerna är under förmedling eller är lagrade*. Signalspaning i försvarsunderrättelseverksamhet får endast ske i de fall regeringen eller en myndighet som anges i 4 § närmare har bestämt inriktningen av signalspaningen.

Signalspaning i försvarsunderrättelseverksamhet får ske endast i syfte att kartlägga

1. yttre militära hot mot landet,
2. förutsättningar för svenskt deltagande i fredsfrämjande och humanitära internationella insatser eller hot mot säkerheten för svenska intressen vid genomförandet av sådana insatser,
3. internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen,
4. utveckling och spridning av massförstörelsevapen, krigsmateriel och produkter som avses i lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd *samt strategiska förhållanden avseende sådana utländska direktinvesteringar som avses i lagen (2023:560) om granskning av utländska direktinvesteringar*,
5. allvarliga yttre hot mot samhällets infrastrukturer,
6. konflikter utomlands med konsekvenser för internationell säkerhet,
7. främmande underrättelseverksamhet mot svenska intressen,
8. främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik, eller
9. sådana företeelser som avses i 1–8, men som inte riktas mot Sverige eller rör svenska intressen, om det är nödvändigt för ett samarbete i underrättelsefrågor med andra länder och internationella organisationer som signalspaningsmyndigheten deltar i.

Om det är nödvändigt för försvarsunderrättelseverksamheten får signaler i elektronisk form inhämtas vid signalspaning även för att

1. följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet, samt
2. fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamhet enligt denna lag.

Paragrafen reglerar bland annat ändamål för signalspaning.

I *första stycket* görs ett tillägg, som innebär att inhämtning av signaler i elektronisk form får ske oavsett om signalerna är under förmedling eller är lagrade. Av tidigare förarbeten framgår att möjligheten att inhämta

signaler i elektronisk form inte är knuten till var signalerna befinner sig. Därmed kan inhämtning ske oavsett om signalerna befinner sig i etern eller i kabel (dvs. är trådburen) eller någon annanstans (se prop. 2006/07:63 s. 137). Ändringen innebär ett förtydligande i lagen om att signaler i elektronisk form får inhämtas oavsett var signalerna befinner sig. Det kan exempelvis vara fråga om signaler som överförs via satellit eller signaler som är lagrade i nätverksansluten utrustning, i såväl mjuk- som hårdvara. Övervägandena finns i avsnitt 6.3.

I *andra stycket* anges i nio punkter de närmare ändamål för vilka signalspaning i försvarsunderrättelseverksamhet får bedrivas för.

Tredje punkten ändras på så sätt att kartläggning enligt det aktuella ändamålet inte längre begränsas till strategiska förhållanden. Detta innebär alltså att kartläggningen får ske på en preciserad nivå. Det kan exempelvis handla om information som i och för sig är tidskritisk och individspecifik. Ändringen medför dock ingen skillnad från nu gällande ordning i fråga om hur uppgifterna som inhämtas får användas inom den brottsbekämpande verksamheten. Uppgifterna kan alltså exempelvis inte användas i en förundersökning. Ändringen är inte heller avsedd att förändra den grundläggande gränsdragning som finns mellan försvarsunderrättelseverksamhet och brottsbekämpande verksamhet. Övervägandena finns i avsnitt 8.5.

I *fjärde punkten* görs ett tillägg, som innebär att signalspaning i försvarsunderrättelseverksamhet får ske för att kartlägga strategiska förhållanden avseende sådana utländska direktinvesteringar som avses i lagen (2023:560) om granskning av utländska direktinvesteringar. Signalspaningens uppgift i detta sammanhang är att kartlägga företeelser på en strategisk nivå för att ge ett övergripande underlag i fråga om granskning av utländska direktinvesteringar enligt nämnda lag. Övervägandena finns i avsnitt 9.2.

1 a § *Om det är nödvändigt för att utveckla förmågan att verka under höjd beredskap får signaler i elektronisk form även inhämtas vid övning.*

Enligt paragrafen, som är ny, får signaler i elektronisk form inhämtas om det är nödvändigt för att utveckla förmåga att verka under höjd beredskap. Övervägandena finns i avsnitt 7.2.

Bestämmelsen innebär att Försvarets radioanstalt får inhämta signaler i elektronisk form vid övningsverksamhet. Sådan verksamhet ska syfta till att utveckla Försvarets radioanstalts och annan myndighets förmåga att verka under höjd beredskap. Övningsverksamhet kan bedrivas av Försvarets radioanstalt ensamt eller tillsammans med andra myndigheter. Övningsverksamheten kan vara såväl nationell som internationell. Bestämmelsen möjliggör för Försvarets radioanstalt att bedriva skarp signalspaning i sådan verksamhet.

2 § Inhämtning som sker i tråd får endast avse signaler som förs över Sveriges gräns i tråd som ägs av en operatör.

Vid inhämtning enligt 1 och 1 a § av signaler i elektronisk form får signalspaningsmyndigheten vidta de tekniska åtgärder som är nödvändiga för att genomföra inhämtningen.

Av paragrafen framgår att inhämtning som sker i tråd endast får avse signaler som förs över Sveriges gräns i tråd som ägs av en operatör.

Andra stycket är nytt. Av bestämmelsen följer att Försvarets radioanstalt får vidta de tekniska åtgärder som är nödvändiga för att inhämta signaler i elektronisk form. Vilken typ av åtgärder som krävs är beroende på vilka företeelser som signalspaningen riktas mot, den tekniska utvecklingen och signalmiljön. Vid exempelvis inhämtning av lagrade uppgifter kan Försvarets radioanstalt behöva utnyttja tekniska sårbarheter, förbiseenden och av leverantören inbyggda åtkomstmöjligheter i nätverksansluten utrustning. När det gäller inhämtning av signaler som inte är lagrade kan det exempelvis röra sig om tekniska åtgärder som vidtas för att ta om hand signalerna från samverkanspunkterna eller för att etablera en satellitinhämtningsmiljö. Övervägandena finns i avsnitt 6.3.

2 a § Inhämtning får inte avse signaler mellan en avsändare och mottagare som båda befinner sig i Sverige. Om sådana signaler inte kan avskiljas redan vid inhämtningen, ska upptagningen eller uppteckningen förstöras så snart det står klart att sådana signaler har inhämtats. Kravet på förstöring gäller även i fråga om upptagningar och uppteckningar som signalspaningsmyndigheten har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete.

Första stycket tillämpas inte i fråga om

1. signaler som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte innehåller personuppgifter,

2. signaler som sänds från eller till utländsk militär personal, utländska statsfartyg, statsluftfartyg eller militära fordon, *eller*

3. signaler mellan en avsändare och en mottagare, vid sådan övningsverksamhet som anges i 1 a §.

Första stycket och andra stycket 2 och 3 tillämpas även på signaler som lagras i Sverige.

Paragrafen reglerar förbud mot signalspaning i vissa fall och undantag från förbudet.

I *andra stycket tredje punkten*, som är ny, införs ett nytt undantag från förbudet i första stycket. Av bestämmelsen följer att förbudet och förstöringsskyldigheten i första stycket inte gäller vid signalspaning i övningsverksamhet i fråga om signaler mellan avsändare och mottagare vid övningsverksamhet som båda befinner sig i Sverige. Signalerna kan sändas från eller till såväl fysiska personer som fartyg, luftfartyg och fordon. Beroende på övningssammanhang kan det vara fråga om både militära och civila avsändare och mottagare. Signalspaning i övningsverksamhet kan användas vid både nationella och internationella övningar. Även internationella avsändare och mottagare på svenskt territorium omfattas därför av undantaget. Det kan därutöver även vara fråga om signaler som sänds till, från eller som utväxlas autonomt mellan tekniska system. Övervägandena finns i avsnitt 7.3.

I *tredje stycket*, som är nytt, förtydligas att förbudet i första stycket och undantagen i andra stycket andra och tredje punkterna också ska tillämpas på signaler som lagras i Sverige. Förstöringsskyldigheten i första stycket ska också tillämpas på sådana signaler som inte har kunnat avskiljas vid inhämtningen. Eftersom signaler som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte innehåller personuppgifter i sin

natur är under förmedling omfattas inte undantaget i andra stycket första punkten. Övervägandena finns i avsnitt 6.3.

2 b § *Bestämmelsen i 2 a § första stycket tillämpas inte i fråga om signaler i sådana brådskande situationer som innebär fara för människors liv eller hälsa eller för omfattande förstörelse av egendom.*

*Om sådana signaler som anges i 2 a § första stycket inte kan avskiljas redan vid inhämtningen, behöver upptagningen eller upptecknin*gen inte förstöras om den innehåller

1. uppgifter om en brådskande situation, och

2. uppgifterna bedöms vara av avgörande betydelse för att skydda människors liv eller hälsa eller för att undvika omfattande förstörelse av egendom.

Paragrafen är ny. Genom bestämmelsen införs två nya undantag från 2 a § första stycket. Övervägandena finns i avsnitt 8.3 och 8.4.

Första stycket innebär att Försvarets radioanstalt får inhämta signaler i elektronisk form mellan en avsändare och en mottagare som båda befinner sig i Sverige, om det föreligger en brådskande situation som innebär fara för människors liv eller hälsa eller för omfattande förstörelse av egendom. Med uttrycket ”brådskande situation som innebär fara” avses situationer där det föreligger en konkret och nära förestående fara. Det ska med andra ord vara fråga om en situation där det är angeläget att omgående förhindra eller avvärja faran för människors liv eller hälsa eller för omfattande förstörelse av egendom.

För att tillämpa undantaget i första stycket krävs tillstånd. Om det redan finns ett tillståndsprövat inhämtningsuppdrag ska ansökan om tillstånd och prövning ske enligt 5 a § tredje stycket. I annat fall får en ny ansökan göras enligt 4 a §.

Av *andra stycket* följer att en upptagning eller uppteckning som härrör från signaler mellan en avsändare och en mottagare som båda befinner sig i Sverige inte måste förstöras om förutsättningarna i första och andra punkten är uppfyllda.

Enligt *andra stycket första punkten* ska upptagningen eller uppteckningen innehålla uppgifter om en brådskande situation. Det ska alltså vara fråga om uppgifter om en nära förestående händelse.

Av *andra stycket andra punkten* följer att upptagningen eller uppteckningen också ska innehålla uppgifter som bedöms vara av avgörande betydelse för att skydda människors liv eller hälsa eller för att undvika omfattande förstörelse av egendom. Det måste således finnas uppgifter om fara som hotar människors liv eller hälsa eller omfattande förstörelse av egendom. Försvarets radioanstalt ska göra en bedömning av om rapportering av uppgifterna skulle få en avgörande betydelse i att förhindra eller avvärja faran. Bedömningen får göras utifrån den kunskap som myndigheten har vid tidpunkten samt uppgifternas art och karaktär. Vid bedömningen bör exempelvis vägas in hur konkreta uppgifterna om faran är.

Om Försvarets radioanstalt bedömer att upptagningen eller uppteckningen inte ska förstöras, och inte heller förstöras enligt någon bestämmelse i 7 §, får rapportering ske till berörda myndigheter i enlighet med 8 §.

Med omfattande förstörelse av egendom avses i båda styckena exempelvis betydande förstörelse av bostadsfastigheter, fastigheter innehållandes samhällsviktiga funktioner eller förstörelse av kritisk infrastruktur.

4 § I lagen (2000:130) om försvarsunderrättelseverksamhet finns bestämmelser om regeringens och myndigheters inriktning av sådan verksamhet. Inriktning av signalspaning får anges endast av regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen, Nationella operativa avdelningen i Polismyndigheten och *Inspektionen för strategiska produkter*.

Regeringen bestämmer inriktningen av sådan verksamhet som bedrivs enligt 1 § andra stycket 9 och tredje stycket.

Regeringen och Försvarsmakten bestämmer inriktningen av sådan verksamhet som bedrivs enligt 1 a §.

En inriktning av signalspaningen får inte avse endast en viss fysisk person.

Paragrafen innehåller bestämmelser om inriktning av signalspaning. Övervägandena finns i avsnitt 7.4 och 9.1.

Första stycket ändras på sådant sätt att Inspektion för strategiska produkter ges rätt att inrikta signalspaning i försvarsunderrättelseverksamhet.

I *tredje stycket*, som får nytt innehåll, anges att regeringen och Försvarsmakten bestämmer inriktningen för signalspaning i övningsverksamhet. Försvarsmaktens inriktning omfattar inte internationellt signalspaningssamarbete i övningsverksamhet eftersom sådan verksamhet sker enligt regeringens närmare bestämmande enligt 9 §.

Det nya *fjärde stycket* motsvarar det tidigare tredje stycket.

4 a § Signalspaningsmyndigheten ska ansöka om tillstånd hos Försvarsunderrättelsedomstolen för signalspaning enligt 1 och *1 a §§*. En sådan ansökan ska innehålla uppgifter om

1. det inhämtningsuppdrag som ansökan avser, med en närmare redogörelse för det behov som föranleder ansökan och uppgift om vilken inriktning uppdraget hänför sig till,
2. vilken eller vilka signalbärare avseende signaler i tråd som signalspaningsmyndigheten behöver ha tillgång till för att fullgöra uppdraget *samt en övergripande redovisning av övrig inhämtning*,
3. de sökbegrepp eller kategorier av sökbegrepp som är avsedda att användas vid inhämtningen,
4. vilken tid tillståndet ska gälla, och
5. de omständigheter i övrigt som myndigheten vill åberopa till stöd för sin ansökan.

Paragrafen innehåller bestämmelser om ansökan om tillstånd för signalspaning.

Första meningen ändras på sådant sätt att 1 a § läggs till. Ändringen innebär att signalspaning i övningsverksamhet omfattas av tillståndskravet. Övervägandena finns i avsnitt 7.5.

Andra punkten ändras genom att en övergripande redovisning av övrig inhämtning läggs till i fråga om vad som ska redovisas i ansökan. Bestämmelsen syftar till att tillgodose att Försvarsunderrättelsedomstolen på ett övergripande plan får information om all den inhämtning som kan

komma att bli aktuell under tillståndets giltighetstid. Övervägandena finns i avsnitt 10.1.

5 a § I ett tillstånd ska anges

1. det inhämtningsuppdrag för vilket inhämtning får ske,
2. vilken eller vilka signalbärare avseende signaler i tråd som signalspaningsmyndigheten ska få tillgång till för att fullgöra uppdraget,
3. vilka sökbegrepp eller kategorier av sökbegrepp som får användas vid inhämtningen,
4. den tid som tillståndet avser, och
5. de villkor i övrigt som behövs för att begränsa intrånget i enskildas personliga integritet.

Ett tillstånd får ges för högst sex månader från dagen för beslutet och kan efter förnyad prövning förlängas med högst sex månader i taget.

Om det för fullgörande av inhämtningsuppdrag för vilket tillstånd *getts* uppstår behov av tillgång till ytterligare signalbärare, användning av andra tillståndspliktiga sökbegrepp *eller undantag enligt 2 b § första stycket*, ska särskilt tillstånd sökas. Vid ansökan och prövning gäller *4 a* och 5 §§ i tillämpliga delar. Ett sådant *särskilt* tillstånd ska *som längst* ha samma varaktighet som tillståndet för det inhämtningsuppdrag *som det särskilda tillståndet hänför sig till*.

I paragrafen anges vad ett tillstånd ska innehålla, ett tillstånds varaktighet och vad som gäller för kompletterande tillstånd.

Genom en ändring i *tredje stycket första meningen* införs en skyldighet för Försvarets radioanstalt att ansöka om särskilt tillstånd om behov av undantag enligt 2 b § första stycket uppstår i ett redan tillståndsprövat inhämtningsuppdrag. Om behov av att tillämpa undantaget uppstår utan att det finns ett redan tillståndsprövat inhämtningsuppdrag får ansökan göras i enlighet med bestämmelserna i 4 a §. Övervägandena finns i avsnitt 8.3.

I *tredje stycket andra meningen* ändras hänvisningen till vilken bestämmelse som i tillämpliga delar gäller vid ansökan om särskilt tillstånd från 4 § till 4 a §. Ändringen innebär att hänvisningen görs till den bestämmelse som reglerar utformningen av ansökan och inte som tidigare den bestämmelse som reglerar inriktning. Ändringen motsvarar vad som anges i fråga om utformning av ansökan i tidigare författningskommentar (se prop. 2008/09:201 s. 112). Övervägandena finns i avsnitt 10.2.

Tredje stycket tredje meningen ändras på sådant sätt att ett särskilt tillstånd kan ges kortare varaktighet än det tillstånd för det inhämtningsuppdrag som det särskilda tillståndet hänför sig till. Varaktigheten av ett särskilt tillstånd behöver således nödvändigtvis inte vara densamma som det ursprungliga tillståndet. Övriga ändringar är endast språkliga. Övervägandena finns i avsnitt 8.3.

7 § En upptagning eller uppteckning av uppgifter som har inhämtats enligt denna lag eller som signalspaningsmyndigheten har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete ska omgående förstöras om innehållet

1 har bedömts sakna betydelse för verksamhet som avses i 1 och *1 a §§,*

2. avser uppgifter för vilka tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen, eller som omfattas av efterforskningsförbudet i 3 kap. 5 § tryckfrihetsförordningen eller 2 kap. 5 § yttrandefrihetsgrundlagen,

3. omfattar uppgifter i sådana meddelanden mellan en person som är misstänkt för brott och hans eller hennes försvarare vilka skyddas enligt 27 kap. 22 § första stycket rättegångsbalken, eller

4. avser uppgifter lämnade under bikt eller enskild själavård, såvida det inte finns synnerliga skäl att behandla uppgifterna för syften som anges i 1 § andra stycket.

Paragrafen innehåller bestämmelser om förstöring av en upptagning eller uppteckning. Övervägandena finns i avsnitt 7.6.

Första punkten ändras på sådant sätt att förstöringsskyldigheten omfattar en upptagning eller upptagning vars innehåll bedömts sakna betydelse för övningsverksamheten. Prövningen av uppgifternas relevans ska ske löpande. Relevansen av de inhämtade uppgifterna upphör, oavsett tidigare bedömning, när övningen avslutats och de slutsatser och erfarenheter som övningen lett till har summerats. Det saknas efter denna tidpunkt skäl att hantera uppgifterna vidare.

8 § Underrättelser med uppgifter som inhämtats enligt denna lag ska rapporteras till berörda myndigheter i enlighet med vad som föreskrivs i lagen (2000:130) om försvarsunderrättelseverksamhet. Om uppgifterna berör en viss fysisk person, får rapporteringen endast avse förhållanden som är av betydelse i de hänseenden som anges i 1 § den lagen.

Uppgifter som inhämtats med stöd av 1 a § får inte resultera i underrättelser.

Paragrafen innehåller bestämmelser om rapportering av underrättelser.

Andra stycket är nytt. Av bestämmelsen framgår att uppgifter som inhämtats vid signalspaning i övningsverksamhet inte får resultera i några underrättelser. Uppgifter som inhämtats i sådan verksamhet får således inte rapporteras. Övervägandena finns i avsnitt 7.7.

9 § I lagen (2000:130) om försvarsunderrättelseverksamhet finns bestämmelser om internationellt samarbete på försvarsunderrättelseområdet.

Signalspaningsmyndigheten får för den verksamhet som anges i 1 § tredje stycket och *1 a §,* enligt regeringens närmare bestämmande, etablera och upprätthålla samarbete i signalspaningsfrågor med andra länder och internationella organisationer.

I paragrafen behandlas internationellt samarbete.

Ändringen i *andra stycket* innebär att Försvarets radioanstalt får bedriva internationellt signalspaningssamarbete i övningsverksamhet, enligt regeringens närmare bestämmande. Övervägandena finns i avsnitt 7.8.

10 a § Ett särskilt beslutandeorgan i kontrollmyndigheten är skyldigt att på begäran av en enskild kontrollera om hans eller hennes meddelanden *eller lagrade uppgifter* har inhämtats i samband med signalspaning enligt denna lag och, om så är fallet, huruvida inhämtningen och behandlingen av inhämtade uppgifter har skett i enlighet med lag. Beslutandeorganet ska underrätta den enskilde om att kontrollen har utförts. Underrättelsen ska innehålla en motivering.

Beslutandeorganet får besluta att inhämtning avseende den som begärt kontrollen ska upphöra eller att upptagning eller uppteckning av inhämtade uppgifter ska förstöras, om det vid kontroll framkommer att inhämtningen inte är förenlig med tillstånd som lämnats enligt denna lag.

Ledamöterna i beslutandeorganet utses av regeringen för en bestämd tid. Ordföranden och vice ordföranden ska vara eller ha varit ordinarie domare eller ha

motsvarande juridisk erfarenhet. Övriga ledamöter ska utses bland personer som föreslagits av partigrupperna i riksdagen.

Paragrafen innehåller bestämmelser om kontroll på begäran av enskild.

Första stycket ändras på sådant sätt att det anges att kontrollen utöver den enskildes meddelanden också omfattar lagrade uppgifter. Övervägandena finns i avsnitt 6.3.

Ändringen, som är en följd av ändringen i 1 § första stycket, innebär att kontrollen avser lagrade uppgifter som inhämtats från den enskilde och som genom urvalsprocessen med sökbegrepp blivit tillgänglig för Försvarets radioanstalt för vidare bearbetning och analys. Det framgår numer tydligt att det avser lagrad information. De utredningsåtgärder som kan vidtas är avhängiga vilken information den enskilde kan tillhandahålla.

12 b § *I lagen (2025:000) om signalspaning i försvarsunderrättelseverksamhet under krig eller krigsfara finns bestämmelser om signalspaning i försvarsunderrättelseverksamhet om Sverige är i krig eller i krigsfara eller det råder sådana extraordinära förhållanden som är föranledda av krig eller av krigsfara som Sverige har befunnit sig i.*

Paragrafen, som är ny, är en upplysningsbestämmelse som innehåller en hänvisning till regleringen om signalspaning i krig och krigsfara som återfinns i lagen om signalspaning i försvarsunderrättelseverksamhet i krig och krigsfara.

13.3 Förslaget till lag om ändring i lagen (2009:966) om Försvarsunderrättelsedomstol

2 § Försvarsunderrättelsedomstolen består av en ordförande, en eller högst två vice ordförande samt minst två och högst *åtta* särskilda ledamöter.

Ledamöterna ska vara svenska medborgare och får inte vara underåriga eller i konkurstillstånd eller ha förvaltare enligt 11 kap. 7 § föräldrabalken. Innan en ledamot börjar tjänstgöra i domstolen, ska han eller hon ha avlagt domared.

I lagen (2010:1390) om utnämning av ordinarie domare finns bestämmelser om utnämning av ordförande i domstolen. Vice ordförande och särskilda ledamöter förordnas av regeringen för *högst* fyra år *i sänder*.

I paragrafen regleras domstolens sammansättning, grundläggande krav på ledamöterna och anställningsförhållande för domstolens ordförande. Övervägandena finns i avsnitt 10.4.1.

Första stycket ändras i fråga om antalet särskilda ledamöter. Ändringen innebär att högst åtta sådana ledamöter kan förordnas, i stället för som tidigare högst sex stycken.

Tredje stycket ändras på sådant sätt att vice ordförande och särskilda ledamöter kan förordnas för en tid om högst fyra år i sänder, i stället för fyra år. Utgångspunkten ska fortsättningsvis vara att förordnande sker för fyra år. Ändringen innebär att regeringen har möjligt att förordna för kortare tid än fyra år om det föreligger skäl för detta. Så kan exempelvis vara fallet om en vice ordförande eller särskild ledamot ska förordnas på

nytt och han eller hon på grund av stundande pensionsavgång eller ålder själv har önskemål om en kortare förordnandetid.

6 § Regeringen förordnar för *högst* fyra år i sänder personer som kan tjänstgöra som integritetsskyddsombud.

Ett integritetsskyddsombud ska vara svensk medborgare och ska vara eller ha varit advokat eller ha varit ordinarie domare. Ett integritetsskyddsombud får inte vara i konkurstillstånd eller ha förvaltare enligt 11 kap. 7 § föräldrabalken.

Regeringen ska inhämta förslag på lämpliga kandidater från Sveriges advokatsamfund och Domarnämnden.

I paragrafen anges hur integritetsskyddsombud förordnas och vilka som ska förordnas till sådana ombud. Övervägandena finns i avsnitt 10.4.2.

Första stycket ändras i fråga om förordnandetiden för integritetsskyddsombuden. Ändringen innebär att integritetsskyddsombuden kan förordnas för högst fyra år, i stället för som tidigare minst fyra år. Utgångspunkten ska fortsättningsvis vara att förordnande sker för fyra år, men ändringen innebär att det finns utrymme att även förordna för en kortare tid om det föreligger skäl för det. Förordnande för kortare än tid än fyra år bör, i likhet med vad som anges i 5 §, exempelvis kunna ske vid ett omförordnande och ombudet på grund av stundande pensionsavgång eller ålder själv har önskemål om en kortare förordnandetid.

10 § Ordföranden får ensam på Försvarsunderrättelsedomstolens vägnar

1. företa förberedande åtgärder och besluta om avskrivning,

2. pröva frågor enligt 5 a § tredje stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet om tillstånd i pågående och tillståndsprövade inhämtningsuppdrag, om prövningen är av enkel beskaffenhet och endast avser tillgång till signalbärare eller användning av sökbegrepp som inte är direkt hänförliga till *en* viss fysisk person, *och*

3. fatta beslut om ersättning till integritetsskyddsombud.

Ordföranden får förordna en lagfaren tjänsteman vid domstolen att ensam på domstolens vägnar vidta förberedande åtgärder.

I paragrafen anges bland annat i vilken utsträckning domstolens ordförande ensam får vidta vissa åtgärder.

I *första stycket tredje punkten*, som är ny, anges att ordföranden ensam får fatta beslut om ersättning till integritetsskyddsombud. Beslut behöver således inte fattas vid sammanträdet. Övervägandena finns i avsnitt 10.4.5.

12 § När en ansökan om tillstånd till signalspaning har kommit in till domstolen, ska domstolen så snart som möjligt hålla ett sammanträde. Vid sammanträdet ska ansökande myndighet *och det integritetsskyddsombud som domstolen utser närvara*. Domstolen får *besluta* att *någon* annan som kan lämna upplysningar av betydelse för prövningen får närvara vid sammanträdet.

Om ärendet är så brådskande att ett dröjsmål allvarligt skulle riskera syftet med ansökan, får sammanträde hållas och beslut fattas utan att ett integritetsskyddsombud har varit närvarande eller annars fått tillfälle att yttra sig.

När ett beslut enligt andra stycket har fattats ska ett integritetsskyddsombud underrättas. När ett beslut enligt 10 § första stycket 2 har fattats av ordföranden på domstolens vägnar ska det integritetsskyddsombud som varit närvarande vid prövningen av det inhämtningsuppdrag till vilket beslutet är hänförligt underrättas.

Om integritetsskyddsombudets förordnande har upphört, får ett annat integritetsskyddsombud underrättas.

Paragrafen innehåller kompletterande bestämmelser om handläggningen av ansökan om tillstånd till signalspaning. Övervägandena finns i avsnitt 10.4.2 och 10.4.3.

Första stycket ändras för att bättre motsvara den faktiska handläggningen i Försvarsunderrättelsedomstolen. I och med ändringen behöver domstolen inte utse ett integritetsskyddsombud så snart som ansökan kommit in.

Tredje stycket första meningen är ny. Bestämmelsen innebär att ett integritetsskyddsombud ska underrättas vid beslut enligt paragrafens andra stycke.

Tredje stycket tredje meningen är ny. Vid beslut av ordföranden i pågående och tillståndsprövade inhämtningsuppdrag gäller enligt huvudregeln i tredje stycket andra meningen att det integritetsskyddsombud som varit närvarande vid prövningen av det inhämtningsuppdrag till vilket beslutet är hänförligt ska underrättas. Tredje stycket tredje meningen innebär ett undantag från denna huvudregel. Bestämmelsen möjliggör för underrättelse till ett annat integritetsskyddsombud i de fall förordnandet för det integritetsskyddsombud som närvarade vid den ursprungliga prövningen har upphört.

13.4 Förslaget till lag om ändring i lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt

1 kap.

2 § Denna lag gäller vid behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse-, utvecklings-, *och övningsverksamhet* samt informationssäkerhetsverksamhet.

I paragrafen regleras lagens tillämpningsområde. Paragrafen ändras så att den också omfattar signalspaning vid övningsverksamhet.

2 kap.

Övningsverksamhet

6 a § *Personuppgifter får behandlas i Försvarets radioanstalts övningsverksamhet om det är nödvändigt för att bedriva sådan verksamhet som anges i 1 a § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.*

Paragrafen, som är ny, reglerar ändamålet för behandlingen av personuppgifter i Försvarets radioanstalts övningsverksamhet. Rubriken före paragrafen är också ny. Övervägandena finns i avsnitt 7.9.

Försvarets radioanstalt får enligt bestämmelsen behandla personuppgifter om det är nödvändigt för att bedriva signalspaning i övningsverksamhet.

6 b § *Personuppgifter som behandlas med stöd av 6 a § får även behandlas om det är nödvändigt för att tillhandahålla information som behövs*

1. med anledning av samverkan med någon annan i fråga om övningsverksamhet, eller

2. med anledning av samarbete om övningsverksamhet med andra länder eller internationella organisationer enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Paragrafen, som är ny, reglerar sekundära ändamål för behandling av personuppgifter som har behandlats i Försvarets radioanstalts övningsverksamhet. Övervägandena finns i avsnitt 7.9.

Enligt *första punkten* får Försvarets radioanstalt även behandla de aktuella personuppgifterna för att tillhandahålla information som behövs med anledning av samverkan med annan i fråga om övningsverksamhet.

Av *andra punkten* följer att Försvarets radioanstalt får behandla personuppgifter med anledning av samarbete om övningsverksamhet med andra länder eller internationella organisationer enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

9 § Försvarets radioanstalt får behandla personuppgifter som utgör allmänt tillgänglig information om det är nödvändigt för den verksamhet som anges i 2, 5, *6 a* och 7 §§.

Paragrafen ger stöd för behandling av personuppgifter som utgör allmänt tillgänglig information.

Genom ändring i paragrafen får Försvarets radioanstalt behandla personuppgifter som utgör allmänt tillgänglig information också om det är nödvändigt för myndighetens signalspaning i övningsverksamhet. Övervägandena finns i avsnitt 7.10.

18 § Hantering av information som innebär behandling av personuppgifter ska inte anses oförenlig med bestämmelserna i 1, 2, 5, *6 a*, 7, 9, 11–14 och 16 §§ i det skede av behandlingen då det inte har kunnat fastställas vilka personuppgifter som informationen innehåller.

Paragrafen reglerar behandling av personuppgifter i vissa fall.

Paragrafen ändras på sådant sätt att 6 a §, som ger Försvarets radioanstalt rätt att behandla personuppgifter i myndighetens övningsverksamhet, också omfattas av bestämmelsen. Övervägandena finns i avsnitt 7.11.

Ändringen innebär att hantering av information som innebär behandling av personuppgifter inte ska anses oförenlig med 6 a § i det skede då det ännu inte har kunnat fastställas vilka personuppgifter som informationen innehåller.

20 § Personuppgifter som behandlas med stöd av denna lag får föras över till ett annat land eller en internationell organisation endast om det är nödvändigt för att Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för det

internationella försvarsunderrättelse- och säkerhetssamarbetet *eller övningssamarbetet* och

1. överföringen riktas till en utländsk underrättelse- eller säkerhetstjänst, eller ett underrättelse- eller säkerhetsorgan i en internationell organisation,
2. sekretess inte hindrar en överföring,
3. mottagaren garanterar tillräckligt skydd för personuppgifterna, och
4. överföringen inte innebär ett oproportionerligt intrång i den registrerades personliga integritet.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att överföring får ske även i andra fall än som anges i första stycket 1.

Regeringen får också besluta om sådan överföring i ett enskilt fall.

Paragrafen innehåller bestämmelser om förutsättningar för överföring av personuppgifter till en mottagare utomlands. Övervägandena finns i avsnitt 7.12.

Första stycket ändras på sådant sätt att övningssamarbete läggs till. Ändringen innebär att personuppgifter får överföras till ett annat land eller en internationell organisation om det är nödvändigt för att Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom det internationella övningssamarbetet. Bestämmelsen är således tillämplig också vid sådan verksamhet. De villkor som enligt första stycket ska vara uppfyllda för att överföring av personuppgifter till en mottagare utomlands ska vara tillåten ska därmed vara uppfyllda vid sådan överföring inom ramen för internationellt samarbete i övningsverksamheten.

Sammanfattning av slutbetänkandet Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning (SOU 2024:59)

Utredningens uppdrag

Utredningen uppdrag består i att göra en översyn av lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (signalspaningslagen). Syftet med uppdraget är att säkerställa en modern och ändamålsenlig reglering som är anpassad efter den tekniska utvecklingen, omvärldsutvecklingen och de försvars- och säkerhetsmässiga behoven samt som beaktar skyddet för den personliga integriteten. Utredningen ska lämna nödvändiga författningsförslag.

Av utredningens direktiv följer att utredningen särskilt ska uppmärksamma vissa frågor. I detta slutbetänkande behandlas således dels vilka åtgärder som krävs för att Försvarets radioanstalt ska kunna bedriva en effektiv signalspaning oavsett säkerhetsläge, dels om fler myndigheter bör få inrikta signalspaning i försvarsunderrättelseverksamhet. Inom ramen för översynen behandlar utredningen därutöver ytterligare några frågor.

En ny lag om signalspaning i krig och krigsfara

Försvarsunderrättelseverksamheten kommer under krigsförhållanden vara betydelsefull för Sveriges förmåga att skydda civilbefolkningen och Sveriges territoriella integritet mot främmande makt. Att det finns en effektiv signalspaningsverksamhet i krigsförhållanden är således av stor vikt. Utredningens bedömning är att signalspaningslagstiftningen i stor utsträckning är effektiv i både freds- och krigstid. Det gäller bland annat i fråga om för vilka ändamål som signalspaning får bedrivas, förstöringsskyldighet och rapportering. På vissa områden innebär dock lagstiftningen att signalspaningsverksamheten inte kan bedrivas på det effektiva sätt som krävs under de särskilda förhållanden som gäller i krig eller krigsfara. Utredningen föreslår därför en ny lag som ska reglera signalspaning i försvarsunderrättelseverksamhet under krigsförhållanden. Bestämmelserna i lagen syftar till att möjliggöra för Försvarets radioanstalt att bedriva en effektiv och ändamålsenlig signalspaning under sådana särskilda förhållanden.

Tidpunkt för tillämpning av lagen

Utredningen föreslår att bestämmelserna i lagen ska tillämpas omedelbart om Sverige är i krig. Är Sverige i krigsfara eller råder det sådana extraordinära förhållanden som är föranledda av krig eller av krigsfara som Sverige har befunnit sig i föreslår utredningen att regeringen får meddela föreskrifter om att bestämmelserna i lagen, helt eller delvis, ska tillämpas. Regeringens föreskrift om att bestämmelserna ska tillämpas ska underställas riksdagen. När krigsförhållanden inte längre råder ska regeringen

föreskriva om att bestämmelserna i den föreslagna lagen inte längre ska tillämpas.

Inhämtningens omfattning

Utredningen föreslår ett särskilt undantag från förbudet mot att inhämta inhemsk trafik, om sådan inhämtning är av betydelse för att hantera yttre hot mot Sveriges säkerhet. Förslaget syftar till att tillgodose att det finns möjlighet att under krigsförhållanden bedriva signalspaning mot sådan fientlig verksamhet i Sverige som utgör hot mot Sveriges suveränitet och territoriella integritet med utgångspunkt även från icke militära plattformar och strukturer.

Inriktning av signalspaning i försvarsunderrättelseverksamhet

Utredningen föreslår att det ska vara möjligt för regeringen att i föreskrift eller i ett enskilt beslut låta även andra myndigheter, än de som i den ordinarie lagstiftningen har inriktningsrätt, få inrikta signalspaning i försvarsunderrättelseverksamhet.

Ett särskilt tillståndsförfarande

Utan tillstånd från Försvarsunderrättelsedomstolen får signaler i elektronisk form inte inhämtas. Om Försvarsunderrättelsedomstolen i en krigssituation inte kan fullgöra sitt uppdrag finns det ingen annan domstol eller myndighet som kan utföra uppdraget. Det innebär en risk för att prövningen av Försvarets radioanstalts ansökningar inte kan komma till stånd i en krigssituation, vilket i förlängningen skulle kunna innebära betydande men för bland annat Sveriges förmåga att skydda sig från hot mot främmande makt. Utredningen föreslår därför ett förenklat tillståndsförfarande som innebär att den befattningshavare vid Försvarets radioanstalt som regeringen bestämmer fattar beslut om tillstånd för signalspaning.

Rådigheten över signalbärare

Utredningen föreslår att Försvarets radioanstalt ska ha rådigheten över signalbärarna i krig och, om regeringen föreskriver om det, vid krigsfara. Utredningen föreslår också att Försvarets radioanstalt ska begränsa tillgången till signalbärare till vad som följer av tillstånd.

Kontroll och tillsyn

Kontroll och tillsyn över Försvarets radioanstalts verksamhet utövas av Statens inspektion för försvarsunderrättelseverksamheten (Siun), Integritetsskyddsrådet och Integritetsskyddsmyndigheten. För att utföra sina respektive uppgifter är de i behov av fysisk tillgång till Försvarets radioanstalt. Möjligheten till sådan tillgång kommer i händelse av krig eller krigsfara med hög sannolikhet vara mycket begränsade. Utredningen föreslår därför att bestämmelserna om efterhandskontroll och kontroll på begäran av enskild i signalspaningslagen samt om tillsyn i lagen (2021:1172) om personuppgiftsbehandling vid Försvarets radioanstalt inte ska tillämpas under sådana förhållanden. Integritetsskyddsrådet ska inte heller utföra sina uppgifter.

För att underlätta kontroll av den föreslagna lagens tillämpning när krigsförhållanden inte längre råder, föreslår utredningen att Försvarets radioanstalt ska ha en skyldighet att vidta åtgärder som kan underlätta den efterföljande kontrollen.

Ett undantag från villkor vid överföring av personuppgifter till en mottagare utomlands.

Vid överföring av personuppgifter till ett annat land eller en internationell organisation ska särskilda villkor vara uppfyllda för att sådan överföring ska vara tillåten. Utredningen föreslår att regeringen ska kunna meddela föreskrifter eller i ett enskilt fall fatta beslut om undantag från villkoret om att mottagaren ska garantera tillräcklig skydd för de överförda uppgifterna. Förslaget innebär att Försvarets radioanstalt, efter föreskrift eller beslut, får överföra personuppgifter till en mottagare utomlands även om Försvarets radioanstalt inte kunnat förvissa sig om skyddet för de överförda personuppgifterna hos mottagaren.

Undantag från skyldigheten att ge enskilda viss information

Utredningen föreslår undantag från skyldigheten för Försvarets radioanstalt att lämna information till en enskild om viss personrelaterad information som denne har rätt till enligt lagen om behandling av personuppgifter vid Försvarets radioanstalt.

Inhämtning av signaler i elektronisk form – ett förtydligande i lag

Utredningen föreslår ett förtydligande i signalspaningslagen om att signaler i elektronisk form får inhämtas oavsett om signalerna är under förmedling eller är lagrade. Utredningen föreslår också att det i signalspaningslagen förtydligas att Försvarets radioanstalt får vidta de tekniska åtgärder som är nödvändiga för att genomföra inhämtning av signaler i elektronisk form. Som en följd av utredningens förslag om förtydligande föreslår utredningen också vissa andra förtydliganden och ändringar i signalspaningslagen.

Signalspaning i övningsverksamhet

Det säkerhetspolitiska läget har de senaste åren försämrats. Det innebär att det finns allt större behov av att stärka och utveckla totalförsvarsförmågan. För att utveckla Försvarets radioanstalts förmåga att verka under höjd beredskap har myndigheten behov av att i övningssyfte bedriva signalspaning i den skarpa signalmiljön. Det saknas möjlighet att bedriva sådan övningsverksamhet enligt nuvarande lagstiftning.

En ny ändamålsbestämmelse

Utredningen föreslår att det införs ett nytt ändamål i signalspaningslagen som möjliggör signalspaning i övningsverksamhet. Syftet med övningsverksamheten är att utveckla förmågan att verka inför och under höjd beredskap. Övningsverksamheten kan bedrivas av Försvarets radioanstalt enskilt eller tillsammans med andra myndigheter. Den kan vara nationell eller internationell.

Inhämtning av inhemsk trafik

För att möjliggöra en ändamålsenlig signalspaning i övningsverksamhet föreslår utredningen att det vid signalspaning i övningsverksamhet ska vara tillåtet att inhämta signaler mellan en avsändare och en mottagare som båda befinner sig i Sverige.

Inriktning av signalspaning i övningsverksamhet

Utredningen föreslår att regeringen och Försvarsmakten ska få inrikta signalspaning i övningsverksamhet. Försvarsmaktens inriktningsrätt omfattar dock inte internationellt samarbete i övningsverksamhet.

Tillstånd till signalspaning i övningsverksamhet

Utredningen föreslår att också signalspaning i övningsverksamhet, som vid alla annan signalspaning, ska föregås av tillstånd av Försvarsunderrättelsedomstolen.

Förstöringsskyldighet

Utredningen föreslår att en upptagning eller uppteckning som inhämtats vid signalspaning i övningsverksamhet – i likhet med vad som gäller för Försvarets radioanstalts övriga signalspaningsverksamhet enligt 7 § 1 signalspaningslagen – ska förstöras om innehållet saknar relevans för övningsverksamhetens behov. Övningsverksamheten ska inte resultera i några underrättelser. Det innebär att relevansen av de inhämtade uppgifterna upphör när övningen avslutats och de slutsatser och erfarenheter som övningen lett till har summerats.

Övningar får inte resultera i underrättelser

För att tydliggöra att övningsverksamheten inte ska resultera i underrättelser föreslår utredningen en särskild bestämmelse med sådan innebörd.

Internationellt samarbete

Utredningen föreslår att Försvarets radioanstalt, efter regeringens närmare bestämmande, ska få bedriva internationellt samarbete inom ramen för signalspaning i övningsverksamhet.

Överföring av personuppgifter till en mottagare utomlands

Utredningen föreslår att bestämmelserna om villkor vid överföring av personuppgifter till ett annat land eller en internationell organisation ska tillämpas vid överföring av personuppgifter vid internationellt samarbete inom ramen för övningsverksamhet.

Personuppgiftsbehandling vid signalspaning i övningsverksamhet

Utredningen föreslår att Försvarets radioanstalt ska få behandla personuppgifter om det är nödvändigt för att bedriva övningsverksamheten. Utredningen föreslår vidare att personuppgifter som behandlas i Försvarets radioanstalts övningsverksamhet får myndigheten även behandla om det är nödvändigt för att tillhandahålla

information som behövs med anledning av samverkan med annan i fråga om övningsverksamhet eller med anledning av samarbete om övningsverksamhet med andra länder eller internationella organisationer enligt signalspaningslagen.

Utredningen föreslår att Försvarets radioanstalt ska få behandla personuppgifter som utgör allmänt tillgänglig information om det är nödvändigt för övningsverksamheten samt att bestämmelsen i lagen om personuppgiftsbehandling vid Försvarets radioanstalt om behandling av personuppgifter i vissa fall också ska omfatta Försvarets radioanstalts signalspaning i övningsverksamhet.

Utredningen föreslår att det vid Försvarets radioanstalt får finnas uppgiftssamlingar för övningsverksamhet som innehåller personuppgifter. Personuppgifter i en uppgiftssamling för övningsverksamhet får inte behandlas längre än ett år efter det att behandlingen av uppgifterna påbörjades.

Inhämtning av inhemsk trafik i vissa brådskande situationer som kan innebära fara för liv, hälsa eller omfattande förstörelse av egendom

Utredningen föreslår undantag från förbudet mot att inhämta signaler mellan en avsändare och en mottagare som båda befinner sig i Sverige och från förstöringsskyldigheten av sådana signaler om de inte kan avskiljas vid inhämtningen. Undantagen är avsedda att tillämpas i nödliknande situationer där bland annat människors liv eller hälsa är i fara. Bestämmelserna syftar till att möjliggöra att Försvarets radioanstalt, i sådana situationer, kan bidra med information som kan rädda människors liv eller hälsa eller för att undvika omfattande förstörelse av egendom.

Inriktning av signalspaning i försvarsunderrättelseverksamhet

Utredningen har bedömt om Försvarets materielverk, Inspektionen för strategiska produkter, Myndigheten för psykologiskt försvar, Totalförsvarets forskningsinstitut och Tullverket bör få inrikta signalspaning i försvarsunderrättelseverksamhet.

Utredningens bedömning är att fortsatt restriktivitet ska gälla i fråga om inriktningsrätten. Enligt utredningen kan Försvarets materielverks, Myndigheten för psykologiskt försvars, Totalförsvarets forskningsinstituts och Tullverkets behov av underrättelser i stor utsträckning tillgodoses inom ramen för en fördjupad dialog med Försvarets radioanstalt. Myndigheterna föreslås därför inte få inriktningsrätt.

Utredningen föreslår att Inspektionen för strategiska produkter ska ges rätt att inrikta signalspaning i försvarsunderrättelseverksamhet bland annat med hänsyn till att myndighetens underrättelsebehov inte i tillräcklig utsträckning bedöms kunna tillgodoses inom ramen för en fördjupad dialog. Utredningen föreslår också att signalspaning i försvarsunderrättelseverksamhet ska få användas för att kartlägga strategiska förhållanden avseende sådana utländska direktinvesteringar som avses i lagen (2023:560) om granskning av utländska direktinvesteringar.

Övriga förslag

En övergripande redovisning av övrig inhämtning i ansökan

Utredningen föreslår att Försvarets radioanstalt i ansökan om tillstånd för signalspaning utöver att ange vilken eller vilka signalbärare avseende signaler i tråd som myndigheten behöver ha tillgång till för att fullgöra uppdraget också ska ange en övergripande redovisning av övrig inhämtning.

Underrättelseskyldigheten till enskild i signalspaningslagen upphävs

Utredningen föreslår att bestämmelserna om underrättelseskyldighet i signalspaningslagen upphävs. Förslaget lämnas mot bakgrund av att utredningen bedömer att underrättelseskyldigheten inte fyller någon praktisk funktion och därmed saknar betydelse ur ett integritetsskyddsperspektiv.

Försvarsunderrättelsedomstolen

Utredningen föreslår vissa ändringar i lagen (2009:966) om Försvarsunderrättelsedomstol som huvudsakligen syftar till att bättre anpassa lagstiftningen till de förhållanden som råder för domstolen och den handläggning som sker där. Utredningen föreslår att det införs en möjlighet att förordna vice ordförande, särskilda ledamöter och integritetsskyddsombud för kortare tid än fyra år. Utredningen föreslår också ändringar i fråga om bland annat när ett integritetsskyddsombud utses i målet, att ordföranden i domstolen kan fatta beslut om ersättning till integritetsskyddsombudet och vilket ombud som i vissa fall ska underrättas om beslut som fattas av ordföranden.

Ikraftträdande av utredningens förslag

Utredningen föreslår att förslagen träder i kraft den 1 oktober 2025.

Konsekvenser av utredningens förslag

De ekonomiska konsekvenser som förslagen kan medföra för berörda myndigheter bedöms rymmas inom respektive myndighets befintliga ekonomiska ramar. Förslagen medför inte i övrigt några kostnadsökningar för det allmänna eller för enskilda. Förslagens konsekvenser för den personliga integriteten bedöms acceptabla och proportionerliga mot bakgrund av syftena med förslagen. De förslag som utredningen lämnar bedöms i övrigt inte få någon betydelse av de slag som anges i kommittéförordningen (1998:1474).

Förslag till lag om signalspaning i försvarsunderrättelseverksamhet i krig eller krigsfara

Härigenom föreskrivs följande

Lagens tillämpning

1 § Är Sverige i krig ska 5–14 §§ tillämpas.

2 § Är Sverige i krigsfara eller råder det sådana extraordinära förhållanden som är föranledda av krig eller av krigsfara som Sverige har befunnit sig i, får regeringen meddela föreskrifter om att 5–14 §§ helt eller delvis ska tillämpas från den tidpunkt som regeringen bestämmer.

En sådan föreskrift ska underställas riksdagen inom en månad från utfärdandet. Föreskriften upphör att gälla, om den inte underställs riksdagen i rätt tid eller om riksdagen inte godkänner den inom två månader från det att den underställdes.

3 § Under den tid som 5–14 §§ tillämpas gäller dessa bestämmelser, eller föreskrifter som meddelats med stöd av dem, i stället för avvikande bestämmelser i annan lag eller författning.

Regeringen ska föreskriva att bestämmelserna i 5–14 §§ inte ska tillämpas, när det inte längre råder sådana förhållanden som avses i 1 § eller 2 § första stycket.

4 § Med signalspaningsmyndighet och kontrollmyndighet i denna lag avses de myndigheter som anges i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Signalspaningens omfattning

5 § Med undantag från 2 a § första stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet får inhämtning avse signaler mellan en avsändare och mottagare som båda befinner sig i Sverige, om sådan inhämtning är av betydelse för att hantera yttre hot mot Sveriges säkerhet.

Inriktning

6 § Regeringen får meddela föreskrifter eller i ett enskilt fall besluta att annan myndighet, än de som anges i 4 § första stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, får inrikta signalspaning i försvarsunderrättelseverksamhet.

Tillstånd

7 § Tillstånd till signalspaning enligt 1 och 1 a §§ lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet får ges av den

befattningshavare vid signalspaningsmyndigheten som regeringen föreskriver.

Tillstånd enligt första stycket får endast lämnas om förutsättningarna för tillstånd enligt 5 § lagen om signalspaning i försvarsunderrättelseverksamhet är uppfyllda.

8 § Tillstånd enligt 7 § ska utformas enligt 5 a § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Om det för fullgörande av inhämtningsuppdrag för vilket till-stånd givits uppstår behov av tillgång till ytterligare signalbärare eller användning av andra tillståndspliktiga sökbegrepp, gäller 5 a § tredje stycket lagen om signalspaning i försvarsunderrättelseverksamhet i tillämpliga delar.

Rådighet över signalbärare

9 § Signalspaningsmyndigheten ska ha rådigheten över sådana signalbärare som avses i 12 § första stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Signalspaningsmyndigheten ska begränsa sin tillgång till signalbärare till vad som följer av tillstånd enligt 7 §.

Överföring av personuppgifter till en mottagare utomlands

10 § Regeringen får meddela föreskrifter eller i ett enskilt fall besluta att personuppgifter som behandlas enligt lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt får överföras till ett annat land eller internationell organisation även om förutsättningarna i 2 kap. 20 § första stycket 3 den lagen inte är uppfyllda.

Enskilds rätt till information

11 § Bestämmelser om skyldighet att lämna information till enskild enligt 5 kap. 2 § lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt ska inte tillämpas.

Kontroll och tillsyn

12 § Bestämmelserna om kontroll enligt 10 § första och andra styckena och 10 a § första och andra styckena lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska inte tillämpas.

13 § Integritetskyddsrådets uppgifter enligt 11 § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska inte utföras.

14 § Tillsyn enligt lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt ska inte utföras.

15 § När det inte längre råder sådana förhållanden som anges i 1 § eller 2 § första stycket, ska kontrollmyndigheten kontrollera att denna lag har följts.

Vid sådan kontroll ska 10 § första och andra styckena lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet tillämpas.

16 § När det inte längre råder sådana förhållanden som anges i 1 § eller 2 § första stycket, ska det särskilda beslutandeorganet i kontrollmyndigheten tillämpa bestämmelserna i 10 a § första och andra stycket lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet på meddelanden och lagrade uppgifter som inhämtats i samband med signalspaning enligt denna lag och på tillstånd som lämnats enligt denna lag.

17 § Signalspaningsmyndigheten ska vidta de åtgärder som är nödvändiga för att underlätta kontroll enligt 15 och 16 §§.

Övriga bestämmelser

18 § Beslut som meddelas enligt denna lag får inte överklagas.

Denna lag träder i kraft den 1 oktober 2025.

Bilaga 2

Förslag till lag om ändring i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet

Härigenom föreskrivs i fråga om lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet[1]

dels att 11 a och 11 b §§ ska upphöra att gälla,

dels att rubriken närmaste före 11 a § ska utgå,

dels att 1–2 a, 4, 4 a,5 a, 7–9 och 10 a §§ ska ha följande lydelse,

dels att det ska införas tre nya paragrafer, 1 a, 2 b och 12 b §§, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 §[2]	
I försvarsunderrättelseverksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet får den myndighet som regeringen bestämmer (signalspaningsmyndigheten) inhämta signaler i elektronisk form vid signalspaning. Signalspaning i försvarsunderrättelseverksamhet får endast ske i de fall regeringen eller en myndighet som anges i 4 § närmare har bestämt inriktningen av signalspaningen.	I försvarsunderrättelseverksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet får den myndighet som regeringen bestämmer (signalspaningsmyndigheten) inhämta signaler i elektronisk form vid signalspaning, *oavsett om signalerna är under förmedling eller är lagrade*. Signalspaning i försvarsunderrättelse-verksamhet får endast ske i de fall regeringen eller en myndighet som anges i 4 § närmare har bestämt inriktningen av signalspaningen.

Signalspaning i försvarsunderrättelseverksamhet får ske endast i syfte att kartlägga

1. yttre militära hot mot landet,

2. förutsättningar för svenskt deltagande i fredsfrämjande och humanitära internationella insatser eller hot mot säkerheten för svenska intressen vid genomförandet av sådana insatser,

3. strategiska förhållanden avseende internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen,

4. utveckling och spridning av massförstörelsevapen, krigsmateriel och produkter som avses i lagen (2000:1064) om kontroll av produkter med dubbla	4. utveckling och spridning av massförstörelsevapen, krigsmateriel och produkter som avses i lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av

[1] Senaste lydelse av
11 a § 2009:967
11 b § 2009:967
rubriken närmast före 11 a § 2009:967.

[2] Senaste lydelse 2021:1173.

användningsområden och av tekniskt bistånd,

tekniskt bistånd *samt strategiska förhållanden avseende sådana utländska direktinvesteringar som avses i lagen (2023:560) om granskning av utländska direktinvesteringar*,

5. allvarliga yttre hot mot samhällets infrastrukturer,
6. konflikter utomlands med konsekvenser för internationell säkerhet,
7. främmande underrättelseverksamhet mot svenska intressen,
8. främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik, eller
9. sådana företeelser som avses i 1–8, men som inte riktas mot Sverige eller rör svenska intressen, om det är nödvändigt för ett samarbete i underrättelsefrågor med andra länder och internationella organisationer som signalspaningsmyndigheten deltar i.

Om det är nödvändigt för försvarsunderrättelseverksamheten får signaler i elektronisk form inhämtas vid signalspaning även för att

1. följa förändringar i signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet, samt
2. fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamhet enligt denna lag.

1 a §

Om det är nödvändigt för att utveckla förmåga att verka under höjd beredskap får signaler i elektronisk form även inhämtas vid övning.

2 §

Inhämtning som sker i tråd får endast avse signaler som förs över Sveriges gräns i tråd som ägs av en operatör.

Vid inhämtning enligt 1 och 1 a §§ av signaler i elektronisk form får signalspaningsmyndigheten vidta de tekniska åtgärder som är nödvändiga för att genomföra inhämtningen.

2 a §[3]

Inhämtning får inte avse signaler mellan en avsändare och mottagare som båda befinner sig i Sverige. Om sådana signaler inte kan avskiljas redan vid inhämtningen, ska upptagningen eller upptecknin gen förstöras så snart det står klart att sådana signaler har inhämtats. Kravet på förstöring gäller även i fråga om upptagningar och upptecknin gar som signalspaningsmyndigheten har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete.

[3] Senaste lydelse 2021:1173.

Första stycket tillämpas inte i fråga om	
1. signaler som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte innehåller personuppgifter, *eller*	1. signaler som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte innehåller personuppgifter,
2. signaler som sänds från eller till utländsk militär personal, utländska statsfartyg, statsluftfartyg eller militära fordon.	2. signaler som sänds från eller till utländsk militär personal, utländska statsfartyg, statsluftfartyg eller militära fordon, *eller*
	3. signaler mellan en avsändare och en mottagare vid sådan övningsverksamhet som anges i 1 a §.
	Första stycket och andra stycket 2 och 3 tillämpas även på signaler som lagras i Sverige.
	2 b §
	Bestämmelsen i 2 a § första stycket tillämpas inte i fråga om signaler i sådana brådskande situationer som innebär fara för människors liv eller hälsa eller för omfattande förstörelse av egendom.
	Om sådana signaler som anges i 2 a § första stycket inte kan avskiljas redan vid inhämtningen, behöver upptagningen eller uppteckningen inte förstöras om den innehåller
	1. uppgifter om en brådskande situation, och
	2. uppgifterna bedöms vara av avgörande betydelse för att skydda människors liv eller hälsa eller för att undvika omfattande förstörelse av egendom.
4 §[4]	
I lagen (2000:130) om försvarsunderrättelseverksamhet finns bestämmelser om regeringens och myndigheters inriktning av sådan verksamhet. Inriktning av signalspaning får anges endast av regeringen, Regeringskansliet,	I lagen (2000:130) om försvarsunderrättelseverksamhet finns bestämmelser om regeringens och myndigheters inriktning av sådan verksamhet. Inriktning av signalspaning får anges endast av regeringen, Regeringskansliet,

[4] Senaste lydelse 2021:1173.

Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten.	Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten *och Inspektionen för strategiska produkter*.

Regeringen bestämmer inriktningen av sådan verksamhet som bedrivs enligt 1 § andra stycket 9 och tredje stycket.

Regeringen och Försvarsmakten bestämmer inriktningen av sådan verksamhet som bedrivs enligt 1 a §.

En inriktning av signalspaningen får inte avse endast en viss fysisk person.

4 a §[5]

Signalspaningsmyndigheten ska ansöka om tillstånd hos Försvarsunderrättelsedomstolen för signalspaning enligt 1 §. En sådan ansökan ska innehålla uppgifter om	Signalspaningsmyndigheten ska ansöka om tillstånd hos Försvarsunderrättelsedomstolen för signalspaning enligt 1 och *1 a §§*. En sådan ansökan ska innehålla uppgifter om
1. det inhämtningsuppdrag som ansökan avser, med en närmare redogörelse för det behov som föranleder ansökan och uppgift om vilken inriktning uppdraget hänför sig till,	
2. vilken eller vilka signalbärare avseende signaler i tråd som signalspaningsmyndigheten behöver ha tillgång till för att fullgöra uppdraget,	2. vilken eller vilka signalbärare avseende signaler i tråd som signalspaningsmyndigheten behöver ha tillgång till för att fullgöra uppdraget *samt en övergripande redovisning av övrig inhämtning*,
3. de sökbegrepp eller kategorier av sökbegrepp som är avsedda att användas vid inhämtningen,	
4. vilken tid tillståndet ska gälla, och	
5. de omständigheter i övrigt som myndigheten vill åberopa till stöd för sin ansökan.	

5 a §[6]

I ett tillstånd ska anges

1. det inhämtningsuppdrag för vilket inhämtning får ske,
2. vilken eller vilka signalbärare avseende signaler i tråd som signalspaningsmyndigheten ska få tillgång till för att fullgöra uppdraget,
3. vilka sökbegrepp eller kategorier av sökbegrepp som får an-vändas vid inhämtningen,
4. den tid som tillståndet avser, och
5. de villkor i övrigt som behövs för att begränsa intrånget i enskildas personliga integritet.

[5] Senaste lydelse 2009:967.
[6] Senaste lydelse 2009:967.

Ett tillstånd får ges för högst sex månader från dagen för beslutet och kan efter förnyad prövning förlängas med högst sex månader i taget.

Om det för fullgörande av inhämtningsuppdrag för vilket tillstånd givits uppstår behov av tillgång till ytterligare signalbärare *eller* användning av andra tillståndspliktiga sökbegrepp, ska särskilt tillstånd sökas. Vid ansökan och prövning gäller *4* och 5 §§ i tillämpliga delar. Ett sådant tillstånd ska ha samma varaktighet som tillståndet för det inhämtningsuppdrag *inom vilket tillgång till signalerna behövs eller sökbegreppen är avsedda att användas.*

Om det för fullgörande av inhämtningsuppdrag för vilket tillstånd givits uppstår behov av tillgång till ytterligare signalbärare, användning av andra tillståndspliktiga sökbegrepp *eller undantag enligt 2 b § första stycket*, ska särskilt tillstånd sökas. Vid ansökan och prövning gäller *4 a* och 5 §§ i tillämpliga delar. Ett sådant särskilt tillstånd ska som längst ha samma varaktighet som tillståndet för det inhämtningsuppdrag *som det särskilda tillståndet hänför sig till*.

7 §[7]

En upptagning eller uppteckning av uppgifter som har inhämtats enligt denna lag eller som signalspaningsmyndigheten har fått från ett annat land eller en internationell organisation inom ramen för ett internationellt samarbete ska omgående förstöras om innehållet

1. har bedömts sakna betydelse för verksamhet som avses i 1 §,

1. har bedömts sakna betydelse för verksamhet som avses i 1 och *1 a §§*,

2. avser uppgifter för vilka tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen, eller som omfattas av efterforskningsförbudet i 3 kap. 5 § tryckfrihetsförordningen eller 2 kap. 5 § yttrandefrihetsgrundlagen,

3. omfattar uppgifter i sådana meddelanden mellan en person som är misstänkt för brott och hans eller hennes försvarare vilka skyddas enligt 27 kap. 22 § första stycket rättegångsbalken, eller

4. avser uppgifter lämnade under bikt eller enskild själavård, såvida det inte finns synnerliga skäl att behandla uppgifterna för syften som anges i 1 § andra stycket.

8 §[8]

Underrättelser med uppgifter som inhämtats enligt denna lag ska rapporteras till berörda myndigheter i enlighet med vad som föreskrivs i lagen (2000:130) om försvarsunderrättelseverksamhet. Om uppgifterna berör en viss fysisk person, får rapporteringen endast avse förhållanden som är av betydelse i de hänseenden som anges i 1 § den lagen.

Uppgifter som inhämtats med stöd av 1 a § får inte resultera i underrättelser.

[7] Senaste lydelse 2024:425.
[8] Senaste lydelse 2009:967.

9 §[9]

I lagen (2000:130) om försvarsunderrättelseverksamhet finns bestämmelser om internationellt samarbete på försvarsunderrättelseområdet.

Signalspaningsmyndigheten får för den verksamhet som anges i 1 § tredje stycket, enligt regeringens närmare bestämmande, etablera och upprätthålla samarbete i signalspaningsfrågor med andra länder och internationella organisationer.	Signalspaningsmyndigheten får för den verksamhet som anges i 1 § tredje stycket och *1 a §*, enligt regeringens närmare bestämmande, etablera och upprätthålla samarbete i signalspaningsfrågor med andra länder och internationella organisationer.

10 a §[10]

Ett särskilt beslutandeorgan i kontrollmyndigheten är skyldigt att på begäran av en enskild kontrollera om hans eller hennes meddelanden har inhämtats i samband med signalspaning enligt denna lag och, om så är fallet, huruvida inhämtningen och behandlingen av inhämtade uppgifter har skett i enlighet med lag. Beslutandeorganet ska underrätta den enskilde om att kontrollen har utförts. Underrättelsen ska innehålla en motivering.	Ett särskilt beslutandeorgan i kontrollmyndigheten är skyldigt att på begäran av en enskild kontrollera om hans eller hennes meddelanden *eller lagrade uppgifter* har inhämtats i samband med signalspaning enligt denna lag och, om så är fallet, huruvida inhämtningen och behandlingen av inhämtade uppgifter har skett i enlighet med lag. Beslutandeorganet ska underrätta den enskilde om att kontrollen har utförts. Underrättelsen ska innehålla en motivering.

Beslutandeorganet får besluta att inhämtning avseende den som begärt kontrollen ska upphöra eller att upptagning eller uppteckning av inhämtade uppgifter ska förstöras, om det vid kontroll framkommer att inhämtningen inte är förenlig med tillstånd som lämnats enligt denna lag.

Ledamöterna i beslutandeorganet utses av regeringen för en bestämd tid. Ordföranden och vice ordföranden ska vara eller ha varit ordinarie domare eller ha motsvarande juridisk erfarenhet. Övriga ledamöter ska utses bland personer som föreslagits av partigrupperna i riksdagen.

	12 b §
	I lagen (2025:000) om signalspaning i försvarsunderrättelseverksamhet under krig eller krigsfara finns bestämmelser om signalspaning i försvarsunderrättelseverksamhet om Sverige är i krig eller i krigsfara eller det råder sådana extraordinära förhållanden som är

[9] Senaste lydelse 2009:967.
[10] Senaste lydelse 2024:425.

föranledda av krig eller av krigsfara som Sverige har befunnit sig i.

Denna lag träder i kraft den 1 oktober 2025.

Förslag till lag om ändring i lagen (2009:966) om Försvarsunderrättelsedomstol

Härigenom föreskrivs att 2, 6, 10 och 12 §§ lagen (2009:966) om Försvarsunderrättelsedomstol ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 §[1]	
Försvarsunderrättelsedomstolen består av en ordförande, en eller högst två vice ordförande samt minst två och högst sex särskilda ledamöter.	
Ledamöterna ska vara svenska medborgare och får inte vara underåriga eller i konkurstillstånd eller ha förvaltare enligt 11 kap. 7 § föräldrabalken. Innan en ledamot börjar tjänstgöra i domstolen, ska han eller hon ha avlagt domared.	
I lagen (2010:1390) om utnämning av ordinarie domare finns bestämmelser om utnämning av ordförande i domstolen. Vice ordförande och särskilda ledamöter förordnas av regeringen för fyra år.	I lagen (2010:1390) om utnämning av ordinarie domare finns bestämmelser om utnämning av ordförande i domstolen. Vice ordförande och särskilda ledamöter förordnas av regeringen för *högst* fyra år *i sänder*.
6 §	
Regeringen förordnar för minst fyra år i sänder personer som kan tjänstgöra som integritetsskydds-ombud. *Under fyraårsperioden får vid behov ytterligare personer förordnas för återstående del av perioden.*	Regeringen förordnar för *högst* fyra år i sänder personer som kan tjänstgöra som integritetsskydds-ombud.
Ett integritetsskyddsombud ska vara svensk medborgare och ska vara eller ha varit advokat eller ha varit ordinarie domare. Ett integritets-skyddsombud får inte vara i konkurstillstånd eller ha förvaltare enligt 11 kap. 7 § föräldrabalken.	
Regeringen ska inhämta förslag på lämpliga kandidater från Sveriges advokatsamfund och Domarnämnden.	
Ett integritetsskyddsombud får trots att regeringens förordnande har upphört slutföra pågående uppdrag.	
10 §	
Ordföranden får ensam på Försvarsunderrättelsedomstolens vägnar	
1. företa förberedande åtgärder och besluta om avskrivning, *och*	1. företa förberedande åtgärder och besluta om avskrivning,
2 pröva frågor enligt 5 a § tredje stycket lagen (2008:717) om	2. pröva frågor enligt 5 a § tredje stycket lagen (2008:717) om

[1] Senaste lydelse 2010:1399.

signalspaning i försvarsunderrättelseverksamhet om tillstånd i pågående och tillståndsprövade inhämtningsuppdrag, om prövningen är av enkel beskaffenhet och endast avser tillgång till signalbärare eller användning av sökbegrepp som inte är direkt hänförliga till viss fysisk person.	signalspaning i försvarsunderrättelseverksamhet om tillstånd i pågående och tillståndsprövade inhämtningsuppdrag, om prövningen är av enkel beskaffenhet och endast avser tillgång till signalbärare eller användning av sökbegrepp som inte är direkt hänförliga till viss fysisk person, *och*
	3. fatta beslut om ersättning till integritetsskyddsombud.

Ordföranden får förordna en lagfaren tjänsteman vid domstolen att ensam på domstolens vägnar vidta förberedande åtgärder.

12 §

När en ansökan om tillstånd till signalspaning har kommit in till domstolen, ska domstolen så snart som möjligt *utse ett integritetsskyddsombud i målet och* hålla ett sammanträde. Vid sammanträdet ska ansökande myndighet och integritetsskyddsombudet närvara. Domstolen får förordna att annan som kan lämna upplysningar av betydelse för prövningen får närvara vid sammanträdet.	När en ansökan om tillstånd till signalspaning har kommit in till domstolen, ska domstolen så snart som möjligt hålla ett sammanträde. Vid sammanträdet ska ansökande myndighet och *det integritetsskyddsombud som domstolen utser* närvara. Domstolen får förordna att annan som kan lämna upplysningar av betydelse för prövningen får närvara vid sammanträdet.

Om ärendet är så brådskande att ett dröjsmål allvarligt skulle riskera syftet med ansökan, får sammanträde hållas och beslut fattas utan att ett integritetsskyddsombud har varit närvarande eller annars fått tillfälle att yttra sig.

När ett beslut enligt 10 § första stycket 2 har fattats av ordföranden på domstolens vägnar ska det integritetsskyddsombud som varit närvarande vid prövningen av det inhämtningsuppdrag till vilket beslutet är hänförligt underrättas.	*När ett beslut enligt andra stycket har fattats ska ett integritetsskyddsombud underrättas.* När ett beslut enligt 10 § första stycket 2 har fattats av ordföranden på domstolens vägnar ska det integritetsskyddsombud som varit närvarande vid prövningen av det inhämtningsuppdrag till vilket beslutet är hänförligt under-rättas. *Om integritetsskyddsombudets förordnande har upphört, får ett annat integritetsskyddsombud underrättas.*

Denna lag träder i kraft den 1 oktober 2025.

Förslag till lag om ändring av lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt

Härigenom föreskrivs i fråga om lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt

dels att 1 kap. 2 § och 2 kap. 9, 18 och 20 §§ ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 2 kap. 6 a och 6 b §§, och närmast före 2 kap. 6 a § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
2 §	
Denna lag gäller vid behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet samt informationssäkerhetsverksamhet.	Denna lag gäller vid behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse-, utvecklings-, och *övningsverksamhet* samt informationssäkerhetsverksamhet.
2 kap.	
	Övningsverksamhet
	6 a §
	Personuppgifter får behandlas i Försvarets radioanstalts övningsverksamhet om det är nödvändigt för att bedriva sådan verksamhet som anges i 1 a § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.
	6 b §
	Personuppgifter som behandlas med stöd av 6 a § får även behandlas om det är nödvändigt för att tillhandahålla information som behövs
	1. med anledning av samverkan med annan i fråga om övningsverksamhet, eller
	2. med anledning av samarbete om övningsverksamhet med andra länder eller internationella organisationer enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

9 §

Försvarets radioanstalt får behandla personuppgifter som utgör allmänt tillgänglig information om det är nödvändigt för den verksamhet som anges i 2, 5 och 7 §§.	Försvarets radioanstalt får behandla personuppgifter som utgör allmänt tillgänglig information om det är nödvändigt för den verksamhet som anges i 2, 5, *6 a* och 7 §§.

18 §

Hantering av information som innebär behandling av personuppgifter ska inte anses oförenlig med bestämmelserna i 1, 2, 5, 7, 9, 11–14 och 16 §§ i det skede av behandlingen då det inte har kunnat fastställas vilka personuppgifter som informationen innehåller.	Hantering av information som innebär behandling av personuppgifter ska inte anses oförenlig med bestämmelserna i 1, 2, 5, *6* a, 7, 9, 11–14 och 16 §§ i det skede av behandlingen då det inte har kunnat fastställas vilka personuppgifter som informationen innehåller.

20 §[1]

Personuppgifter som behandlas med stöd av denna lag får föras över till ett annat land eller en internationell organisation endast om det är nödvändigt för att Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet och	Personuppgifter som behandlas med stöd av denna lag får föras över till ett annat land eller en internationell organisation endast om det är nödvändigt för att Försvarets radioanstalt ska kunna fullgöra sina uppgifter inom ramen för det internationella försvarsunderrättelse- och säkerhetssamarbetet *eller övningssamarbetet* och

1. överföringen riktas till en utländsk underrättelse- eller säkerhetstjänst, eller ett underrättelse- eller säkerhetsorgan i en internationell organisation,
2. sekretess inte hindrar en överföring,
3. mottagaren garanterar tillräckligt skydd för personuppgifterna, och
4. överföringen inte innebär ett oproportionerligt intrång i den registrerades personliga integritet.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela föreskrifter om att överföring får ske även i andra fall än som anges i första stycket 1.

Regeringen får också besluta om sådan överföring i ett enskilt fall.

Denna lag träder i kraft den 1 oktober 2025.

[1] Senaste lydelse 2024:426.

Förteckning över remissinstanserna

Efter remiss av betänkandet Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning (SOU 2024:59) har yttranden kommit in från Arbetsgivarverket, Centrum för rättvisa, Fortifikationsverket, Försvarets materielverk, Försvarets radioanstalt, Försvarshögskolan, Försvarsmakten, Försvarsunderrättelsedomstolen, Förvaltningsrätten i Stockholm, Göteborgs tingsrätt, Inspektionen för strategiska produkter, Institutet för mänskliga rättigheter, Integritetsskyddsmyndigheten, Justitiekanslern, Myndigheten för samhällsskydd och beredskap, Myndigheten för psykologiskt försvar, Polismyndigheten, Post- och telestyrelsen, Riksarkivet, Statens inspektion för försvarsunderrättelseverksamheten, Statskontoret, Svea hovrätt, Sveriges advokatsamfund, Säkerhetspolisen, Tjänstemännens centralorganisation (TCO), Totalförsvarets forskningsinstitut, Tullverket, Umeå universitet och Åklagarmyndigheten.

Därutöver har yttranden kommit in från Föreningen för Digitala Fri- och Rättigheter, Journalistförbundet och två privatpersoner.

Följande remissinstanser har inte svarat eller angett att de avstår från att lämna några synpunkter: Civil Rights Defenders, Forum för Dataskydd, GlobalConnect AB, Hi3G Access AB, Internetstiftelsen, Landsorganisationen i Sverige (LO), Regelrådet, Riksdagens ombudsmän (JO), Svenska Stadsnätsföreningen, Sveriges Akademikers Centralorganisation (SACO), TechSverige, Tele2 AB, Telenor Sverige AB och Telia Company AB.