Utkast till lagrådsremiss

Datalagring och tillgång till elektronisk information

Stockholm XXXXXX

XXXXXX

XXXXXX
(Justitiedepartementet)

Utkastets huvudsakliga innehåll

Regelverket om datalagring innebär bland annat skyldigheter för tillhandahållare av elektroniska kommunikationsnät och elektroniska kommunikationstjänster att lagra viss information i brottsbekämpande syfte.

Det är av vikt att tillgången till information upprätthålls över tid i takt med samhällsutvecklingen, teknikutvecklingen och förändrade kommunikationsvanor, samtidigt som respekten för grundläggande fri- och rättigheter säkerställs. I utkastet lämnas därför lagförslag om bland annat följande:

- Säkerhetspolisen ska kunna besluta om en mer omfattande lagringsskyldighet om landet står inför ett allvarligt hot mot nationell säkerhet.
- Tillhandahållare av nummeroberoende interpersonella kommunikationstjänster ska omfattas av regler om lagringsskyldighet och ska anpassa sin verksamhet så att hemliga tvångsmedel kan verkställas.
- Lagringstiden för uppgifter om abonnemang ska förlängas, det ska införas sanktioner för bristande uppfyllelse av lagringsskyldighet och reglerna ska i övrigt uppdateras och göras tydligare för både tillhandahållare och myndigheter.

Lagändringarna föreslås träda i kraft den 1 mars 2026.

Innehållsförteckning

1 Lagtext

1.1 Förslag till lag om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet

Härigenom föreskrivs följande.

Lagens innehåll

1 § Denna lag innehåller bestämmelser om när uppgifter om elektronisk kommunikation får lagras och lämnas ut för att skydda Sveriges säkerhet.

Nationell säkerhetslagring

2 § Säkerhetspolisen får besluta att den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § lagen (2022:482) om elektronisk kommunikation eller den som tillhandahåller en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst enligt samma lag ska lagra uppgifter i enlighet med vad som följer av denna lag (beslut om nationell säkerhetslagring). Ett sådant beslut får endast fattas om det finns ett allvarligt hot mot Sveriges säkerhet och det är absolut nödvändigt.

Ett beslut får gälla i högst ett år och omfattningen ska begränsas till vad som är absolut nödvändigt. Säkerhetspolisen får genom ett nytt beslut förlänga lagringsskyldigheten om hotet mot Sveriges säkerhet består. Om det inte längre finns skäl för nationell säkerhetslagring, ska Säkerhetspolisen upphäva beslutet.

I 9 kap. 19 b och 22 §§ lagen om elektronisk kommunikation anges vilka uppgifter som får omfattas av ett beslut om nationell säkerhetslagring respektive hur länge uppgifterna ska lagras.

Ett beslut om nationell säkerhetslagring får verkställas omedelbart.

Offentligt ombud för nationell säkerhetslagring

3 § Ett offentligt ombud för nationell säkerhetslagring ska bevaka enskildas intressen i ärenden om nationell säkerhetslagring.

4 § Regeringen förordnar för högst tre år i sänder en person som ska tjänstgöra som ordinarie offentligt ombud för nationell säkerhetslagring och två personer som ska vara det ordinarie ombudets ställföreträdare.

Ombudet ska vara svensk medborgare och ska

– ha varit ordinarie domare, eller

– vara eller ha varit advokat eller ha motsvarande juridisk erfarenhet.

Ombudet får inte vara i konkurstillstånd eller ha förvaltare enligt 11 kap. 7 § föräldrabalken.

Regeringen ska inhämta förslag på lämpliga kandidater från Domarnämnden och Sveriges advokatsamfund.

Ombudet får trots att regeringens förordnande har upphört slutföra pågående uppdrag.

5 § Den som har förordnats som offentligt ombud för nationell säkerhetslagring får inte obehörigen röja vad han eller hon har fått kännedom om i ett ärende om nationell säkerhetslagring.

Underställning av beslutet hos Försvarsunderrättelsedomstolen

6 § När ett beslut om nationell säkerhetslagring har fattats ska beslutet omedelbart underställas Försvarsunderrättelsedomstolen.

Försvarsunderrättelsedomstolen ska så snart som möjligt hålla ett sammanträde. Vid sammanträdet ska Säkerhetspolisen och det offentliga ombudet för nationell säkerhetslagring närvara. Försvarsunderrättelsedomstolen har vid sammanträdet rätt att ta del av de omständigheter som ligger till grund för beslutet om nationell säkerhetslagring. Vid sammanträdet ska Säkerhetspolisen redogöra för beslutet och ombudet har rätt att yttra sig.

7 § Försvarsunderrättelsedomstolen ska pröva om Säkerhetspolisens beslut om nationell säkerhetslagring ska fortsätta att gälla. Domstolen ska även besluta om ersättning till det offentliga ombudet för nationell säkerhetslagring. I fråga om ersättning till ombudet tillämpas bestämmelserna i 21 kap. 10 § första och andra styckena rättegångsbalken. Försvarsunderrättelsedomstolens beslut om nationell säkerhetslagring och ersättning får inte överklagas.

Tillgång till lagrade uppgifter

8 § Uppgifter som har lagrats enligt ett beslut enligt 2 § får endast hämtas in efter ett tillstånd till hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation enligt 27 kap. 18 eller 19 § rättegångsbalken eller ett tillstånd till inhämtning enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Uppgifter får endast hämtas in enligt första stycket om det i tillståndet har angetts att inhämtningen får avse uppgifter som har lagrats med stöd av denna lag.

9 § Uppgifter får hämtas in enligt 8 § endast i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott som anges i andra stycket eller för att utreda och beivra sådana brott.

De brott som ger rätt till inhämtning av uppgifter som lagrats enligt ett beslut enligt 2 § är

1. sabotage eller grovt sabotage enligt 13 kap. 4 eller 5 § brottsbalken,
2. mordbrand, grov mordbrand, allmänfarlig ödeläggelse, kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 1, 2, 3, 5 a eller 5 b § brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
3. uppror, väpnat hot mot laglig ordning eller brott mot medborgerlig frihet enligt 18 kap. 1, 3 eller 5 § brottsbalken,
4. högförräderi, krigsanstiftan, spionerі, grovt spionerі, utlandsspionerі, grovt utlandsspionerі, obehörig befattning med hemlig uppgift, grov obe-

hörig befattning med hemlig uppgift eller olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person enligt 19 kap. 1, 2, 5, 6, 6 a, 6 b, 7, 8, 10, 10 a eller 10 b § brottsbalken,

5. företagsspionerі enligt 26 § lagen (2018:558) om företagshemligheter, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning,

6. terroristbrott, deltagande i en terroristorganisation, samröre med en terroristorganisation, finansiering av terrorism eller särskilt allvarlig brottslighet, offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet, rekrytering till terrorism eller särskilt allvarlig brottslighet, utbildning för terrorism eller särskilt allvarlig brottslighet eller resa för terrorism eller särskilt allvarlig brottslighet enligt 4, 4 a, 5, 6, 7, 8, 9 eller 10 § terroristbrottslagen (2022:666),

7. andra brott än de som anges i 1–6 och som på grund av sin omfattning eller karaktär utgör ett allvarligt hot mot Sveriges säkerhet, om det för brottet inte är föreskrivet lindrigare straff än fängelse i två år, eller

8. försök, förberedelse eller stämpling till brott som avses i 1–7, om en sådan gärning är belagd med straff.

Denna lag träder i kraft den 1 mars 2026.

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

Härigenom föreskrivs att 10 kap. 10 §, 18 kap. 19 §, 29 kap. 2 §, 35 kap. 1 och 24 §§, och 44 kap. 4 och 5 §§ offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

10 kap.

10 §[1]

Sekretess hindrar inte att den som är knuten till en myndighet på det sätt som anges i 2 kap. 1 § andra stycket och som är misstänkt för brott eller mot vilken rättegång eller annat jämförbart rättsligt förfarande har inletts, lämnar uppgift till sitt ombud eller biträde i saken eller till någon annan enskild, om det behövs för att han eller hon ska kunna ta till vara sin rätt.

Sekretess hindrar inte att uppgift i ett ärende hos domstol eller i ett beslut i ett sådant ärende lämnas till ett offentligt ombud enligt rättegångsbalken eller till ett integritetsskyddsombud enligt lagen (2009:966) om Försvarsunderrättelsedomstol.

Sekretess hindrar inte att uppgift i ett ärende om nationell säkerhetslagring lämnas till ett offentligt ombud för nationell säkerhetslagring enligt lagen (2025:000) om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

18 kap.

19 §[2]

Den tystnadsplikt som följer av 5–7, 8, 9 och 10 §§, 11 § första stycket, 12, 12 a och 13 §§ inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning *eller* hemlig dataavläsning på grund av beslut av domstol, undersöknings-

Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning, hemlig dataavläsning på grund av beslut av domstol, undersökningsledare eller

[1] Senaste lydelse 2009:1020.
[2] Senaste lydelse 2024:477.

ledare eller åklagare *eller* inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.	åklagare*,* inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet *eller nationell säkerhetslagring enligt lagen (2025:000) om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.*

Den tystnadsplikt som följer av 17 § inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning på grund av beslut av domstol eller åklagare.

Att den tystnadsplikt som följer av 1–3 §§ i vissa fall inskränker rätten att meddela och offentliggöra uppgifter utöver det som anges i andra stycket följer av 7 kap. 10 §, 12–18 §§, 20 § 3 och 22 § första stycket 1 och andra stycket tryckfrihetsförordningen samt 5 kap. 1 § och 4 § första stycket 1 och andra stycket yttrandefrihetsgrundlagen.

29 kap.

2 §[3]

Sekretess gäller hos en myndighet som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst för uppgift om innehållet i ett elektroniskt meddelande eller *annan uppgift som angår ett särskilt elektroniskt meddelande*. Om sekretess inte följer av någon annan bestämmelse, får dock sådan uppgift lämnas till den som har tagit del i utväxlingen av ett elektroniskt meddelande eller som på något annat sätt har sänt eller tagit emot ett sådant meddelande. Detsamma gäller innehavaren av ett abonnemang som använts för ett elektroniskt meddelande när det är fråga om uppgift om något annat än innehållet i meddelandet.	Sekretess gäller hos en myndighet som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst för uppgift om innehållet i ett elektroniskt meddelande eller *en trafikuppgift*. Om sekretess inte följer av någon annan bestämmelse, får dock *en* sådan uppgift lämnas till den som har tagit del i utväxlingen av ett elektroniskt meddelande eller som på något annat sätt har sänt eller tagit emot ett sådant meddelande. Detsamma gäller innehavaren av ett abonnemang som använts för ett elektroniskt meddelande när det är fråga om uppgift om något annat än innehållet i meddelandet.

[3] Senaste lydelse 2012:288.

35 kap.

1 §[4]

Sekretess gäller för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i

1. utredning enligt bestämmelserna om förundersökning i brottmål,
2. angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott eller i ärende enligt lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder,
3. angelägenhet som avser säkerhetsprövning enligt säkerhetsskyddslagen (2018:585),
4. annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott eller verkställa uppbörd och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen,
5. register som förs av Polismyndigheten enligt 5 kap. lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas med stöd av de bestämmelserna, eller uppgifter som behandlas av Säkerhetspolisen eller Polismyndigheten med stöd av lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter,
6. register som förs enligt lagen (1998:621) om misstankeregister,
7. register som förs av Skatteverket enligt lagen (2018:1696) om Skatteverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag,
8. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 5 kap. 1 §,
9. register som förs av Tullverket enligt lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag, *eller*
10. utredning om självständigt förverkande.

9. register som förs av Tullverket enligt lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag,
10. utredning om självständigt förverkande*, eller*
11. angelägenhet som avser nationell säkerhetslagring enligt lagen (2025:000) om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

Sekretessen enligt första stycket 2 gäller hos domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till honom eller henne lider skada eller men om uppgiften röjs. Vid förhandling om användning av tvångsmedel gäller sekretess för uppgift om vem som är misstänkt endast om det kan antas att fara uppkommer för att den misstänkte eller någon närstående till honom

[4] Senaste lydelse 2024:788.

eller henne utsätts för våld eller lider annat allvarligt men om uppgiften röjs.

Första stycket gäller inte om annat följer av 2, 6 eller 7 §.

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

Lydelse enligt prop. 2024/25:20	*Föreslagen lydelse*
24 §	
Den tystnadsplikt som följer av 11 §, 12 a § och den tystnadsplikt som följer av ett förbehåll som har gjorts med stöd av 9 § andra stycket inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.	Den tystnadsplikt som följer av *1 § 11,* 11, 12 a § och den tystnadsplikt som följer av ett förbehåll som har gjorts med stöd av 9 § andra stycket inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Den tystnadsplikt som följer av 15 och 16 §§ inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift vars röjande kan antas medföra fara för att någon utsätts för våld eller lider annat allvarligt men.

Nuvarande lydelse	*Föreslagen lydelse*
44 kap.	
4 §[5]	
Rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter inskränks av den tystnadsplikt som följer av	
1. 5 kap. 1 § första stycket 1 samt 2 och 3 §§ postlagen (2010:1045),	
2. 1 kap. 15 § lagen (2022:482) om elektronisk kommunikation, när det är fråga om uppgift om förhållanden av betydelse för att förebygga eller hantera fredstida krissituationer,	
3. 9 kap. 31 § lagen om elektronisk kommunikation, när det är fråga om uppgift om innehållet i ett elektroniskt meddelande eller som annars rör ett särskilt sådant meddelande, och	
4. 9 kap. 32 § lagen om elektronisk kommunikation, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation på grund av beslut av domstol, undersökningsledare eller åklagare *eller* om inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brotts-	4. 9 kap. 32 § lagen om elektronisk kommunikation, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation på grund av beslut av domstol, undersökningsledare eller åklagare*,* om inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brotts-

[5] Senaste lydelse 2024:191.

bekämpande myndigheternas underrättelseverksamhet.	bekämpande myndigheternas underrättelseverksamhet *eller om nationell säkerhetslagring enligt lagen (2025:000) om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.*

5 §[6]

Rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter inskränks av den tystnadsplikt som följer

1. av beslut som har meddelats med stöd av 7 § lagen (1999:988) om förhör m.m. hos kommissionen för granskning av de svenska säkerhetstjänsternas författningsskyddande verksamhet,
2. av 7 kap. 1 § 1 lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap,
3. av 4 kap. 16 § försäkringsrörelselagen (2010:2043),
4. av 5 kap. 15 § lagen (1998:293) om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige,

5. av 32 § lagen (2020:62) om hemlig dataavläsning, *och*	5. av 32 § lagen (2020:62) om hemlig dataavläsning,
6. av 4 § lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter.	6. av 4 § lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter*, och*
	7. av 5 § lagen (2025:000) om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

Denna lag träder i kraft den 1 mars 2026.

[6] Senaste lydelse 2023:335.

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

Härigenom föreskrivs att 1 och 5 §§ lagen (2009:966) om Försvarsunderrättelsedomstol ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 §
Försvarsunderrättelsedomstolen ska pröva frågor om tillstånd till signalspaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.	Försvarsunderrättelsedomstolen ska pröva frågor om tillstånd till signalspaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet. *Försvarsunderrättelsedomstolen ska även överpröva Säkerhetspolisens beslut om nationell säkerhetslagring enligt lagen (2025:000) om lagring av och tillgång till uppgifter om elektronisk information i syfte att skydda Sveriges säkerhet.*
	5 §
Ett integritetsskyddsombud ska bevaka enskildas integritetsintresse i mål vid domstolen. Ombudet har rätt att ta del av det som förekommer i målet och att yttra sig.	Ett integritetsskyddsombud ska bevaka enskildas integritetsintresse i mål vid domstolen *om tillstånd till signalspaning*. Ombudet har rätt att ta del av det som förekommer i målet och att yttra sig.

Denna lag träder i kraft den 1 mars 2026.

1.4 Förslag till lag om ändring i säkerhetsskyddslagen (2018:585)

Härigenom föreskrivs att 3 kap. 1 § säkerhetsskyddslagen (2018:585) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
3 kap.	
1 §[7]	
Den som genom en anställning eller på något annat sätt ska delta i säkerhetskänslig verksamhet ska säkerhetsprövas. Säkerhetsprövning ska dock inte göras när det gäller	
1. uppdrag som statsråd, ledamot av Europaparlamentet, riksdagen eller kommun- och regionfullmäktige, eller	1. uppdrag som statsråd *eller som* ledamot av Europaparlamentet, riksdagen eller kommun- och regionfullmäktige, eller
2. annat uppdrag som offentlig försvarare eller ombud inför domstol än sådant som avser offentligt ombud enligt 27 kap. 27 § rättegångsbalken *eller* integritetsskyddsombud enligt 6 § lagen (2009:966) om Försvarsunderrättelsedomstol.	2. annat uppdrag som offentlig försvarare eller ombud inför domstol än sådant som avser offentligt ombud enligt 27 kap. 27 § rättegångsbalken, integritetsskyddsombud enligt 6 § lagen (2009:966) om Försvarsunderrättelsedomstol *eller ombud för nationell säkerhetslagring enligt lagen (2025:000) om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet*.

Denna lag träder i kraft den 1 mars 2026.

[7] Senaste lydelse 2019:985.

1.5 Förslag till lag om ändring i lagen (2022:482) om elektronisk kommunikation

Härigenom föreskrivs i fråga om lagen (2022:482) om elektronisk kommunikation

dels att 8 kap. 5 §, 9 kap. 1, 10, 19–23, 29–29 b, 31–33 §§ och 12 kap. 1 § ska ha följande lydelse,

dels att det ska införas fyra nya paragrafer, 9 kap. 19 a, 19 b, 19 c och 22 a §§, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
8 kap.	
5 §[8]	
Den som enligt 9 kap. 19 *§* är skyldig att lagra uppgifter ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling.	Den som enligt 9 kap. 19*, 19 a eller 19 b §* är skyldig att lagra uppgifter ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling.
Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § och som har förelagts enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift ska avseende den uppgiften vidta sådana åtgärder som anges i första stycket.	Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § *eller tillhandahåller en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst* och som har förelagts enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift ska avseende den uppgiften vidta sådana åtgärder som anges i första stycket.
Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om sådana skyddsåtgärder.	
9 kap.	
1 §	
Den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst ska utplåna eller avidentifiera trafikuppgifter som har lagrats eller behandlats på något annat sätt när de inte längre behövs för överföring av ett elektroniskt meddelande. Detta gäller under förutsättning att uppgifterna avser användare som är fysiska personer eller abonnenter.	
Första stycket *avser* inte uppgifter som sparas för sådan behandling som anges i 2, 15, 19 eller 21 § eller om uppgifterna behövs för en sådan behandling som är tillåten enligt Europaparlamentets och rådets förordning (EU) 2021/1232 av den 14 juli 2021 om ett tillfälligt undan-	Första stycket *gäller* inte uppgifter som sparas för sådan behandling som anges i 2, 15, 19*, 19 b* eller 21 § eller om uppgifterna behövs för en sådan behandling som är tillåten enligt Europaparlamentets och rådets förordning (EU) 2021/1232 av den 14 juli 2021 om ett tillfälligt

[8] Senaste lydelse 2022:1086.

tag från vissa bestämmelser i direktiv 2002/58/EG vad gäller användning av teknik hos tillhandahållare av nummeroberoende interpersonella kommunikationstjänster för behandling av personuppgifter och andra uppgifter i syfte att bekämpa sexuella övergrepp mot barn på nätet.

undantag från vissa bestämmelser i direktiv 2002/58/EG vad gäller användning av teknik hos tillhandahållare av nummeroberoende interpersonella kommunikationstjänster för behandling av personuppgifter och andra uppgifter i syfte att bekämpa sexuella övergrepp mot barn på nätet.

10 §

Lokaliseringsuppgifter som omfattas av ett beslut om inhämtning av uppgifter enligt 27 kap. rättegångsbalken eller lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet får behandlas trots 7–9 §§.

Lokaliseringsuppgifter som lagras enligt 19 b § får behandlas trots 7–9 §§.

19 §

Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § ska lagra sådana uppgifter som avses i 31 § första stycket 1 och 3 som är nödvändiga för att spåra och identifiera kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning vid kommunikationens början och slut.

Lagringsskyldigheten omfattar uppgifter som genereras eller behandlas vid

1. telefonitjänst eller meddelandehantering via mobil nätanslutningspunkt, eller
2. internetåtkomst.

Även vid misslyckad uppringning gäller skyldigheten att lagra uppgifter som genereras eller behandlas. För telefonitjänst gäller lagringsskyldigheten inte uppgift om nummer som ett samtal styrts till.

Den som enligt denna paragraf ska lagra uppgifter får uppdra åt någon annan att utföra lagringen.

19 a §

Den som tillhandahåller en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst ska lagra sådana uppgifter som avses i 31 § första stycket 1 som kan användas för att identifiera en abonnent och registrerad användare.

Lagringsskyldigheten som gäller för allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster omfattar upp-

gifter som genereras eller behandlas vid tjänster som tillhandahåller samtal och meddelandehantering vid kommunikation som sker till, från eller inom Sverige.

Vid lagring enligt 19 b § av uppgifter som avses i 31 § första stycket 4 omfattar lagringsskyldigheten endast uppgifter som avser lokalisering i Sverige.

Även vid misslyckad uppringning gäller skyldigheten att lagra uppgifter som genereras eller behandlas.

19 b §

Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § och den som tillhandahåller en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst ska lagra de uppgifter som framgår av ett beslut enligt lagen (2025:000) om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

Beslutet får omfatta sådana uppgifter som avses i 31 § första stycket 1, 3 och 4 som är nödvändiga för att spåra och identifiera kommunikationskällan och slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning, lokalisering av kommunikationsutrustning vid kommunikationen samt lokaliseringsuppgifter som inte är trafikuppgifter.

19 c §

Den som ska lagra uppgifter enligt 19, 19 a eller 19 b § får ge någon annan i uppdrag att utföra lagringen.

20 §

Tillsynsmyndigheten får i enskilda fall besluta om undantag från skyldigheten enligt 19 § att lagra upp-

Tillsynsmyndigheten får i enskilda fall besluta om undantag från skyldigheten enligt 19 *eller 19 a §* att

gifter, om det finns synnerliga skäl för det. Beslutet får förenas med villkor.

lagra uppgifter, om det finns synnerliga skäl för det. Beslutet får förenas med villkor.

Beslutet om undantag får återkallas om villkoren i beslutet inte har följts eller det finns andra särskilda skäl för återkallelse.

21 §

Uppgifter som har lagrats enligt 19 § får behandlas endast för att lämnas ut enligt

Trafikuppgifter som avses i 31 § första stycket 3 och som har lagrats enligt 19 § får behandlas endast för att lämnas ut enligt

1. 33 § första stycket 2 eller 5,
2. 27 kap. 19 § rättegångsbalken, eller
3. lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Uppgifter som har lagrats enligt 19 b § får behandlas enbart för att lämnas ut enligt 8 § lagen (2025:000) om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

22 §

Uppgifter som avses i 19 § ska lagras enligt följande:

– Uppgifter som genereras eller behandlas vid telefonitjänst och meddelandehantering via mobil nätanslutningspunkt ska lagras i sex månader. Lokaliseringsuppgifter ska dock lagras i endast två månader.

– Uppgifter som genereras eller behandlas vid telefonitjänst och meddelandehantering via mobil nätanslutningspunkt ska lagras i sex månader. Lokaliseringsuppgifter ska dock lagras i endast två månader. *Uppgifter som avses i 31 § första stycket 1 ska lagras i ett år.*

– Uppgifter som genereras eller behandlas vid internetåtkomst ska lagras i tio månader. Om uppgifterna identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten, ska de dock lagras i endast sex månader.

– Uppgifter som genereras eller behandlas vid internetåtkomst ska lagras i tio månader. Om uppgifterna identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten, ska de dock lagras i endast sex månader. *Uppgifter som avses i 31 § första stycket 1 ska lagras i ett år.*

Uppgifter som avses i 19 a § första stycket ska lagras i ett år.

Uppgifter som avses i 19 b § ska lagras enligt följande:

– Uppgifter i 31 § första stycket 1 och 3 ska lagras i två år.

	– Uppgifter i 31 § första stycket 4 ska lagras i ett år.
Lagringstiden räknas från den dag kommunikationen avslutades.	

När lagringstiden har löpt ut ska den lagringsskyldige genast utplåna uppgifterna. Om en begäran om utlämnande i fall som avses i 21 § har kommit in eller ett föreläggande enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift har meddelats innan lagringstiden löpt ut, ska den lagringsskyldige dock fortsätta lagra uppgifterna till dess att de har lämnats ut eller tiden för bevarande har löpt ut. Därefter ska uppgifterna genast utplånas.

	22 a § *Lagringstiden enligt 22 § räknas från den dag kommunikationen avslutades. Om uppgift saknas om när kommunikationen avslutades räknas lagringstiden från den dag uppgifterna genererades.* *För uppgifter som avses i 31 § första stycket 1 räknas lagringstiden från den dag abonnemanget eller tilldelningen av en tillfällig identifierare upphörde.* *För lokaliseringsuppgifter som inte är trafikuppgifter räknas lagringstiden från den dag uppgifterna genererades.* *Vid meddelandehantering via en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst räknas lagringstiden från den dag meddelandet skickades.*

23 §[9]

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om

1. vilka uppgifter som ska lagras enligt 19 *§*, och	1. vilka uppgifter som ska lagras enligt 19*, 19 a och 19 b §§*, och
2. lagringstiden enligt 22 § *första stycket*.	2. lagringstiden enligt 22 § *första–tredje styckena och 22 a §*.

29 §[10]

En verksamhet ska bedrivas så att beslut om hemlig avlyssning av elektronisk kommunikation *och* hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs*, om verksamheten avser tillhandahållande av*	*Den som är skyldig att lagra uppgifter enligt 19, 19 a eller 19 b § ska bedriva sin verksamhet* så att beslut om hemlig avlyssning av elektronisk kommunikation*,* hemlig övervakning av elektronisk kommunikation *och inhämtning enligt lagen (2012:278) om inhämtning av*

[9] Senaste lydelse 2022:1086.
[10] Senaste lydelse 2022:1086.

uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet kan verkställas och så att verkställandet inte röjs.

1. ett allmänt elektroniskt kommunikationsnät som inte enbart är avsett för utsändning till allmänheten av program som avses i 1 kap. 2 § yttrandefrihetsgrundlagen, eller

2. tjänster inom ett allmänt elektroniskt kommunikationsnät som består av

a) en allmänt tillgänglig telefonitjänst till en fast nätanslutningspunkt som medger överföring av lokala, nationella och internationella samtal, telefax och datakommunikation med en sådan lägsta datahastighet som medger funktionell tillgång till internet, eller

b) en allmänt tillgänglig elektronisk kommunikationstjänst till en mobil nätanslutningspunkt.

Första stycket gäller inte vid tillhandahållande av maskin-till-maskin-tjänster.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om frågor som avses i första stycket samt får i enskilda fall besluta om undantag från kravet i första stycket.

29 a §[11]

Den som *bedriver verksamhet som ska anmälas enligt 2 kap. 1 §* har rätt till ersättning för kostnader som uppstår när uppgifter som avses i 31 § första stycket lämnas ut till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott. I de fall det är särskilt föreskrivet ska ersättningen beräknas enligt schablon. Ersättningen ska betalas av den myndighet som har begärt uppgifterna.

Den som *är skyldig att lagra uppgifter enligt 19, 19 a eller 19 b §* har rätt till ersättning för kostnader som uppstår när uppgifter som avses i 31 § första stycket lämnas ut till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott. I de fall det är särskilt föreskrivet ska ersättningen beräknas enligt schablon. Ersättningen ska betalas av den myndighet som har begärt uppgifterna.

[11] Senaste lydelse 2022:1086. Ändringen innebär bl.a. att andra stycket tas bort.

Första stycket gäller även lokaliseringsuppgifter som inte är trafikuppgifter.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om ersättningen och schablonberäkningen.

29 b §[12]

När den som *bedriver verksamhet som ska anmälas enligt 2 kap. 1 §* lämnar ut uppgifter som avses i 31 § första stycket till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott, ska utlämnandet, om uppgifterna gäller brottslig verksamhet eller misstanke om brott, göras utan dröjsmål och på ett sådant sätt att utlämnandet inte röjs.

När den som *är skyldig att lagra uppgifter enligt 19, 19 a eller 19 b §* lämnar ut uppgifter som avses i 31 § första stycket till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott, ska utlämnandet, om uppgifterna gäller brottslig verksamhet eller misstanke om brott, göras utan dröjsmål och på ett sådant sätt att utlämnandet inte röjs.

Uppgifterna ska ordnas och göras tillgängliga i ett format som gör att de enkelt kan tas om hand.

Första och andra styckena gäller även lokaliseringsuppgifter som inte är trafikuppgifter.

Tillsynsmyndigheten får i enskilda fall besluta om undantag från kravet i andra stycket, om det finns särskilda skäl för det.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om hur uppgifterna ska lämnas ut.

31 §

Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst *som inte är en nummeroberoende interpersonell kommunikationstjänst,* får inte obehörigen föra vidare eller utnyttja det som han eller hon i samband med tillhandahållandet har fått del av eller tillgång till i form av

1. en uppgift om abonnemang,
2. innehållet i ett elektroniskt meddelande, *eller*
3. en *annan uppgift som angår ett särskilt elektroniskt meddelande.*

Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst får inte obehörigen föra vidare eller utnyttja det som han eller hon i samband med tillhandahållandet har fått del av eller tillgång till i form av

2. innehållet i ett elektroniskt meddelande,
3. en *trafikuppgift, eller*
4. *en lokaliseringsuppgift som inte är en trafikuppgift och som rör*

[12] Senaste lydelse 2022:1086. Ändringen innebär bl.a. att tredje stycket tas bort.

användare som är fysiska personer eller abonnenter.

För tillhandahållare av nummeroberoende interpersonella kommunikationstjänster gäller tystnadsplikten enligt första stycket endast vid sådan kommunikation som sker till, från eller inom Sverige samt för lokaliseringsuppgifter som inte är trafikuppgifter och som avser lokalisering i Sverige.

Tystnadsplikt som följer av första stycket gäller inte i förhållande till den som har tagit del i utväxlingen av ett elektroniskt meddelande eller som på något annat sätt har sänt eller tagit emot ett sådant meddelande.

Tystnadsplikt som följer av första stycket 1 *och* 3 gäller inte heller i förhållande till innehavaren av *ett abonnemang som har använts för ett elektroniskt meddelande*.

Tystnadsplikt som följer av första stycket 1*,* 3 *och 4* gäller inte heller i förhållande till innehavaren av *abonnemanget*.

32 §

Tystnadsplikt som följer av 31 § första stycket gäller även för en uppgift som hänför sig till

1. en åtgärd att med stöd av 27 kap. 9 § rättegångsbalken hålla kvar försändelser,
2. en angelägenhet som avser användning av hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation enligt 27 kap. 18 eller 19 § rättegångsbalken eller som gäller tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation eller med hemlig övervakning av elektronisk kommunikation enligt 4 kap. 25 b § lagen (2000:562) om internationell rättslig hjälp i brottmål,
3. en angelägenhet som avser inhämtning av signaler i elektronisk form enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet,
4. inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet,
5. en begäran enligt 33 § första stycket 2 om att en uppgift om abonnemang ska lämnas,
6. ett föreläggande enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift, *eller*
7. en begäran enligt 33 § första stycket 5 om att en uppgift om tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster ska lämnas.

6. ett föreläggande enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift,
7. en begäran enligt 33 § första stycket 5 om att en uppgift om tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster ska lämnas*, eller*
8. en angelägenhet som avser nationell säkerhetslagring enligt lagen (2025:000) om lagring av

och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

33 §[13]

Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst *som inte är en nummeroberoende interpersonell kommunikationstjänst* och som har fått del av eller tillgång till en uppgift som avses i 31 § första stycket ska på begäran lämna

Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och som har fått del av eller tillgång till en uppgift som avses i 31 § första stycket ska på begäran lämna

1. en uppgift som avses i 31 § första stycket 1 till

a) en myndighet som i ett särskilt fall behöver en sådan uppgift för delgivning enligt delgivningslagen (2010:1932), om myndigheten bedömer att det kan antas att den som söks för delgivning håller sig undan eller att det annars finns synnerliga skäl,

b) Finansinspektionen, om inspektionen bedömer att uppgiften är av väsentlig betydelse för utredningen av en misstänkt överträdelse av Europaparlamentets och rådets förordning (EU) nr 596/2014 av den 16 april 2014 om marknadsmissbruk (marknadsmissbruksförordning) och om upphävande av Europaparlamentets och rådets direktiv 2003/6/EG och kommissionens direktiv 2003/124/EG, 2003/125/EG och 2004/72/EG,

c) Finansinspektionen, om inspektionen bedömer att uppgiften är av väsentlig betydelse i ett ärende om tillsyn när det gäller någon av bestämmelserna i 4 a kap. 1–8 §§ lagen (2010:751) om betaltjänster eller 1 kap. 5 § eller 4 kap. 7, 8, 9, 10, 11 eller 14 § lagen (2016:1024) om verksamhet med bostadskrediter,

d) Konsumentombudsmannen, om ombudsmannen bedömer att uppgiften är av väsentlig betydelse i ett ärende om tillsyn enligt lagen (1994:1512) om avtalsvillkor i konsumentförhållanden eller marknadsföringslagen (2008:486), när det är fråga om en misstänkt överträdelse av unionslagstiftning som skyddar konsumenternas intressen enligt bilagan till Europaparlamentets och rådets förordning (EU) 2017/2394 av den 12 december 2017 om samarbete mellan de nationella myndigheter som har tillsynsansvar för konsumentskyddslagstiftningen och om upphävande av förordning (EG) nr 2006/2004,

e) Konsumentverket, om verket bedömer att uppgiften är av väsentlig betydelse i ett ärende om tillsyn enligt lagen (2019:59) med kompletterande bestämmelser till EU:s geoblockeringsförordning,

f) Kronofogdemyndigheten, om myndigheten behöver uppgiften i exekutiv verksamhet och myndigheten bedömer att uppgiften är av väsentlig betydelse för handläggningen av ett ärende,

g) Läkemedelsverket, om verket bedömer att uppgiften är av väsentlig betydelse i ett ärende om tillsyn när det gäller bestämmelserna om marknadsföring i 12 kap. läkemedelslagen (2015:315),

[13] Senaste lydelse 2024:330.

h) Polismyndigheten, om myndigheten bedömer att uppgiften behövs i samband med underrättelse, efterforskning eller identifiering vid olyckor eller dödsfall eller för att myndigheten ska kunna fullgöra en uppgift som avses i 12 § polislagen (1984:387),

i) Polismyndigheten, om myndigheten bedömer att uppgiften behövs i ett särskilt fall för att myndigheten ska kunna lokalisera en person som är dömd till fängelse, rättspsykiatrisk vård eller sluten ungdomsvård i syfte att möjliggöra verkställighet av påföljden,

j) Polismyndigheten eller en åklagarmyndighet, om myndigheten bedömer att uppgiften behövs i ett särskilt fall för att myndigheten ska kunna fullgöra en underrättelseskyldighet enligt 33 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare,

k) Skatteverket, om verket bedömer att uppgiften är av väsentlig betydelse för handläggningen av ett ärende som avser kontroll av skatt eller avgift eller rätt folkbokföringsort enligt folkbokföringslagen (1991:481), och

l) Säkerhetspolisen, om myndigheten bedömer att uppgiften behövs i ett särskilt fall för att myndigheten ska kunna lokalisera en utlänning som inte har fullgjort sin anmälningsskyldighet enligt lagen (2022:700) om särskild kontroll av vissa utlänningar,

2. en uppgift som avses i 31 § första stycket 1 och som gäller brottslig verksamhet eller misstanke om brott till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brottet eller den brottsliga verksamheten,

3. en uppgift som avses i 31 § första stycket 1 eller 3 till en regional alarmeringscentral som avses i lagen (1981:1104) om verksamheten hos vissa regionala alarmeringscentraler,

4. en uppgift som avses i 31 § första stycket 1 eller 3 samt uppgift om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits till Polismyndigheten, om myndigheten bedömer att uppgiften behövs i samband med efterforskning av personer som har försvunnit under sådana omständigheter att det kan antas att det då fanns eller fortfarande finns fara för deras liv eller allvarlig risk för deras hälsa, och

5. en uppgift som avses i 31 § första stycket 3 om vilka övriga tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster som har deltagit vid överföringen av ett meddelande som omfattas av ett föreläggande enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift till den myndighet som meddelat föreläggandet.

Ersättning för att lämna ut andra uppgifter enligt första stycket 3 än lokaliseringsuppgifter ska vara skälig med hänsyn till kostnaderna för utlämnandet.

12 kap.

1 §[14]

Tillsynsmyndigheten ska ta ut en sanktionsavgift av den som

[14] Senaste lydelse 2022:1086.

1. inte tillhandahåller en sammanfattning av avtalet i enlighet med 7 kap. 1 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 102.3 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,

2. inte tillämpar villkor om bindningstid eller uppsägningstid i enlighet med 7 kap. 8, 13 eller 14 §,

3. inte uppfyller kraven på nummerportabilitet i enlighet med 7 kap. 19 och 20 §§ eller föreskrifter om nummerportabilitet som har meddelats med stöd av 7 kap. 21 § första stycket,

4. inte vidtar åtgärder för att hantera risker som hotar säkerheten i nät och tjänster i enlighet med 8 kap. 1 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,

5. inte rapporterar om säkerhetsincidenter i enlighet med 8 kap. 3 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,

6. inte informerar om hot om säkerhetsincidenter i enlighet med 8 kap. 4 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,

7. inte vidtar skyddsåtgärder enligt 8 kap. 5 § eller föreskrifter som har meddelats med stöd av den paragrafen,

8. inte vidtar åtgärder för att säkerställa skydd av uppgifter som behandlas i samband med tillhandahållandet av en tjänst i enlighet med 8 kap. 6 § eller föreskrifter som har meddelats med stöd av den paragrafen,

9. inte informerar abonnenten om särskilda risker för bristande skydd av behandlade uppgifter i enlighet med 8 kap. 7 §,

10. inte underrättar om integritetsincidenter i enlighet med 8 kap. 8 § eller kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets direktiv 2002/58/EG vad gäller personlig integritet och elektronisk kommunikation,

11. inte behandlar uppgifter i ett elektroniskt meddelande eller trafikuppgifter som hör till detta meddelande i enlighet med 9 kap. 27 §,

12. inte bedriver sin verksamhet så att beslut om hemlig avlyssning av elektronisk kommunikation *och* hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs i enlighet med 9 kap. 29 § första stycket eller föreskrifter som har meddelats i anslutning till det stycket,

12. inte bedriver sin verksamhet så att beslut om hemlig avlyssning av elektronisk kommunikation*,* hemlig övervakning av elektronisk kommunikation *och inhämtning enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet* kan verkställas och så att verkställandet inte röjs i enlighet med 9 kap. 29 § första stycket eller föreskrifter som har meddelats i anslutning till det stycket,

13. inte ordnar uppgifter och gör dem tillgängliga i ett format som gör att de enkelt kan tas om hand i enlighet med 9 kap. 29 b § andra stycket eller föreskrifter som har meddelats i anslutning till det stycket,

14. inte överför signaler till samverkanspunkter i enlighet med 9 kap. 30 § eller föreskrifter som har meddelats med stöd av den paragrafen, *eller*

15. inte lämnar ut en uppgift i enlighet med 9 kap. 33 §.

14. inte överför signaler till samverkanspunkter i enlighet med 9 kap. 30 § eller föreskrifter som har meddelats med stöd av den paragrafen,

15. inte lämnar ut en uppgift i enlighet med 9 kap. 33 §, *eller*

16. inte lagrar uppgifter i enlighet med 9 kap. 19, 19 a, 19 b, 22 och 22 a §§ eller föreskrifter som har meddelats i anslutning till de paragraferna.

En sanktionsavgift enligt första stycket 2 ska, när det är fråga om ett paket enligt 7 kap. 26 §, tas ut endast om överträdelsen avser en allmänt tillgänglig elektronisk kommunikationstjänst som inte är en nummeroberoende interpersonell kommunikationstjänst eller en överföringstjänst som används för tillhandahållande av maskin-till-maskin-tjänster.

---

1. Denna lag träder i kraft den 1 mars 2026.

2. De nya bestämmelserna om sanktionsavgifter i 12 kap. 1 § första stycket 12 och 16 tillämpas endast på överträdelser som har skett efter ikraftträdandet.

2 Ärendet och dess beredning

Regeringen beslutade i augusti 2021 att ge en särskild utredare i uppdrag att se över den lagstiftning som medför en skyldighet för tillhandahållare av elektroniska kommunikationstjänster att lagra uppgifter om elektronisk kommunikation för brottsbekämpande syften, samt vissa anknytande frågor om myndigheternas tillgång till sådana uppgifter (dir. 2021:58). Utredningen, som antog namnet 2021 års datalagringsutredning, överlämnande i maj 2023 betänkandet Datalagring och åtkomst till elektronisk information (SOU 2023:22). En sammanfattning av betänkandet finns i *bilaga 1*. Betänkandets lagförslag finns i *bilaga 2*. Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 3*. Remissyttrandena finns tillgängliga i Justitiedepartementet (Ju2023/01326).

Som ett led i den fortsatta beredningen av detta lagstiftningsärende har det utarbetats ett utkast till lagrådsremiss. I utkastet behandlas merparten av förslagen i betänkandet. Utkastet behandlar dock inte betänkandets förslag om införande av s.k. riktad lagring för att bekämpa grov brottslighet. I denna del beslutade regeringen i juli 2023 att ge Brottsförebyggande rådet (Brå) i uppdrag att komplettera beredningsunderlaget (Ju2023/01666). Brå redovisade uppdraget den 1 november 2023.

3 Regelverket om datalagring och tillgång till elektronisk kommunikation

3.1 Grundläggande rättigheter och datalagring

Grundläggande rättigheter som tillförsäkras enskilda finns i bl.a. regeringsformen, den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) och i Europeiska unionens stadga om de grundläggande rättigheterna (EU:s rättighetsstadga).

I 2 kap. 6 § andra stycket regeringsformen anges att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Begränsningar i detta skydd får endast ske genom lag och endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningarna får inte heller gå utöver vad som är nödvändigt med hänsyn till det ändamål som föranlett dem och inte heller sträcka sig så lång att de utgör ett hot mot den fria åsiktsbildningen. Begränsningarna får inte göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning (2 kap. 20 och 21 §§). Av artikel 8 i Europakonventionen följer att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Behandling av personuppgifter berör rätten till respekt för privatlivet. Offentlig myndighet får inte inskränka dessa rättigheter annat än 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. Konventionen gäller som svensk lag, se lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna. Lag eller annan föreskrift får inte meddelas i strid med Sveriges åtaganden på grund av Europakonventionen (2 kap. 19 § regeringsformen). I EU:s rättighetsstadga regleras rätten till respekt för bl.a. privatliv i artikel 7, rätten till skydd för personuppgifter i artikel 8 och rätten till yttrandefrihet och informationsfrihet i artikel 11. Varje begränsning i utövandet av de fri- och rättigheter som erkänns i EU:s rättighetsstadga måste vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa fri- och rättigheter. Begränsningar får, med beaktande av proportionalitetsprincipen, göras endast om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors fri- och rättigheter (artikel 52.1).

Det finns två sidor av enskildas grundläggande rättigheter: dels enskildas rätt att bli fredade från kränkningar från statens sida, dels statens plikt att vidta åtgärder för att skydda enskilda mot kränkningar från andra enskilda, t.ex. genom ingripande åtgärder i en brottsutredning. Det är staten som ska se till att det finns ett ramverk som är förenligt med dessa delvis konkurrerande principer.

De rättigheter som främst är av intresse när det gäller lagring av uppgifter om elektronisk kommunikation (s.k. datalagring) är rätten till respekt för privatlivet och den personliga integriteten och rätten till skydd för personuppgifter.

För att säkerställa rätten till respekt för privatlivet och rätten till skydd för personuppgifter inom sektorn för elektronisk kommunikation har EU antagit Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), i det följande e-dataskyddsdirektivet 2002/58/EG. Direktivet föreskriver bl.a. att medlemsstaterna ska säkerställa konfidentialitet vid elektronisk kommunikation och därmed förbundna trafikuppgifter. Uppgifter som inte längre behövs ska enligt direktivet utplånas eller avidentifieras. Medlemsstaterna får dock göra undantag från dessa åliggganden om det behövs för bl.a. brottsbekämpande verksamhet.

I december 2016 meddelade EU-domstolen dom i målen C-203/15 och C-698/15, Tele2 Sverige AB m.fl., i det följande Tele2-domen. Domstolen uttalade att EU-rätten utgör hinder för nationell lagstiftning i ett antal närmare angivna fall. Till följd av Tele2-domen ändrades de svenska reglerna, bl.a. genom att vissa uppgiftstyper togs bort från lagringsskyldigheten och att lagringstiderna differentierades, se propositionen Datalagring vid brottsbekämpning – anpassningar till EU-rätten (prop. 2018/19:86).

Den 11 december 2018 antogs Europaparlamentets och rådets direktiv (EU) 2018/1972 om inrättande av en europeisk kodex för elektronisk kommunikation (e-kodexdirektivet). E-kodexdirektivet genomfördes bl.a. genom införandet av den nya lagen (2022:482) om elektronisk kommunikation. Även e-dataskyddsdirektivet 2002/58/EG är genomfört främst genom regler i lagen om elektronisk kommunikation.

Frågor som rör datalagring och åtkomst till elektronisk kommunikation påverkas således i stor utsträckning av EU-rätten. EU-domstolen har sedan Tele2-domen meddelat domar i flera mål om datalagring och tolkningen av e-dataskyddsdirektivet 2002/58/EG, bl.a. C-207/16, Ministerio Fiscal, C-623/17 Privacy International, de förenade målen C-511/18, C-512/18 och C-520/18, La Quadrature du Net m.fl., C-140/20, Commissioner of An Garda Síochána m.fl., de förenade målen C-793/19 och C-794/19, SpaceNet AG m.fl., samt La Quadrature du Net m.fl., C-470/21, i det följande Ministero Fiscal, Privacy International, La Quadrature du Net I, An Garda Síochána, SpaceNet respektive La Quadrature du Net II.

3.2 Lagen om elektronisk kommunikation

Reglerna om datalagring finns i lagen (2022:482) om elektronisk kommunikation. I lagen finns också regler som rör bl.a. tillhandahållarnas behandling av uppgifter och de brottsbekämpande myndigheternas inhämtning av information om kommunikation. Lagen trädde i kraft den 1 augusti 2022 och ersatte då den tidigare lagen (2003:389) om elektronisk kommunikation, se propositionen Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation (prop. 2021/22:136). Lagen syftar bl.a. till att enskilda och myndigheter ska få tillgång till säkra och effektiva elektroniska kommunikationer och gäller elektroniska kommunikationsnät och kommunikationstjänster.

Uppgifter om elektronisk kommunikation har i svensk rätt delats in i tre olika grupper: uppgifter om abonnemang, trafikuppgifter och lokaliseringsuppgifter. Med uppgifter om abonnemang (jfr 9 kap. 31 § första stycket 1 lagen om elektronisk kommunikation) avses främst uppgifter om abonnenten, exempelvis abonnentens nummer och namn. Med trafikuppgifter avses uppgifter som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande (1 kap. 7 §). Med lokaliseringsuppgifter avses bl.a. uppgifter som behandlas i ett allmänt mobilt elektroniskt kommunikationsnät och som anger den geografiska positionen för en slutanvändares terminalutrustning (1 kap. 7 §). Det kan t.ex. vara fråga om vilken cell (antenn på basstation) som utrustningen kopplat upp sig mot. De olika uppgiftskategorierna är delvis överlappande.

Lagen om elektronisk kommunikation innehåller ett antal bestämmelser som är av särskild relevans för det nu aktuella lagstiftningsärendet. Det gäller bl.a. bestämmelser med krav på åtgärder för att skydda lagrade uppgifter (8 kap. 5 §) och den centrala bestämmelsen som reglerar skyldigheten att lagra uppgifter om elektronisk kommunikation (9 kap. 19 §). När det gäller vilka uppgifter som ska lagras hänvisar bestämmelsen om lagringsskyldighet till paragrafen om tystnadsplikt för innehållet i kommunikationen och uppgifter om kommunikationen (9 kap. 31 §). De uppgifter som omfattas av tystnadsplikten är en uppgift om abonnemang, innehållet i ett elektroniskt meddelande och en annan uppgift som angår ett särskilt elektroniskt meddelande (i avsnitt 5.3 föreslås att den senare uppgiftstypen ersätts med begreppet trafikuppgift). En annan uppgift som angår ett elektroniskt meddelande omfattar även lokaliseringsuppgifter

som är kopplade till meddelandet. Lagringsskyldigheten omfattar inte innehållet i ett elektroniskt meddelande. Vidare finns regler om utlämning av uppgifter till vissa myndigheter och regionala alarmeringscentraler (9 kap. 33 §).

I lagen stadgas även den s.k. anpassningsskyldigheten, som innebär att tillhandahållare av elektroniska kommunikationstjänster ska bedriva verksamheten så att hemlig avlyssning och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs (9 kap. 29 §). Liknande bestämmelser, med bl.a. krav på att uppgifter ska lämnas ut till brottsbekämpande myndigheter utan dröjsmål och i ett format som gör att de enkelt kan tas om hand, finns också i lagen (9 kap. 29 b §). Där finns även regler om rätt till ersättning för kostnader som uppstår när uppgifter lämnas ut till brottsbekämpande myndigheter (9 kap. 29 a §) och om att sanktionsavgift ska tas ut vid bristande uppfyllelse av vissa av bestämmelserna i lagen (12 kap. 1 §).

Lagen kompletteras av reglerna i förordningen (2022:511) om elektronisk kommunikation. I förordningen finns bl.a. närmare regler om lagringsskyldigheten. Av förordningen framgår också att Post- och telestyrelsen är regleringsmyndighet och tillsynsmyndighet enligt lagen om elektronisk kommunikation.

3.3 De brottsbekämpande myndigheternas verksamhet och tillgången till lagrade uppgifter

Brottsbekämpande verksamhet kan i detta sammanhang delas in i två övergripande delar, underrättelseverksamhet och utredande verksamhet. Underrättelseverksamheten är i huvudsak inriktad på att avslöja om en viss inte närmare specificerad brottslighet har ägt rum, pågår eller kan antas komma att begås. Ett övergripande mål med underrättelseverksamheten är att förse de brottsbekämpande myndigheterna med kunskap som kan omsättas i operativ verksamhet. Den utredande verksamheten utgår i stället från en uppkommen händelse. Myndigheterna ska, inom en förundersökning, utreda om brott har begåtts och vem som i så fall skäligen kan misstänkas för brottet samt skaffa tillräckligt material för bedömning av frågan om åtal ska väckas.

För både brottsutredande verksamhet och underrättelseverksamhet finns det bestämmelser som reglerar förutsättningarna för att få tillgång till uppgifter från tillhandahållare av elektronisk kommunikation. Sådan tillgång sker främst genom tillstånd till hemliga tvångsmedel. De huvudsakliga reglerna om hemliga tvångsmedel finns i 27 kap. rättegångsbalken, där användningen av hemliga tvångsmedel under förundersökning regleras. Regler om användningen av hemliga tvångsmedel i underrättelseverksamheten finns i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen) och i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen). Bestämmelser om det hemliga tvångsmedlet hemlig dataavläsning finns i lagen (2020:62) om hemlig dataavläsning. Hemliga tvångsmedel kan även användas med stöd av lagen (2022:700) om särskild kontroll av vissa

utlänningar, lagen (2000:562) om internationell rättslig hjälp i brottmål och lagen (2017:1000) om en europeisk utredningsorder.

För all användning av tvångsmedel gäller tre allmänna principer, ändamålsprincipen, behovsprincipen och proportionalitetsprincipen. Säkerhets- och integritetsskyddsnämnden har till uppgift att utöva tillsyn över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel. Riksdagens ombudsmän (JO) och Justitiekanslern utövar tillsyn över de brottsbekämpande myndigheternas verksamhet och kan inom ramen för sin respektive tillsyn uttala sig i frågor om användningen av hemliga tvångsmedel.

Tillgången till abonnemangsuppgifter har inte bedömts utgöra ett hemligt tvångsmedel och regleras direkt i 9 kap. 33 § första stycket 1 och 2 lagen om elektronisk kommunikation (se t.ex. propositionen Hemliga tvångsmedel mot allvarliga brott [prop. 2013/14:237] s. 134). Tillgången till uppgifter om abonnemang kräver inget domstolsbeslut utan får beslutas av den brottsbekämpande myndigheten själv. Det krävs inte heller att brottet är av viss svårighetsgrad. Tillgång till trafik- och lokaliseringsuppgifter i den brottsutredande verksamheten kräver däremot domstolsbeslut och är endast möjlig vid allvarliga brott. I underrättelseverksamheten är tillgången till trafikuppgifter något mer begränsad. Vad gäller inhämtningslagen krävs åklagarbeslut för att få tillgång till uppgifterna.

I det här lagstiftningsärendet behandlas regler som främst berör de två hemliga tvångsmedel som riktar sig mot elektronisk kommunikation, dvs. hemlig avlyssning och hemlig övervakning av elektronisk kommunikation. Förslagen som lämnas medför inte några förändringar i reglerna om hemliga tvångsmedel, men påverkar däremot det praktiska tillämpningsområdet för de hemliga tvångsmedlen.

4 Behovet av att uppdatera regelverket

Samhällsutvecklingen innebär att kommunikation sker på andra sätt än tidigare. Kommunikationsvanorna och den teknik som används utvecklas ständigt. Det rättsliga ramverket på området styrs i stor grad av utvecklingen i rättspraxis, inte minst på europeisk nivå.

Regelverket om datalagring innebär skyldigheter för tillhandahållare av elektroniska kommunikationsnät och elektroniska kommunikationstjänster att lagra information i brottsbekämpande syfte. Det är av stor vikt att brottsbekämpande myndigheter har goda möjligheter att komma åt bevisning i form av information från elektronisk kommunikation. Det gäller särskilt i de fall där traditionell bevisning som vittnesiakttagelser är svåra att inhämta. Information från elektronisk kommunikation är ofta av särskilt stor betydelse i utredningar av allvarlig brottslighet. Med hjälp av hemlig övervakning av elektronisk kommunikation kan brottsbekämpande myndigheter få åtkomst till information om kommunikation, såsom vilka som befunnit sig på en viss plats vid en viss tid, eller vilka som varit i kontakt med en misstänkt gärningsman. Med hemlig avlyssning av elektronisk kommunikation är det möjligt att ta del av innehåll i samtal och meddelanden.

De hemliga tvångsmedlen fyller en allt viktigare funktion i den brottsbekämpande verksamheten. Trafik- och lokaliseringsuppgifter används ofta i utredningar rörande grova brott och är många gånger den enda ingången i sådana utredningar. Tillgången till uppgifter om elektronisk kommunikation på underrättelsestadiet kan vara avgörande för att aktörer, platser och tidpunkter ska kunna kopplas samman och ge ett tillräckligt underlag för att inleda en förundersökning.

Samtidigt som behovet av elektronisk information blir av allt större vikt innebär den fortsatta teknik- och kommunikationsutvecklingen att det praktiska användningsområdet för hemlig avlyssning och hemlig övervakning av elektronisk kommunikation krymper. Mycket av den information som tidigare varit tillgänglig för brottsbekämpande myndigheter har blivit svårare att komma åt. Det blir allt vanligare att kommunikation sker genom tjänster som inte omfattas av någon rättslig skyldighet att lagra och tillhandahålla uppgifter. Det rör inte minst tjänster som tillhandahålls av andra än de traditionella teleoperatörerna, ofta i form av kommunikationsappar (s.k. nummeroberoende interpersonella kommunikationstjänster, förkortat NOIK, även kallat OTT-tjänster, från engelskans over the top). Som utredningen anger är behovet av uppgifter om elektronisk kommunikation lika påtagligt oavsett vilken typ av tillhandahållare som sköter kommunikationstjänsten.

Utbudet av informations- och kommunikationstjänster genom internet, smarta telefoner och andra tekniska hjälpmedel är mycket stort, och tjänsterna är i regel lättillgängliga. Tjänsterna, som det finns ett stort behov av i helt legala syften, kan samtidigt utnyttjas av kriminella aktörer för planering och kommunikation eller som direkta brottsverktyg. Det förekommer exempelvis att tjänsterna används för att rekrytera både vuxna och unga till att utföra grova våldsbrott.

Staten har ett ansvar för att upprätthålla rättstryggheten för enskilda, vilket omfattar skydd av enskildas privatliv och personliga integritet mot intrång som begås av andra enskilda. I det ansvaret ligger att säkerställa att det finns en väl fungerande och effektiv brottsbekämpning.

Reglerna i lagen (2022:482) om elektronisk kommunikation, bl.a. skyldigheten att lagra information och anpassningsskyldigheten, är avgörande för att hemlig avlyssning och hemlig övervakning av elektronisk kommunikation ska fungera i praktiken. Reglerna om elektronisk kommunikation påverkas i hög grad av den snabba tekniska utvecklingen. Det sker också en utveckling av de EU-rättsliga ramarna för reglerna.

Det är vidare angeläget att bl.a. Säkerhetspolisen har goda förutsättningar att utföra sitt uppdrag att skydda rikets säkerhet. Säkerhetspolisen får sällan in anmälningar från allmänheten om begångna brott. Myndigheten måste i stället utföra ett aktivt underrättelsearbete utifrån flera olika informationskällor. Det finns därför starka skäl för att förbättra även åtkomsten till information om kommunikation i syfte att bekämpa brottslighet som kan utgöra ett hot mot den nationella säkerheten.

Det finns sammantaget ett påtagligt behov av att uppdatera regelverket. En utgångspunkt för ändringarna är att de ska vara i linje med hur kommunikationen sker i samhället och vara så teknikneutrala som möjligt för att undvika att reglerna ska behöva ändras utifrån teknikutveckling och förändrade kommunikationsvanor. Detsamma gäller i förhållande till den rättsliga utvecklingen på området som bl.a. sker på europeisk nivå. En

annan utgångspunkt är att brottsutvecklingen gör att de brottsbekämpande myndigheterna bör ges så goda förutsättningar som möjligt att utföra sitt uppdrag, inom de ramar som följer av enskildas rätt till skydd för sina grundläggande fri- och rättigheter. En ytterligare utgångspunkt är att de följder som ändringarna kan få för tillhandahållare av elektronisk kommunikation och andra aktörer inte får bli mer långtgående än vad som motiveras av brottsbekämpningens och samhällets behov. Det är därvid av vikt att bördan och kostnaden för aktörerna blir rimlig i förhållande till ändamålen.

5 Förlängd lagringstid för uppgifter om abonnemang och förtydliganden av vissa regler

5.1 Förlängd lagringstid för uppgifter om abonnemang och borttagande av vissa begränsningar

Utkastets förslag: Uppgifter om abonnemang ska lagras till dess att ett år har förflutit sedan abonnemanget eller tilldelningen av en tillfällig identifierare upphörde.

Uppgifter om abonnemang som har lagrats på grund av lagringsskyldigheten ska få behandlas även för andra ändamål än utlämning till brottsbekämpande myndigheter.

Utredningens förslag överensstämmer delvis med utkastets. Utredningen föreslår ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela föreskrifter om vilka uppgifter om abonnemang som ska lagras.

Remissinstanserna: En majoritet tillstyrker eller har inget att invända mot förslaget. *Bahnhof AB* för fram att begreppet uppgift om abonnemang bör utmönstras. Bolaget gör även gällande att uppgifter om abonnemang inte bör kunna lämnas ut utan domstolsprövning och att en ip-adress, mot bakgrund av EU-domstolens praxis, inte är att betrakta som en sådan uppgift. *Hi3G Access AB* för fram att förslaget inte är tillräckligt tydligt i fråga om vilka uppgifter om abonnemang som ska lagras. Bolaget anser att det bör framgå direkt av författning vad begreppet avser och ifrågasätter utredningens uttalanden om att avtal och fakturering omfattas. *Tech Sverige* och *Telenor Sverige AB* gör gällande att det inte är klart när en ip-adress ska anses utgöra en uppgift om abonnemang och när den är en trafikuppgift.

Skälen för utkastets förslag: Den som är skyldig att lagra uppgifter om elektronisk kommunikation ska lagra bl.a. uppgifter om abonnemang (9 kap. 19 § första stycket lagen om elektronisk kommunikation). Det finns inte någon författningsreglerad definition av begreppet uppgift om abonnemang i vare sig nationell rätt eller EU-rätt. I förarbetena till lagen om elektronisk kommunikation uttalas att med uppgift om abonnemang

avses t.ex. uppgifter om abonnentens nummer, namn, titel och adress (prop. 2018/19:86 s. 93). Av samma förarbeten och i utredningen framgår vidare att fasta och dynamiska ip-adresser och andra tekniker för styrning av kommunikation till ip-adresser anses vara uppgifter om abonnemang, när syftet med uppgifterna är att identifiera en abonnent eller registrerad användare. När det gäller definitionen av uppgifter om abonnemang anser *Hi3G Access AB* att det bör framgå direkt av författning vad som avses med det begreppet medan *Bahnhof AB* anser att begreppet helt bör utmönstras ur lagen. *Telenor Sverige AB* och *TechSverige* gör gällande att det är oklart när en ip-adress ska anses utgöra en uppgift om abonnemang och när det är fråga om en trafikuppgift. Det har tidigare bedömts att det inte finns skäl att definiera begreppet uppgift om abonnemang i författning (prop. 2018/19:86 s. 91–94 och propositionen Registrering av kontantkort [prop. 2021/22:183] s. 16). Utredningen har kommit fram till att det inte finns något behov av att vare sig revidera begreppet uppgift om abonnemang eller innebörden av begreppet. Såväl utredningens resonemang som de nämnda bolagens synpunkter tydliggör svårigheterna med att närmare definiera begreppet i lag. Beträffande den närmare tillämpningen finns utöver praxis också föreskrifter på området som meddelas av Post- och telestyrelsen. Mot denna bakgrund bedöms det inte lämpligt att i lag definiera begreppet eller att utmönstra det ur lagen.

Uppgifter om abonnemang som genereras eller behandlas vid telefonitjänst och meddelandehantering via mobil nätanslutningspunkt ska lagras i sex månader. Uppgifter som genereras eller behandlas vid internetåtkomst ska lagras i tio månader (9 kap. 22 § första stycket första och andra strecksatserna lagen om elektronisk kommunikation). Det innebär att olika lagringstid gäller för uppgifter om abonnemang beroende på vilken typ av tjänst de behandlas vid. De brottsbekämpande myndigheternas behov av att kunna identifiera vem som står bakom viss kommunikation är stort. Lagringstiden behöver ge utrymme för att uppgifter ska vara tillgängliga både i komplexa utredningar och för brott som är svårupptäckta eller där anmälan kommer in först en tid efter gärningen. Behovet finns även i underrättelseverksamheten.

Utredningen föreslår att uppgifter om abonnemang ska lagras i ett år och oberoende av vid vilken typ av tjänst de behandlas. Uppgifter om abonnemang är typiskt sett mindre integritetskänsliga än t.ex. trafik- och lokaliseringsuppgifter (jfr t.ex. EU-domstolens avgöranden La Quadrature du Net I och La Quadrature du Net II). Det finns därför utrymme för att ha längre lagringstider för uppgifter om abonnemang. En längre och enhetlig lagringstid ger brottsbekämpningen bättre möjligheter att kunna identifiera vem som står bakom viss kommunikation, oavhängigt vilken typ av kommunikationstjänst det är fråga om. Utredningens förslag om att förlänga lagringstiden för uppgifter om abonnemang till ett år för uppgifter om abonnemang oavsett vilken typ av tjänst de behandlas vid bedöms vara väl avvägt. I 9 kap. 22 § första stycket bör det därför föreskrivas att uppgifter om abonnemang ska lagras i ett år vid såväl telefonitjänster som vid internetåtkomst.

Lagringstiden bör räknas från den tidpunkt att uppgiften om abonnemang senast kunde knytas till den aktuella abonnenten. Det innebär som utredningen föreslår att lagringstiden om ett år bör utgå från det att abonnemanget eller tilldelningen av en tillfällig identifierare upphörde (exempel-

vis en dynamisk ip-adress). Med anledning av att fler ändringar föreslås i nya stycken i 9 kap. 22 § bör vilken tidpunkt som lagringstiden räknas från regleras i en ny paragraf, 9 kap. 22 a §.

Utredningen föreslår vidare att regeringen eller den myndighet som regeringen bestämmer ska bemyndigas att meddela föreskrifter om vilka uppgifter om abonnemang som ska lagras. Det har inte framkommit tillräckliga behov av att införa ett sådant bemyndigande utöver det utrymme som redan finns att meddela verkställighetsföreskrifter (se upplysningsbestämmelsen i 9 kap. 23 § 1). Ett sådant bemyndigande för uppgifter om abonnemang föranleder också frågor om varför motsvarande bemyndigande inte ska införas beträffande andra typer av uppgifter, vilket det inte finns något beredningsunderlag för.

Utredningen har även föreslagit att uppgifter om abonnemang som omfattas av lagringsskyldigheten ska få behandlas för andra syften än brottsbekämpning genom ändring i 9 kap. 21 §. Som utredningen för fram finns det redan en skyldighet att lämna ut uppgifter om abonnemang i andra syften än brottsbekämpning och till flera andra myndigheter än de brottsbekämpande myndigheterna. Uppgifterna är mindre känsliga än trafik- och lokaliseringsuppgifter. Det saknas därför anledning att behandlingen av uppgifterna om abonnemang som är lagrade med stöd av lagringsskyldigheten ska vara begränsad till brottsbekämpande ändamål. Begränsningen riskerar dessutom att leda till att uppgifterna behöver hållas separerade från andra uppgifter om abonnemang och att samma uppgifter lagras dubbelt, vilket kan innebära en ökad börda för de lagringsskyldiga. Uppgifter om abonnemang bör därför undantas från begränsningen i 9 kap. 21 §, genom att det i bestämmelsen anges att begränsningen enbart gäller trafikuppgifter.

5.2 Vissa ändringar av anpassningsskyldigheten

Utkastets förslag: Skyldigheten att bedriva sin verksamhet så att beslut om hemliga tvångsmedel kan verkställas och så att verkställandet inte röjs ska gälla för de som är lagringsskyldiga. Skyldigheten ska inte gälla för maskin-till-maskin-tjänster.

De tillhandahållare som omfattas av lagringsskyldighet ska bedriva sin verksamhet så att inhämtning enligt inhämtningslagen kan verkställas och så att verkställandet inte röjs.

Skyldigheten att lämna ut uppgifter som gäller brottslig verksamhet eller misstanke om brott utan dröjsmål och så att utlämnandet inte röjs ska gälla de som är lagringsskyldiga.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: *Tullverket* och *Polismyndigheten* anser att det inte bör göras något undantag för maskin-till-maskin-tjänster, eftersom teknikutvecklingen gör att behovet av att kunna hämta in uppgifter från sådana tjänster ökar. Polismyndigheten pekar särskilt på behovet av åtkomst till uppgifter från maskin-till-maskin-tjänster kopplade till fordon. *Justitiekanslern* lyfter frågan om förslaget innebär en skillnad i tillämpningsområdet i förhållande till nuvarande undantag för verksamhet som enbart består

i överföring av signaler via tråd för utsändning till allmänheten av program som avses i 1 kap. 2 § yttrandefrihetsgrundlagen.

Skälen för utkastets förslag

Anpassningsskyldigheten ska gälla för de aktörer som är lagringsskyldiga

De tjänsteleverantörer som enligt lagen om elektronisk kommunikation tillhandahåller allmänna kommunikationsnät eller elektroniska kommunikationstjänster spelar en viktig roll när brottsbekämpande myndigheter hämtar in elektronisk kommunikation och uppgifter om kommunikationen. För att underlätta myndigheternas inhämtning har de ålagts vissa skyldigheter. Tillhandahållarna ska bedriva verksamheten så att beslut om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs, den s.k. anpassningsskyldigheten (9 kap. 29 § första stycket till lagen om elektronisk kommunikation). Anpassningsskyldigheten gäller enligt nuvarande ordning för tillhandahållande av ett allmänt elektroniskt kommunikationsnät som inte enbart är avsett för utsändning till allmänheten av program som avses i 1 kap. 2 § yttrandefrihetsgrundlagen (9 kap. 29 § första stycket 1). Vidare gäller den för tillhandahållande av tjänster inom ett allmänt elektroniskt kommunikationsnät som består av en allmänt tillgänglig telefonitjänst till en fast nätanslutningspunkt i vissa närmare avseenden eller en allmänt tillgänglig elektronisk kommunikationstjänst till en mobil nätanslutningspunkt (9 kap. 29 § första stycket 2).

När den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § lagen om elektronisk kommunikation lämnar ut vissa uppgifter till brottsbekämpande myndigheter, ska utlämnandet ske utan dröjsmål och på ett sådant sätt att utlämnandet inte röjs. Uppgifterna ska ordnas och göras tillgängliga i ett format som gör att de enkelt kan tas om hand (9 kap. 29 b § första och andra styckena).

Utredningen har angett att bestämmelserna om anpassningsskyldigheten i 9 kap. 29 § är otydliga i flera avseenden och att det råder osäkerhet kring vilka verksamheter som omfattas. Utredningen pekar på att avgränsningen till en fast nätanslutningspunkt är ålderdomlig och stämmer dåligt överens med definitionerna i lagen. Den tekniska utvecklingen innebär att tjänster kan tillhandahållas på nya sätt och att gränserna för olika typer av tjänster flyter ihop. Det gör att anpassningsskyldighetens omfattning bör anges på ett så teknikneutralt sätt som möjligt och utan avgränsning till viss typ av överföringsteknik med viss lägsta datahastighet.

Anpassningsskyldigheten är i praktiken ofta en förutsättning för att beslut om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation ska kunna verkställas och att verkställandet ska kunna ske i nära anslutning till tvångsmedelsbeslutet. Det är viktigt att anpassningsskyldigheten är utformad så att tolkningsproblem kan undvikas. Den nuvarande utformningen tillgodoser inte detta behov. I enlighet med utredningens förslag bör anpassningsskyldigheten i 9 kap. 29 § första stycket därför ändras till att i stället omfatta de aktörer som enligt 9 kap. 19 § första stycket är lagringsskyldiga och träffar således de som är anmälningspliktiga enligt 2 kap. 1 §. Anpassningsskyldigheten kommer därmed att omfatta fler tillhandahållare, exempelvis vissa internetleverantörer som

inte tillhandahåller telefonitjänster. Motsvarande anpassningsskyldighet föreslås gälla för den som tillhandahåller en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst (avsnitt 7.4). Ändringen att knyta anpassningsskyldigheten till lagringsskyldigheten innebär vidare att anpassningsskyldigheten för allmänna elektroniska kommunikationsnät endast gäller beträffande sådana tjänster som vanligtvis tillhandahålls mot betalning. Såsom ett allmänt elektroniskt kommunikationsnät definieras bör det dock inte innebära någon egentlig förändring av kretsen av anpassningsskyldiga (1 kap. 7 § lagen om elektronisk kommunikation).

I enlighet med utredningens förslag bör även 9 kap. 29 b § ändras från att gälla de som är anmälningspliktiga enligt 2 kap. 1 § till att gälla de som är lagringsskyldiga. Eftersom lagringsskyldigheten i 9 kap. 19 § träffar de som är anmälningspliktiga innebär förslaget i denna del inte någon ändring i sak. Ändringen medför dels att bestämmelsen språkligt anpassas till förslaget i 9 kap. 29 § första stycket, dels att det lagtekniskt underlättar för förslaget att låta även nummeroberoende interpersonella kommunikationstjänster omfattas av bestämmelsen (avsnitt 7.4).

Justitiekanslern lyfter frågan om utredningens förslag i 9 kap. 29 b § innebär ett förändrat tillämpningsområde i förhållande till nuvarande undantag för verksamhet som enbart består i överföring av signaler via tråd för utsändning till allmänheten av program som avses i 1 kap. 2 § yttrandefrihetsgrundlagen. Regeringens förslag till utformning av anpassningsskyldigheten innebär en hänvisning till kretsen av lagringsskyldiga i 9 kap. 19 § lagen om elektronisk kommunikation. Den paragrafen hänvisar i sin tur till 2 kap. 1 § samma lag där den aktuella verksamheten är undantagen. Verksamhet som består enbart i överföring av signaler via tråd för utsändning till allmänheten av program som avses i 1 kap. 2 § yttrandefrihetsgrundlagen kommer alltså alltjämt att vara undantagen från anpassningsskyldigheten.

Utredningen har även övervägt om det behöver göras några ändringar i bestämmelserna om anpassningsskyldighet med anledning av möjligheten att kryptera elektronisk kommunikation, som teknikutvecklingen ger ökade möjligheter till. *Tech Sverige*, *Tele2 Sverige AB*, *Telenor Sverige AB*, *Telia Sverige AB* och *Netnod AB* ifrågasätter delar av utredningens resonemang i fråga om kryptering och slutsatserna om vilket ansvar som tillhandahållarna har för att göra uppgifter tillgängliga i läsbar form. Utredningen anger att någon ändring av regelverket beträffande den här frågan inte behövs och lämnar inte något förslag om det. Utkastets förslag om vissa andra ändringar i anpassningsskyldigheten påverkar följaktligen inte de aktuella frågorna om kryptering och tillhandahållarnas ansvar.

Anpassningsskyldigheten ska inte gälla för maskin-till-maskin-tjänster

Utredningen föreslår att maskin-till-maskin-tjänster ska vara undantagna från anpassningsskyldigheten i 9 kap. 29 § lagen om elektronisk kommunikation. Sådana tjänster kan exempelvis omfatta övervakning, mätning, styrning, transport och logistik i bl.a. bilar, tåg, elmätare, hemlarm och gräsklippare. Utredningen bedömer att det skulle vara oproportionerligt att införa en anpassningsskyldighet för dessa tjänster då det främst skulle avse lokaliseringsuppgifter för fordon och behovet inte framstår som påtagligt. Även med beaktande av synpunkterna från *Tullverket* och *Polismyndigheten* har det inte framkommit tillräckliga skäl för att göra

någon annan bedömning än den som utredningen har gjort. Det saknas också närmare beredningsunderlag för konsekvenserna av en sådan skyldighet. Maskin-till-maskin-tjänster bör därför undantas från anpassningsskyldigheten i 9 kap. 29 §.

Tillhandahållare av maskin-till-maskin-tjänster kommer dock alltjämt att omfattas av skyldigheten att lämna ut uppgifter om bl.a. abonnemang enligt 9 kap. 33 §. De omfattas då av kraven på skyndsamhet och format vid utlämnandet av uppgifter enligt 9 kap 29 b § och rätten till ersättning vid sådant utlämnande enligt 9 kap. 29 a §.

Förtydligande i förhållande till inhämtningslagen

Anpassningsskyldigheten i 9 kap. 29 § första stycket lagen om elektronisk kommunikation anses gälla såväl vid beslut om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation enligt rättegångsbalkens regler som vid beslut om inhämtning med stöd av inhämtningslagen, se t.ex. departementspromemorian Registrering av kontantkort, m.m., Ds 2020:12 s. 121–122.

Utredningen för fram att det i vissa fall har ifrågasatts om anpassningsskyldigheten gäller vid beslut om inhämtning enligt inhämtningslagen och att det därför av tydlighetsskäl bör framgå av lagtexten att även inhämtning enligt inhämtningslagen omfattas. I enlighet med utredningens förslag bör ett sådant förtydligande införas i 9 kap. 29 § lagen om elektronisk kommunikation.

5.3 Begreppet annan uppgift som angår ett särskilt elektroniskt meddelande ersätts med begreppet trafikuppgift

Utkastets förslag: Begreppet annan uppgift som angår ett särskilt elektroniskt meddelande i lagen om elektronisk kommunikation ska ersättas med begreppet trafikuppgift. Motsvarande ändring ska göras i offentlighets- och sekretesslagen.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna tillstyrker eller har inga invändningar mot utredningens förslag. *Sveriges advokatsamfund* påtalar att lokaliseringsuppgifter kan förekomma utan att de har något samband med ett elektroniskt meddelande och att förslaget kan uppfattas som att sekretessen inte skyddar en sådan uppgift.

Skälen för utkastets förslag: Begreppet annan uppgift som angår ett särskilt elektroniskt meddelande finns i bestämmelsen som reglerar tystnadsplikt för den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk tjänst (9 kap. 31 § första stycket 3 lagen om elektronisk kommunikation). Bestämmelsen innebär att tillhandahållarna som huvudregel inte obehörigen får föra vidare det som de fått tillgång till i form av uppgifter om abonnemang, innehållet i ett elektroniskt meddelande eller en annan uppgift som angår ett elektroniskt meddelande. Begreppet har betydelse även för lagringsskyldigheten eftersom bestämmelsen om lagringsskyldighet i 9 kap. 19 § hänvisar till bestämmelsen om tystnadsplikt.

Begreppet annan uppgift som angår ett särskilt elektroniskt meddelande finns även i 29 kap. 2 § offentlighets- och sekretesslagen (2009:400), där det föreskrivs sekretess för bl.a. sådana uppgifter.

Med trafikuppgift avses en uppgift som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera meddelandet (1 kap. 7 § lagen om elektronisk kommunikation). Begreppet trafikuppgift är hämtat från Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (e-dataskyddsdirektivet). Av artikel 2 b framgår att trafikuppgifter är alla uppgifter som behandlas i syfte att överföra en kommunikation via ett elektroniskt kommunikationsnät eller för att fakturera den. Begreppet trafikuppgift omfattar även lokaliseringsuppgifter som är trafikuppgifter, dvs. lokaliseringsuppgifter som är kopplade till ett elektroniskt meddelande (jfr skäl 15 i e-dataskyddsdirektivet 2002/58/EG).

I utredningen föreslås att begreppet annan uppgift som angår ett särskilt elektroniskt meddelande i lagen om elektronisk kommunikation ska ersättas med begreppet trafikuppgift. Det föreslås även att motsvarande ändring ska göras i offentlighets- och sekretesslagen. Som skäl för ändringarna anförs att begreppet trafikuppgift har samma innebörd som begreppet annan uppgift som angår ett särskilt elektroniskt meddelande och att det kan medföra tolkningssvårigheter att det finns två begrepp med samma innebörd.

I enlighet med utredningens bedömning riskerar användningen av begreppet annan uppgift som angår ett särskilt elektroniskt meddelande att ge upphov till oklarhet i tillämpningen, både i fråga om omfattningen av tystnadsplikten och vad som omfattas av sekretess och lagringsskyldighet. Begreppet trafikuppgift bör därför ersätta begreppet annan uppgift som angår ett särskilt elektroniskt meddelande i 9 kap. 31 § första stycket 3 lagen om elektronisk kommunikation.

Även i offentlighets- och sekretesslagen (2009:400) bör begreppet annan uppgift som angår ett särskilt elektroniskt meddelande ersättas med begreppet trafikuppgift (29 kap. 2 §). *Sveriges advokatsamfund* lyfter med anledning av det föreslagna begreppsbytet frågan om även lokaliseringsuppgifter som inte är trafikuppgifter bör omfattas av sekretessbestämmelsen. Sådana uppgifter omfattas dock inte av den gällande lydelsen av bestämmelsen och påverkas inte av att begreppet trafikuppgift införs. Frågor om sekretess och tystnadsplikt för lokaliseringsuppgifter som inte är trafikuppgifter behandlas i avsnitt 6.8.

6 Nya regler om datalagring i syfte att skydda nationell säkerhet

6.1 En mer omfattande lagring i syfte att skydda nationell säkerhet

Utkastets bedömning: Det finns behov av att införa regler om lagring av och tillgång till uppgifter i syfte att skydda nationell säkerhet.

Utkastets förslag: Förutsättningarna för lagringen ska framgå av en ny lag.

Utredningens bedömning och förslag överensstämmer med utkastets.

Remissinstanserna: Många remissinstanser instämmer i eller har inget att invända mot bedömningen eller förslaget. *Ekobrottsmyndigheten*, *Polismyndigheten*, *Säkerhetspolisen*, *Åklagarmyndigheten* och *Tullverket* för fram att det finns behov av att införa en särskild möjlighet till lagring av trafik- och lokaliseringsuppgifter i syfte att skydda nationell säkerhet. *Sveriges advokatsamfund* påtalar att intresset att tillvarata det nationella säkerhetsintresset är berättigat. *Svenska Journalistförbundet* ifrågasätter inte att det finns ett stort behov av uppgifter från elektronisk kommunikation i brottsbekämpningen och att datalagring är ett effektivt sätt att anskaffa uppgifterna. *Bahnhof AB* för på ett övergripande plan fram att bolaget inte har någon erinran mot att regler införs om lagring av uppgifter i syfte att skydda nationell säkerhet. *Hi3G Access AB* anser att regeringen bör avvakta med att införa nationell säkerhetslagring och i stället invänta harmonisering på EU-nivå. Bolaget anser att lagstiftningen i vart fall bör vara tidsbestämd och utvärderas. Även *TechSverige* m.fl. anser att reglering bör ske på EU-nivå. *Stockholms universitet (Juridiska fakulteten)* och *Tele2 Sverige AB* anser inte att underlaget är fullgott för att avgöra om de åtgärder som föreslås är effektiva för syftet. *Förvaltningsrätten i Stockholm* påtalar att det behöver göras en avvägning mellan syftet med lagringen och rättssäkerhetsaspekter samt skyddet för den personliga integriteten.

Skälen för utkastets förslag

Nationell säkerhetslagring

De uppgifter om elektronisk kommunikation som i dag omfattas av lagringsskyldighet enligt 9 kap. 19 § lagen om elektronisk kommunikation är dels uppgifter om abonnemang, dels andra uppgifter som angår ett särskilt elektroniskt meddelande (trafikuppgifter enligt förslaget i avsnitt 5.3). Olika lagringstider gäller för olika uppgifter, allt räknat från den dag kommunikationen avslutades. Som huvudregel ska uppgifter som genereras eller behandlas vid telefonitjänst och meddelandehantering via mobil nätanslutningspunkt lagras i sex månader och uppgifter som genereras eller behandlas vid internetåtkomst lagras i tio månader. För vissa uppgifter är lagringstiden kortare (9 kap. 22 §).

De författningsändringar som gjordes i Sverige år 2019 med begränsningar i lagringsskyldigheten syftade till att tillgodose det EU-rättsliga kravet på att lagringsskyldigheten inte får vara generell och odifferentierad (jfr Tele2-domen). Några särskilda överväganden kring vilka uppgifter som får lagras för nationell säkerhet gjordes inte i samband med ändringarna. I stället konstaterades att det inte fanns något beredningsunderlag för en särskild reglering avseende datalagring som sker med anledning av brottsbekämpning kopplad till nationell säkerhet, exempelvis genom Säkerhetspolisens verksamhet. Det ansågs inte heller finnas skäl att före EU-domstolens dom i La Quadrature du Net I överväga att göra åtskillnad i nationell lagstiftning mellan lagring av uppgifter som sker för brottsbekämpande ändamål och lagring av uppgifter på området för nationell säkerhet (prop. 2018/19:86 s. 21).

Den 6 oktober 2020 meddelade EU-domstolen dom i La Quadrature du Net I. Av domen följer att det finns möjlighet att i nationell rätt ålägga tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster en mer omfattande lagringsskyldighet för trafik- och lokaliseringsuppgifter i syfte att skydda nationell säkerhet, i fortsättningen nationell säkerhetslagring. En sådan lagring innebär i korthet att behöriga myndigheter kan ges rätt att ålägga tjänsteleverantörer en mer långtgående lagringsskyldighet under en begränsad tid avseende trafik- och lokaliseringsuppgifter, om målet är att skydda den nationella säkerheten. För att en sådan skyldighet ska kunna beslutas krävs att det finns tillräckligt konkreta omständigheter för att anse att staten står inför ett allvarligt hot mot nationell säkerhet som visat sig vara verkligt och aktuellt eller förutsebart, att lagringsskyldigheten kan bli föremål för en effektiv kontroll av en domstol eller ett annat oberoende organ och att den är tidsmässigt begränsad till vad som är strängt nödvändigt. Den nationella säkerhetslagringen innebär alltså att ramarna för lagringen vid ett allvarligt hot mot den nationella säkerheten kan vara vidare än vad som annars gäller.

Det finns ett behov av att införa nationell säkerhetslagring

Tillgången till information från elektroniska kommunikationer är ofta av stor betydelse för den brottsbekämpande verksamheten, inte minst den som bedrivs av Säkerhetspolisen i syfte att skydda rikets säkerhet. Som exempel kan nämnas att Säkerhetspolisen sällan får in anmälningar från allmänheten om begångna brott. I stället måste myndigheten i underrättelseverksamheten dels leta efter intressanta personer och grupperingar samt företeelser, skeenden och modus som är eller som senare kan komma att utvecklas till brottslighet som kan hota nationell säkerhet, dels ta ställning till tips och information om hot som myndigheten får del av. Underrättelseverksamheten är därför tyngdpunkten i Säkerhetspolisens bekämpning av t.ex. spioneri och terrorism.

En mycket stor del av de utredningar och annat arbete som Säkerhetspolisen genomför, såväl i underrättelseverksamheten som i den brottsutredande verksamheten, har en koppling till kvalificerade aktörer som är tränade och styrda av främmande makt eller av större organisationer, som exempelvis terroristorganisationer. Personerna har många gånger goda kunskaper om hur man döljer elektroniska spår. Grunden i Säkerhetspolisens arbete i dessa fall är att hitta de mönster som aktörerna har i sin kommunikation och de avvikelser som finns eller de misstag som görs, samt att analysera vilka slutsatser som kan dras av dessa. I arbetet behöver Säkerhetspolisen ha tillgång till ändamålsenliga och verkningsfulla verktyg. De verktyg som är tillgängliga för Säkerhetspolisen utgör en viktig förutsättning för myndighetens förmåga att förebygga, förhindra, upptäcka, utreda och lagföra brottslighet som hotar Sveriges grundläggande nationella säkerhetsintressen. Detsamma gäller andra brottsbekämpande myndigheter.

Utredningen föreslår att nationell säkerhetslagring ska införas i nationell rätt. Detta innebär att vid ett allvarligt hot mot nationell säkerhet kan lagringen av uppgifter om elektronisk kommunikation vara mer omfattande än vad som annars gäller. Det är mycket angeläget att myndigheterna har bästa möjliga förutsättningar att bekämpa allvarliga hot mot nationell säkerhet. Flera brottsbekämpande myndigheter, däribland *Säkerhetspolisen*, *Polismyndigheten* och *Åklagarmyndig-*

heten, för fram att det finns behov av att införa en särskild möjlighet till lagring av uppgifter i syfte att skydda nationell säkerhet.

Det kan konstateras att säkerhetsläget under senare tid har allvarligt försämrats. Av Säkerhetspolisens lägesbild 2023–2024 framgår att en orolig omvärld påverkar Sverige och att det allvarliga säkerhetspolitiska läget sannolikt kommer att bestå under en längre tid. I lägesbilden konstateras även att det allvarliga omvärldsläget gör det än mer viktigt att skydda säkerhetskänslig verksamhet och olika samhällsviktiga funktioner. Det finns mot denna bakgrund ett påtagligt behov av att nationell säkerhetslagring införs i svensk rätt.

Det är proportionerligt att införa nationell säkerhetslagring i svensk rätt

En lagringsskyldighet för det uttalade syftet att skydda den nationella säkerheten finns inte i Sverige i dag. Vid bedömningen av om nationell säkerhetslagring ska införas krävs därför att det bedöms vara förenligt med de grundläggande fri- och rättigheterna i såväl regeringsformen som Europakonventionen och EU:s rättighetsstadga. Vid dessa överväganden är rätten till privatliv och rätten till skydd mot intrång i den personliga integriteten av särskild betydelse. Begränsningar i dessa rättigheter får bara göras för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle och får aldrig gå utöver vad som är nödvändigt med hänsyn till de ändamål som har föranlett dem.

Mot bakgrund av vad som anförs ovan får, till skillnad mot vad bl.a. *Stockholms universitet (Juridiska fakulteten)* för fram, en utvidgad möjlighet att inhämta trafik- och lokaliseringsuppgifter förväntas bidra till myndigheternas arbete med att skydda den nationella säkerheten på ett sådant sätt att det finns ett faktiskt behov av att nationell säkerhetslagring införs i nationell rätt. Detta utgör i sig ett godtagbart skäl för att begränsa enskildas fri- och rättigheter enligt regeringsformen, Europakonventionen och EU:s rättighetsstadga. Förslagen förväntas också leda till en ökad rättstrygghet för enskilda.

Den nationella säkerhetslagringen kan i många fall även förväntas innebära ett intrång i enskildas rättigheter. Som *Förvaltningsrätten i Stockholm* för fram behöver det därför göras vissa avvägningar i detta avseende.

Ett beslut om nationell säkerhetslagring innebär en utökad lagring. Uppgifter som lagrats med stöd av ett beslut om nationell säkerhetslagring kommer att kunna inhämtas efter tillstånd till vissa hemliga tvångsmedel. Detta kan väntas leda till att fler personer utsätts för hemliga tvångsmedel, vilket innebär ett integritetsintrång. Därtill innebär den utökade informationsinhämtningen en risk för att det i fler fall kommer att samlas in information som senare visar sig sakna betydelse för syftet med insamlingen. Ett beslut om nationell säkerhetslagring ska dock kunna beslutas endast om det finns ett allvarligt hot mot Sveriges säkerhet, för att stärka de brottsbekämpande myndigheternas förmåga vid en sådan situation. Relativt långtgående intrång i den personliga integriteten får accepteras när det behövs för att skydda den nationella säkerheten. Därtill ska ett beslut föregås av en robust och allsidig prövning. Ett beslut om nationell säkerhetslagring kommer också att överprövas av ett kontrollorgan och vid den prövningen kommer enskildas intressen att bevakas av ett ombud. Ett sådant regelverk får, vid ett tillräckligt allvarligt hot mot den nationella säkerheten, på ett godtagbart sätt anses tillgodose den enskildes behov av skydd för och kontroll av sina rättigheter.

Med anledning av dessa avvägningar får behovet och den förväntade effekten av ett beslut om nationell säkerhetslagring antas väga tyngre än det väntade rättighetssintrång som lagringen kan innebära för den enskilde. Det bedöms inte vara möjligt att uppnå motsvarande resultat genom andra mindre ingripande åtgärder. Behovet väger även tyngre än de motstående intressen som talar emot att låta tillhandahållarna omfattas av reglerna. Att låta tillhandahållarna omfattas av de aktuella skyldigheterna utgör därmed en proportionerlig åtgärd som är förenlig med regeringsformen, Europakonventionen och EU:s rättighetsstadga.

Vissa remissinstanser, däribland *Hi3G Access AB*, anser att regleringen bör avvakta och att lagringsskyldigheten i stället bör införas efter ytterligare EU-åtgärder. Även om Sverige driver frågorna aktivt på EU-nivå kan någon EU-harmonisering av frågorna inte förväntas i tillräcklig närtid. Nationella lagstiftningsåtgärder bör därför inte avvakta. Nationell säkerhetslagring bör därmed införas i svensk rätt.

Det bör införas en ny lag om nationell säkerhetslagring

Utredningen föreslår att det ska införas en ny paragraf i lagen om elektronisk kommunikation, 9 kap. 19 b §, där det ska föreskrivas att den som är lagringsskyldig enligt gällande regler ska lagra de uppgifter som framgår av en ny lag om nationell säkerhetslagring. Förslaget innebär att reglerna om lagring av och tillgång till uppgifter i syfte att skydda nationell säkerhet kommer att framgå av den nya lagen.

För att nationell säkerhetslagring ska kunna införas behöver förutsättningarna för lagringen och tillgången till uppgifterna närmare regleras. Det framstår inte som lämpligt att endast komplettera annan befintlig lagstiftning som huvudsakligen har andra syften med utförliga bestämmelser om nationell säkerhetslagring (jfr prop. 2022/23:43 s. 16). I enlighet med utredningens förslag är det lämpligt att bestämmelserna om nationell säkerhetslagring huvudsakligen framgår av en ny lag. Det bör därför införas en ny lag, lag om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet, som reglerar förutsättningarna för den nationella säkerhetslagringen. Lagen bör innehålla bestämmelser om när uppgifter får lagras och lämnas ut för att skydda Sveriges säkerhet.

Hi3G Access AB för fram att lagstiftningen bör vara tidsbestämd och att den, i vart fall, bör utvärderas. Införandet av nationell säkerhetslagring innebär dock inte ett nytt eller utvidgat tvångsmedel. Lagringen innebär inte heller att befintliga tvångsmedel ska användas under andra förutsättningar än tidigare (jfr propositionen Hemliga tvångsmedel – effektiva verktyg för att förhindra och utreda allvarliga brott [prop. 2022/23:126] s. 84 f). Detta i kombination med Säkerhetspolisens kompetens att bedöma det nationella säkerhetsläget och de rättssäkerhetsgarantier som kommer att finnas för enskilda gör att det inte finns tillräckliga skäl att tidsbegränsa lagstiftningen.

6.2 Behörig myndighet och bedömningen av hotet mot Sveriges säkerhet

Utkastets förslag: Säkerhetspolisen ska få besluta om en mer omfattande lagringsskyldighet för de tillhandahållare som är lagringsskyldiga, när det finns ett allvarligt hot mot Sveriges säkerhet och det är absolut nödvändigt att besluta om ett sådant föreläggande.

Beslutet ska få gälla i högst ett år och omfattningen ska begränsas till vad som är absolut nödvändigt. Säkerhetspolisen ska genom ett nytt beslut få förlänga lagringsskyldigheten om hotet mot Sveriges säkerhet består. Om det inte längre finns skäl för lagringen ska Säkerhetspolisen upphäva beslutet.

Utredningens förslag överensstämmer i huvudsak med utkastets. Utredningen föreslår att det ska framgå av lagtext att hotet mot Sveriges säkerhet ska vara verkligt och aktuellt eller förutsebart. Vidare föreslås att det ska anges att beslutet ska begränsas till vad som är absolut nödvändigt för syftet med lagringen i vissa särskilt angivna avseenden. Utredningen föreslår även att det ska anges att Säkerhetspolisen inför sin bedömning av hotet mot Sveriges säkerhet ska samråda med Försvarsmakten.

Remissinstanserna: Många remissinstanser instämmer i eller har inget att invända mot förslagen. *Försvarsmakten* håller med om att det bör vara Säkerhetspolisen som beslutar om nationell säkerhetslagring. *Försvarsunderrättelsedomstolen* delar uppfattningen att det bör vara Säkerhetspolisen som gör bedömningen av hoten mot den nationella säkerheten. *Sveriges advokatsamfund* för fram att möjligheten att besluta om nationell säkerhetslagring kommer att vara begränsad eftersom det ställs höga krav på behovet av lagringen. Enligt samfundet innebär detta att nationell säkerhetslagring bara borde komma i fråga efter en rimlig och proportionerlig avvägning mot integritetsintresset. Vidare framförs förståelse för svårigheten att i detalj redogöra för när ett beslut om nationell säkerhetslagring ska få fattas, vilket dock kommer att innebära att det inte går att förutse när lagringsskyldigheten blir aktuell. *Svenska Journalistförbundet* påtalar, liksom *Tidningsutgivarna (TU)*, att det inte är tillräckligt tydligt när ett lagringsbeslut får fattas. Förbundet och TU ifrågasätter även om det är lämpligt att samma myndighet beslutar om terrornivå och lagring. Förbundet menar att beslutet bör underställas domstolsprövning. Därutöver för förbundet och TU fram att den föreslagna giltighetstiden är för lång. *Bahnhof AB* anser att beslutet bör fattas av domstol. *Uppsala universitet (Juridiska fakulteten)* menar att en bättre ordning hade varit att låta beslutsmyndigheten fatta interimistiska lagringsbeslut, som sedan underställs kontrollorganet. *Hi3G Access AB* påtalar att lagstiftningen inte får vara mer omfattande än vad som är absolut nödvändigt. Därutöver förs fram att den föreslagna lagstiftningen inte är förutsebar, eftersom förutsättningarna för lagringen kommer att framgå först av Säkerhetspolisens beslut. Även *Telia Sverige AB* menar att förutsättningarna för nationell säkerhetslagring behöver bli tydligare. *TechSverige* för fram att lagringen är oklar och riskerar att permanenteras. Vidare påtalas att antalet uppgiftskategorier bör minskas till det som kan bedömas som strikt nödvändigt. Liknande synpunkter förs fram av *Telenor Sverige AB* som anser att det är osäkert när lagringen kan aktualiseras och menar

att det finns risk för att den blir permanent. *Stockholms universitet (Juridiska fakulteten)* instämmer i att det finns en risk för att den nationella säkerhetslagringen permanentas. *Göteborgs universitet (Juridiska institutionen)*, *TU* och Svenska Journalistförbundet påtalar att det vore önskvärt med vägledning för bedömningen av när det kan anses finns ett tillräckligt allvarligt hot mot den nationella säkerheten. *Försvarsunderrättelsedomstolen* för fram att om avsikten är att hotet mot Sveriges säkerhet ska vara av mer kvalificerad art bör det utvecklas. Att beslutet bara ska få fattas när det är absolut nödvändigt för att skydda Sveriges säkerhet menar domstolen för tankarna till att lagringsskyldigheten måste vara en nödvändig betingelse för att uppnå detta skydd. Domstolens uppfattning är vidare att det bara är i förhållande till tidsaspekten som EU-rätten ställer krav på att lagringsskyldigheten ska begränsas till vad som är strängt nödvändigt. *Åklagarmyndigheten*, *Ekobrottsmyndigheten*, *Hovrätten för Västra Sverige*, *Polismyndigheten* och *Säkerhetspolisen* lyfter – i likhet med Försvarsunderrättelsedomstolen – att utredningen genom att uppställa krav på vilka tillhandahållare och uppgifter som ska omfattas av lagringsskyldigheten begränsar lagringen i större utsträckning än vad som krävs enligt EU-rätten. Säkerhetspolisen anser vidare, vilket även *Försvarsmakten* för fram, att det är tillräckligt att myndigheterna samråder vid behov. Därutöver påtalas att innan begreppet nationell säkerhets utvidgas bör konsekvenserna av ett utvidgande analyseras, bl.a. hur det förhåller sig till skyldigheter och uppdrag i andra regelverk. *Säkerhets- och integritetsskyddsnämnden* understryker att regleringen inte får tillämpas så att en mer omfattande lagring blir ett normaltillstånd. Nämnden anser därför att det är positivt att det i lagtexten anges att ett beslut om nationell säkerhetslagring bara får meddelas när det är absolut nödvändigt för att skydda Sveriges säkerhet och att beslutet ska begränsas till vad som är absolut nödvändigt i vissa avseenden.

Skälen för utkastets förslag

Säkerhetspolisen bör få besluta om nationell säkerhetslagring om det finns ett allvarligt hot mot Sveriges säkerhet

Utredningen föreslår att Säkerhetspolisen ska bedöma om det finns ett allvarligt hot mot Sveriges säkerhet och besluta om lagringsskyldigheten.

Säkerhetspolisen är den myndighet som har bäst förutsättningar att avgöra om det finns ett tillräckligt allvarligt hot mot den nationella säkerheten för att nationell säkerhetslagring ska kunna aktualiseras. Till skillnad mot vad *TU* och *Svenska Journalistförbundet* för fram är det lämpligt att det är samma myndighet, dvs. Säkerhetspolisen, som bedömer säkerhetsläget och beslutar om lagringsskyldigheten.

Den behöriga myndighetens beslut att förelägga tillhandahållare om nationell säkerhetslagring ska enligt EU-domstolens praxis grunda sig på bedömningen att det finns tillräckligt konkreta omständigheter för att anse att staten står inför ett allvarligt hot mot nationell säkerhet som visat sig vara verkligt och aktuellt eller förutsebart (se punkten 137 i La Quadrature du Net I-domen). Utredningen konstaterar att det inte med någon större säkerhet går att förutse vilka omständigheter som kan innebära ett hot mot den nationella säkerheten. Utredningens bedömning är därför att det inte är lämpligt att i författning precisera vilka omständigheter

som ska föreligga för att hotet mot den nationella säkerheten ska anses vara sådant att det motiverar en mer omfattande lagring. En sådan reglering menar utredningen bl.a. skulle kunna utesluta en anpassning över tid. När det gäller hotet konstaterar dock utredningen att det, exempelvis, kan vara av betydelse om terrornivån i Sverige är förhöjd, om det finns ett hot om ett väpnat angrepp mot Sverige eller om det finns andra allvarliga hot mot den inre eller yttre säkerheten.

Det går inte med någon större säkerhet att förutse vilka företeelser som kan komma att innebära ett tillräckligt hot mot den nationella säkerheten. Det är i stället mer ändamålsenligt att den behöriga myndigheten, på ett så komplett underlag som möjligt, avgör om det finns tillräckligt konkreta omständigheter för att anse att det finns ett allvarligt hot mot Sveriges säkerhet som är verkligt, aktuellt eller förutsebart. Sådana omständigheter som utredningen för fram kan dock vara av betydelse vid den bedömningen. Till skillnad mot vad ett antal remissinstanser för fram är det därför inte lämpligt att ytterligare precisera vilka omständigheter som ska föreligga för att bedöma hotet mot den nationella säkerheten och besluta om nationell säkerhetslagring. Det är inte heller lämpligt att inom ramen för detta lagstiftningsärende analysera de vidare konsekvenserna av användningen av begreppet nationell säkerhet, bl.a. eftersom liknande uttryck också förekommer i andra regelverk.

De EU-rättsliga kraven för lagringen gäller oberoende av svenska regler. Detta innebär att hotet måste vara allvarligt på de sätt som EU-domstolen preciserar, dvs. bl.a. verkligt och aktuellt eller förutsebart. Detta behöver inte särskilt anges i lagtext. Det kan heller inte uteslutas att kraven i framtiden förändras eller uttrycks på annat sätt i rättspraxis. Förutsättningarna för lagringsskyldigheten bör därför i lagtext inte vara mer preciserad än att det ska finnas ett allvarligt hot mot Sveriges säkerhet. Detta innebär att det i lagtext bör anges att det ska finnas ett allvarligt hot mot Sveriges säkerhet för att ett beslut om nationell säkerhetslagring ska kunna fattas.

Utredningen föreslår vidare att det ska vara obligatoriskt för Säkerhetspolisen att samråda med Försvarsmakten inför sin bedömning av hotet mot Sveriges säkerhet. Som *Säkerhetspolisen* och *Försvarsmakten* för fram är det tillräckligt att myndigheterna samråder vid behov. Detta behöver dock inte anges i lagtext. Det kan därutöver finnas behov av att Säkerhetspolisen samråder med andra, t.ex. Polismyndigheten. Behovet av samråd får alltså avgöras i det enskilda fallet. Det finns inte heller hinder mot att myndigheter som har information om hot mot den nationella säkerheten på eget initiativ uppmärksammar Säkerhetspolisen om dessa förhållanden.

Beslutet bör få gälla i högst ett år, men får förlängas och ska upphävas om det inte längre finns skäl för det

Av EU-domstolens praxis följer att ett beslut om nationell säkerhetslagring ska gälla under en viss tid. Detta innebär att beslutet bara får meddelas för en period som måste vara tidsmässigt begränsad till vad som är strängt nödvändigt, men som kan förlängas om hotet fortfarande kvarstår (se punkten 138 i La Quadrature du Net I-domen). Som utredningen konstaterar bör det därför föreskrivas en längsta tid som beslutet får gälla.

Utredningen föreslår att ett beslut om nationell säkerhetslagring ska få gälla under högst ett år, med möjlighet till förlängning. *Svenska Journalistförbundet* och *TU* menar att den föreslagna giltighetstiden är för lång. Med hänsyn till att ett allvarligt hot mot den nationella säkerheten kan finnas under en inte obetydlig tid bör den längsta tiden för ett beslut inte vara alltför kort. I utredningen konstateras vidare att brott mot nationell säkerhet, som spionerі och terrorism, är speciella till sin karaktär i den meningen att brottsligheten ofta pågår under mycket lång tid. Det kan även antas att de förhållanden som har lagts till grund för bedömningen av ett allvarligt hot mot den nationella säkerheten inte ändras särskilt snabbt. Det är därför rimligt att ett beslut om nationell säkerhetslagring ska få gälla i högst ett år. Om Säkerhetspolisen gör bedömningen att det allvarliga hotet mot den nationella säkerheten kvarstår kan myndigheten sedan, genom ett nytt beslut, förlänga lagringsskyldigheten. Det finns inget hinder mot att förfarandet påbörjas och förlängningsbeslutet fattas innan det tidigare beslutet har upphört att gälla. Inför att Säkerhetspolisen avser att fatta ett sådant beslut måste samma förfaranderegler som vid det ursprungliga beslutet följas. Säkerhetspolisen ska därtill även ha en skyldighet att löpande ompröva om hotet består och upphäva lagringsskyldigheten om det inte längre finns skäl för beslutet.

Detta innebär att beslutet bör få gälla i högst ett år och att Säkerhetspolisen genom ett nytt beslut får förlänga lagringsskyldigheten om hotet mot Sveriges säkerhet består. Om det inte längre finns skäl för lagringen ska Säkerhetspolisen upphäva beslutet.

Ett beslut får fattas endast när det är absolut nödvändigt och omfattningen ska begränsas till vad som är absolut nödvändigt

Utredningen föreslår att det i lagtext ska anges att ett beslut får fattas endast när det är absolut nödvändigt för att skydda Sveriges säkerhet och att det ska begränsas till vad som är absolut nödvändigt för syftet med lagringen i ett antal närmare angivna fall. Utredningens förslag är ett uttryck för proportionalitetsprincipen.

Som utredningen redogör för finns proportionalitetsprincipen reglerad i olika regelverk. Vad gäller iakttagandet av proportionalitetsprincipen i regelverken om elektronisk kommunikation föreskrivs bl.a. i artikel 15.1 första meningen i e-dataskyddsdirektivet 2002/58/EG att medlemsstaterna får vidta en åtgärd som avviker från principen om konfidentialitet vid kommunikation och därmed tillhörande trafikuppgifter, när en sådan åtgärd är nödvändig, lämplig och proportionerlig i ett demokratiskt samhälle, för att bl.a. skydda nationell säkerhet. I skäl 11 i direktivet anges att en åtgärd av detta slag ska vara i strikt proportion till det avsedda ändamålet. Kravet på proportionalitet följer även av EU-domstolens praxis. Det har bl.a. uttalats att för att kravet ska vara uppfyllt måste det i lagstiftning föreskrivas klara och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden samt anges minimikrav, så att de personer vars personuppgifter berörs har tillräckliga garantier för att uppgifterna på ett effektivt sätt är skyddade mot riskerna för missbruk. Denna lagstiftning ska vara rättsligt bindande enligt nationell rätt och i synnerhet ange under vilka omständigheter och på vilka villkor en åtgärd avseende behandling av sådana uppgifter får vidtas, vilket säkerställer att ingreppet begränsas till vad som är strängt nödvändigt (SpaceNet-domen p. 69).

Frågan om att reglera proportionalitetsprincipen har varit föremål för överväganden i olika lagstiftningsärenden. I den tidigare lagen om elektronisk kommunikation angavs att åtgärder som vidtas med stöd av lagen inte får vara mer ingripande än vad som framstår som rimligt och att åtgärderna ska vara proportionella med hänsyn till lagens syfte och de övriga intressen som anges i lagens första paragraf, se 1 kap. 2 § lagen (2003:389) om elektronisk kommunikation. Vid införandet av den nya lagen om elektronisk kommunikation ansågs det inte finnas något behov av att ha med en sådan reglering, bl.a. med anledning av att proportionalitetsprincipen numera är lagfäst i 5 § tredje stycket förvaltningslagen (2017:900), se prop. 2021/22:136 s. 119. I propositionen Datalagring vid brottsbekämpning – anpassningar till EU-rätten lyftes frågan om en reglering av proportionalitetsprincipen i samband med frågan om lagringstid. Det bedömdes dock att det inte fanns något behov av en sådan reglering då det följer direkt av EU-rätten att en proportionalitetsbedömning ska göras i det avseendet (prop. 2018/19:86 s. 49).

Proportionalitetsprincipen gäller alltså vid beslut om nationell säkerhetslagring även om den inte regleras i lag. Det föranleder frågan om att det finns behov av en sådan reglering i det här fallet. Ett beslut om nationell säkerhetslagring ska meddelas endast under omständigheter som utgör hot mot den nationella säkerheten. Det är ett ingripande beslut som påverkar många aktörer och personer. Det är också fråga om ny lagstiftning och en ny typ av ärende. Mot denna bakgrund är det motiverat att ha en uttrycklig bestämmelse som erinrar om proportionalitetsprincipen och den restriktivitet som ska iakttas vid beslut om nationell säkerhetslagring. I linje med vad utredningen anger bör därför proportionalitetsprincipen komma till uttryck i den nya lagen.

Som *Försvarsunderrättelsedomstolen* för fram kan den av utredningen föreslagna utformningen att beslutet får fattas endast om det är absolut nödvändigt för att skydda Sveriges säkerhet ge sken av att lagringsskyldigheten måste vara en nödvändig betingelse för att skydda den nationella säkerheten. I likhet med vad domstolen anger kan ett skäl för lagringen vara att uppgifterna kan komma att bidra till att säkerhetshotande brottslighet förhindras, upptäcks, utreds och lagförs. Det är därför tillräckligt att det i bestämmelsen anges att beslutet får fattas endast när det är absolut nödvändigt, utan den av utredningen föreslagna preciseringen. Vad som är absolut nödvändigt beror på omständigheterna i det enskilda fallet. En bedömning behöver alltså i varje enskilt fall göras av om ett beslut om nationell säkerhetslagring står i rimlig proportion till vad som är att vinna med åtgärden. Exempelvis har det betydelse vilken typ av hot det är fråga om och vilka alternativ till nationell säkerhetslagring som finns tillgängliga.

Utredningen föreslår vidare att beslutet ska begränsas till vad som är absolut nödvändigt för vissa angivna syften med lagringen. Det gäller i fråga om vilka tillhandahållare som omfattas av lagringsskyldigheten, beslutets giltighetstid och vilka typer av uppgifter som ska omfattas av lagringsskyldigheten. Som bl.a. *Åklagarmyndigheten* och *Polismyndigheten* påtalar kan en bestämmelse som upplyser om att beslutet ska begränsas i vissa särskilt angivna avseenden verka för begränsande. Ett beslut kan behöva begränsas även på andra sätt. Om hotet mot den nationella säkerheten är tillräckligt allvarligt kan inte heller uteslutas att det bedöms vara nödvändigt att t.ex. alla tillhandahållare åläggs en skyldighet att

lagra samtliga uppgifter som omfattas av lagstiftningen. I enlighet med detta bör det i lagtext inte anges vilka närmare begränsningar som ska omfattas av beslutet.

För att tydliggöra de överväganden som behöver göras innan ett beslut om nationell säkerhetslagring fattas finns det däremot, i linje med vad *Hi3G Access AB* och *TechSverige* för fram, skäl att särskilt ange att omfattningen av beslutet ska begränsas till vad som är absolut nödvändigt. Vilka begränsningar som kan bli aktuella preciseras i författningskommentaren. Den behöriga myndigheten har då, inom ramen för nödvändighetsprövningen, att ta ställning till bl.a. vilka tillhandahållare och uppgifter som ska omfattas av lagringsskyldigheten samt beslutets giltighetstid. En sådan reglering får, till skillnad mot vad bl.a. *Svenska Journalistförbundet* och *Telia Sverige AB* för fram, skapa tydliga och väl avgränsade ramar för beslutets omfattning.

6.3 En effektiv kontroll av lagringsskyldigheten

Utkastets förslag: Försvarsunderrättelsedomstolen ska vara kontrollorgan.

Utredningens förslag överensstämmer inte med utkastets. Utredningen föreslår att en ny delegation inom Säkerhets- och integritetsskyddsnämnden ska vara kontrollorgan.

Remissinstanserna: Många remissinstanser instämmer i eller har inget att invända mot förslaget. *Brottsoffermyndigheten* menar att införandet av ett kontrollorgan och regleringen kring kontrollorganet är viktiga för att värna rättssäkerheten och förslagens legitimitet. *Säkerhets- och integritetsskyddsnämnden* har förståelse för slutsatsen att en nyinrättad delegation inom myndigheten skulle kunna utgöra ett lämpligt kontrollorgan, men anser att det hade varit önskvärt att detta föregicks av en organisationsöversyn. *Försvarsunderrättelsedomstolen* anser att det finns goda skäl att överväga om domstolen bör vara kontrollorgan. Domstolen har kompetens att bedöma hot mot den nationella säkerheten, att pröva integritetsskyddsaspekter och är van vid att hantera kvalificerat hemliga uppgifter. Även *Åklagarmyndigheten* menar att Försvarsunderrättelsedomstolen bör vara kontrollorgan. I detta avseende förs särskilt fram att domstolen har betydande kunskaper när det gäller frågor om hot mot Sveriges säkerhet. Myndigheten påtalar även att kunskaper på området bör begränsas till en så liten personkrets som möjligt. Vidare förs fram att det är systematiskt olämpligt att lägga en central beslutsfunktion på Säkerhets- och integritetsskyddsnämnden. *TU* anser att lagringsbeslutet bör fattas av en domstol. *Säkerhetspolisen* för fram att valet av kontrollorgan behöver övervägas ytterligare. *Sveriges Domareförbund* påtalar att delegationen kommer ha svårt att göra någon närmare granskning av eller ifrågasätta Säkerhetspolisens bedömning av skälen för beslutet. Kontrollorganet kommer därtill antagligen bara att pröva några enstaka överklaganden, varför det kan ifrågasättas om systemet uppfyller det EU-rättsliga kravet på effektiv kontroll. Förbundet har även betänkligheter kring om den föreslagna delegationen, inordnad under en politisk sammansatt nämnd, är att betrakta som oberoende i europarättslig mening. Förbundet föreslår därför att det inordnas en domstolsprövning i den ordinarie domstolsorganisationen, att Försvarsunderrättelsedomstolens ansvars-

område utvidgas eller att det inrättas en ny specialdomstol för prövningen. Även *Svea hovrätt* efterfrågar en domstolsprövning av lagringsskyldigheten. *Tele2 Sverige AB* lyfter att det bara är Säkerhetspolisen och Försvarsmakten som kommer att ha en helhetsbild av säkerhetsläget och hotbilden mot Sverige, varför den effektiva kontrollen kan ifrågasättas. *Stockholms universitet (Juridiska fakulteten)* för fram att samtliga prövningsaktörer är förvaltningsmyndigheter. Det framstår därför som mer lämpligt att beslutet prövas antingen av Högsta domstolen eller Försvarsunderrättelsedomstolen. Universitetet påtalar vidare att om frågan om nationell säkerhetslagring bara bedöms på myndighetsnivå innebär det i praktiken ett monopol för regeringsmakten beträffande tolkningen av vad som ska anses vara ett tillräckligt hot.

Skälen för utkastets förslag: Lagringsskyldigheten behöver kunna bli föremål för en effektiv kontroll av en domstol eller en oberoende myndighet. Den effektiva kontrollen ska syfta till en granskning av att förutsättningarna för lagringsskyldigheten är uppfyllda (se t.ex. punkterna 137–139 i La Quadrature du Net I-domen). Kontrollorganet måste kunna göra en egen bedömning av hotet mot den nationella säkerheten. Kontrollorganet behöver därför ha kompetens att bedöma sådana frågor, men även kunna göra de komplicerande avvägningar som krävs vad gäller elektronisk kommunikation och integritetsskydd.

I utredningen görs överväganden av för- och nackdelar med domstolar och vissa andra myndigheter som kontrollorgan. Utredningens bedömning är att Försvarsunderrättelsedomstolen och ett nytt beslutsorgan inom Säkerhets- och integritetsskyddsnämnden framstår som mest lämpliga att vara kontrollorgan. Utredningen menar dock att ett nytt beslutsorgan inom Säkerhets- och integritetsskyddsnämnden är ett bättre alternativ än Försvarsunderrättelsedomstolen. Nämnden hanterar redan idag frågor som rör brottsbekämpning och har ett etablerat samarbete med Säkerhetspolisen vad gäller praktiska frågor, som hantering av känslig information. Därtill menar utredningen att det i Sverige finns en relativt skarp gräns mellan organ på den militära respektive civila sidan, vilket talar mot Försvarsunderrättelsedomstolen som kontrollorgan. Ett flertal remissinstanser delar dock inte utredningens bedömning att Säkerhets- och integritetsskyddsnämnden ska vara kontrollorgan, utan anser att Försvarsunderrättelsedomstolen är ett bättre alternativ.

Den prövning som kontrollorganet ska göra rör frågor om allvarliga hot mot rikets säkerhet och innebär en överprövning av beslut som kan påverka en stor krets. Det är därför viktigt att kontrollorganet har erforderlig erfarenhet och kompetens inom de områden som är relevanta att bedöma.

Försvarets radioanstalt ska enligt 4 a § lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (signalspaningslagen) ansöka om tillstånd för signalspaning hos Försvarsunderrättelsedomstolen, vilket också är en form av teknisk inhämtning. Tillstånd får enligt 5 § signalspaningslagen endast lämnas om uppdraget är förenligt med lagen (2000:130) 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. Försvarsunderrättelseverksamhet ska enligt 1 § lagen om försvarsunderrättelseverksamhet 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.

Försvarsunderrättelsedomstolen gör alltså i andra sammanhang en prövning som har likheter med den som blir aktuell vid en överprövning av ett beslut om nationell säkerhetslagring, även om det då rör sig om utländska förhållanden. *Försvarsunderrättelsedomstolen* påtalar att sambandet mellan inre och yttre säkerhet är mer direkt än tidigare till följd av globaliseringen. Även inre hot mot den nationella säkerheten har således ofta en internationell dimension. Som Försvarsunderrättelsedomstolen för fram får domstolen därför anses ha kompetens att bedöma hot mot den nationella säkerheten och att pröva integritetsskyddsaspekter, även vad gäller den nationella säkerhetslagringen. I enlighet med vad *Åklagarmyndigheten* framhåller har Försvarsunderrättelsedomstolen betydande kunskaper när det gäller de aktuella frågorna om hot mot Sveriges säkerhet.

Försvarsunderrättelsedomstolens ordförande utnämns efter prövning i Domarnämnden. Domstolen består även av 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 tillgodose domstolens behov av kompetens rörande bl.a. underrättelseverksamhet och integritetsskydd (2 och 3 §§ lagen [2009:966] om Försvarsunderrättelsedomstol). Detta skiljer sig från Säkerhets- och integritetsskyddsnämndens sammansättning, där ett flertal ledamöter är tillsatta för att representera allmänheten och garantera en medborglig insyn i verksamheten (5 § lagen [2007:980] om tillsyn över viss brottsbekämpande verksamhet). Försvarsunderrättelsedomstolens sammansättning talar för att domstolen är ett lämpligare kontrollorgan. Som *Sveriges Domareförbund* för fram får Försvarsunderrättelsedomstolens sammansättning även utgöra en extra garant för kontrollorganets oberoende.

Som ett argument mot Försvarsunderrättelsedomstolen som kontrollorgan för utredningen fram att det i Sverige finns en relativt skarp gräns mellan organ på den militära respektive civila sidan. Domstolen påtalar dock att mandatet för försvarsunderrättelseverksamheten anpassats från kartläggning av ”yttre militära hot” till ”yttre hot”, vilket bl.a. innebär att även internationell terrorism och grov gränsöverskridande brottslighet med säkerhetspolitiska konsekvenser kan omfattas av försvarsunderrättelseverksamheten. Domstolen delar därför inte uppfattningen att det finns en risk för sammanblandning av uppgifter och myndigheter på den militära respektive civila sidan. Det finns inte skäl att ha någon annan uppfattning än Försvarsunderrättelsedomstolen i dessa frågor.

Det föreslås vidare en prövningsordning där kontrollorganet kommer få ta del av de omständigheter som ligger till grund för beslutet om nationell säkerhetslagring vid ett sammanträde (avsnitt 6.4.2). En sådan ordning får anses skapa goda förutsättningar för beslutsfattandet. Mot bakgrund av detta och den kompetens som Försvarsunderrättelsedomstolen besitter finns det inte, som *Sveriges Domareförbund* och *Tele2 Sverige AB* för fram, skäl att tro att kontrollorganet kommer ha svårt att göra en tillräcklig prövning. Vad Sveriges Domareförbund påtalar om att

kontrollorganet antagligen bara kommer att överpröva något enstaka beslut per år förändrar inte att det finns förutsättningar för att göra en välgrundad bedömning.

Mot bakgrund av detta får Försvarsunderrättelsedomstolen anses vara det lämpligaste kontrollorganet när det gäller överprövningen av Säkerhetspolisens beslut om nationell säkerhetslagring. Detta innebär att Försvarsunderrättelsedomstolen bör vara kontrollorgan vid överprövningen av beslut om nationell säkerhetslagring. Utöver att det anges i den nya lagen bör det också framgå av domstolens uppgifter i 1 § lagen (2009:966) om Försvarsunderrättelsedomstol. Den närmare regleringen av kontrollorganets uppgifter bör, som utredningen föreslår, finnas i förordning.

6.4 Regler om ombud och förfarandet

6.4.1 Ett ombud bör bevaka enskildas intressen

Utkastets förslag: Ett offentligt ombud för nationell säkerhetslagring ska bevaka enskildas intressen i ärenden om nationell säkerhetslagring.

Regeringen ska för högst tre år i sänder förordna en person som ska tjänstgöra som ordinarie offentligt ombud för nationell säkerhetslagring och två personer som ska vara det ordinarie ombudets ställföreträdare.

Ombudet ska vara svensk medborgare och ha varit ordinarie domare, vara eller ha varit advokat eller ha motsvarande juridisk erfarenhet. Ombudet ska inte få vara i konkurstillstånd eller ha förvaltare.

Regeringen ska inhämta förslag på lämpliga kandidater från Domarnämnden och Sveriges advokatsamfund.

Ombudet ska trots att regeringens förordnande har upphört få slutföra pågående uppdrag.

Ett ombud för nationell säkerhetslagring ska säkerhetsprövas enligt säkerhetsskyddslagen.

Utredningens förslag överensstämmer i huvudsak med utkastets. Utredningen föreslår att regeringen ska förordna en person som i första hand och en person som i andra hand ska vara det ordinarie ombudets ställföreträdare.

Remissinstanserna: Många remissinstanser instämmer i eller har inget att invända mot förslagen. *Domarnämnden* har inte något att invända mot uppgiften att lämna förslag på personer som är lämpliga att tjänstgöra som ombud. *Sveriges advokatsamfund*, som i och för sig ser positivt på att ett ombud ska tillvarata allmänhetens integritetsintressen, anser att det finns en risk för att ombudens möjligheter att agera för att skydda den personliga integriteten kommer att bli begränsade. En liknande synpunkt förs fram av *Tele2 Sverige AB* som påtalar att ombudet inte kommer ha en helhetsbild av säkerhetsläget och hotbilden mot Sverige. *Sveriges Domareförbund* för fram att det framstår som sårbart att ombudet förordnas under en relativt kort tid. *Uppsala universitet (Juridiska fakulteten)* menar att det är tveksamt att knyta tillsynen över lagringsskyldigheten till en persons omdöme. *Försvarsunderrättelsedomstolen* för fram att det hos domstolen finns en

ordning med integritetsskyddsombud som skulle kunna fylla funktionen som ombud.

Skälen för utkastets förslag

Ett ombud bör bevaka enskildas intressen

Det är av stor vikt att enskildas intressen kan bevakas i ärenden om nationell säkerhetslagring. Utredningen föreslår att detta ska ske genom en ordning med ett ombud som bevakar den enskildes intressen.

För att säkerställa att reglerna och tillämpningen av reglerna lever upp till högt ställda krav på rättssäkerhet behövs det en ordning som tillgodoser enskildas intressen. En fördel med att ha ett ombud är att förfarandet blir mer kontradiktoriskt, vilket främjar frågornas allsidiga belysning. Detta är särskilt viktigt eftersom enskilda inte kommer att ha kännedom om att förfarandet pågår. En ordning med ett ombud som bevakar enskildas intressen i ärenden om nationell säkerhetslagring bör därför införas. Som utredningen konstaterar avses med enskildas intressen inte bara fysiska personers intressen utan även tillhandahållarnas. Uttrycket kan avse personliga, ekonomiska och andra förhållanden. Ett ombud enligt den nya lagen kommer alltså ha delvis andra intressen att bevaka än ett offentligt ombud enligt rättegångsbalken (jfr 27 kap. 26 § rättegångsbalken). Detsamma gäller i förhållande till integritetskyddsombud enligt lagen (2009:966) om försvarsunderrättelsedomstol (jfr 5 §). Ombudet bör i lagtext benämnas offentligt ombud för nationell säkerhetslagring.

Det bör införas regler om ombudet i den nya lagen

Det finns behov av regler som närmare anger hur det offentliga ombudet för nationell säkerhetslagring ska förordnas samt vilka kvalifikationer ombudet ska ha. Motsvarande regler som gäller för offentliga ombud enligt rättegångsbalken bör finnas i den nya lagen om nationell säkerhetslagring (jfr 27 kap. 26–30 §§ rättegångsbalken). I några avseenden finns det dock skäl att anpassa bestämmelserna till vad som specifikt gäller i ärenden om nationell säkerhetslagring.

Ett alternativ som *Försvarsunderrättelsedomstolen* för fram är att låta de integritetsskyddsombud som finns hos domstolen fylla funktionen som ombud enligt den nya lagen. De ombuden fyller dock i alla delar inte samma funktion som ett ombud i ärenden om nationell säkerhetslagring. En sådan ordning bör därför inte införas.

I enlighet med utredningens förslag bör det vara regeringen som utser ombudet. Det är viktigt att kretsen av personer som får tillgång till den känsliga informationen minimeras. Det kan också förväntas bli fråga om endast ett fåtal ärenden. Det bör därför finnas enbart ett ordinarie ombud. Detta innebär även att ombudet inte kommer att förordnas i ett specifikt ärende om nationell säkerhetslagring. För att undvika att systemet blir för sårbart bör det finnas ersättare för det ordinarie ombudet i form av två personer som ska vara det ombudets ställföreträdare. Det finns inte tillräckliga skäl för att ha en inbördes ordning mellan ställföreträdarna, som utredningen föreslår. Samtliga bör förordnas för en period om högst tre år. Detta får, till skillnad mot vad *Sveriges Domareförbund* för fram, anses vara en rimlig tid för åtagandet. Förslaget möjliggör också en viss flexibilitet för regeringen att förordna för en kortare tid.

För att bredda kretsen av personer som kan komma i fråga som offentligt ombud för nationell säkerhetslagring bör ombudet, till skillnad från vad som gäller för offentliga ombud enligt rättegångsbalken, även kunna ha motsvarande juridisk erfarenhet som en advokat. Det bör alltså inte ställas något absolut krav på att personen är eller har varit advokat eller ordinarie domare. I övrigt bör samma krav gälla (jfr 27 kap. 27 § andra och tredje styckena rättegångsbalken). Detta innebär att ett offentligt ombud för nationell säkerhetslagring ska vara svensk medborgare och ha varit ordinarie domare, vara eller ha varit advokat eller ha motsvarande juridisk erfarenhet. Ombudet ska inte vara i konkurstillstånd eller ha förvaltare. Regeringen ska inhämta förslag på lämpliga kandidater från Sveriges advokatsamfund och Domarnämnden. Det finns inte något hinder mot att regeringen inhämtar förslag på och relevant information om lämpliga personer även från annat håll. Kompetenskraven i kombination med de förfaranderegler som föreslås nedan, enligt vilka ombudet ges möjlighet att bevaka den enskildes rätt, gör att det inte finns skäl att instämma i *Sveriges advokatsamfunds* och *Tele2 Sverige AB:s* påpekanden om att ombudet kommer ha svårt att tillvarata enskildas rättigheter. Det finns inte heller skäl att instämma i vad *Uppsala universitet (Juridiska fakulteten)* för fram om att det är tveksamt att knyta tillsynen till en persons omdöme, eftersom de personer som utses enligt föreslagna kompetenskrav får förutsättas vara väl lämpade för uppgiften. Kompetenskravet är vidare ett sätt att säkerställa ombudets oberoende. Vidare föreslås att beslut om nationell säkerhetslagring alltid ska underställas kontrollorganets prövning (avsnitt 6.4.2). Överprövningen kommer därmed med regeringens förslag inte vara beroende av ombudets bedömning av om beslutet bör överklagas eller inte.

För offentliga ombud enligt rättegångsbalken gäller att ombudet trots att regeringens förordnande har upphört får slutföra pågående uppdrag. Motsvarande bör gälla för offentliga ombud för nationell säkerhetslagring när det gäller att slutföra uppdraget i ett specifikt ärende om nationell säkerhetslagring (jfr 27 kap. 27 § fjärde stycket rättegångsbalken).

I säkerhetsskyddslagen (2018:585) finns bestämmelser om vem som ska säkerhetsprövas (se 3 kap. 1 § i den lagen). I likhet med vad som gäller för ett integritetsskyddsombud enligt lagen (2009:966) om Försvarsunderrättelsedomstol bör ett ombud för nationell säkerhetslagen enligt den nya lagen säkerhetsprövas.

Frågor om tystnadsplikt och meddelarfrihet för ombud enligt den nya lagen behandlas i avsnitt 6.8.

6.4.2 Vissa ytterligare regler om handläggningen bör finnas i den nya lagen

Utkastets förslag: Ett beslut om nationell säkerhetslagring ska få verkställas omedelbart.

När ett beslut om nationell säkerhetslagring har fattats ska beslutet omedelbart underställas Försvarsunderrättelsedomstolen. Försvarsunderrättelsedomstolen ska så snart som möjligt hålla ett sammanträde. Vid sammanträdet ska Säkerhetspolisen och det offentliga ombudet för nationell säkerhetslagring närvara. Försvarsunderrättelsedomstolen ska vid sammanträdet ha rätt att ta del

av de omständigheter som ligger till grund för beslutet om nationell säkerhetslagring. Vid sammanträdet ska Säkerhetspolisen redogöra för beslutet och ombudet ha rätt att yttra sig.

Försvarsunderrättelsedomstolen ska pröva om Säkerhetspolisens beslut om nationell säkerhetslagring ska fortsätta att gälla. Domstolen ska även besluta om ersättning till det offentliga ombudet för nationell säkerhetslagring. I fråga om ersättning till ombudet ska bestämmelserna i 21 kap. 10 § första och andra styckena rättegångsbalken tillämpas. Försvarsunderrättelsedomstolens beslut om nationell säkerhetslagring och ersättning ska inte få överklagas.

Utredningens förslag överensstämmer delvis med utkastets. Utredningen föreslår att Säkerhetspolisen inför ett beslut om nationell säkerhetslagring ska hålla ett sammanträde, till vilket det offentliga ombudet ska kallas. Utredningen föreslår att beslutet om nationell säkerhetslagring ska få överklagas av ett ombud. Utredningen föreslår också att kontrollorganet ska pröva om Säkerhetspolisens beslut om nationell säkerhetslagring ska fastställas eller upphävas. Vidare föreslås att beslutet ska få verkställas om det inte har överklagats inom föreskriven tid, om ombudet har avgett en förklaring om att beslutet inte kommer att överklagas eller om det har fastställts av kontrollorganet. Det föreslås också att Säkerhetspolisen ska besluta om ersättning till ombudet om beslutet inte överklagas. Utredningen föreslår inte någon reglering om att kontrollorganets beslut om ersättning inte får överklagas.

Remissinstanserna: Många remissinstanser instämmer i eller har inget att invända mot förslagen. *Säkerhets- och integritetsskyddsnämnden* instämmer i att kontrollorganet inte ska kunna göra ändringar i beslutet om nationell säkerhetslagring, utan endast upphäva eller fastställa det. Vidare förs fram att det bör finnas en bortre tidsgräns för överklagande av ersättningsbeslutet. Nämnden påtalar därutöver att det inte framgår att överklagandeförbudet även gäller kontrollorganets beslut om ersättning till ombudet. Enligt *Försvarsunderrättelsedomstolen* är ett tillståndsförfarande att föredra, där Säkerhetspolisen efter en prövning av ett oberoende organ får tillstånd att förelägga om lagringsskyldighet för de i tillståndet angivna uppgifterna. Liknande synpunkter förs fram av *Svea hovrätt* och *Sveriges Domareförbund* som efterfrågar att lagringsskyldigheten alltid prövas av domstol. Sveriges Domareförbund påtalar även att kontrollorganets beslut inte kommer att kunna överklagas, varför det kan ifrågasättas om systemet uppfyller det EU-rättsliga kravet på effektiv kontroll. Vidare anförs att det framstår som betänkligt att Säkerhetspolisen ska bestämma ersättning till ombudet, samtidigt som myndigheten ska meddela ett beslut som ombudet ska granska. Även *Stockholms universitet (Juridiska fakulteten)* ifrågasätter att beslutsmyndigheten ska bestämma ersättningen till ombudet. *Svenska Journalistförbundet* är av uppfattningen att beslut om nationell säkerhetslagring bör underställas domstolsprövning innan det börjar gälla och att ett kontrollorgan därefter kan övervaka att reglerna följs. *Sveriges advokatsamfund* menar att det är en brist att kontrollorganet inte ska utöva kontroll av hur lagringen fortlöper, särskilt eftersom lagringsskyldigheten kan vara vidsträckt och utgör ett allvarligt integritetsintrång. *Säkerhetspolisen* för fram att hotet kan vara omedelbart förestående och kräva mycket snabba insatser,

varför lagringsbeslutet bör kunna verkställas omedelbart. Även *Polismyndigheten* anser att lagringsbeslutet bör kunna verkställas omedelbart.

Skälen för utkastets förslag

Den nya lagen bör innehålla regler om omedelbar verkställighet, överprövning och sammanträde hos kontrollorganet

Nationell säkerhetslagring kommer att vara aktuellt vid allvarliga hot mot den nationella säkerheten. Detta innebär att det finns behov av ett skyndsamt förfarande, samtidigt som rättssäkerheten behöver upprätthållas för enskilda. Det offentliga ombudet för nationell säkerhetslagring behöver ges möjlighet att ta tillvara enskildas rätt. För att säkerställa detta och samtidigt skapa förutsättningar för en effektiv tillämpning behövs vissa förfaranderegler i den nya lagen.

Med hänsyn till beslutets brådskande karaktär, och i linje med de synpunkter som *Säkerhetspolisen* och *Polismyndigheten* för fram om att lagringen bör kunna påbörjas skyndsamt bör Säkerhetspolisens beslut om nationell säkerhetslagring till skillnad mot vad utredningen för fram få verkställas omedelbart.

Utredningen föreslår att beslutet om nationell säkerhetslagring ska få överklagas till kontrollorganet av ombudet. Ett par remissinstanser efterfrågar en domstolsprövning av beslutet eller att beslutsmyndighetens beslut alltid ska underställas kontrollorganet. Beslut om nationell säkerhetslagring är av ingripande karaktär. En ordning där besluten alltid underställs kontrollorganet innebär ökad rättssäkerhet, eftersom överprövningen inte görs beroende av ombudets bedömning av om det finns ett behov av att beslutet överprövas. Säkerhetspolisens beslut om nationell säkerhetslagring bör därför alltid underställas kontrollorganet. Ett beslut om nationell säkerhetslagring bör underställas kontrollorganet omedelbart, vilket är av stor vikt bland annat eftersom Säkerhetspolisens beslut föreslås kunna verkställas omedelbart. Med anledning av att Säkerhetspolisens beslut om nationell säkerhetslagring alltid ska underställas kontrollorganet finns inte samma behov av att hålla ett sammanträde hos Säkerhetspolisen där ombudet närvarar. En sådan ordning bör därför inte införas.

Det offentliga ombudet för nationell säkerhetslagring bör ha rätt till ersättning för arbetet i överprövningsförfarandet. I linje med utredningens förslag och vad bl.a. *Sveriges Domareförbund* för fram bör kontrollorganet vid sin överprövning av beslutet om nationell säkerhetslagring även besluta om ersättningen. I enlighet med utredningens förslag bör 21 kap. 10 § första och andra styckena rättegångsbalken tillämpas vid bestämmandet av ersättningens storlek (jfr 27 kap. 29 § rättegångsbalken).

Säkerhetskänslig information kommer även att förekomma hos kontrollorganet. Kontrollorganets prövning bör därför ske vid ett sammanträde, vid vilket Säkerhetspolisen och ombudet närvarar. Sammanträdet bör hållas så snart som möjligt och ska inte heller vid överprövningen kunna ersättas av skriftlig handläggning. Kontrollorganet bör vid sammanträdet få del av Säkerhetspolisens beslut och ett underlag som redovisar de omständigheter som ligger till grund för beslutet. Säkerhetspolisen bör även vid detta sammanträde redogöra för beslutet och de omständigheter som ligger till grund för det. Vidare bör ombudet få yttra sig och ställa frågor.

Med anledning av att det införs en ny typ av ombud i Försvarsunderrättelsedomstolen bör det göras en redaktionell ändring i 5 § lagen (2009:966) om Försvarsunderrättelsedomstol. Ändringen innebär att det preciseras att regleringen av domstolens integritetsskyddsombud endast avser målen om tillstånd till signalspaning.

Kontrollorganet bör pröva om lagringsbeslutet ska fortsätta att gälla och kontrollorganets beslut bör inte få överklagas

En särskild fråga är vilken prövning kontrollorganet ska göra av Säkerhetspolisens beslut om nationell säkerhetslagring. *Försvarsunderrättelsedomstolen* anser att ett tillståndsförfarande är att föredra, där det oberoende organet efter en ansökan ger Säkerhetspolisen tillstånd att förelägga den som är lagringsskyldig att lagra de i tillståndet angivna uppgifterna. En sådan ordning skulle dock innebära en risk för att det oberoende organet anses vara den egentliga beslutsfattaren. Det skulle även innebära att kontrollorganet får en annan roll i förfarandet. I linje med vad utredningen för fram i sak är det i stället rimligt att kontrollorganet prövar om lagringsbeslutet ska fortsätta att gälla. Det innebär att kontrollorganet prövar om det finns ett tillräckligt hot mot den nationella säkerheten och om lagringsskyldigheten är författningsenlig i övrigt, t.ex. att lagringsskyldigheten står i proportion till det bedömda hotet. Ordningen innebär att kontrollorganet inte kan göra ändringar i beslutet utan blir en mer renodlad kontrollinstans.

I enlighet med vad som anges av utredningen är det själva beslutet om lagring som ska kunna bli föremål för en effektiv kontroll och inte den efterföljande lagringen (jfr även EU-domstolens dom den 2 mars 2021 i mål C-746/18, Prokuratuur, punkterna 50–52). I motsats till vad *Svenska Journalistförbundet*, *Sveriges Domareförbund* och *Sveriges advokatsamfund* för fram bör detta inte innebära ett krav på att även kontrollorganets beslut måste kunna bli föremål för överprövning eller att det organet utövar en löpande tillsyn. Det har inte framkommit att det finns något sådant behov och det kan därtill framstå som överflödigt att besluten alltid och löpande blir föremål för ytterligare kontroll. Det finns, som *Säkerhets- och integritetsskyddsnämnden* för fram, skäl att i lagtext förtydliga att kontrollorganets ersättningsbeslut inte får överklagas. Kontrollorganets prövning bör inte hindra Säkerhetspolisen från att fatta ett nytt beslut om lagring, som sedan kan bli föremål för ny överprövning, eller att upphäva ett gällande beslut om lagring.

6.5 Lagringsskyldighetens omfattning

Utkastets förslag: Den som bedriver verksamhet som ska anmälas och den som tillhandahåller en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst ska kunna omfattas av lagringsskyldighet enligt ett beslut om nationell säkerhetslagring.

Beslutet ska få omfatta uppgifter om abonnemang, trafikuppgifter och lokaliseringsuppgifter som inte är trafikuppgifter och som rör användare som är fysiska personer eller abonnenter. Uppgifterna ska vara nödvändiga för att spåra

och identifiera kommunikationskällan och slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning, lokalisering av kommunikationsutrustning vid kommunikationen samt lokaliseringsuppgifter som inte är trafikuppgifter.

Lagringstiden för uppgifter om abonnemang och trafikuppgifter ska vara två år från den dag kommunikationen avslutades. Om uppgift saknas om när kommunikationen avslutades ska lagringstiden räknas från den dag uppgifterna genererades. För lokaliseringsuppgifter som inte är trafikuppgifter ska lagringstiden vara ett år och räknas från den dag uppgifterna genererades.

Det ska upplysas om att regeringen eller den myndighet som regeringen bestämmer kan meddela närmare föreskrifter om vilka uppgifter som får lagras enligt ett beslut om nationell säkerhetslagring.

Utredningens förslag överensstämmer i huvudsak med utkastets. Utredningen föreslår att lagringstiden ska vara två år för lokaliseringsuppgifter som inte är trafikuppgifter. Utredningen föreslår även att lagringen vid ett beslut om nationell säkerhetslagring ska ske utan dröjsmål.

Remissinstanserna: Många remissinstanser instämmer i eller har inget att invända mot förslaget. *Telia Sverige AB* för fram att det behöver visas att nyttan av lagringen väger upp de nackdelar som lagringen innebär i form av kostnader för tillhandahållarna och integritetsintrång för användarna. Vidare saknas bärande skäl för att lagringstiden ska förlängas. Ytterligare remissinstanser har betänkligheter kring lagringstidens längd och varför så många uppgifter ska lagras, däribland *Telenor Sverige AB*, *TechSverige*, *Bahnhof AB* och *Hi3G Access AB*. *Säkerhets- och integritetsskyddsnämnden* anser att lagringstiden bör vara ett år. *Svenska Journalistförbundet* menar att det inte är motiverat att lagringstiden alltid ska vara två år och att det bör finnas en skyldighet att radera uppgifter när den omständighet som låg till grund för beslutet inte längre finns.

Enligt Telenor Sverige AB är det inte tydligt om de lagrade uppgifterna omedelbart ska utplånas när förutsättningar för nationell säkerhetslagring inte längre finns. Telia Sverige AB ifrågasätter om det är förenligt med EU-domstolens praxis att lagringsskyldigheten även ska gälla om beslutet upphävs. *Tele2 Sverige AB* anser att det är oklart hur de brottsbekämpande myndigheterna ska extrahera operativt relevanta underrättelser ur en stor mängd nättekniska signaleringsuppgifter. Därutöver förs fram, vilket även påtalas av andra tillhandahållare, att den omständigheten att även lokaliseringsuppgifter som inte är trafikuppgifter ska kunna omfattas av ett beslut om nationell säkerhetslagring gör att operatörernas totala lagringskapacitet behöver mångdubblas. Operatörerna skulle även tvingas att lagra uppgifter som de inte har behov av i sin verksamhet. Hi3G Access AB menar, vilket också påtalas av Svenska Journalistförbundet, att omfattningen av lagringsskyldigheten inte kommer att vara förutsebar. Bolaget anser också, vilket även TechSverige och Telenor Sverige AB för fram, att det inte bör föreskrivas att lagringen ska ske utan dröjsmål, eftersom hänsyn behöver tas till vad som krävs för verkställigheten av beslutet.

Svenska Journalistförbundet anser att det är problematiskt ur ett källskyddsperspektiv att lagringsskyldigheten i högre utsträckning än i dag kommer att kunna

omfatta lokaliseringsuppgifter. Även *TU* ifrågasätter hur källskyddet ska kunna säkerställas i förhållande till journalister och medier.

Skälen för utkastets förslag

Ett beslut om nationell säkerhetslagring bör få rikta sig till de tillhandahållare som är skyldiga att lagra uppgifter om elektronisk kommunikation

Enligt nuvarande regelverk är de som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § lagen om elektronisk kommunikation skyldiga att lagra vissa uppgifter (9 kap. 19 § samma lag). Att dessa tillhandahållare ska kunna omfattas av den utökade lagringsskyldigheten framstår som rimligt, eftersom det är dessa aktörer som enligt nuvarande regelverk har ålagts att lagra uppgifter om elektronisk kommunikation. I avsnitt 7.2 föreslås därutöver att den som tillhandahåller en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst ska omfattas av lagringsskyldighet, inklusive lagring enligt ett beslut om nationell säkerhetslagring. Ett föreläggande om nationell säkerhetslagring bör därför kunna riktas mot den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § lagen om elektronisk kommunikation samt tillhandahållare av nummeroberoende interpersonella kommunikationstjänster.

Utredningens förslag innebär även att det i lagtext ska anges att lagring ska ske utan dröjsmål, bl.a. när det gäller lagring enligt ett föreläggande om nationell säkerhetslagring. Det har inte har framkommit att den lagring som sker enligt nu gällande regler inte sker i tillräckligt god tid. Det får vidare förutsättas att lagringen, även vid ett beslut om nationell säkerhetslagring, kommer att ske utan onödigt dröjsmål. Det finns därför skäl att dela *Hi3G Access AB:s*, *Telenor Sverige AB:s* och *TechSveriges* uppfattning att det inte har framkommit ett tillräckligt starkt behov av en sådan reglering.

Ramarna för vilka uppgifter som ska kunna omfattas av ett beslut om nationell säkerhetslagring

När det gäller telefonitjänst och meddelandehantering gäller lagringsskyldigheten i dag enbart kommunikation via mobil nätanslutningspunkt. Före reformen 2019 omfattades även uppgifter från såväl fast telefoni som fast ip-telefoni av lagringsskyldigheten. Lagringsskyldigheten omfattade tidigare också flera slags uppgifter än enligt nuvarande regler. När det gäller internetåtkomst omfattades före reformen 2019 uppgifter om den typ av kapacitet för överföring som hade använts av lagringsskyldigheten, vilket inte är fallet i dag. Med kapacitet för överföring avses hur abonnenten får internetåtkomst, t.ex. genom fast fiberanslutning.

De författningsändringar som gjordes 2019 syftade till att tillgodose det EU-rättsliga kravet på att lagringsskyldigheten inte får vara generell och odifferentierad. Ändringarna innebar att vissa typer av uppgifter inte längre omfattas av lagringsskyldigheten. Några särskilda överväganden kring vilka uppgifter som får lagras specifikt i syfte att skydda nationell säkerhet gjordes inte då (se prop. 2018/19:86 s. 20 f).

När det finns ett allvarligt hot mot den nationella säkerheten får lagringsskyldigheten vara mer omfattande än annars (avsnitt 6.1). Följaktligen får ramarna för ett beslut om en sådan lagringsskyldighet vara vidare än vad som gäller enligt

dagens reglering. I enlighet med utgångspunkterna för lagstiftningsärendet, och för att tillgodose myndigheternas behov av uppgifter när det finns ett allvarligt hot mot Sveriges säkerhet, bör i enlighet med utredningens bedömning de uppgiftskategorier som togs bort 2019 kunna omfattas av ett beslut om nationell säkerhetslagring.

Principer för lagringsskyldighetens omfattning

Av EU-domstolens praxis följer att det i nationell lagstiftning måste föreskrivas klara och precisa bestämmelser som reglerar räckvidden och tillämpningen av åtgärder som inskränker rätten till respekt för privatlivet och skyddet för personuppgifter. Lagstiftningen ska enligt EU-domstolen vara rättsligt bindande och i synnerhet ange under vilka omständigheter och på vilka villkor en åtgärd avseende behandling av sådana uppgifter får vidtas, vilket säkerställer att ingreppet begränsas till vad som är strängt nödvändigt (se bl.a. SpaceNet-domen p. 69, An Garda Síochána-domen p. 54 och La Quadrature du Net I-domen p. 132).

Hi3G Access AB och *Svenska Journalistförbundet* för fram att omfattningen av lagringsskyldigheten inte kommer att vara förutsebar. Det finns dock starka skäl för att regleringen inte bör vara för detaljerad i förhållande till hur enskilda kommunicerar med varandra och vilken specifik teknik eller tjänst de använder. För att syftet med lagringen ska uppnås bör lagringsskyldighetens utformning i likhet med nuvarande regler ske utifrån hur uppgifterna kan användas, såsom uppgifter som är nödvändiga för att spåra och identifiera kommunikationskällan. En sådan reglering innebär t.ex. att det saknar betydelse om kommunikation sker genom fast telefoni, mobiltelefoni, ip-telefoni eller en nummeroberoende interpersonell kommunikationstjänst. Som redogörs för nedan innebär den föreslagna utformningen även att mer detaljerade föreskrifter kommer kunna ges i förordning. En sådan reglering är ändamålsenlig men främjar även förutsebarheten för lagringsskyldighetens omfattning.

En viktig utgångspunkt är vidare att regleringen av lagringsskyldighetens omfattning utgår från vad som genereras eller behandlas i tillhandahållarnas verksamhet. Det betyder att tillhandahållaren inte har någon skyldighet att införskaffa uppgifter som denne annars inte genererar eller behandlar. Funktionalitet för dataskydd ska dock utformas på ett sådant sätt att lagringsskyldigheten kan uppfyllas (jfr 1 kap. 5 § lagen om elektronisk kommunikation). Tillhandahållarna får därför inte radera uppgifter som i någon utsträckning behandlas, om de omfattas av lagringsskyldighet.

Ett beslut om nationell säkerhetslagring bör få omfatta uppgifter om abonnemang och trafikuppgifter samt lokaliseringsuppgifter som inte är trafikuppgifter och som rör användare som är fysiska personer eller abonnenter

Utredningen föreslår att ett beslut om nationell säkerhetslagring ska kunna omfatta uppgifter om abonnemang och trafikuppgifter samt lokaliseringsuppgifter som inte är trafikuppgifter och som rör användare som är fysiska personer eller abonnenter. Beslutets omfattning ska, enligt utredningens förslag, begränsas till uppgifter som är nödvändiga för att spåra och identifiera kommunikationskällan och slutmålet för kommunikationen, datum, tidpunkt och varaktighet för

kommunikationen, typ av kommunikation, kommunikationsutrustning, lokalisering av kommunikationsutrustning vid kommunikationen samt lokaliseringsuppgifter som inte är trafikuppgifter.

Uppgifter om abonnemang och andra uppgifter som angår ett särskilt elektroniskt meddelande omfattas av den nuvarande lagringsskyldigheten enligt 9 kap. 19 § lagen om elektronisk kommunikation. I avsnitt 5.3 föreslås att begreppet annan uppgift som angår ett särskilt elektroniskt meddelande ska bytas ut mot trafikuppgift. Det är av stor vikt att abonnemangsuppgifter och trafikuppgifter kan lagras under längre tid när det finns ett allvarligt hot mot den nationella säkerheten. Behovet överväger det intrång som en lagring av sådana uppgifter kan innebära. Abonnemangsuppgifter och trafikuppgifter bör därför kunna omfattas av ett beslut om nationell säkerhetslagring.

Lagring av lokaliseringsuppgifter som inte är trafikuppgifter och som rör användare som är fysiska personer eller abonnenter har betydelse för kartläggning av var enskilda har befunnit sig. Uppgifterna kan vara av stor betydelse för att bekämpa hot mot den nationella säkerheten och är därmed även av stor betydelse i de brottsbekämpande myndigheternas arbete, vilket understryks av myndigheternas tillstyrkande av förslaget. *Åklagarmyndigheten* understryker att det självfallet finns behov av att införa en särskild möjlighet till lagring av trafik- och lokaliseringsuppgifter i syfte att skydda nationell säkerhet. Även om det kan vara fråga om känsliga uppgifter får en lagringsskyldighet för sådana uppgifter anses vara proportionerlig, eftersom lagringen kan påbörjas först om och när Sverige står inför ett allvarligt hot mot den nationella säkerheten. Åtkomsten till lagrade uppgifter är vidare omgärdad av rättssäkerhetsgarantier och det grundlagsskyddade efterforskningsförbudet vad gäller den som är meddelare till en viss uppgift (se avsnitt 6.6, 3 kap. 5 § tryckfrihetsförordningen och 2 kap. 5 § yttrandefrihetsgrundlagen). Förslagen bör därför inte, som *Svenska Journalistförbundet* och *TU* för fram, innebära några tillkommande risker för källskyddet i förhållande till nuvarande regler. I en sådan situation med ett allvarligt hot mot Sveriges säkerhet som det kommer att vara fråga om bör lokaliseringsuppgifter, till skillnad från vad bl.a. *Telia Sverige AB*, *Tele2 Sverige AB* och *Telenor Sverige AB* för fram, kunna omfattas av ett beslut om nationell säkerhetslagring. Detta innebär dock inte att tillhandahållarna, vilket Tele2 Sverige AB har farhågor kring, kommer att ha en skyldighet att införskaffa uppgifter som de annars inte genererar eller behandlar. Som upplyses i 9 kap. 23 § lagen om elektronisk kommunikation kan det också meddelas närmare föreskrifter på lägre nivå än lag beträffande vilka uppgifter som ska lagras. Sådana föreskrifter kan underlätta hanteringen av vad som närmare ska lagras och bidra till att mängden uppgifter står i rimlig proportion till syftet med lagringen. Att de brottsbekämpande myndigheterna inte skulle kunna tillgodogöra sig uppgifterna har inte framkommit. Tvärtom har det uttryckts att förslaget är angeläget. Ett beslut om nationell säkerhetslagring bör därför även få omfatta lokaliseringsuppgifter som inte är trafikuppgifter och som rör användare som är fysiska personer eller abonnenter.

Utredningens förslag om begränsning av beslutets omfattning skiljer sig delvis från vad som föreskrivs i 9 kap. 19 § lagen om elektronisk kommunikation. Den nationella säkerhetslagringen kommer att kunna omfatta lokalisering av mobil och fast kommunikationsutrustning.

Detta får sammanfattningsvis, till skillnad från vad *Svenska Journalistförbundet* för fram, anses vara ett tydligt och därutöver proportionerligt angivande av vilka uppgifter som kan omfattas av ett beslut om nationell säkerhetslagring. Den mer detaljerade regleringen kan som utredningen anger framgå av bestämmelser på lägre normgivningsnivå än lag. Utredningen har redogjort för vilka närmare uppgifter som kan omfattas (betänkandet s. 218–221).

Lagringstiden bör vara två år för uppgifter om abonnemang och trafikuppgifter samt ett år för lokaliseringsuppgifter som inte är trafikuppgifter

Enligt den nu gällande lagringsskyldigheten gäller olika lagringstider för olika slags uppgifter, räknat från den dag kommunikationen avslutades. Uppgifter som genereras eller behandlas vid telefonitjänst och meddelandehantering via mobil nätanslutningspunkt ska lagras i sex månader. Lokaliseringsuppgifter ska lagras i två månader. Uppgifter som genereras eller behandlas vid internetåtkomst ska lagras i tio månader. Om uppgifterna identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilde abonnenten ska de lagras i sex månader (9 kap. 22 § lagen om elektronisk kommunikation). Ett beslut om nationell säkerhetslagring föreslås kunna gälla i högst ett år. Frågan är hur länge de uppgifter som omfattas av ett sådant beslut ska lagras.

Utredningen föreslår att lagringstiden för alla uppgifter som kan lagras enligt ett beslut om nationell säkerhetslagring ska vara två år, vilket alltså innebär en förlängning i förhållande till vad som gäller enligt nuvarande regler.

Som de brottsbekämpande myndigheterna har påtalat finns det, för bl.a. syftet att bekämpa hot mot den nationella säkerheten, behov av att uppgifter lagras under längre tid än i dag. Lagringstiden vid ett beslut om nationell säkerhetslagring bör alltså, med hänsyn tagen även till arten av den brottslighet som ska bekämpas, vara längre än enligt gällande regler. EU-domstolen har dock slagit fast att lagringstiden för de uppgifter som omfattas av ett beslut om nationell säkerhetslagring ska begränsas till vad som är strängt nödvändigt (se bl.a. punkten 147 i La Quadrature du Net I-domen). För att lagringstiden inte ska riskera att bli längre än vad som kan anses vara tillåtet måste den alltså begränsas.

När det gäller lokaliseringsuppgifter som inte är trafikuppgifter kan konstateras att dessa inte omfattas av den lagringsskyldighet som gäller i dag. Sådana uppgifter kan exempelvis röra periodiska uppdateringar, registrering- och bortkoppling från mobilnät och andra uppgifter som genererats i syfte att initiera, upprätthålla och avsluta sessioner och tjänster under pågående internetåtkomst. Flera remissinstanser ifrågasätter att lagringstiden ska vara två år för dessa uppgifter, bl.a. *Tele2 Sverige AB* som påtalar att den omständigheten att även lokaliseringsuppgifter som inte är trafikuppgifter ska kunna omfattas av ett beslut om nationell säkerhetslagring gör att mobiloperatörernas totala lagringskapacitet behöver mångdubblas. Mot bakgrund av risken för att operatörerna kan bli skyldiga att lagra ett stort antal uppgifter under lång tid finns det skäl att skilja ut lokaliseringsuppgifter som inte är trafikuppgifter från övriga uppgifter som kan omfattas av ett beslut. Vid en avvägning av det behov som kan antas finnas av uppgiftstypen och det besvär lagringen kan förväntas medföra för de som är lagringsskyldiga finns det skäl att instämma i *Säkerhets- och integritetsskyddsnämndens* bedömning att en lagrings-

tid om ett år är rimlig. Detta innebär att lokaliseringsuppgifter som inte är trafikuppgifter bör lagras i ett år.

När det gäller övriga uppgifter som kan omfattas av lagringsskyldigheten vid ett föreläggande om nationell säkerhetslagring framstår en längre lagringstid inte som lika betungande. Till skillnad mot vad *Svenska Journalistförbundet* och *Telia Sverige AB* m.fl. för fram bör samma lagringstid gälla för dessa uppgifter. Med hänsyn till detta får utredningens förslag om en lagringstid på två år anses vara väl avvägt för abonnemangsuppgifter och trafikuppgifter.

Som huvudregel räknas lagringstiden från den dag som kommunikationen avslutades. I enlighet med utredningens förslag bör lagringstiden räknas från den dag uppgifterna genererades, om uppgift saknas om när kommunikationen avslutades. Det bör gälla generellt och inte endast i förhållande till nationell säkerhetslagring. Lokaliseringsuppgifter som inte är trafikuppgifter har inte någon koppling till kommunikation. För sådana uppgifter bör också, i enlighet med enligt utredningens förslag, lagringstiden räknas från den dag uppgifterna genererades.

Ett beslut om nationell säkerhetslagring kommer att kunna gälla i högst ett år. Den föreslagna ordningen innebär alltså att uppgifter kommer att lagras även efter det att ett beslut om nationell säkerhetslagring har upphört. Det finns inte något hinder mot detta. Tvärtom kan det motverka syftet att bekämpa brottslighet som kan utgöra hot mot den nationella säkerheten om det inte går att inhämta uppgifter i utredningar som pågår en tid efter att beslutet upphört.

Det bör upplysas om att regeringen eller den myndighet som regeringen bestämmer ska kunna meddela närmare föreskrifter

För att nödvändiga anpassningar ska kunna göras och syftet med lagringsskyldigheten uppnås över tid bör ramarna för vad skyldigheten får omfatta framgå av lag och mer detaljerade föreskrifter ges i förordning. En sådan utformning innebär t.ex. att det i förordning eller i föreskrifter kommer att kunna preciseras i vilken närmare omfattning lokaliseringsuppgifter som inte är trafikuppgifter ska lagras.

Som utredningen för fram finns det i 9 kap. 23 § lagen om elektronisk kommunikation en upplysning om att regeringen eller den myndighet som regeringen bestämmer får meddela närmare föreskrifter om vilka uppgifter som får lagras enligt 9 kap. 19 § och om lagringstiden enligt 9 kap. 22 §. Regeringen har tidigare gjort bedömningen att upplysningsbestämmelsen i 9 kap. 23 § kan bidra till att regleringen blir transparent och tydlig (se prop. 2021/22:136 s. 326). Det saknas skäl att nu göra en annan bedömning. Det bör därför upplysas om att regeringen eller den myndighet som regeringen bestämmer får meddela närmare föreskrifter om vilka uppgifter som ska lagras enligt 9 kap. 19 a § lagen om elektronisk kommunikation.

6.6 Tillgången till lagrade uppgifter

Utredningens förslag: Uppgifter som har lagrats med stöd av ett beslut om nationell säkerhetslagring ska endast få hämtas in efter ett tillstånd till hemlig

avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation eller inhämtning enligt inhämtningslagen.

Uppgifter ska endast få hämtas in om det i tillståndet har angetts att inhämtningen får avse uppgifter som har lagrats med stöd av lagen om nationell säkerhetslagring.

Uppgifter ska få hämtas in endast i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar vissa brott eller för att utreda och beivra sådana brott. De brott som ska ge rätt till inhämtning är

- sabotage eller grovt sabotage,
- mordbrand, grov mordbrand, allmänfarlig ödeläggelse, kapning, sjö- eller luftfartssabotage eller flygplatssabotage, om brottet innefattar brottet sabotage,
- uppror, väpnat hot mot laglig ordning eller brott mot medborgerlig frihet,
- högförräderi, krigsanstiftan, spionerі, grovt spionerі, utlandsspionerі, grovt utlandsspionerі, obehörig befattning med hemlig uppgift, grov obehörig befattning med hemlig uppgift eller olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person,
- företagsspionerі, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning,
- terroristbrott, deltagande i en terroristorganisation, samröre med terroristorganisation, finansiering av terrorism eller särskilt allvarlig brottslighet, offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet, rekrytering till terrorism eller särskilt allvarlig brottslighet, utbildning för terrorism eller särskilt allvarlig brottslighet eller resa för terrorism eller särskilt allvarlig brottslighet,
- andra brott som på grund av sin omfattning eller karaktär utgör ett allvarligt hot mot Sveriges säkerhet, om det för brottet inte är föreskrivet lindrigare straff än fängelse i två år, eller
- försök, förberedelse eller stämpling till de brott som anges ovan, om en sådan gärning är belagd med straff.

Den som är skyldig att lagra uppgifter enligt ett beslut om nationell säkerhetslagring ska omfattas av rätten till ersättning för kostnader som uppstår när uppgifter om abonnemang, trafikuppgifter och lokaliseringsuppgifter som inte är trafikuppgifter lämnas ut till de brottsbekämpande myndigheterna.

Utredningens förslag överensstämmer i huvudsak med utkastets. Utredningen lämnar inget förslag om att brotten utlandsspionerі, grovt utlandsspionerі och deltagande i en terroristorganisation ska ge rätt till inhämtning.

Remissinstanserna: Många remissinstanser instämmer i eller har inget att invända mot förslaget. *Polismyndigheten* anser att det är positivt att det införs en ventil för brott som på grund av sin omfattning eller karaktär utgör ett allvarligt hot mot Sveriges säkerhet. *Telenor Sverige AB* för fram att det framstår som befogat att inskränka åtkomsten till lagrade uppgifter till åtgärder som syftar till att förebygga, förhindra eller upptäcka hot mot Sveriges säkerhet. *Försvarsunderrättelsedomstolen* menar att det kan innebära en konflikt i förhållande till EU-rätten att inhämtningen inte bedöms i förhållande till det hot som ligger till grund

för lagringsskyldigheten. *Säkerhets- och integritetsskyddsnämnden* påtalar att det kan övervägas om det även av rättegångsbalken, preventivlagen och inhämtningslagen ska framgå att det i tillståndet ska anges att inhämtningen får avse uppgifter som lagrats enligt beslutet.

Skälen för utkastets förslag

Uppgifter som har lagrats med stöd av ett beslut om nationell säkerhetslagring bör bara få inhämtas efter tillstånd till vissa tvångsmedel

Ett beslut om nationell säkerhetslagring kan innebära att tillhandahållare som är skyldiga att lagra uppgifter om elektronisk kommunikation blir skyldiga att lagra abonnemangsuppgifter, trafikuppgifter och lokaliseringsuppgifter som inte är trafikuppgifter och som rör användare som är fysiska personer eller abonnenter (2 § i den nya lagen och föreslagna 9 kap. 19 b § lagen om elektronisk kommunikation). För att de brottsbekämpande myndigheterna ska få tillgång till uppgifterna som har lagrats i syfte att skydda nationell säkerhet behöver uppgifterna kunna inhämtas.

Nationell säkerhetslagring får beslutas endast om det finns ett allvarligt hot mot Sveriges säkerhet och om det är absolut nödvändigt i förhållande till syftet med lagringen. En sådan lagring kan tidsmässigt och innehållsmässigt omfatta fler uppgifter än annan lagring.

Utredningen föreslår att uppgifter som har lagrats enligt ett beslut om nationell säkerhetslagring endast ska få inhämtas efter tillstånd till hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation enligt 27 kap. 18 eller 19 § rättegångsbalken eller inhämtning enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen). Rent praktiskt är det dessa tvångsmedel som kommer att kunna användas för att inhämta de lagrade uppgifterna. Reglerna om dessa tvångsmedel innehåller ett flertal skyddsmekanismer som syftar till att säkra att tillämpningen är rättssäker och inte innebär obefogade intrång i enskildas integritet (jfr prop. 2022/23:126 s. 170 f). Uppgifter som har lagrats enligt ett beslut om nationell säkerhetslagring bör därför endast få inhämtas efter tillstånd till dessa särskilt angivna hemliga tvångsmedel.

Utredningen föreslår vidare att inhämtning av uppgifter som har lagrats enligt ett beslut om nationell säkerhetslagring endast ska få ske om det i tillståndet har angetts att inhämtningen får avse uppgifter som har lagrats enligt beslutet. Det är av rättssäkerhetsskäl viktigt att de aktuella uppgifterna får inhämtas endast för att bekämpa vissa särskilda brott som utgör hot mot nationell säkerhet. Det underlättar också för tillhandahållarna när de ska lämna ut uppgifterna att veta att tillståndet omfattar dessa uppgifter. Det finns därför skäl att ställa sig bakom utredningens förslag. *Säkerhets- och integritetsskyddsnämnden* lyfter frågan om detta även bör framgå av bestämmelserna som reglerar vad ett tillstånd ska innehålla i rättegångsbalken, preventivlagen och inhämtningslagen. Den aktuella skyldigheten rör specifikt frågor om nationell säkerhetslagring. Det bedöms därför vara tillräckligt att regleringen om vad som ska ingå i tillståndet införs i den nya lagen.

Uppgifter som lagrats med stöd av ett beslut om nationell säkerhetslagring bör bara få inhämtas för viss brottslighet

EU-domstolen har klargjort att uppgifter som har lagrats för att skydda den nationella säkerheten inte får lämnas ut för annan brottsbekämpande verksamhet än sådan som sker i syfte att skydda den nationella säkerheten (se t.ex. p. 100 i SpaceNet-domen). Utredningen föreslår därför – för att skilja åtkomsten till uppgifter som har lagrats för att skydda den nationella säkerheten från åtkomsten till andra uppgifter – att det ska införas en katalog över de brott som medger utlämnande av uppgifter som lagrats enligt ett beslut om nationell säkerhetslagring.

I Sverige är det i huvudsak Säkerhetspolisen som har ansvar för att bekämpa hot mot den nationella säkerheten, även om Polismyndigheten i vissa situationer bistår Säkerhetspolisen. I Säkerhetspolisens instruktion definieras vilka brott eller vilka typer av brottslighet som myndigheten ansvarar för att förebygga, förhindra och upptäcka samt utreda och beivra, se 3 § förordningen (2022:1719) med instruktion för Säkerhetspolisen.

I enlighet med utredningens bedömning, och till skillnad från vad *Försvarsunderrättelsedomstolen* för fram, är det lämpligt att utgå från brotten eller brottslighetens karaktär för att ringa in sådan brottslighet som har påverkan på den nationella säkerheten. Det kan konstateras att samtliga brott och brottslig verksamhet som Säkerhetspolisen har att bekämpa får anses ha en koppling till nationell säkerhet. Detta gäller även den brottslighet som utredningen i övrigt föreslår ska kunna ge rätt till inhämtning, dvs. andra brott som på grund av sin omfattning eller karaktär utgör ett allvarligt hot mot Sveriges säkerhet, om det för brottet inte är föreskrivet lindrigare straff än fängelse i två år. Den brottslighet som utredningen föreslår bör ge rätt till inhämtning av uppgifter vid ett beslut om nationell säkerhetslagring.

I den nya lagen bör det därför regleras att inhämtning av uppgifter som lagrats enligt ett beslut om nationell säkerhetslagring endast får ske för de brott som närmare anges i brottskatalogen, i enlighet med utredningens förslag. Sedan den 1 juni 2023 omfattar även brottet deltagande i terroristorganisation av terroristbrottslagens tillämpningsområde. Även det brottet är säkerhetshotande för Sverige och bör ge rätt till inhämtning enligt den nya lagen. Detsamma bör gälla brotten utlandsspionerі och grovt utlandsspionerі enligt 19 kap. 6 a och 6 b §§ brottsbalken.

Den som lämnar ut uppgifter bör ha rätt till ersättning

Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § lagen om elektronisk kommunikation har rätt till ersättning för kostnader som uppstår när uppgifter om abonnemang, innehållet i ett elektroniskt meddelande eller andra uppgifter som angår ett särskilt elektroniskt meddelande lämnas ut till brottsbekämpande myndigheter (9 kap. 29 a §). Ersättningsrätten omfattar samma tillhandahållare som är lagringsskyldiga enligt nuvarande regler (9 kap. 19 §).

I avsnitt 7.5 föreslås att tillhandahållare av nummeroberoende interpersonella kommunikationstjänster ska omfattas av rätten till ersättning. Som utredningen föreslår bör även den som är skyldig att lagra uppgifter enligt ett beslut om nationell säkerhetslagring ha rätt till ersättning för kostnader som uppstår när

uppgifter som lagrats enligt ett beslut om nationell säkerhetslagring lämnas ut. Den som är skyldig att lagra uppgifter enligt ett beslut om nationell säkerhetslagring bör därför omfattas av rätten till ersättning för kostnader som uppstår när uppgifter om abonnemang, trafikuppgifter och lokaliseringsuppgifter som inte är trafikuppgifter lämnas ut till brottsbekämpande myndigheter.

6.7 Personuppgiftsbehandling vid lagring för nationell säkerhet

Utkastets förslag: Det som föreskrivs om utplåning och avidentifiering av trafikuppgifter ska inte gälla vid behandling av uppgifter som sker enligt ett beslut om nationell säkerhetslagring.

Vad som föreskrivs om avidentifiering och samtycke till behandling av lokaliseringsuppgifter som inte är trafikuppgifter ska inte gälla vid behandling av uppgifter som sker enligt ett beslut om nationell säkerhetslagring.

Uppgifter som har lagrats enligt ett beslut om nationell säkerhetslagring ska få behandlas enbart för att lämnas ut enligt lagen om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt om förslaget.

Skälen för utkastets förslag: Utgångspunkten är att fysiska personers och abonnenters trafikuppgifter ska utplånas eller avidentifieras när de inte längre behövs för överföring av ett elektroniskt meddelande (9 kap. 1 § första stycket lagen om elektronisk kommunikation). Från huvudregeln finns vissa undantag. Exempelvis får trafikuppgifter behandlas för brottsbekämpande ändamål enligt 9 kap. 19 § lagen om elektronisk kommunikation (9 kap. 1 § andra stycket).

I avsnitt 6.5 föreslås att tillhandahållarnas lagringsskyldighet enligt ett beslut om nationell säkerhetslagring ska regleras i en ny paragraf i lagen om elektronisk kommunikation, 9 kap. 19 b §. För att även trafikuppgifter som lagras vid nationell säkerhetslagring ska få behandlas behöver 9 kap. 1 § andra stycket samma lag kompletteras med en hänvisning till 9 kap. 19 b §.

Ett beslut om nationell säkerhetslagring kommer även kunna omfatta lokaliseringsuppgifter som inte är trafikuppgifter. Sådana uppgifter som rör användare som är fysiska personer eller abonnenter får behandlas endast sedan de har avidentifierats eller om samtycke har getts till behandlingen och enligt vissa ytterligare angivna förutsättningar (9 kap. 7–9 §§ lagen om elektronisk kommunikation). Undantag från detta finns för lokaliseringsuppgifter som omfattas av ett beslut om inhämtning av uppgifter enligt 27 kap. rättegångsbalken eller lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (9 kap. 10 § lagen om elektronisk kommunikation). I enlighet med vad som anges i betänkandet behövs ett undantag även för de lokaliseringsuppgifter som kan omfattas av den nationella säkerhetslagringen. I 9 kap. 10 § lagen om elektronisk kommunikation bör därför även föreskrivas att lokaliseringsuppgifter som ska lagras enligt ett beslut om nationell säkerhetslagring får behandlas trots vad som föreskrivs i 9 kap. 7–9 §§.

För att tillhandahållarna ska kunna lämna ut uppgifter som lagrats i syfte att skydda den nationella säkerheten behövs författningsstöd för behandling av sådana uppgifter. Det behöver också vara tydligt att uppgifterna inte får behandlas för andra ändamål. I 9 kap. 21 § lagen om elektronisk kommunikation bör därför även föreskrivas att uppgifter som lagrats enligt ett beslut om nationell säkerhetslagring får behandlas enbart för att lämnas ut enligt den nya lagen om nationell säkerhetslagring.

6.8 Sekretess och tystnadsplikt

Utkastets förslag: Sekretess ska gälla för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i en angelägenhet enligt lagen om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst får inte obehörigen föra vidare eller utnyttja det som han eller hon i samband med tillhandahållandet har fått del av eller tillgång till i form av en uppgift som hänför sig till nationell säkerhetslagring enligt den nya lagen.

Tystnadsplikten ska även gälla det som han eller hon i samband med tillhandahållandet har fått del av eller tillgång till i form av en lokaliseringsuppgift som inte är en trafikuppgift och som rör användare som är fysiska personer eller abonnenter. Tystnadsplikten ska inte gälla i förhållande till innehavaren av abonnemanget.

Ett offentligt ombud för nationell säkerhetslagring får inte obehörigen röja vad han eller hon har fått kännedom om i ett ärende om nationell säkerhetslagring. Sekretess ska inte hindra att uppgift i ett ärende om nationell säkerhetslagring lämnas till ett ombud enligt den nya lagen.

Tystnadsplikten ska ges företräde framför rätten att meddela och offentliggöra uppgifter när det är fråga om uppgift om nationell säkerhetslagring enligt den nya lagen. Detta ska även omfatta uppgifter om enskildas personliga och ekonomiska förhållanden.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: Många remissinstanser instämmer i eller har inget att invända mot förslaget. *Sveriges advokatsamfund* för på ett övergripande plan fram att den föreslagna sekretessen i och för sig är nödvändig och adekvat när det gäller underrättelseverksamhet av aktuellt slag. Samfundet påtalar dock att det finns beaktansvärda risker med att ett beslut fattas utan att den som är föremål för beslutet eller allmänheten har någon möjlighet att bedöma vilka omständigheter som ligger till grund för bedömningen. Även *Svenska Journalistförbundet* och *TU* för fram att möjligheten till insyn i hur lagringen kommer att gå till är bristfällig. Bland annat förs fram att ombudet, om än med sekretessbegränsningar, måste ha förutsättningar att verka som offentligt i meningen att representera och tydliggöra

för medborgarna. Sekretessbestämmelsens utformning, med ett omvänt skaderekvisit, innebär att uppgifter sällan eller aldrig kommer att lämnas ut. Uppgifter om enskilda bör därför i stället skyddas med ett rakt skaderekvisit, medan besluten inte bör omfattas av sekretess. Vidare påtalas att meddelarfriheten fyller en viktig funktion, särskilt eftersom risken för intrång i den personliga integriteten är stor. Svenska Journalistförbundet avstyrker förslaget att inskränka meddelarfriheten och TU för fram att den inte bör begränsas på det sätt som föreslås. *HI3G Access AB* önskar ett förtydligande av hur den föreslagna regleringen förhåller sig till den enskildes rättigheter enligt dataskyddsförordningen, bl.a. rätten till registerutdrag. Bolaget önskar därtill klargörande av om tystnadsplikten även omfattar de uppgifter som lagras och om den gäller mot den registrerade.

Skälen för utkastets förslag

Sekretess bör gälla för uppgift om en enskilds personliga och ekonomiska förhållanden i en angelägenhet om nationell säkerhetslagring

När det gäller lagring av uppgifter i syfte att skydda nationell säkerhet kommer flera aktörer att vara involverade. Säkerhetspolisen ska bedöma om det finns ett allvarligt hot mot den nationella säkerheten och får, om förutsättningar för nationell säkerhetslagring är uppfyllda, besluta att tillhandahållare ska lagra uppgifter om abonnemang samt trafik- och lokaliseringsuppgifter. Under beredningen kan Säkerhetspolisen se behov av att samråda med t.ex. Försvarsmakten. Ett lagringsbeslut kommer att kunna överprövas av Försvarsunderrättelsedomstolen. Vid verkställighet av beslut om lagring involveras tillhandahållare och vid tillsyn även Post- och telestyrelsen. Om Post- och telestyrelsens beslut överklagas involveras dessutom de allmänna förvaltningsdomstolarna.

Åtgärder vid beredning och beslut i ett ärende om nationell säkerhetslagring kommer att ske inom ramen för Säkerhetspolisens underrättelseverksamhet. I 18 kap. 1–3 och 17–17 a §§ samt 35 kap. 1 § offentlighets- och sekretesslagen (2009:400) finns bestämmelser om sekretess i den verksamheten. Därtill kan ärenden om nationell säkerhetslagring även aktualisera hantering av uppgifter som regleras av annan sekretess. Det kan t.ex. handla om uppgifter som omfattas av utrikes- och försvarssekretess, sekretess för uppgifter i annat internationellt samarbete samt sekretess för uppgifter om säkerhets- eller bevakningsåtgärd enligt 15 kap. 1, 1 a och 2 §§ och 18 kap. 8 § samma lag. Bestämmelserna är tillämpliga i all offentlig verksamhet, dvs. de utgör primära sekretessregler för den myndighet som får tillgång till uppgifterna. Utredningen har gjort bedömningen att dessa sekretessregler ger ett tillräckligt sekretesskydd för allmänna intressen i ärenden om nationell säkerhetslagring. Det finns inte skäl att göra någon annan bedömning

Som utredningen konstaterar behöver det finnas ett fullgott sekretesskydd även för uppgifter om enskilda som förekommer i ett ärende om nationell säkerhetslagring. Det kan röra sig om personer som både direkt och indirekt har koppling till det nationella säkerhetshotet. Det kan även omfatta tillhandahållarnas förhållanden. I 21 kap. finns vissa minimiskyddsregler till skydd för enskildas personliga integritet. Den sekretess som följer av kapitlet kan dock inte anses vara tillräcklig för att skydda de uppgifter som kan förekomma i ett ärende om nationell säkerhetslagring. I motsats till vad som föreskrivs i 18 kap. 1 och 2 §§ gäller inte sek-

retess enligt 35 kap. 1 § första stycket 4 utanför de brottsbekämpande myndigheternas verksamhet. Det innebär att uppgifter som rör enskildas personliga och ekonomiska förhållanden enligt hittillsvarande reglering inte skulle få ett tillräckligt sekretesskydd hos vissa av de aktörer som kan involveras i ett ärende om nationell säkerhetslagring. Uppgifterna skulle exempelvis ha ett adekvat sekretesskydd när de överförs mellan Polismyndigheten och Säkerhetspolisen men inte när en uppgift överförs från Säkerhetspolisen till Försvarsmakten eller Försvarsunderrättelsedomstolen eftersom dessa inte omfattas av 35 kap. 1 § första stycket 4. Bestämmelsen i 38 kap. 4 § gäller bara hos Försvarsmakten i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten samt hos Försvarets radioanstalt i underrättelse- och säkerhetsverksamheten.

Utgångspunkten bör inte, som *TU* och *Svenska Journalistförbundet* för fram, vara att uppgifterna ska vara offentliga och att sekretessen bara ska gälla om det kan antas att en viss skada uppkommer om uppgiften röjs. Om det blir allmänt känt att Sverige står inför ett nationellt säkerhetshot kan detta begränsa handlingsutrymmet för Säkerhetspolisen och andra brottsbekämpande myndigheter. Exempelvis skulle det, som utredningen för fram, kunna röja Säkerhetspolisens metoder om ett beslut om nationell säkerhetslagring meddelas i anslutning till åtgärder som Säkerhetspolisen har vidtagit. Det kan också finnas en risk för att syftet med den tänkta åtgärden inte kan uppnås om uppgiften röjs. Omständigheten att Säkerhetspolisen har bedömt att Sverige står inför ett nationellt säkerhetshot och angelägenheter hänförliga till detta har alltså ett starkt allmänt skyddsintresse. Ett sådant skydd får, som utgångspunkt, anses väga tyngre än intresset av insyn. Det kan därtill även finnas ett starkt enskilt skyddsintresse när det gäller de uppgifter om enskildas förhållanden som kan finnas i ett ärende.

Genom att beslutet överprövas och att tillgången till uppgifterna i senare led förutsätter tillstånd till användning av hemliga tvångsmedel, bedöms enskilda tillförsäkras tillräckliga rättssäkerhetsgarantier. Som utredningen påtalar är sekretessen inte heller absolut. Om det efter skadeprövning kan konstateras att ett utlämnande av en uppgift, exempelvis uppgiften om att Sverige står inför ett nationellt säkerhetshot, inte innebär några risker för de allmänna eller enskilda intressen som sekretessregleringen avser att skydda, kan uppgiften lämnas ut. Det behöver alltså, även med ett omvänt skaderekvisit, göras en bedömning i varje enskilt fall.

I enlighet med utredningens förslag bör därför en ny punkt införas i 35 kap. 1 § offentlighets- och sekretesslagen, enligt vilken sekretess ska gälla för uppgift om enskildas personliga och ekonomiska förhållanden i angelägenhet om nationell säkerhetslagring, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men. En sådan bestämmelse motsvarar det skydd som enskilda åtnjuter i bl.a. Säkerhetspolisens brottsbekämpande verksamhet vad gäller hemliga tvångsmedel enligt 35 kap. 1 § första stycket 2 (jfr prop. 2023/24 s. 108). Behovet av sekretess är detsamma oavsett hos vilken myndighet uppgiften förekommer. Sekretesstiden bör vara densamma som för övriga punkter i paragrafen.

När det gäller tillämpningen av sekretessbestämmelsen kan, på ett övergripande plan och med hänsyn till det önskemål om förtydligande som *Hi3G Access AB* efterfrågar, konstateras att den enskilde inte kommer ha rätt att ta del av uppgifter i t.ex. ett registerutdrag om hinder för utlämnande finns i offentlighets- och sekre-

tesslagen. Detta behandlas exempelvis i artikel 23 i Europaparlamentets och rådets förordning (EU) 2016/679 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) och artikel 15 i Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

Även beslut om nationell säkerhetslagring bör omfattas av sekretess

Som konstaterats ovan kan uppgiften att Säkerhetspolisen bedömt att Sverige står inför ett nationellt säkerhetshot, om den blir allmänt känd, begränsa handlingsutrymmet för Säkerhetspolisen. *TU* menar att beslutet om nationell säkerhetslagring är ingripande och inte bör omfattas av sekretess.

Genom att beslutet överprövas och att tillgången till uppgifterna i senare led förutsätter tillstånd till användning av hemliga tvångsmedel bedöms enskilda tillförsäkras fullgoda rättssäkerhetsgarantier. Sekretessen kommer inte heller att vara absolut. Om det efter skadeprövning kan konstateras att ett utlämnande av en uppgift, exempelvis uppgiften om att Sverige står inför ett allvarligt hot mot nationell säkerhet, inte innebär några risker för de allmänna eller enskilda intressen som sekretessregleringen avser att skydda så kan uppgiften lämnas ut. Det bör dock ankomma på Säkerhetspolisen att i det enskilda fallet göra en sådan prövning.

Detta innebär alltså att det inte bör föreskrivas något undantag för sekretessen beträffande beslut om nationell säkerhetslagring. Det finns samma behov av att skydda uppgifterna hos Försvarsunderrättelsedomstolen som hos Säkerhetspolisen. Det innebär även att sekretessen också bör omfatta beslut av Försvarsunderrättelsedomstolen i samband med överprövning av Säkerhetspolisens beslut.

Tystnadsplikt för tillhandahållare i ett ärende om nationell säkerhetslagring

Säkerhetspolisen kan både under handläggningen och vid verkställighet av beslut om nationell säkerhetslagring behöva komma i kontakt med tillhandahållarna. Vid en sådan kontakt är det viktigt att skyddet för de uppgifter som lämnas kan bibehållas.

Tillhandahållarna träffas inte av regleringen i offentlighets- och sekretesslagen. Tillhandahållarnas tystnadsplikt regleras i stället i 9 kap. 31 och 32 §§ lagen om elektronisk kommunikation. I 9 kap. 32 § finns en straffsanktionerad tystnadsplikt för uppgifter som hänför sig till vissa angelägenheter, bl.a. avseende användning av hemliga tvångsmedel. Utredningen föreslår att tystnadsplikten även ska gälla för en uppgift som hänför sig till nationell säkerhetslagring enligt den nya lagen. Enligt utredningens förslag ska tystnadsplikten omfatta ärendet i dess helhet. Sådana uppgifter innefattar exempelvis, vilket *Hi3G Access AB* önskar förtydligande om, information om att Säkerhetspolisen har varit i kontakt med tillhandahållaren, vad som har kommunicerats, beslut om lagring och att lagring har påbörjats eller avslutats.

Författningsreglerad tystnadsplikt utgör en inskränkning av yttrandefriheten. Yttrandefriheten får endast begränsas genom lag. En sådan begränsning får göras endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningen får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar. För yttrandefriheten gäller vidare att den får begränsas med hänsyn till bl.a. rikets säkerhet, allmän ordning och säkerhet, förebyggandet och beivrandet av brott eller om särskilt viktiga skäl föranleder det. Vid bedömandet av vilka begränsningar som får göras ska särskilt beaktas vikten av vidaste möjliga yttrandefrihet och informationsfrihet i politiska, religiösa, fackliga, vetenskapliga och kulturella angelägenheter (2 kap. 20 § första stycket, 21 § och 23 § första och andra styckena regeringsformen). Yttrandefriheten skyddas även av artikel 10 i Europakonventionen. Enligt artikel 10.2 i Europakonventionen får yttrandefriheten bl.a. underkastas inskränkningar som är föreskrivna i lag och som i ett demokratiskt samhälle är nödvändiga med hänsyn till bl.a. statens säkerhet, till den territoriella integriteten eller den allmänna säkerheten, till förebyggande av oordning eller brott.

Det är av stor betydelse att uppgifter som rör angelägenheter om nationell säkerhetslagring får ett ändamålsenligt skydd. I realiteten kan det inte anses innebära någon påtaglig inskränkning i yttrandefriheten att som tillhandahållare inte få yttra sig fritt i angelägenheter om nationell säkerhetslagring. Behovet av tystnadsplikt för tillhandahållare i angelägenheter som rör nationell säkerhetslagring väger därför tyngre än intresset av yttrandefrihet. Den föreslagna tystnadsplikten får anses vara proportionerlig och uppfylla de krav som gäller för begränsningar i yttrandefriheten enligt regeringsformen och Europakonventionen. Den av utredningen föreslagna bestämmelsen bör därför införas i 9 kap. 32 § lagen om elektronisk kommunikation. Detta innebär att den tystnadsplikt som följer av 9 kap. 31 § första stycket samma lag även kommer att gälla för en uppgift som hänför sig till nationell säkerhetslagring enligt den nya lagen.

Som utredningen konstaterar kommer även lagringsskyldigheten enligt ett beslut om nationell säkerhetslagring kunna omfatta lokaliseringsuppgifter som inte är trafikuppgifter. Även dessa uppgifter kan vara känsliga för enskilda och bör omfattas av tystnadsplikten. Det finns därför skäl att dela utredningens bedömning att lokaliseringsuppgifter som inte är trafikuppgifter bör omfattas av tystnadsplikten. I likhet med nu gällande regler bör tystnadsplikten för sådana lokaliseringsuppgifter avgränsas till uppgifter som rör användare som är fysiska personer eller abonnenter (jfr 9 kap. 1 och 7 §§ lagen om elektronisk kommunikation). En sådan tystnadsplikt bör därför införas i 9 kap. 31 § första stycket. På samma sätt som för uppgift om abonnemang och annan uppgift som angår ett särskilt elektroniskt meddelande (trafikuppgift enligt förslaget i avsnitt 5.3) bör tystnadsplikten för lokaliseringsuppgifter som inte är trafikuppgifter inte gälla i förhållande till innehavaren av abonnemanget. Detta bör särskilt föreskrivas i 9 kap. 31 § tredje stycket. Eftersom lokaliseringsuppgifter som inte är trafikuppgifter inte är kopplade till ett elektroniskt meddelande bör preciseringen att abonnemanget ska ha använts för ett elektroniskt meddelande tas bort.

Tystnadsplikt och sekretessbrytande bestämmelse för ett offentligt ombud för nationell säkerhetslagring

Det offentliga ombudet för nationell säkerhetslagrings uppdrag innebär att han eller hon kan få del av många uppgifter som omfattas av sekretess. *TU* för fram att ombudet, trots detta, måste ha förutsättningar att verka som ett offentligt sådant. Med hänsyn till graden av känslighet hos de uppgifter som kan förväntas förekomma i ett ärende om nationell säkerhetslagring är det av stor vikt att ombudet inte lämnar ut uppgifter som han eller hon har fått del av genom sitt uppdrag.

Ombudet företräder enskildas intressen och är inte knuten till det allmännas verksamhet. Han eller hon omfattas därför inte av offentlighets- och sekretesslagens bestämmelser om tystnadsplikt enligt 2 kap. 1 § offentlighets- och sekretesslagen. För att även det offentliga ombudet för nationell säkerhetslagring ska vara skyldig att inte obehörigen röja vad han eller hon erfar under sitt uppdrag behövs en särskild regel om tystnadsplikt, i likhet med vad som gäller för offentliga ombud enligt rättegångsbalken (jfr 27 kap. 30 § rättegångsbalken). Det bör därför införas en bestämmelse i den nya lagen som anger att den som förordnats som offentligt ombud för nationell säkerhetslagring inte obehörigen får röja vad han eller hon har fått kännedom om i ett ärende om nationell säkerhetslagring. En sådan tystnadsplikt får, likt tystnadsplikten för tillhandahållare i ett ärende om nationell säkerhetslagring, anses vara proportionerlig och även i övrigt uppfylla de krav som gäller för begränsningar i yttrandefriheten enligt regeringsformen och Europakonventionen.

Enligt 8 kap. 1 § offentlighets- och sekretesslagen får en sekretessbelagd uppgift inte röjas för en enskild eller för andra myndigheter i annat fall än när det särskilt anges i offentlighets- och sekretesslagen, eller i annan lag eller förordning till vilken den lagen hänvisar. I likhet med vad som gäller för ett offentligt ombud eller integritetsskyddsombud enligt 10 kap. 10 § andra stycket offentlighets- och sekretesslagen kommer ett offentligt ombud för nationell säkerhetslagring inte anses vara part. Ombudet är inte heller knuten till det allmännas verksamhet. Utan en sekretessbrytande bestämmelse saknas det därför lagliga möjligheter att lämna ut uppgifter som omfattas av sekretess till ombudet. I 10 kap. 10 § offentlighets- och sekretesslagen bör därför införas en bestämmelse som anger att sekretessen inte hindrar att uppgift i ett ärende om nationell säkerhetslagring lämnas till ett offentligt ombud för nationell säkerhetslagring.

Tystnadsplikten bör ges företräde framför rätten att meddela och offentliggöra uppgifter vid berörda myndigheter i ärenden om nationell säkerhetslagring

Med rätten att meddela och offentliggöra uppgifter avses de rättigheter som följer av 1 kap. 1 § tryckfrihetsförordningen och 1 kap. 1 § yttrandefrihetsgrundlagen. Enligt 1 kap. 7 § tryckfrihetsförordningen och 1 kap. 10 § yttrandefrihetsgrundlagen står det envar fritt att meddela uppgifter i vilket ämne som helst till de personkategorier och organ som anges i sistnämnda bestämmelser för publicering i de medier som de båda grundlagarna omfattar. Rätten att meddela och offentliggöra uppgifter är ett vidare begrepp än meddelarfrihet och innefattar, förutom rätten att lämna uppgifter till någon annan för publicering eller på något annat sätt

medverka till någon annans publicering, också rätten att själv, som ansvarig enligt grundlagarnas bestämmelser om ensamansvar, offentliggöra uppgifter.

Av 3 kap. 1 § offentlighets- och sekretesslagen följer att sekretess innebär ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt. Sekretess innebär alltså både en handlingssekretess och en tystnadsplikt. Den rätt att meddela och offentliggöra uppgifter som följer av tryckfrihetsförordningen och yttrandefrihetsgrundlagen har som huvudregel företräde framför tystnadsplikten. I ett antal fall har dock bestämmelser om tystnadsplikt företräde, vilket innebär att rätten att meddela och offentliggöra uppgifter är helt inskränkt (se 35 kap. 24 § offentlighets- och sekretesslagen).

Nationell säkerhetslagring syftar till att förbättra förutsättningarna för Säkerhetspolisen och andra brottsbekämpande myndigheter att bekämpa brottslighet som kan utgöra ett hot mot den nationella säkerheten. Uppgifter som rör Säkerhetspolisens handläggning av ärenden om nationell säkerhet kommer att höra till de känsligare delarna av underrättelseverksamheten, bl.a. med hänsyn till att uppgifterna rör hot mot Sveriges säkerhet. Ett röjande av sådana uppgifter skulle kunna leda till allvarlig skada för Sveriges säkerhet. Som *Svenska Journalistförbundet* för fram fyller rätten att meddela och offentliggöra uppgifter en viktig funktion, som kan förhindra intrång i den personliga integriteten. *TU* anser att den rätten inte bör begränsas på det sätt som utredningen föreslår. Som utredningen för fram får dock sekretessintresset i dessa fall anses vara starkare än det allmänna intresset av insyn i den verksamhet som bedrivs av de berörda myndigheterna. Detta gäller även insynen i enskildas personliga och ekonomiska förhållanden i angelägenheter om nationell säkerhetslagring.

Av 18 kap. 19 § andra stycket följer att den tystnadsplikt som gäller enligt 1–3 §§ inskränker rätten att meddela och offentliggöra uppgifter i vissa fall. Eftersom den tystnadsplikt som följer av 18 kap. 1–3 §§ alltså bör ha företräde framför rätten att meddela och offentliggöra uppgifter i ärenden om nationell säkerhetslagring bör 18 kap. 19 § andra stycket kompletteras så att tystnadsplikten även ska inskränka rätten att meddela och offentliggöra uppgifter när det är fråga om uppgift om nationell säkerhetslagring enligt den nya lagen. För att detta ska gälla uppgifter om enskildas personliga och ekonomiska förhållande behöver ett särskilt tillägg om detta göras. I 35 kap. 24 § offentlighets- och sekretesslagen bör därför föreskrivas att den tystnadsplikt som gäller för en angelägenhet som avser nationell säkerhetslagring inskränker rätten att meddela och offentliggöra uppgifter i angelägenheter som avser nationell säkerhetslagring enligt den nya lagen.

Tystnadsplikten bör även ges företräde framför rätten att meddela och offentliggöra uppgifter för tillhandahållarna och ombudet

Motsvarande inskränkning i rätten att meddela och offentliggöra uppgifter som föreslås för medarbetare vid berörda myndigheter bör gälla för tillhandahållarna och det offentliga ombudet för nationell säkerhetslagring. För att detta ska gälla även för dem behövs ytterligare reglering. I 44 kap. offentlighets- och sekretesslagen finns bestämmelser som reglerar situationer där tystnadsplikt som följer av andra författningar än offentlighets- och sekretesslagen ska ha företräde framför rätten att meddela och offentliggöra uppgifter. Enligt 44 kap. 4 § 3

inskränks den rätten för tillhandahållare i fråga om straffprocessuella tvångsmedel. En motsvarande inskränkning bör i samma paragraf införas för angelägenheter om nationell säkerhetslagring. I paragrafen bör därför föreskrivas att rätten att meddela och offentliggöra uppgifter ska inskränkas av den tystnadsplikt som följer av nationell säkerhetslagring enligt den nya lagen.

Rätten att meddela och offentliggöra uppgifter för ett offentligt ombud för nationell säkerhetslagring behöver också regleras. När det gäller ett offentligt ombud enligt rättegångsbalken finns möjligheten för rätten att förordna att en uppgift som lagts fram inom stängda dörrar inte får uppenbaras enligt 5 kap. 4 § rättegångsbalken. Bestämmelsen ger domstol möjlighet att ålägga de närvarande personerna tystnadsplikt. Den som omfattas av ett sådant förordnande har inte rätt att meddela och offentliggöra uppgifter i fråga om de uppgifter som förordnandet avser, se 44 kap. 2 § offentlighets- och sekretesslagen. Eftersom ett offentligt ombud för nationell säkerhetslagring inte omfattas av rättegångsbalkens regler behöver en särskild bestämmelse införas om detta. I 44 kap. 5 § offentlighets- och sekretesslagen bör därför föreskrivas att rätten att meddela och offentliggöra uppgifter ska inskränkas av den tystnadsplikt som följer av den nya lagen om nationell säkerhetslagring.

7 Nya regler för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster

7.1 Tillhandahållarna bör omfattas av lagrings- och anpassningsskyldighet och vissa andra regler

Utkastets bedömning: Tillhandahållare av nummeroberoende interpersonella kommunikationstjänster bör omfattas av lagrings- och anpassningsskyldighet och vissa andra regler som har anknytning till dessa skyldigheter.

Utredningens bedömning överensstämmer med utkastets.

Remissinstanserna: En majoritet av remissinstanserna, bl.a. *Svea hovrätt*, *Brottsoffermyndigheten*, *ECPAT Sverige*, *Ekobrottsmyndigheten*, *Åklagarmyndigheten*, *Skatteverket*, *Stockholms universitet (Juridiska fakulteten)*, *Polismyndigheten*, *Post- och telestyrelsen*, *Säkerhetspolisen*, *Tullverket* och *Hi3G Access AB* instämmer i eller har inget att invända mot förslaget. *ECPAT Sverige* pekar särskilt på vikten av att tillhandahållare av nummeroberoende interpersonella kommunikationstjänster omfattas av lagringsskyldighet och för fram att organisationen ser att barn i stor utsträckning utsätts för brott på sådana tjänster. *Åklagarmyndigheten* betonar att det är positivt att lagringsskyldigheten blir teknikneutral. *Säkerhets- och integritetsskyddsnämnden* delar utredningens bedömning att den teknik som används för att förmedla uppgifter inte i sig har någon större betydelse ur integritetssynpunkt. Nämnden anger att en lagringsskyldighet för tillhandahållarna

medför en ökad datalagring, vilket bör påverka den proportionalitetsbedömning som ska göras vid utformningen av reglerna. *Stockholms universitet (Juridiska fakulteten)* påpekar att det finns risk att förslaget inte får den effekt som eftersträvas eftersom de företag som tillhandahåller tjänsterna till stor del är belägna utanför EU och att det inte är självklart att de kommer att hörsamma lagrings- och anpassningskrav i Sverige. *Apple Aktiebolag* lyfter frågan om vilka tjänster som är att betrakta som nummeroberoende interpersonella kommunikationstjänster.

Skälen för utkastets bedömning

Nummeroberoende interpersonella kommunikationstjänster

En interpersonell kommunikationstjänst är en tjänst som vanligen tillhandahålls mot ersättning och som möjliggör ett direkt interpersonellt och interaktivt informationsutbyte via elektroniska kommunikationsnät mellan ett begränsat antal personer. De personer som inleder eller deltar i kommunikationen bestämmer vem eller vilka som ska vara mottagare. Definitionen omfattar inte tjänster som möjliggör kommunikation enbart som en extrafunktion av mindre betydelse som är direkt kopplad till en annan tjänst (1 kap. 7 § lagen om elektronisk kommunikation).

Interpersonella kommunikationstjänster kan vara antingen nummerbaserade eller nummeroberoende. De nummerbaserade tjänsterna etablerar en förbindelse till nummer i nationella eller internationella nummerplaner eller möjliggör kommunikation med sådana nummer, till skillnad från de nummeroberoende tjänsterna som varken etablerar en sådan förbindelse eller möjliggör sådan kommunikation (1 kap. 7 §). Nummeroberoende interpersonella kommunikationstjänster kan använda traditionella telefonnummer för att identifiera slutanvändare så att de ska kunna nå varandra, men möjliggör inte kommunikation med sådana nummer.

Utredningen ger en närmare beskrivning av vilka tjänster som kan omfattas av definitionen av de aktuella kommunikationstjänsterna (se t.ex. s. 325–330 i betänkandet). Exempel på dessa tjänster är olika former av kommunikationsapplikationer på mobiltelefoner eller datorer. Som utredningen anger kan flera olika typer av tjänster omfattas. Vilka tjänster som i enskilda fall är att betrakta som nummeroberoende interpersonella kommunikationstjänster bestäms genom tillämpningen.

Elektroniska kommunikationstjänster som är allmänt tillgängliga är sådana som erbjuder en allmän möjlighet att ansluta sig. De som inte är allmänt tillgängliga är exempelvis kommunikationstjänster som myndigheter, företag eller privatpersoner kan skapa för att använda enbart inom en begränsad krets.

Tillhandahållarna av de aktuella tjänsterna omfattas redan i viss utsträckning av regelverket om elektronisk kommunikation. Tillhandahållarna omfattas exempelvis av kraven på att vidta tekniska och organisatoriska åtgärder för att på ett lämpligt sätt hantera risker som hotar säkerheten i nät och tjänster. De omfattas också av kraven på att rapportera säkerhetsincidenter och ska vidta åtgärder för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av tjänsten skyddas (8 kap. 1, 3 och 6 §§ lagen om elektronisk kommunikation).

Det finns ett behov av att tillhandahållarna omfattas av lagrings- och anpassningsskyldighet och vissa andra regler

Tillgången till information från elektronisk kommunikation är ofta av stor betydelse för den brottsbekämpande verksamheten. Utredningen har framhållit att det blir allt vanligare att kommunikation sker genom tjänster vars tillhandahållare inte omfattas av någon rättslig skyldighet att lagra eller tillhandahålla uppgifter. När det exempelvis gäller brott som begås inom ramen för kriminella nätverk är dessa ofta svåra att utreda eftersom brottsoffer och vittnen av olika anledningar kan vara obenägna att lämna information till de brottsbekämpande myndigheterna. Det är därför av stor vikt att brottsbekämpande myndigheter har goda möjligheter att komma åt annan bevisning, såsom information från elektronisk kommunikation. Informationen har även betydelse i myndigheternas underrättelseverksamhet.

Nyttan av uppgifter om elektronisk kommunikation är lika påtaglig oavsett vilken typ av leverantör som tillhandahåller kommunikationstjänsten. I takt med att allt fler använder nummeroberoende interpersonella kommunikationstjänster ökar behovet av uppgifter om elektronisk kommunikation som genereras och behandlas hos tillhandahållare av sådana tjänster.

Med nuvarande regler kan uppgifter om abonnemang, såsom identitetsuppgifter om en användare, inhämtas direkt med stöd av 9 kap. 33 § lagen om elektronisk kommunikation. Bestämmelsen omfattar inte tillhandahållare av nummeroberoende interpersonella kommunikationstjänster. Tillhandahållarna kan på frivillig basis lämna ut information till de brottsbekämpande myndigheterna. En sådan ordning är dock inte tillräcklig för att säkerställa att myndigheterna får tillgång till uppgifterna.

De brottsbekämpande myndigheterna kan i vissa fall komma åt uppgifter om elektronisk kommunikation hos tillhandahållare av nummeroberoende interpersonella kommunikationstjänster genom användning av olika straffprocessuella tvångsmedel. Reglerna om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation är teknikneutrala i den bemärkelsen att användningsområdet inte är begränsat till vissa elektroniska kommunikationstjänster. Dessa tvångsmedel skulle alltså kunna användas mot tillhandahållarna av de aktuella tjänsterna. Tillhandahållare av sådana tjänster omfattas dock inte av någon anpassnings- eller lagringsskyldighet. Anpassningsskyldigheten är en förutsättning för att tvångsmedlen ska gå att genomföra på ett effektivt sätt och utan risk för att verkställigheten röjs. Tillhandahållarna har inte heller någon skyldighet att lagra uppgifter i brottsbekämpande syfte. Avsaknaden av en lagringsskyldighet får till konsekvens att tillhandahållarna i stället ska utplåna eller avidentifiera uppgifter enligt huvudregeln i 9 kap. 1 § lagen om elektronisk kommunikation. Möjligheterna att hämta in historisk information om kommunikation från en tillhandahållare av en nummeroberoende interpersonell kommunikationstjänst genom ett tillstånd till hemlig övervakning av elektronisk kommunikation är därmed beroende av vad tillhandahållaren lagrar för egna ändamål.

Det kan i vissa fall vara möjligt att få fram uppgifter från tillhandahållarna med hjälp av öppna straffprocessuella tvångsmedel, såsom husrannsakan och beslag samt genomsökning på distans. Som utredningen anger kan det dock vara svårt att på egen hand hitta den eftersökta informationen vid en husrannsakan och vid genomsökning på distans krävs autentisering i det avsedda systemet. Använd-

ningsområdet för husrannsakan och beslag samt genomsökning på distans är därför mindre än för hemlig avlyssning och hemlig övervakning av elektronisk kommunikation. Myndigheterna kan också i vissa fall komma åt uppgifter om elektronisk kommunikation genom hemlig dataavläsning. Hemlig dataavläsning tar dock bl.a. mer resurser i anspråk.

Det är möjligt att förelägga den som i elektronisk form innehar en viss lagrad uppgift som skäligen kan antas ha betydelse för utredningen om ett brott att bevara uppgiften genom ett s.k. bevarandeföreläggande (27 kap. 16 § rättegångsbalken). Ett sådant föreläggande kan riktas mot en tillhandahållare av en nummeroberoende interpersonell kommunikationstjänst. Ett bevarandeföreläggande kan dock bara användas om myndigheterna känner till att viss elektronisk information finns lagrad hos en tillhandahållare. Ett bevarandeföreläggande kan dessutom endast användas i en brottsutredning och inte i underrättelseverksamheten.

De möjligheter som lagstiftningen ger brottsbekämpande myndigheter att komma åt uppgifter från de aktuella tillhandahållarna är följaktligen inte tillräckliga. I enlighet med utredningens bedömning finns det sammantaget ett påtagligt behov av att låta tillhandahållarna omfattas av lagrings- och anpassningsskyldigheten samt andra regler om datalagring som har anknytning till dessa skyldigheter.

Det är proportionerligt att tillhandahållarna omfattas av skyldigheterna

För att tillhandahållare av nummeroberoende interpersonella kommunikationstjänster ska kunna omfattas av de aktuella skyldigheterna i regelverket om datalagring krävs att införandet av sådana regler bedöms vara förenligt med de grundläggande fri- och rättigheterna i såväl regeringsformen som Europakonventionen och EU:s rättighetsstadga. Vid dessa överväganden är rätten till privatliv och rätten till skydd mot intrång i den personliga integriteten av särskild betydelse. Begränsningar i dessa rättigheter får bara göras för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle och får aldrig gå utöver vad som är nödvändigt med hänsyn till de ändamål som har föranlett dem.

Syftet med att låta reglerna om lagrings- och anpassningsskyldighet omfatta de aktuella tillhandahållarna är att ge de brottsbekämpande myndigheterna förbättrade möjligheter att bekämpa grov brottslighet. Detta utgör i sig ett angeläget intresse och är ett godtagbart skäl för att begränsa enskildas fri- och rättigheter enligt såväl Europakonventionen som EU:s rättighetsstadga. Detsamma gäller i förhållande till regeringsformen. En följd av införandet av skyldigheter för sådana tillhandahållare kan dessutom innebära ökad trygghet för enskilda genom att brott både kan förebyggas och utredas mer effektivt.

Att låta reglerna omfatta även tillhandahållare av nummeroberoende interpersonella kommunikationstjänster syftar i huvudsak till att möjliggöra bättre åtkomst till information i den brottsbekämpande verksamheten, bl.a. genom användning av hemliga tvångsmedel. Som *Säkerhets- och integritetsskyddsnämnden* för fram innebär en lagringsskyldighet för de aktuella tillhandahållarna att en större mängd kommunikation omfattas av en sådan skyldighet än vad som är fallet idag. Det innebär samtidigt att de brottsbekämpande myndigheterna återfår en förmåga som de tidigare haft när kommunikationen främst skedde genom teleoperatörernas telefonitjänster. De brottsbekämpande myndigheternas behov får anses vara så starkt

att det väger tyngre än nackdelarna med den ökade lagring som en sådan skyldighet kan innebära.

Kommunikation som sker genom nummeroberoende interpersonella kommunikationstjänster är generellt sett inte att bedöma annorlunda än kommunikation som sker genom teleoperatörernas tjänster. En viss kommunikation är lika skyddsvärd oavsett vilken tjänst som används för att förmedla den. Det har enligt utredningen inte framkommit några uppenbara omständigheter som pekar på att lagrings- och anpassningsskyldighet för de aktuella tillhandahållarna skulle innebära större ingrepp i enskildas grundläggande fri- och rättigheter än motsvarande skyldigheter för en teleoperatör. Som utredningen för fram motsvarar nummeroberoende interpersonella kommunikationstjänster funktionsmässigt de tjänster som tillhandahålls av teleoperatörerna. Det torde inte för den enskilde användaren spela någon roll om tillhandahållaren själv överför kommunikationen genom egna nät eller om det sker över internet genom andras nät. Vilken teknik som används bör därmed inte heller vara avgörande för om en tillhandahållare ska omfattas av de aktuella skyldigheterna. Som utredningen för fram skulle det leda till en mer teknikneutral reglering att låta tillhandahållarna omfattas av skyldigheterna.

Sammantaget utgör ett införande av lagrings- och anpassningsskyldighet och andra anknytande skyldigheter för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster en åtgärd som skulle innebära nytta för brottsbekämpningen och som brottsbekämpande myndigheter har ett påtagligt behov av. Det bedöms inte vara möjligt att uppnå motsvarande resultat genom andra mindre ingripande åtgärder. Behovet väger tyngre än de motstående intressen som talar emot att låta sådana tjänster omfattas av reglerna. Att låta tillhandahållarna omfattas av de aktuella skyldigheterna utgör därmed en proportionerlig åtgärd som är förenlig med regeringsformen, Europakonventionen och EU:s rättighetsstadga. Genom att tillhandahållarna omfattas av de aktuella skyldigheterna kommer de också att omfattas av de rättssäkerhetsgarantier som redan följer av regelverket. I enlighet med det som *Säkerhets- och integritetsskyddsnämnden* anför ska proportionalitetsprincipen beaktas även vid den närmare utformningen av reglerna.

Tillhandahållare av nummeroberoende interpersonella kommunikationstjänster bör omfattas av reglerna om lagrings- och anpassningsskyldighet samt av vissa andra regler

Utredningen anger att de stora tillhandahållarna av de aktuella tjänsterna i Sverige är globala bolag som tillhandahåller sina tjänster i flera länder och inte har säte i Sverige. Det föranleder frågor om Sverige kan införa krav på dessa tillhandahållare och om hur efterlevnad kan säkerställas. Som utredningen anger finns det inte något hinder mot att införa sådana krav för verksamheter som har anknytning till Sverige, som att tjänsterna tillhandahålls här i landet. Huruvida rättslig hjälp kan ges för att verkställa exempelvis beslut om vite beror på i vilket land åtgärden ska vidtas och vilka avtal Sverige har med det landet. Det som *Stockholms universitet (Juridiska fakulteten)* för fram om att det kan finnas en risk för att reglerna inte efterlevs av tillhandahållare som är belägna utanför EU utgör inte ett tillräckligt starkt skäl för att avstå från att genomföra utredningens förslag.

Det finns ett påtagligt behov av och är proportionerligt att låta tillhandahållarna omfattas av lagrings- och anpassningsskyldighet och andra regler som har anknyt-

ning till dessa skyldigheter. Exempelvis *Polismyndigheten*, *Tullverket* och *Åklagarmyndigheten* betonar vikten av att tillhandahållarna omfattas. I enlighet med utredningens bedömning och i linje med utgångspunkterna för lagstiftningsärendet bör tillhandahållarna därför omfattas av de aktuella skyldigheterna. Förutom lagrings- och anpassningsskyldigheterna så handlar det exempelvis om tystnadsplikt och rätt till ersättning, skyldighet att lämna ut uppgifter till myndigheter och alarmeringscentraler samt skyldighet att skydda och bevara uppgifter.

7.2 Lagring av uppgifter om abonnemang och lagring enligt ett beslut om nationell säkerhetslagring

Utkastets förslag: Tillhandahållare av allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster ska vara skyldiga att lagra uppgifter om abonnemang som kan användas för att identifiera en abonnent och registrerad användare.

De ska också vara skyldiga att lagra uppgifter som framgår av ett beslut enligt lagen om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

Lagringsskyldigheten ska omfatta uppgifter som genereras eller behandlas vid tjänster som tillhandahåller samtal och meddelandehantering vid kommunikation som sker till, från eller inom Sverige.

Vid lagring av lokaliseringsuppgifter som inte är trafikuppgifter, som ska lagras i syfte att skydda Sveriges säkerhet, ska lagringsskyldigheten omfatta endast uppgifter som avser lokalisering i Sverige.

Lagringsskyldigheten ska gälla även vid misslyckad uppringning.

Tillhandahållarna ska få ge någon annan i uppdrag att utföra lagringen.

Tillsynsmyndigheten ska i enskilda fall få besluta om undantag från tillhandahållarnas skyldighet att lagra uppgifter om abonnemang.

Utredningens förslag överensstämmer i huvudsak med utkastets. Utredningen föreslår inom ramen för förslaget om riktad lagring att tillhandahållarna ska vara skyldiga att lagra även trafikuppgifter och lokaliseringsuppgifter som inte är trafikuppgifter. Utredningen föreslår vidare att paragrafen som reglerar möjlighet för tillsynsmyndigheten att besluta om undantag i enskilda fall ska tas bort.

Remissinstanserna: En majoritet tillstyrker eller har inget att invända mot förslaget. *ECPAT Sverige* betonar behovet av datalagring för att kunna utreda sexualbrott mot barn och vikten av att även tillhandahållare av nummeroberoende interpersonella kommunikationstjänster omfattas av en lagringsskyldighet. Organisationen pekar även på brottsbekämpande myndigheters behov av att kunna koppla ip-adresser till uppgifter om abonnemang vid misstanke om brott. *Försvarsmakten* tillstyrker att skyldigheten begränsas till allmänt tillgängliga tjänster, eftersom det ur säkerhetsskyddsperspektiv är viktigt att myndighetens kommunikationstjänster inte omfattas. *Post- och telestyrelsen* anser att förslagen kan innebära ett ökat integritetsintrång i den mån gps-positioner lagras. *Åklagarmyndigheten* ställer sig bakom förslaget att det ska finnas en anknytning till Sverige för att tillhandahållarna ska vara skyldiga att lagra uppgifter. *Svea hovrätt*

för fram att det, med hänsyn till de utmaningar som föreligger beträffande att fastställa inom vilka geografiska områden som uppgifter genererats, kan finnas anledning att ytterligare analysera frågan om hur det ska fastställas om kommunikationen till någon del sker i Sverige. *Institutet för mänskliga rättigheter* anser att det utifrån underlaget är svårt att veta den faktiska nyttan för brottsbekämpande myndigheter om tillhandahållarna skulle omfattas av lagringsskyldigheten.

Skälen för utkastets förslag

Tillhandahållarna bör omfattas av skyldigheten att lagra uppgifter om abonnemang

Uppgifter om abonnemang är mindre känsliga än uppgifter som ger information om kommunikation. Uppgifterna är att betrakta som sådana uppgifter som EU-domstolen benämner uppgifter om fysisk identitet och som får behandlas i större utsträckning än uppgifter om kommunikation (se La Quadrature du Net I-domen punkt 158). Även det senare avgörandet La Quadrature du Net II går i denna riktning.

En första fråga är om tillhandahållare av nummeroberoende interpersonella kommunikationstjänster har tillgång till sådana uppgifter om abonnemang att det finns en nytta med att ålägga dem en lagringsskyldighet för sådana uppgifter. Utredningen anger att vilka uppgifter om användaren som tjänsterna har tillgång till kan skilja sig åt, men att relevanta uppgifter i detta avseende kan finnas hos tillhandahållarna. Användningen av en sådan tjänst kräver enligt utredningen någon form av kontouppgifter hos tillhandahållaren. De uppgifter om abonnemang som tillhandahållare av de aktuella kommunikationstjänsterna kan ha tillgång till kan vara namn och adress, telefonnummer, e-postadress eller ett användarnamn. Tillhandahållarna kan även ha tillgång till andra uppgifter som kan identifiera en användare, såsom uppgifter om betalkort. För att kunna förmedla kommunikation behöver tillhandahållarna information om den ip-adress och i förekommande fall det portnummer som användarens kommunikationsutrustning använder för att koppla upp sig mot tjänsten. De aktuella tillhandahållarna kan således, i enlighet med vad utredningen anger, ha tillgång till uppgifter om abonnemang som kan omfattas av lagringsskyldighet och som är av nytta vid utredande av brott.

Uppgifterna om abonnemang har betydelse för att utreda många olika typer av brott, såväl grov brottslighet som mindre grova brott. Som betonas av *ECPAT Sverige* är möjligheten att komma åt uppgifter om abonnemang av särskilt stor vikt i utredningar om brott som kan begås över internet, såsom sexuella övergrepp mot barn och barnpornografibrott. Det gäller även exempelvis hatbrott, bedrägerier, hets mot folkgrupp, förtal och immaterialrättsbrott. Europadomstolen har också konstaterat att det kan innebära ett brott mot artikel 8 i Europakonventionen om rätten till skydd för privatliv om det inte finns möjlighet för brottsbekämpande myndigheter att få reda på uppgift om innehavare av en ip-adress som kan vara en uppgift om abonnemang (Europadomstolens dom den 2 december 2008 i målet K.U. mot Finland, nr 2872/02).

De brottsbekämpande myndigheternas behov av åtkomst till uppgifter om abonnemang är betydande, oavsett om uppgifterna härrör från traditionella kom-

munikationstjänster eller från nummeroberoende interpersonella kommunikationstjänster. Behovet väger tyngre än de motstående intressen som talar emot att låta tillhandahållarna omfattas av en lagringsskyldighet för uppgifter om abonnemang. Tillhandahållarna bör därför vara skyldiga att lagra uppgifter om abonnemang som kan användas för att identifiera en abonnent och registrerad användare. Lagringsskyldigheten innebär att de uppgifter om abonnemang som kan finnas i form av exempelvis uppgivet namn, användarnamn, e-postadress, ip-adress och telefonnummer ska lagras, i den utsträckning sådana uppgifter genereras eller behandlas.

I enlighet med vad utredningen anger finns det inte skäl att ålägga lagringsskyldighet för de som tillhandahåller mindre tjänster som inte är tillgängliga för allmänheten utan enbart riktar sig till en mindre krets, såsom inom ett företag eller en myndighet. Som *Försvarsmakten* för fram talar tvärtom starka skäl emot att låta lagringsskyldigheten omfatta även sådana tjänster som inte är allmänt tillgängliga. I likhet med nu gällande lagringsskyldighet bör således enbart tillhandahållare av allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster omfattas av lagringsskyldigheten.

Det nu aktuella förslaget innebär att tillhandahållarna åläggs en lagringsskyldighet som är mindre omfattande än utredningens förslag som, utöver uppgifter om abonnemang, även omfattar lagringsskyldighet avseende trafikuppgifter och lokaliseringsuppgifter. Utredningens förslag i den delen är avhängigt förslaget om s.k. riktad lagring, som inte behandlas inom ramen för detta lagstiftningsprojekt. Det saknas därför förutsättningar att gå vidare med det mer omfattande förslaget. Lagring av trafikuppgifter och lokaliseringsuppgifter blir däremot aktuellt för tillhandahållarna inom ramen för nationell säkerhetslagring (avsnitt 6.5).

Tillhandahållarna bör också lagra uppgifter i syfte att skydda nationell säkerhet

Säkerhetspolisen föreslås få möjlighet att besluta om en mer omfattande lagring av uppgifter för tillhandahållare av elektroniska kommunikationstjänster, om det finns ett allvarligt hot mot nationell säkerhet (avsnitt 6.2). Det är fråga om en lagringsskyldighet som ska kunna beslutas när det finns ett allvarligt hot mot Sveriges säkerhet och har till syfte att skydda Sveriges grundläggande nationella säkerhetsintressen. Utredningen föreslår att även tillhandahållare av nummeroberoende interpersonella kommunikationstjänster ska omfattas av sådan lagringsskyldighet. Vikten av de intressen som de föreslagna reglerna syftar till att skydda talar för att de bör omfatta även dessa tillhandahållare och inte begränsas till de som omfattas av nuvarande lagringsskyldighet.

Lagringsskyldigheten enligt ett beslut om nationell säkerhetslagring föreslås i avsnitt 6.5 kunna omfatta uppgifter om abonnemang, trafikuppgifter och lokaliseringsuppgifter som inte är trafikuppgifter (9 kap. 19 b § lagen om elektronisk kommunikation). Utredningen anger att tillhandahållare av nummeroberoende interpersonella kommunikationstjänster kan ha tillgång till de aktuella uppgifterna. Tillhandahållarna kan ha tillgång till uppgifter om abonnemang, även om tillgången till uppgifterna kan skilja sig åt mellan tjänsterna. Beträffande trafikuppgifter och lokaliseringsuppgifter anger utredningen att tillhandahållarna kan ha tillgång till uppgifterna, men att det även för dessa uppgifter skiljer sig åt bero-

ende på hur tjänsten är uppbyggd. Utredningen anger att tillhandahållarna bör ha tillgång till uppgifter om vilka användaridentiteter och ip-adresser som deltagit i ett samtal samt under vilken tid samtalet ägt rum. Detsamma gäller uppgift om vilka användaridentiteter och ip-adresser som är avsändare och mottagare till ett meddelande och tidpunkt när meddelandet skickades. Därutöver bör de enligt utredningen också ha uppgifter om kommunikationsutrustningen. Eftersom tillhandahållare av nummeroberoende interpersonella kommunikationstjänster vanligen inte äger den infrastruktur som används för att etablera kontakt med användarnas utrustning har de i regel inte tillgång till uppgifter om vilken telefonmast, dvs. basstation, som en viss kommunikationsutrustning varit ansluten till. Utredningen anger att de genom tillgången till användarnas ip-adresser ändå kan få tillgång till ungefärliga lokaliseringsuppgifter för kommunikationsutrustningen och att även mer detaljerade uppgifter om utrustningens position kan finnas, såsom gps-position.

Det har inte framkommit något som ger skäl att ifrågasätta det utredningen anger om vilka uppgifter som tillhandahållarna kan ha tillgång till. Det finns följaktligen förutsättningar för att låta de aktuella tillhandahållarna omfattas av samma lagringsskyldighet vid nationell säkerhetslagring som ska gälla för andra tjänsteleverantörer, dvs. uppgifter om abonnemang, trafikuppgifter och lokaliseringsuppgifter som inte är trafikuppgifter. Som *Post- och telestyrelsen* för fram kan behandling av de mer precisa lokaliseringsuppgifter som kan förekomma hos tillhandahållare av nummeroberoende interpersonella kommunikationstjänster innebära ett större integritetsintrång för enskilda än behandling av t.ex. basstationsuppgifter. Som utredningen påpekar kan den enskilde användaren dock i regel välja att stänga av en sådan funktion, såsom gps-funktionen i en telefon.

De uppgifter som tillhandahållarna kan ha tillgång till kan vara av betydelse för att bekämpa brottslighet som utgör ett hot mot den nationella säkerheten. Det saknas skäl att ur integritetsperspektiv bedöma kommunikation som sker genom de nu aktuella kommunikationstjänsterna annorlunda än kommunikation genom de tjänster som omfattas av nuvarande lagringsskyldighet. I likhet med befintlig lagringsskyldighet rör den lagringsskyldighet som det nu är fråga om inte innehållet i kommunikation.

Förslaget om nationell säkerhetslagring innebär en mer omfattande lagring som ska kunna beslutas vid ett allvarligt hot mot Sveriges säkerhet. Det är uppenbart att behovet av tillgång till information för att kunna bekämpa allvarliga hot mot den nationella säkerheten är angeläget. Behovet väger tyngre än de motstående intressen som talar emot att låta tillhandahållarna omfattas av en lagringsskyldighet enligt ett beslut om nationell säkerhetslagring. Det finns också praktiska förutsättningar att låta dem omfattas av skyldigheten. Tillhandahållarna bör därför vara skyldiga att lagra uppgifter enligt ett beslut om nationell säkerhetslagring.

Eftersom lagringsskyldigheten är teknikneutralt formulerad finns det inte någon anledning att vare sig inskränka eller utvidga lagringsskyldigheten. Om en viss typ av uppgift inte genereras eller behandlas i tillhandahållarens verksamhet, omfattas den inte av lagringsskyldigheten.

Lagringsskyldigheten bör omfatta uppgifter som genereras eller behandlas vid tjänster som förmedlar samtal och meddelanden med anknytning till Sverige

Den nuvarande lagringsskyldigheten omfattar uppgifter som genereras eller behandlas vid telefonitjänst eller meddelandehantering via mobil nätanslutningspunkt. Som utredningen konstaterar kan begreppet telefonitjänst inte användas i förhållande till tillhandahållare av nummeroberoende interpersonella kommunikationstjänster. Detta eftersom det kräver att tjänsten ska innebära en möjlighet att ringa upp eller ta emot samtal via nummer inom en nationell eller internationell nummerplan (1 kap. 7 § lagen om elektronisk kommunikation). Nummeroberoende interpersonella kommunikationstjänster har inte en sådan möjlighet. Samtidigt erbjuder många tillhandahållare av sådana tjänster en samtalstjänst som funktionsmässigt motsvarar telefonsamtal. Utredningen föreslår i stället att begreppen samtal och meddelandehantering används för att reglera lagringsskyldigheten för tillhandahållarna. Meddelandehantering innebär utbyte eller överföring av ett elektroniskt meddelande som inte är ett samtal och inte heller är information som överförs som en del av sändningar av ljudradio- och tv-program (1 kap. 7 §). Med samtal avses en förbindelse genom en allmänt tillgänglig interpersonell kommunikationstjänst som möjliggör talkommunikation i båda riktningarna (1 kap. 7 §). Begreppet meddelandehantering kan tillämpas även på nummeroberoende interpersonella kommunikationstjänster och begreppet samtal kan användas i förhållande till de som tillhandahåller samtalstjänster. Begreppen samtal och meddelandehantering bör därmed i enlighet med utredningens förslag användas vid bestämmande av lagringsskyldigheten för de aktuella tillhandahållarna.

Tillhandahållare av nummeroberoende interpersonella kommunikationstjänster erbjuder i regel sina tjänster i flera länder och lagringsskyldigheten bör kräva någon anknytning till Sverige. I enlighet med vad utredningen föreslår bör lagringsskyldigheten omfatta sådan kommunikation som sker till, från eller inom Sverige. I fråga om lokaliseringsuppgifter som inte är trafikuppgifter bör lagringsskyldigheten avgränsas till sådana uppgifter i Sverige, dvs. sådana som avser lokalisering i Sverige. Sådana uppgifter kommer endast att omfattas av lagringsskyldighet när det finns ett beslut om lagring av sådana uppgifter enligt 2 § lagen om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

Svea hovrätt lyfter frågan om hur det ska fastställas att kommunikationen till någon del sker i Sverige. I enlighet med utredningens uppfattning bör det finnas förutsättningar för tillhandahållare att bedöma huruvida viss kommunikation har anknytning till Sverige. Tillhandahållarna bör vara bäst lämpade att avgöra vilken metod som ska användas för att bedöma om viss kommunikation omfattas av lagringsskyldigheten. Det bör alltså inte i lag anges hur tillhandahållarna ska avgöra om det är fråga om kommunikation som sker till, från eller inom Sverige utan regleringen bör såsom utredningen föreslår vara teknikneutral.

Lagringsskyldighet vid misslyckad uppringning, möjlighet att ge någon annan i uppdrag att utföra lagringen samt undantag från lagringsskyldigheten

Nuvarande lagringsskyldighet omfattar även uppgifter vid misslyckad uppringning, dvs. en uppringning som kopplas fram utan att nå en mottagare, såsom när

mottagaren inte svarar (1 kap. 7 § och 9 kap. 19 § tredje stycket lagen om elektronisk kommunikation). Därutöver får lagringsskyldiga uppdra åt någon annan att utföra lagringen (9 kap. 19 § fjärde stycket). Utredningen föreslår att samma regler ska gälla för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster. Uppgifter om misslyckad uppringning kan ge information som är av betydelse för den brottsbekämpande verksamheten, oavsett genom vilken tjänst uppringningen har skett. I enlighet med vad som gäller för andra tillhandahållare bör även de nu aktuella tillhandahållarna ha möjlighet att låta någon annan utföra lagringen. Förslagen om lagringsskyldighet vid misslyckad uppringning och möjlighet att uppdra åt annan att utföra lagringen bör därför genomföras. Förslaget om misslyckad uppringning bör regleras i samma paragraf som bestämmelsen om lagringsskyldighet (föreslagna 9 kap. 19 a §). Att den som ska lagra uppgifter enligt 19, 19 a och 19 b §§ får uppdra åt någon annan att utföra lagringen bör regleras i en ny paragraf, den nya 19 c §.

Nuvarande regelverk innehåller vidare en möjlighet för tillsynsmyndigheten att i enskilda fall besluta om undantag från skyldigheten att lagra uppgifter, om det finns synnerliga skäl. Ett sådant beslut får förenas med villkor (9 kap. 20 § första stycket). Utredningen föreslår att denna möjlighet ska tas bort. Förslaget har samband med utredningens förslag om att införa riktad lagring som inte behandlas inom ramen för detta lagstiftningsprojekt. Möjligheten att besluta om undantag bör gälla även i förhållande till tillhandahållare av nummeroberoende interpersonella kommunikationstjänster när de lagrar uppgifter om abonnemang. En ändring med denna innebörd bör därför göras i 9 kap. 20 § första stycket. När det gäller lagring i syfte att skydda Sveriges säkerhet bör i enlighet med utredningens förslag någon motsvarande möjlighet inte finnas eftersom sådan lagringsskyldighet grundas på beslut av annan myndighet.

7.3 Lagringstider och upplysning om verkställighetsföreskrifter

Utkastets förslag: Uppgifter om abonnemang som kan användas för att identifiera en abonnent och registrerad användare ska lagras av tillhandahållare av nummeroberoende interpersonella kommunikationstjänster i ett år.

Vid meddelandehantering ska lagringstiden räknas från den dag meddelandet skickades.

Det ska upplysas om att regeringen eller den myndighet regeringen bestämmer kan meddela närmare föreskrifter om vilka uppgifter om abonnemang som ska lagras och om lagringstiden.

Utredningens förslag överensstämmer med utkastets.
Remissinstanserna: Ingen remissinstans yttrar sig särskilt om förslaget.

Skälen för utkastets förslag

Lagringstider

Enligt nuvarande regler om lagringsskyldighet varierar den föreskrivna lagringstiden för uppgifter om abonnemang mellan sex och tio månader beroende på om uppgifterna härstammar från telefonitjänst och meddelandehantering via mobil nätanslutningspunkt eller från internetåtkomst (9 kap. 22 § första stycket lagen om elektronisk kommunikation). Lagringstiden räknas från den dag kommunikationen avslutades (9 kap. 22 § andra stycket).

Ju längre tid uppgifter finns lagrade hos tillhandahållarna, desto bättre förutsättningar har de brottsbekämpande myndigheterna att utföra sitt uppdrag. Det gäller i synnerhet i förhållande till brott som är svårupptäckta, där anmälningsfrekvensen är låg eller vid komplicerade utredningar som tar längre tid. Uppgifterna har även betydelse i myndigheternas underrättelseverksamhet. Lagringstiden bör dock inte vara längre än vad som får anses motiverat av målen att bekämpa brottslighet och att uppfylla statens positiva skyldighet att effektivt kunna beivra brott.

I avsnitt 5.1 föreslås att uppgifter om abonnemang ska lagras i ett år. De brottsbekämpande myndigheternas behov av uppgifter om abonnemang är lika stort oavsett om uppgifterna härstammar från traditionella kommunikationstjänster eller nummeroberoende interpersonella kommunikationstjänster. Det har inte framkommit något som motiverar att lagringstiden för uppgifter hos tillhandahållare av nummeroberoende interpersonella kommunikationstjänster ska skilja sig från vad som gäller för motsvarande uppgifter hos andra tillhandahållare. Lagringstiden för uppgifter om abonnemang bör således vara ett år även för de aktuella tillhandahållarna. Detta föreslås regleras i 9 kap. 22 § andra stycket. Lagringstiden utgår från det att abonnemanget eller tilldelningen av en tillfällig identifierare upphörde.

När det gäller ett beslut om nationell säkerhetslagring föreslås i avsnitt 6.5 att lagringstiden bör vara två år för uppgifter om abonnemang och trafikuppgifter samt ett år för lokaliseringsuppgifter som inte är trafikuppgifter. I och med att tillhandahållare av nummeroberoende interpersonella kommunikationstjänster föreslås omfattas av reglerna om nationell säkerhetslagring kommer samma lagringstid att gälla för dessa tillhandahållare när de omfattas av ett beslut om nationell säkerhetslagring.

En särskild fråga när det gäller meddelanden som skickas via de aktuella kommunikationstjänsterna är vid vilken tidpunkt lagringstiden bör utgå från. Detta blir aktuellt när tillhandahållarna ska lagra trafikuppgifter och lokaliseringsuppgifter som inte är trafikuppgifter inom ramen för nationell säkerhetslagring. Ett meddelande som skickas via en nummeroberoende interpersonell kommunikationstjänst kan i motsats till vad som vanligen gäller för sms-meddelanden tas emot vid flera olika tillfällen. Det gäller exempelvis om användaren är inloggad på flera enheter. En reglering där lagringstiden utgår från när ett meddelande togs emot skulle alltså riskera att bli svårtillämpad. Som utredningen föreslår bör därför lagringstiden för meddelanden gälla från det att meddelandet skickades. För lokaliseringsuppgifter som inte är trafikuppgifter kommer lagringstiden i enlighet med vad som föreslås gälla för andra tillhandahållare att gälla från den dag uppgifterna genererades (avsnitt 6.5).

Upplysning om verkställighetsföreskrifter

Nuvarande reglering innehåller en upplysning om att lagringsskyldigheten och lagringstiden kan bli föremål för närmare föreskrifter från regeringen eller den myndighet som regeringen bestämmer (9 kap. 23 § lagen om elektronisk kommunikation). I enlighet med vad som anges i avsnitt 5.1 finns det inte tillräckliga skäl att gå vidare med förslaget att införa ett särskilt bemyndigande endast för lagring av uppgifter om abonnemang. Däremot bör det tydliggöras att den befintliga upplysningsbestämmelsen även ska omfatta uppgifter om lagring och lagringstid för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster. Det innebär att det i 9 kap. 23 § bör upplysas om att regeringen eller den myndighet regeringen bestämmer med stöd av 8 kap. 7 § regeringsformen kan meddela närmare föreskrifter om vilka uppgifter som tillhandahållarna ska lagra och om lagringstiden.

7.4 Anpassningsskyldighet

Utkastets förslag: Skyldigheten att bedriva sin verksamhet så att beslut om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation samt inhämtning enligt inhämtningslagen kan verkställas och så att verkställandet inte röjs ska även omfatta tillhandahållare av allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster.

Tillhandahållare av allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster ska lämna ut uppgifter till brottsbekämpande myndigheter utan dröjsmål och på ett sådant sätt att utlämnandet inte röjs, om uppgifterna gäller brottslig verksamhet eller misstanke om brott.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: En majoritet av remissinstanserna, bl.a. *Säkerhets- och integritetsskyddsnämnden*, *Brottsoffermyndigheten*, *Ekobrottsmyndigheten*, *ECPAT Sverige*, *Tullverket*, *Stockholms universitet (Juridiska fakulteten)*, *Post- och telestyrelsen*, *Säkerhetspolisen* och *Polismyndigheten*, instämmer i eller har inget att invända mot förslaget. *ECPAT Sverige* betonar vikten av att lagstiftningen är teknikneutral. *Säkerhetspolisen* pekar på att förslaget minskar behovet av att använda hemlig dataavläsning, som är resurskrävande och ingripande för den enskildes integritet. *TechSverige* för fram att telekomoperatörernas tjänster och nummeroberoende interpersonella kommunikationstjänster skiljer sig åt och att totalsträckskrypterade tjänster inte kan dekrypteras. Organisationen pekar på att det av Europaparlamentets och rådets direktiv 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS2-direktivet) följer att totalsträckskryptering är en kritisk teknik som inte bör försvagas för bl.a. brottsbekämpning. Även *Södertörns tingsrätt* gör gällande att förslagen kan leda till en situation där skyddet för kommunikationssekretessen genom totalsträckskryptering försvagas. *Netnod*, *Dataskydd.net Sverige*, *Föreningen för Digitala fri- och rättigheter* och *ISOC-SE* för fram liknande synpunkter. *Internetstiftelsen* för fram att befogenheter

att agera mot grov brottslighet har starkt stöd hos en stor del av befolkningen, men att bryta eller försvaga krypteringslösningar kan äventyra användarnas integritet och säkerhet. *Journalistförbundet* avstyrker förslaget eftersom det enligt förbundet skulle kunna få stora negativa konsekvenser för källskyddet.

Skälen för utkastets förslag: Enligt nuvarande regler ska en verksamhet bedrivas så att beslut om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs, den s.k. anpassningsskyldigheten (9 kap. 29 § första stycket lagen om elektronisk kommunikation). Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om frågor som avses i första stycket samt får i enskilda fall besluta om undantag från kravet i första stycket (9 kap. 29 § andra stycket). I avsnitt 5.2 föreslås att kretsen av aktörer som ska omfattas av anpassningsskyldigheten knyts till de som är lagringsskyldiga.

När den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § lämnar ut uppgifter om abonnemang, innehållet i ett elektroniskt meddelande, andra uppgifter som angår ett särskilt elektroniskt meddelande eller lokaliseringsuppgifter som inte är trafikuppgifter till brottsbekämpande myndigheter, ska utlämnandet, om uppgifterna gäller brottslig verksamhet eller misstanke om brott, göras utan dröjsmål och på ett sådant sätt att utlämnandet inte röjs (9 kap. 29 b § första stycket). Enligt förslaget i avsnitt 5.2 knyts skyldigheten till de som är lagringsskyldiga. Uppgifterna ska ordnas och göras tillgängliga i ett format som gör att de enkelt kan tas om hand (9 kap. 29 b § andra stycket). Tillsynsmyndigheten får i enskilda fall besluta om undantag från kravet på format, om det finns särskilda skäl (9 kap. 29 b § fjärde stycket). Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om hur uppgifterna ska lämnas ut (9 kap. 29 b § femte stycket).

Nuvarande regler om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation är teknikneutrala. I teorin kan alltså uppgifter om elektronisk kommunikation och innehållet i meddelanden redan hämtas in från tillhandahållare av nummeroberoende interpersonella kommunikationstjänster. Sådana tillhandahållare omfattas dock inte av anpassningsskyldigheten. De omfattas heller inte av bestämmelserna om skyndsamhet och att uppgifterna ska lämnas ut på ett sätt att utlämnandet inte röjs.

Tillsammans med de övriga nämnda reglerna är anpassningsskyldigheten i praktiken en förutsättning för att tillstånd till hemlig avlyssning och hemlig övervakning av elektronisk kommunikation ska kunna verkställas och för att verkställandet ska kunna ske i nära anslutning till att ett tillstånd har meddelats. För att brottsbekämpande myndigheter ska ha möjlighet att inhämta information från nummeroberoende interpersonella kommunikationstjänster på ett ändamålsenligt sätt är det alltså viktigt att tillhandahållare av sådana tjänster omfattas av de aktuella reglerna. I enlighet med vad som anges i avsnitt 7.1 har brottsbekämpande myndigheter ett påtagligt behov av sådan inhämtning.

Netnod m.fl. lyfter frågor om informationssäkerhet och kryptering. Utredningen för fram att kommunikation genom nummeroberoende interpersonella kommunikationstjänster kan vara krypterad på ett sådant sätt att innehållet inte är möjligt att läsa i klartext för någon annan än avsändaren och mottagaren. Utredningen pekar på att krav att kunna verkställa tvångsmedelsbeslut redan gäller för tele-

operatörer och att det inte finns något skäl att inte ställa samma krav på tillhandahållare av nummeroberoende interpersonella kommunikationstjänster. När det gäller hur anpassningsskyldigheten skulle kunna genomföras vid krypterad kommunikation kan som anges i avsnitt 5.2 konstateras att utredningen inte lämnar något förslag på materiella ändringar av anpassningsskyldigheten. I enlighet med vad utredningen för fram innebär förslaget i sig inte att någon generell sårbarhet ska införas i kryptering eller att systematiska bakdörrar introduceras. Utredningen anger att det är fullt möjligt för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster att utforma sina tjänster så att kraven på säkerhet och skyddet för kommunikation tillgodoses. Genom att de aktuella tillhandahållarna omfattas av anpassningsskyldigheten blir de, likt vad som gäller för teleoperatörerna, skyldiga att samarbeta med brottsbekämpande myndigheter för att hemliga tvångsmedel ska kunna verkställas. Den närmare skyldigheten i de enskilda fallen, exempelvis vad som kan krävas i form av olika tekniska lösningar, blir i slutändan en fråga för rättstillämpningen och praxis att avgöra. Det är av vikt att exempelvis totalsträckskrypterade tjänster alltjämt kan användas.

Journalistförbundet lyfter att det kan finnas en risk för att källskyddet försvagas. I det sammanhanget kan nämnas att det grundlagsskyddade efterforskningsförbudet vad gäller den som är meddelare till en viss uppgift alltjämt är tillämpligt på myndigheternas verksamhet (3 kap. 5 § tryckfrihetsförordningen och 2 kap. 5 § yttrandefrihetsgrundlagen).

Beträffande anknytningen till Sverige anför utredningen att det för anpassningsskyldigheten inte behövs någon reglering om att den enbart ska gälla vid kommunikation som till någon del sker i Sverige. Anledningen till att någon sådan reglering inte behövs är att frågan om vilka uppgifter som de brottsbekämpande myndigheterna får hämta in styrs av de bestämmelser som reglerar åtkomsten. De bestämmelserna gäller även anpassningsskyldigheten eftersom den avser verkställighet av beslut om åtkomst. Det saknas skäl att göra någon annan bedömning än den utredningen har gjort beträffande anknytningen till Sverige.

Kommunikation bör inte behandlas annorlunda enbart för att den förmedlas genom en tjänst som är uppbyggd på ett visst sätt rent tekniskt. Tvärtom är det, som *ECPAT Sverige* pekar på, angeläget att lagstiftningen är teknikneutral. Det finns förutsättningar att låta anpassningsskyldigheten och övriga regler med anknytning till denna gälla för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster, på samma sätt som enligt nuvarande regler gäller för bl.a. teleoperatörer. Som *Säkerhetspolisen* anger innebär det också ett minskat behov av att använda hemlig dataavläsning, som är mer resurskrävande. Med hänsyn till den stora nytta som en sådan ändring kan väntas innebära för brottsbekämpningen, vilket väger tyngre än motstående intressen, bör alltså tillhandahållare av allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster omfattas av de nu aktuella skyldigheterna.

Tech Sverige lyfter frågan om kryptering och förhållandet till det s.k. NIS2-direktivet. I direktivet framgår av skäl 98 att användningen av krypteringsteknik bör främjas för att trygga säkerheten för bl.a. allmänt tillgängliga elektroniska kommunikationstjänster. Vidare anges att användning av totalsträckskryptering bör förenas med medlemsstaternas befogenheter att säkerställa skyddet av sina väsentliga säkerhetsintressen, sin allmänna säkerhet och att möjliggöra före-

byggande, utredning, upptäckt och lagföring av brott. I det sammanhanget nämns även att detta dock inte bör försvaga totalsträckskrypteringen. Det nu aktuella förslaget innebär inte någon materiell ändring av anpassningsskyldigheten eller ändring i tillämpningen av den, utan endast att tillhandahållarna av nummeroberoende interpersonella kommunikationstjänster inlemmas i det befintliga regelverket. I och med att samma krav kommer att gälla för tillhandahållarna som redan gäller för andra aktörer, bör förslaget i sig inte hamna i konflikt med övriga regelverk.

Förslaget innebär att de aktuella tillhandahållarna ska bedriva sin verksamhet så att beslut om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation, samt inhämtning enligt inhämtningslagen, kan verkställas och att de ska bedriva verksamheten så att verkställandet inte röjs. Det innebär också att de ska omfattas av skyldigheten att lämna ut uppgifter utan dröjsmål och på ett sådant sätt att utlämnandet inte röjs. I enlighet med utredningens förslag ska anpassningsskyldigheten i likhet med vad som gäller för tillhandahållare av andra elektroniska kommunikationstjänster enbart gälla sådana kommunikationstjänster som är allmänt tillgängliga. Följaktligen bör de aktuella tillhandahållarna läggas till i 9 kap. 29 § första stycket och 29 b § första stycket genom hänvisning till bestämmelsen där lagringsskyldigheten för tillhandahållarna föreslås regleras (föreslagna 9 kap. 19 a §).

En följd av att tillhandahållarna av kommunikationstjänsterna föreslås omfattas av de nu aktuella reglerna är att dessa omfattas av bestämmelsen som upplyser om att regeringen eller den myndighet som regeringen bestämmer kan meddela närmare föreskrifter om frågor rörande anpassningsskyldigheten samt att undantag får beslutas i enskilda fall (9 kap. 29 § tredje stycket). På motsvarande sätt omfattas tillhandahållarna av bestämmelserna i de övriga styckena i 9 kap. 29 b § som anger att uppgifterna ska ordnas och göras tillgängliga i ett format som gör att de kan verkställas, att tillsynsmyndigheten i enskilda fall får besluta om undantag, samt att regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om hur uppgifterna ska lämnas ut.

7.5 Tystnadsplikt och ersättning

Utkastets förslag: Reglerna om tystnadsplikt för uppgifter om abonnemang, innehållet i ett elektroniskt meddelande, trafikuppgifter och lokaliseringsuppgifter som inte är trafikuppgifter ska även omfatta tillhandahållare av nummeroberoende interpersonella kommunikationstjänster.

För tillhandahållare av nummeroberoende interpersonella kommunikationstjänster ska tystnadsplikten endast gälla vid sådan kommunikation som sker till, från eller inom Sverige samt för lokaliseringsuppgifter som inte är trafikuppgifter och som avser lokalisering i Sverige.

Tillhandahållarna ska omfattas av rätten till ersättning för kostnader som uppstår när uppgifter om abonnemang, innehållet i ett elektroniskt meddelande, trafikuppgifter eller lokaliseringsuppgifter som inte är trafikuppgifter lämnas ut till brottsbekämpande myndigheter.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: De flesta remissinstanserna yttrar sig inte särskilt om utredningens förslag om tystnadsplikt för tillhandahållarna. *Polismyndigheten* för fram att det är mycket angeläget att tillhandahållarna omfattas av reglerna om tystnadsplikt. Även *Tullverket* och *Åklagarmyndigheten* välkomnar förslaget.

Skälen för utkastets förslag

Tystnadsplikt

För att lagrings- och anpassningsskyldigheterna ska utföras på ett korrekt sätt och för att samarbetet mellan tillhandahållarna och myndigheterna ska vara välfungerande finns bestämmelser i lagen om elektronisk kommunikation som reglerar bl.a. tystnadsplikt. Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst får inte obehörigen föra vidare eller utnyttja det som han eller hon i samband med tillhandahållandet har fått del av eller tillgång till (9 kap. 31 § lagen om elektronisk kommunikation). Tystnadsplikt gäller även för användningen av hemliga tvångsmedel och andra liknande åtgärder, såsom förfrågningar om utlämnande av uppgifter om abonnemang, bevarandeföreläggande och inhämtning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (9 kap. 32 § lagen om elektronisk kommunikation). Tystnadsplikten omfattar enligt nuvarande regler inte tillhandahållare av en nummeroberoende interpersonell kommunikationstjänst. En sådan författningsreglerad tystnadsplikt utgör en inskränkning av yttrandefriheten som endast får begränsas genom lag (se avsnitt 6.8).

Reglerna om tystnadsplikt syftar i första hand till att skydda enskildas integritet. Behovet av ett sådant skydd är lika starkt oavsett vilken teknisk utformning kommunikationstjänsten har. Tystnadsplikten är också, tillsammans med anpassningsskyldigheten, avgörande för att hemliga tvångsmedel ska kunna verkställas på ett säkert och ändamålsenligt sätt. Som utredningen för fram skulle det utan tystnadsplikt inte finnas något rättsligt hinder mot att uppgifter om användningen av hemliga tvångsmedel röjs. Ett röjande skulle kunna innebära skada för enskilda och för den brottsbekämpande verksamheten. Det är konsekvent att låta reglerna om tystnadsplikt gälla också för de aktuella tillhandahållarna, vilket ett antal remissinstanser också understryker betydelsen av. Reglerna om tystnadsplikt bör därför gälla även för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster. Detta får anses vara proportionerlig och uppfylla de krav som gäller för begränsningar i yttrandefriheten enligt regeringsformen och Europakonventionen. Tystnadsplikten bör regleras genom att nuvarande undantag i 9 kap. 31 § första stycket lagen om elektronisk kommunikation tas bort. Som en följd av det kommer tillhandahållarna även att omfattas av tystnadsplikten för uppgifter som hänför sig till bl.a. användningen av hemliga tvångsmedel i 9 kap. 32 §.

Tillhandahållarna erbjuder i regel sina tjänster i många olika länder. I enlighet med utredningens förslag bör tystnadsplikten avgränsas på samma sätt som lagringsskyldigheten, dvs. att den bör gälla för sådan kommunikation som sker till, från eller inom Sverige. Vad gäller lokaliseringsuppgifter som inte är trafikuppgifter bör avgränsningen ske till uppgifter om lokalisering i Sverige. Detta bör regleras i ett nytt andra stycke i 9 kap. 31 § lagen om elektronisk kommunikation.

Till skillnad från lagringsskyldigheten bör tystnadsplikten gälla samtliga tillhandahållare av nummeroberoende interpersonella kommunikationstjänster och inte enbart allmänt tillgängliga sådana. Detta eftersom även kommunikation genom tjänster som inte är allmänna bör omfattas av det skydd för enskildas personliga integritet som tystnadsplikten innebär.

Ersättning

Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § har rätt till ersättning för kostnader som uppstår när uppgifter lämnas ut till brottsbekämpande myndigheter (9 kap. 29 a § lagen om elektronisk kommunikation). Bestämmelsen är kopplad till de uppgifter som avses i regleringen om tystnadsplikt i 9 kap. 31 § första stycket. Ersättningsregleringen utgår från en kostnadsfördelning mellan det allmänna och tillhandahållarna som innebär att tillhandahållarna står för kostnaderna för anpassning, drift och underhåll och de brottsbekämpande myndigheterna står för kostnader som hänför sig till utlämnanden av uppgifter i enskilda ärenden (prop. 2021/22:183 s. 57–60).

Utredningen föreslår att tillhandahållare av nummeroberoende interpersonella kommunikationstjänster också ska ha rätt till ersättning när de lämnar ut uppgifter. Eftersom tillhandahållarna föreslås omfattas av lagringsskyldighet och vissa skyldigheter när det gäller brottsbekämpande myndigheters åtkomst till uppgifter om elektronisk kommunikation bör de också omfattas av reglerna om ersättning. I enlighet med utredningens förslag bör förslaget genomföras genom att 9 kap. 29 a § ändras så att den hänvisar till kretsen av lagringsskyldiga i stället för till de som bedriver anmälningspliktig verksamhet.

I 9 kap. 29 a § andra stycket regleras separat att lokaliseringsuppgifter som inte är trafikuppgifter omfattas av rätten till ersättning. I och med att dessa uppgifter i avsnitt 6.8 föreslås läggas till i bestämmelsen om tystnadsplikt, som första stycket hänvisar till, behövs inte längre regleringen i andra stycket.

7.6 Skyldigheten att lämna ut uppgifter till myndigheter och alarmeringscentraler

Utkastets förslag: Skyldigheten att lämna ut uppgifter om abonnemang och andra uppgifter som angår ett särskilt elektroniskt meddelande till myndigheter och alarmeringscentraler ska gälla även för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: De flesta remissinstanserna yttrar sig inte särskilt om utredningens förslag. *Skatteverket* för fram att det är positivt att myndigheten kommer att kunna begära uppgifter om abonnemang från nummeroberoende interpersonella kommunikationstjänster.

Skälen för utkastets förslag: Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst som inte är en nummeroberoende interpersonell kommunikationstjänst är skyldig att på begäran lämna ut

uppgifter om abonnemang, och i vissa fall trafikuppgifter, till brottsbekämpande myndigheter och vissa andra myndigheter samt alarmeringscentraler (9 kap. 33 § lagen om elektronisk kommunikation).

Tillhandahållare av elektroniska kommunikationstjänster omfattas av den gällande skyldigheten att lämna ut uppgifter om abonnemang till brottsbekämpande myndigheter. Brottsbekämpande myndigheters behov av uppgifter om abonnemang är samtidigt lika stort oavsett vilken utformning en viss elektronisk kommunikationstjänst har. En skyldighet för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster att lämna ut sådana uppgifter innebär i sig inte någon större inskränkning i den enskildes fri- och rättigheter än vad en sådan skyldighet innebär för andra tillhandahållare. Skyldigheten att lämna ut uppgifter om abonnemang till brottsbekämpande myndigheter som finns i 9 kap. 33 § första stycket 2 bör därför i enlighet med utredningens förslag omfatta även tillhandahållare av nummeroberoende interpersonella kommunikationstjänster.

Uppgifter om abonnemang ska även lämnas ut till andra myndigheter för andra syften än brottsbekämpning (9 kap. 33 § första stycket 1). I likhet med brottsbekämpande myndigheter har även de myndigheterna ett behov av uppgifterna oavsett vem som tillhandahåller kommunikationstjänsten. Det finns inte heller något som tyder på att utlämnande av uppgifter om abonnemang till andra myndigheter än de brottsbekämpande skulle innebära ett större integritetsintrång enbart för att uppgifterna kommer från en nummeroberoende interpersonell kommunikationstjänst. Som *Skatteverket* anger är det positivt för myndigheterna att kunna få del av uppgifter från dessa kommunikationstjänster. Skyldigheten att lämna ut uppgifter om abonnemang även enligt 9 kap. 33 § första stycket 1 bör därför omfatta tillhandahållare av nummeroberoende interpersonella kommunikationstjänster.

Förutom uppgifter om abonnemang ska en annan uppgift som angår ett särskilt meddelande (trafikuppgift enligt förslaget i avsnitt 5.3) lämnas till en regional alarmeringscentral (9 kap. 33 § första stycket 3). Motsvarande uppgifter samt uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits ska lämnas till Polismyndigheten, om myndigheten bedömer att uppgiften behövs i samband med efterforskning av personer som har försvunnit under sådana omständigheter att det kan antas att det då fanns eller fortfarande finns fara för deras liv eller allvarlig risk för deras hälsa (9 kap. 33 § första stycket 4). Utlämningsskyldigheten enligt de nu nämnda bestämmelserna gäller alltså även andra uppgifter än uppgifter om abonnemang, i syfte att kunna säkra utförandet av viktiga samhällsuppgifter. Behovet av uppgifterna är lika stort oavsett från vilken kommunikationstjänst de härstammar. Inte heller bör intrånget i den personliga integriteten skilja sig åt enbart på grund av hur kommunikationstjänsten är uppbyggd. Det är proportionerligt att inkludera tillhandahållare av nummeroberoende interpersonella kommunikationstjänster även i skyldigheterna att lämna ut uppgifter till regionala alarmeringscentraler samt till Polismyndigheten i syfte att leta efter försvunna personer.

Slutligen finns en skyldighet att lämna ut uppgifter om vilka övriga tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster som har deltagit vid överföringen av ett meddelande som omfattas av ett bevarandeföreläggande enligt 27 kap. 16 § rättegångsbalken till den myndighet

som meddelat föreläggandet (9 kap. 33 § första stycket 5). Skyldigheten infördes i samband med Sveriges tillträde till Europarådets konvention om it-relaterad brottslighet (Budapestkonventionen). Utredningen gör bedömningen att nummeroberoende interpersonella kommunikationstjänster, som redan med nuvarande regler kan bli föremål för ett bevarandeföreläggande, bör omfattas av skyldigheten att lämna information om vilka tillhandahållare som har deltagit vid överföringen av ett meddelade. En sådan skyldighet kan vara av vikt för de brottsbekämpande myndigheterna, eftersom de aktuella kommunikationstjänsterna ofta inte ansvarar för själva överföringen av meddelandet. Tillhandahållare av nummeroberoende interpersonella kommunikationstjänster bör därför omfattas av skyldigheten att lämna information om vilka eventuella övriga tillhandahållare som deltagit vid överföringen av ett meddelande. Mot bakgrund av att ett bevarandeföreläggande kan riktas mot vem som helst bör skyldigheten i enlighet med utredningens förslag omfatta alla tillhandahållare av nummeroberoende interpersonella kommunikationstjänster och inte bara tillhandahållare av allmänt tillgängliga sådana.

Sammanfattningsvis föreslås att samtliga skyldigheter att lämna ut uppgifter enligt 9 kap. 33 § bör gälla även för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster. Det innebär också att sådana tillhandahållare omfattas av den särskilda regeln om ersättning i 9 kap. 33 § andra stycket. I enlighet med vad utredningen anger gäller utlämningsskyldigheten enbart sådana uppgifter som tillhandahållaren får del av eller annars har tillgång till.

7.7 Skyddande och bevarande av uppgifter

Utkastets förslag: Tillhandahållare av allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster ska omfattas av kraven på att vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda lagrade uppgifter vid behandling.

Tillhandahållarna ska vidta sådana åtgärder också om de har förelagts att bevara en viss lagrad uppgift.

Utredningens förslag överensstämmer i huvudsak med utkastets. Utredningen föreslår en annan lagteknisk utformning.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt om förslaget.

Skälen för utkastets förslag: För marknadens aktörer och för samhället i stort är det centralt med ett tillförlitligt och säkert utbyte av information via elektroniska kommunikationsnät och elektroniska kommunikationstjänster. Det finns flera krav på säkerhet i nät och tjänster som tillhandahållare av allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster redan omfattas av. Det gäller exempelvis kraven på att vidta tekniska och organisatoriska åtgärder för att på ett lämpligt sätt hantera risker som hotar säkerheten i nät och tjänster och kraven på att rapportera säkerhetsincidenter till tillsynsmyndigheten (8 kap. 1 och 3 §§ lagen om elektronisk kommunikation). Tillhandahållarna ska också bl.a. vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av tjänsten skyddas (8 kap. 6 § samma lag).

Den som är skyldig att lagra uppgifter enligt lagen om elektronisk kommunikation ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling (8 kap. 5 § första stycket lagen om elektronisk kommunikation). Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § lagen om elektronisk kommunikation och som har förelagts enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift ska även avseende den uppgiften vidta sådana åtgärder (8 kap. 5 § andra stycket lagen om elektronisk kommunikation). Kraven omfattar enligt nuvarande ordning inte tillhandahållare av nummeroberoende interpersonella kommunikationstjänster.

Skyldigheten att vidta tekniska och organisatoriska åtgärder till skydd för uppgifter som lagras är en viktig förutsättning för ett säkert genomförande av lagringsskyldigheten. I och med att tillhandahållare av allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster föreslås omfattas av lagringsskyldighet (avsnitt 7.2) bör de också omfattas av skyldigheten i 8 kap. 5 § första stycket att vida de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna. Tillhandahållarna bör därför läggas till i den nämnda bestämmelsen genom att en hänvisning görs till den föreslagna 9 kap. 19 a § där lagringsskyldigheten regleras. Förslaget har samma innebörd som utredningens förslag, men har en annan lagteknisk utformning, vilket har att göra med att förslaget om riktad lagring inte behandlas inom ramen för detta lagstiftningsprojekt.

Vad gäller skyldigheten anknuten till bevarandeföreläggande i 8 kap. 5 § andra stycket kan konstateras att ett bevarandeföreläggande redan idag kan riktas mot en tillhandahållare av de aktuella kommunikationstjänsterna. I enlighet med utredningens bedömning bör tillhandahållarna även omfattas av kraven på att vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda uppgifter som omfattas av ett sådant föreläggande. Utredningens föreslagna lagtext kan tolkas som att samtliga som är föremål för bevarandeföreläggande ska vidta sådana åtgärder som nämns i bestämmelsen, vilket skulle kunna innebära att bestämmelsen får en större räckvidd än endast utvidgningen till de nu aktuella tillhandahållarna. Lagtexten bör därför utformas på ett något annat sätt än vad utredningen föreslår.

8 Sanktionsavgifter

Utkastets förslag: Tillsynsmyndigheten ska få besluta att ta ut en sanktionsavgift av den som inte lagrar uppgifter om elektronisk kommunikation i enlighet med bestämmelserna om lagringsskyldighet och lagringstid i lagen om elektronisk kommunikation och föreskrifter som har meddelats i anslutning till de bestämmelserna.

Bestämmelsen om sanktionsavgift vid bristande lagring ska omfatta tillhandahållare av nummeroberoende interpersonella kommunikationstjänster.

Möjligheten att ta ut en sanktionsavgift vid bristande uppfyllelse av anpassningsskyldigheten ska gälla även i förhållande till inhämtningslagen.

Utredningens förslag överensstämmer med utkastets.

Remissinstanserna: *TechSverige*, *Telenor Sverige AB* och *Telia Sverige AB* avstyrker förslaget och för fram att uttagande av sanktionsavgift kräver tydlighet, vilket de inte anser att förslagen om lagringsskyldighet uppfyller. Bolagen anser vidare att den möjlighet som finns för tillsynsmyndigheten att bedriva tillsyn och meddela förelägganden torde vara tillräcklig för att säkerställa efterlevnad av de nya reglerna. *Telenor Sverige AB* menar att sanktioner inte heller är motiverade utifrån tidigare erfarenheter av tillämpning av de existerande skyldigheterna för telekomoperatörer, vilka har gjort stora ansträngningar för att på ett effektivt sätt bistå de brottsutredande myndigheterna med lagrade uppgifter. Bolaget menar vidare att då skyldigheten nu blir mer komplex och svårare att efterleva är det direkt olämpligt att förena den med hot om sanktionsavgift. *Hi3G Access AB* avstyrker förslaget om sanktionsavgift ifall förslaget om geografisk riktad lagring genomförs.

Skälen för utkastets förslag

Sanktionsavgifter enligt lagen om elektronisk kommunikation

Tillsynsmyndigheten ska besluta att ta ut en sanktionsavgift av tillhandahållare av vissa elektroniska kommunikationstjänster om de inte följer de skyldigheter som anges i 12 kap. 1 § första stycket lagen om elektronisk kommunikation. Det nuvarande sanktionsavgiftssystemet infördes vid genomförandet av e-kodexdirektivet, se propositionen Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation (prop. 2021/22:136 s. 355–365). Sanktionsavgifterna avser överträdelser av de krav som följer av lagen, i föreskrifter som har meddelats i anslutning till lagen och i genomförandeakter som Europeiska kommissionen har meddelat. Det handlar bl.a. om krav på olika former av skydds- och säkerhetsåtgärder, rapportering av säkerhetsincidenter, information till abonnenter samt anpassningsskyldigheten och skyldigheten att lämna ut uppgifter. Sanktionsavgift beslutas av tillsynsmyndigheten.

Utredningen föreslår att det ska införas en möjlighet att meddela sanktionsavgift vid bristande efterlevnad i ett antal ytterligare fall. Det gäller om uppgifter inte lagras i enlighet med bestämmelserna om lagringsskyldighet och lagringstid samt föreskrifter som har meddelats i anslutning till dessa. Sanktionsavgift föreslås vidare kunna tas ut av tillhandahållare av allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster. Därutöver föreslås att det ska förtydligas att sanktionsavgift kan tas ut i förhållande till anpassningsskyldigheten även vad gäller inhämtning enligt inhämtningslagen.

Sanktionsavgift vid bristande uppfyllelse av lagringsskyldigheten

Det finns för närvarande ingen möjlighet att ta ut sanktionsavgift vid bristande uppfyllelse av lagringsskyldigheten i 9 kap. 19 och 22 §§ lagen om elektronisk kommunikation. Utredningen för fram att en bristande efterlevnad av lagringsskyldigheten kan få stora konsekvenser för den brottsbekämpande verksamheten. Utan tillgång till uppgifter som omfattas av lagringsskyldigheten blir det svårare för brottsbekämpande myndigheter att utreda vissa typer av brott. I andra fall kan för-

undersökningar behöva läggas ned i brist på bevis. Det är viktigt för det allmänna att det finns starka incitament att följa lagringsskyldigheten. Att uppgifter lagras är även av betydelse för underrättelseverksamheten. För säkerställandet av lagringsskyldighetens efterlevnad kan det, till skillnad mot vad *TechSverige*, *Telenor Sverige AB* och *Telia Sverige AB* för fram, inte anses vara tillräckligt med möjligheten för tillsynsmyndigheten att genom förelägganden förenade med vite ålägga tillhandahållare att fullgöra sin lagringsskyldighet. I det sammanhanget ska beaktas att det enligt utredningen totalt sett finns ett relativt stort antal aktörer på marknaden och att marknaden är föränderlig.

Lagringsskyldigheten är en viktig förutsättning för det brottsbekämpande arbetet. I enlighet med utgångspunkterna för lagstiftningsärendet är det angeläget med så goda förutsättningar som möjligt för att kunna förebygga, förhindra, utreda och lagföra brott. Förslagen om lagringsskyldighet bedöms, till skillnad från vad *TechSverige*, *Telenor Sverige AB* och *Telia Sverige AB* anför, uppfylla de krav på tydlighet som krävs för att reglerna ska kunna omfattas av möjligheten att ta ut sanktionsavgift. Beträffande tolkningen och tillämpningen finns möjlighet för regeringen eller den myndighet som regeringen bestämmer att meddela närmare föreskrifter. En sanktionsavgift bör därför kunna tas ut av den som inte lagrar uppgift enligt bestämmelserna i lagen om elektronisk kommunikation och föreskrifter som har meddelats i anslutning till lagringsbestämmelserna. Förslaget innebär att det kommer att vara möjligt för tillsynsmyndigheten att ta ut sanktionsavgift vid bristande uppfyllelse av bestämmelserna om lagring och lagringstid (9 kap. 19 och 22 §§ samt föreslagna 9 kap. 19 a, 19 b och 22 a §§).

Sanktionsavgift för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster

Flera av de regler i lagen om elektronisk kommunikation som omfattas av bestämmelsen om sanktionsavgift träffar redan enligt nuvarande regler tillhandahållare av nummeroberoende interpersonella kommunikationstjänster. Exempelvis ska sanktionsavgift tas ut från en sådan tillhandahållare om den inte tillhandahåller en sammanfattning av ett avtal med en konsument (12 kap. 1 § första stycket 1), inte vidtar åtgärder för att hantera risker som hotar säkerheten i nät och tjänster (12 kap. 1 § första stycket 4) eller inte rapporterar om säkerhetsincidenter (12 kap. 1 § första stycket 5).

Den föreslagna lagringsskyldigheten för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster i 9 kap. 19 a § (avsnitt 7.2) bör åtföljas av samma regler om sanktionsavgift som föreslås gälla för andra lagringsskyldiga. Den tillhandahållare som inte uppfyller sin lagringsskyldighet bör således kunna bli föremål för sanktionsavgift. Det gäller dels bristande efterlevnad av lagringsskyldigheten avseende uppgifter om abonnemang (9 kap. 19 a §), dels om tillhandahållaren inte lagrar uppgifter enligt ett beslut om nationell säkerhetslagring (9 kap. 19 b §). Det gäller också vid bristande uppfyllelse av bestämmelsen om lagringstid i 9 kap. 22 och 22 a §§.

Som en följd av övriga förslag i detta lagstiftningsärende kommer tillhandahållare av nummeroberoende interpersonella kommunikationstjänster kunna bli föremål för sanktionsavgift även i andra situationer. Sanktionsavgift kommer att aktualiseras om de inte vidtar skyddsåtgärder enligt 8 kap. 5 §, om de inte iakttar

anpassningsskyldigheten, om de inte ordnar uppgifter och gör dem tillgängliga i ett format som gör att de enkelt kan tas om hand samt om de inte lämnar ut en uppgift i enlighet med 9 kap. 33 § (12 kap 1 § första stycket 7, 12, 13 och 15).

Sanktionsavgift i förhållande till inhämtning enligt inhämtningslagen

Den som inte iakttar anpassningsskyldigheten i 9 kap. 29 § lagen om elektronisk kommunikation kan bli föremål för sanktionsavgift enligt 12 kap. 1 § första stycket 12. I avsnitt 5.2 föreslås att anpassningsskyldigheten i 9 kap. 29 § uttryckligen ska omfatta även inhämtning enligt inhämtningslagen. Med anledning av det förslaget bör det, i enlighet med utredningens förslag, göras ett tillägg i bestämmelsen om sanktionsavgift som innebär att sanktionsbestämmelsen även omfattar inhämtning enligt inhämtningslagen. Bestämmelsen avser samtliga aktörer som omfattas av anpassningsskyldigheten.

9 Ikraftträdande- och övergångsbestämmelser

Utkastets förslag: Lagändringarna ska träda i kraft den 1 mars 2026.
De ändrade bestämmelserna om sanktionsavgift ska tillämpas endast på överträdelser som har ägt rum efter det att de nya bestämmelserna har trätt i kraft.

Utredningens förslag stämmer delvis överens med utkastets. Utredningen föreslår en övergångsbestämmelse för trafik- och lokaliseringsuppgifter som lagrats innan de nya reglerna träder i kraft. Utredningen föreslår inte någon övergångsbestämmelse för de ändrade bestämmelserna om sanktionsavgift.

Remissinstanserna: Ingen remissinstans yttrar sig särskilt om förslaget.

Skälen för utkastets förslag: Lagändringarna bör träda i kraft så snart som möjligt. Som utredningen för fram behöver tillhandahållarna ha tillräckligt med tid för att göra de ändringar i it-stöd som krävs med anledning av förslagen om bl.a. lagringsskyldighet. Lagändringarna bör kunna träda i kraft den 1 mars 2026.

Utredningen föreslår en övergångsbestämmelse rörande lagring av trafik- och lokaliseringsuppgifter. Förslaget avser det förslag om riktad lagring som inte behandlas inom ramen för detta lagstiftningsprojekt. Någon sådan övergångsbestämmelse bör därför inte införas.

Av 2 kap. 10 § första stycket regeringsformen framgår att bestämmelser om straff eller annan brottspåföljd samt förverkande och annan särskild rättsverkan av brott inte får ges retroaktiv verkan. De ändringar som föreslås i reglerna om sanktionsavgifter har en straffliknande karaktär och förbudet mot retroaktiv strafflag får därmed anses tillämpligt även på dem. Sanktionsavgift enligt de förändrade regler som nu föreslås bör därför endast kunna tas ut för överträdelser som har begåtts efter ändringarnas ikraftträdande. Det bör införas en övergångsbestämmelse om detta.

10 Konsekvenser

10.1 Samhällspolitiska konsekvenser

Utkastets bedömning: Förslagen om att uppgifter om abonnemang ska lagras under längre tid, om den nationella säkerhetslagringen och om att tillhandahållare av allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster ska omfattas av lagringsskyldigheten ökar risken för intrång i den personliga integriteten. Den ökade risken för integritetsintrång bedöms dock vara proportionerlig och nödvändig för förslagens syften.

Lagring av uppgifter om abonnemang, lagringsskyldighet för tillhandahållare av allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster, nationell säkerhetslagring och modernisering av anpassningsskyldigheten kommer att vara positivt för brottsbekämpningen, eftersom de brottsbekämpande myndigheterna ges bättre förutsättningar att bekämpa brott.

Utredningens bedömning överensstämmer med utkastets.

Remissinstanserna: Merparten av remissinstanserna yttrar sig inte särskilt i denna del. *ECPAT Sverige* anser att behovet och nyttan av förslagen motiverar att en inskränkning görs i enskildas fri- och rättigheter. *Integritetsskyddsmyndigheten* har förståelse för de brottsbekämpande myndigheternas behov av tillgång till elektronisk information för att förebygga och utreda grov brottslighet. Åtgärderna behöver dock balanseras mot enskildas grundläggande rättigheter. *Internetstiftelsen* ser positivt på att en översyn görs av befintliga datalagringsregler, men ser svårigheter med flera av förslagen utifrån ett proportionalitets- och rättssäkerhetsperspektiv. *Dataskydd.net Sverige*, *Föreningen för Digitala fri- och rättigheter* och *ISOC-SE* anser att förslagen har stora brister i analysen av konsekvenser för informationsfriheten, den personliga integriteten och möjligheterna att kommunicera på ett säkert sätt. *Institutet för mänskliga rättigheter* för fram liknande synpunkter, särskilt i förhållande till skyddet för privat- och familjeliv och den personliga integriteten. Även *Riksdagens ombudsmän (JO)* och *Svenska Journalistförbundet* ser risker för den personliga integriteten. *Stockholms universitet (Juridiska fakulteten)* menar att utredningen inte har tillräckligt underlag för att avgöra om åtgärderna är effektiva för syftet att bekämpa hot mot den nationella säkerheten och grov brottslighet. Även *Sveriges advokatsamfund* ifrågasätter åtgärdernas effektivitet och menar att förslagen innebär risker ur ett integritets- och rättssäkerhetsperspektiv som behövt analyseras mer, bl.a. i vilken utsträckning förslagen kan leda till att enskilda upplever sig övervakade. Samfundet, som i och för sig har förståelse för att kraftfulla åtgärder behövs, menar att förslagen innebär ökade ingrepp i den personliga integriteten för en större krets än vad som krävs för ändamålet. Det vore i stället mer effektivt att ge de brottsbekämpande myndigheterna mer resurser och att omprioritera deras verksamhet. Vidare förs fram att informationssäkerhetsaspekter behöver beaktas och konsekvenserna av vissa EU-rättsakter utredas. Därutöver påtalas att skyddet mot obehörig åtkomst eller andra säkerhetsåtgärder kan variera och att säkerheten och tillförlitligheten därmed kommer att vara olika beträffande de uppgifter som lagras

hos olika aktörer. *Tidningsutgivarna (TU)* saknar ett resonemang om användningen av överskottsinformation. *Myndigheten för samhällsskydd och beredskap* anser att informationssäkerhetsaspekter och riskhanteringsåtgärder bör beaktas särskilt, exempelvis genom upprättande av en kravförteckning gällande skyddsnivåer. *TU* gör gällande att förslagen om att ta med nummeroberoende interpersonella kommunikationstjänster i regelverket skulle innebära en betydande risk för att meddelare i viktiga frågor av allmänintresse inte vågar kontakta medier. *Journalistförbundet* framför liknande synpunkter. *Kommerskollegium* lyfter frågan om anmälningsplikt enligt anmälningsdirektivet för tekniska föreskrifter.

Skälen för utkastets bedömning

Konsekvenser för den personliga integriteten

I lagrådsremissen lämnas flera förslag som rör skyldigheten att lagra elektronisk kommunikation. Det föreslås att uppgifter om abonnemang ska lagras under en längre tid (avsnitt 5.1), att det ska införas en möjlighet till mer omfattande lagringsskyldighet vid ett allvarligt hot mot nationell säkerhet (avsnitt 6.2) och att tillhandahållare av allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster ska omfattas av lagringsskyldighet (avsnitt 7.2).

När det gäller uppgifter om abonnemang föreslås att lagringstiden utökas till ett år. Enligt nuvarande regelverk är lagringstiden som huvudregel mellan sex och tio månader, bl.a. beroende på om uppgifterna behandlas vid mobil nätanslutningspunkt eller vid internetåtkomst. Tillhandahållare av allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster föreslås bli skyldiga att lagra uppgifter om abonnemang i ett år. Vid nationell säkerhetslagring föreslås lagringstiden vara två år för uppgifter om abonnemang och trafikuppgifter samt ett år för lokaliseringsuppgifter som inte är trafikuppgifter. Lokaliseringsuppgifter som inte är trafikuppgifter är inte föremål för lagring i dag. Med sådana uppgifter avses uppgifter om position som genererats i en användares utrustning oberoende av att den aktivt används för kommunikation, t.ex. gps-positioner.

På ett övergripande plan kan konstateras att uppgifter om abonnemang, typiskt sett, är mindre integritetskänsliga än t.ex. trafik- och lokaliseringsuppgifter. Uppgifter om rörelsemönster är däremot särskilt känsliga ur ett integritetsperspektiv. Förslag om en lagringsskyldighet för sådana uppgifter ökar därför risken för integritetsintrång. Att fler uppgifter lagras, som en följd av en större krets av lagringsskyldiga tillhandahållare och att fler uppgiftskategorier kan bli föremål för lagring, innebär också att risken för integritetsintrång ökar. Att lagringstiderna förlängs medför generellt sett en ökad risk för integritetsintrång. Fler uppgifter kan också, potentiellt, komma till användning under längre tid. Detta innebär, vid en sammantagen bedömning av de förslag som lämnas om utökad skyldighet att lagra elektronisk kommunikation, att riskerna för intrång i den personliga integriteten kommer att öka. Som *Sveriges advokatsamfund* för fram kan dessutom fler personer känna sig övervakade. Det behöver följaktligen, vilket ett flertal remissinstanser påtalar, göras en noggrann analys av de risker som lagringen kan förväntas medföra för den personliga integriteten.

Enligt 2 kap. 6 § andra stycket regeringsformen 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. Flera av de åtgärder som föreslås träffas av den bestämmelsen (jfr propositionen En reformerad grundlag [prop. 2009/10:80] s. 182–185 och 250).

Begränsningar i skyddet mot betydande intrång får ske genom lag enligt de förutsättningar som anges i 2 kap. 20–22 §§ regeringsformen. Det innebär bl.a. att en begränsning är tillåten endast under förutsättning att den tillgodoser ändamål som är godtagbara i ett demokratiskt samhälle. Det innebär också att en begränsning inte får 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, eller göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning.

I bedömningen av om begränsningen av skyddet för den personliga integriteten som lagförslagen innebär är proportionerligt får, i likhet med vad utredningen för fram, de konsekvenser som förslagen kan förväntas medföra vägas mot den nytta som förslagen kan förväntas medföra. I detta avseende har teknik- och samhällsutvecklingen med en ökad brottslighet som förslagen tar sikte på betydelse. En stor andel av befolkningen använder sig numera av kommunikationslösningar som inte omfattas av datalagring, vilket medför ett ökat behov av förändrade verktyg för de brottsbekämpande myndigheterna för att effektivt kunna bekämpa brottslighet som innefattar hot mot den nationella säkerheten och annan grov brottslighet.

Förslagen att nya tillhandahållare ska omfattas av lagringsskyldigheten innebär anpassningar till teknikutvecklingen. Det innebär även ett återställande av en möjlighet att ta del av kommunikation som de brottsbekämpande myndigheterna tidigare har haft. Fler brott mot enskilda kan komma att klaras upp och också leda till att fler brottsoffer får upprättelse. Förslagen förväntas alltså leda till en ökad rättstrygghet för enskilda.

Inom ramen för proportionalitetsbedömningen bör dessutom konstateras att det finns strikta regler som syftar till att skydda den personliga integriteten i såväl tillhandahållarnas som de brottsbekämpande myndigheternas verksamhet. Bestämmelser om behandling av personuppgifter finns förutom i lagen om elektronisk kommunikation (se främst 8 och 9 kap.) även i 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) och i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning samt i föreskrifter som har meddelats i anslutning till den lagen (1 kap. 5 § LEK). För den behandling som sker hos myndigheter finns bestämmelser i Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF och i brottsdatalagen (2018:1177).

Vid bedömningen av om den begränsning av skyddet mot intrång som lagförslagen medför är berättigad utifrån 2 kap. 21 § regeringsformen bör alltså det regelverk som redan finns på plats beaktas. Vidare kan, när det gäller abonne-

mangsuppgifter, som exempel nämnas att uppgifterna omfattas av tystnadsplikten och endast får lämnas ut för vissa författningsreglerade ändamål (9 kap. 31 och 33 §§ lagen om elektronisk kommunikation). För den nationella säkerhetslagringen föreslås olika rättssäkerhetsgarantier, som att ett ombud ska bevaka den enskildes rätt och att besluten ska underställas Försvarsunderrättelsedomstolen. Ett beslut om lagring ska vidare, vid ett tillräckligt allvarligt hot mot den nationella säkerheten, begränsas till vad som är absolut nödvändigt för syftet med lagringen. Tillgång till uppgifter som lagrats för den nationella säkerheten får därtill endast medges för att bekämpa brottslighet som utgör ett hot mot den nationella säkerheten. Det innebär att sådana uppgifter inte får användas för att bekämpa annan grov brottslighet. Vidare föreslås regler om sekretess och tystnadsplikt, vilket kommer att begränsa de lagrade uppgifternas spridning.

Förändringar av regelverket kring datalagring innebär inte att de brottsbekämpande myndigheterna automatiskt får tillgång till de uppgifter som lagras. Lagringen skapar i stället förutsättningar för en effektiv framtida användning av hemliga tvångsmedel. I förhållande till bestämmelserna om hemliga tvångsmedel finns det skäl att särskilt lyfta att regelverket omgärdas av rättssäkerhetsgarantier och kontrollmekanismer som säkerställer att tillståndsgivningen är rättssäker och att intrången i den personliga integriteten inte blir större än vad som kan godtas enligt regeringsformen, Europakonventionen och EU:s rättighetsstadga (se bl.a. de bedömningar som görs i prop. 2022/23:126 s.80 f). Vad ett flertal remissinstanser för fram om förslagens konsekvenser för informationsfriheten och dess förhållande till skyddet för privat- och familjeliv och andra rättssäkerhetsaspekter får, genom befintligt regelverk och de förslag som nu lämnas, anses vara tillgodosedda på ett godtagbart sätt. Beträffande den synpunkt som *TU* för fram om användningen av överskottsinformation kan vidare konstateras att de förslag som lämnas i huvudsak avser lagring av uppgifter. Frågor om överskottsinformation aktualiseras först när tillgång ges till lagrade uppgifter, t.ex. vid ett tillstånd till hemliga tvångsmedel. Regelverket om överskottsinformation ändrades nyligen och påverkas inte av de förslag som nu lämnas (jfr prop. 2022/23:126 s. 171 f).

Utredningen för vidare fram att den tekniska utvecklingen har lett till att lokaliseringsuppgifter som inte är trafikuppgifter redan i dag lagras av operatörerna. Exempelvis lämnar en mobiltelefon vid samtal eller datatrafik kontinuerlig uppgift om plats när den används i ett traditionellt telenät. Det kan även, vilket gör sig gällande för samtliga uppgiftskategorier, konstateras att tillhandahållarna bara kommer att vara skyldiga att bevara uppgifter som redan förekommer i deras verksamhet. De har alltså inte någon skyldighet att modifiera sina tjänster i syfte att få tillgång till uppgifter som inte redan genereras eller behandlas i verksamheten. Om en användare exempelvis stänger av funktioner i sin utrustning som leder till att tillhandahållarna inte får del av vissa uppgifter, såsom gps-positioner, kommer sådana uppgifter heller inte att bli föremål för lagring. Att enskilda har inflytande över vilka uppgifter som blir föremål för lagring, i vart fall när teknisk utrustning används som möjliggör avstängning av nämnda funktioner, minskar det integritetsintrång som aktualiseras med anledning av förslagen gällande lagring av lokaliseringsuppgifter som inte är trafikuppgifter.

Vid en sammantagen bedömning konstateras att begränsningen av regeringsformens skydd mot intrång i den personliga integriteten görs för att tillgodose

ändamål – främst intresset av en effektiv brottsbekämpning – som är godtagbara i ett demokratiskt samhälle. Begränsningen kan vidare inte anses gå utöver vad som är nödvändigt med hänsyn till dessa ändamål och utgör inte ett hot mot den fria åsiktsbildningen. Som redogjorts för i bl.a. avsnitt 6.1 och 7.1–3 bedöms den personuppgiftsbehandling som förslagen aktualiserar vidare utgöra en proportionerlig inskränkning av det skydd för den personliga integriteten som kommer till uttryck i Europakonventionen och EU:s rättighetsstadga.

Det finns därför goda skäl för de förslag som lämnas. Den ökade risken för integritetsintrång bedöms vara nödvändig och proportionerlig för förslagens syften. Den samlade bedömningen är alltså att förslagen är proportionerliga i fråga om enskildas personliga integritet.

Konsekvenser för det brottsbekämpande arbetet

Förslagen förväntas, som de brottsbekämpande myndigheterna och bl.a. *Brottsoffermyndigheten*, *Brottsofferjouren*, *ECPAT Sverige* och *Helsingborgs tingsrätt* framhåller, leda till bättre förutsättningar för det brottsbekämpande arbetet i flera avseenden. De kan även förväntas ha betydelse i underrättelseverksamheten. Uppgifter om abonnemang kommer att lagras under längre tid och anpassningsskyldigheten kommer att bli tydligare (avsnitt 5). Vid ett allvarligt hot mot nationell säkerhet kommer det finnas möjlighet till en mer omfattande lagringsskyldighet, såväl innehållsmässigt som tidsmässigt (avsnitt 6). Tillhandahållare av allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster kommer omfattas av ett antal skyldigheter (avsnitt 7). Det gäller bl.a. skyldighet att lagra uppgifter om abonnemang och skyldigheten att anpassa sin verksamhet så att beslut om olika tvångsmedel kan verkställas. Även förslaget om sanktionsavgifter kan väntas leda till bättre efterlevnad och därmed förbättra förutsättningarna för det brottsbekämpande arbetet (avsnitt 8).

Förslagen medför inte några förändringar i reglerna om hemliga tvångsmedel. Däremot utökas det praktiska tillämpningsområdet för de hemliga tvångsmedlen eftersom de brottsbekämpande myndigheterna, genom inhämtning av de uppgifter som har lagrats, får tillgång till ett bättre underlag för brottsbekämpningen. Detta innebär att de brottsbekämpande myndigheternas verktyg blir mer effektiva i arbetet med att förebygga, förhindra, upptäcka, utreda och lagföra allvarliga brott.

Förslagen kan väntas få betydelse för alla led i den brottsbekämpande verksamheten. Vad gäller begångna brott kan förslagen förväntas förbättra förutsättningarna för utredning av samtliga de brott som hemlig avlyssning och hemlig övervakning av elektronisk kommunikation kan användas mot. Även avseende andra brott kan det förväntas att förutsättningarna för en effektiv utredning förbättras, som en följd av framför allt förslagen om längre lagringstid för abonnemangsuppgifter och att tillhandahållare av nummeroberoende interpersonella kommunikationstjänster ska omfattas av skyldigheten att lagra och lämna ut abonnemangsuppgifter. Det kan till exempel vara fråga bedrägerier som begås på nätet.

Det finns ett stort behov av att få tillgång till elektronisk kommunikation, inte minst i arbetet mot att bekämpa den organiserade brottsligheten. Det har särskilt uppmärksammats att uppdrag om grova våldsbrott sker genom rekrytering av barn och unga via digitala kanaler. Problematiken har bland annat aktualiserats i sam-

band med att arbetet tillsammans med Danmark mot den gränsöverskridande organiserade brottsligheten har intensifierats. Förslaget att tillhandahållare av allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster ska inlemmas i regelverket om datalagring är av vikt i arbetet mot den organiserade brottsligheten.

Som *ECPAT Sverige* för fram är datalagring vidare ofta av avgörande betydelse vad gäller sexuell exploatering av barn på nätet. Lagrade uppgifter kan användas för att identifiera förövare och barn, vilket förväntas bidra till lagföringen och motverkandet av sådana brott.

Genom att brottsbekämpande myndigheters utredningsmöjligheter förbättras ökar också upptäcktsrisken, vilket kan ha en brottsavskräckande effekt. Även konsekvenserna för användningen av hemliga tvångsmedel vid utlänningskontroll förväntas vara positiva.

Konsekvenser för miljön, jämställdheten, barn och andra konsekvenser

Förslagen om att uppgifter om abonnemang ska lagras under längre tid, att tillhandahållare av nummeroberoende interpersonella kommunikationstjänster ska lagra sådana uppgifter samt lagringen inom ramen för nationell säkerhetslagring kan innebära större behov av lagringsmedia och därmed ökad energikonsumtion. Detta kan ha viss påverkan på miljön.

Samtliga förslag är könsneutrala. Förslagen innebär bättre förutsättningar för det brottsbekämpande arbetet beträffande flera olika typer av brott, bl.a. mäns våld mot kvinnor och våld i nära relationer. Det innebär att förslagen kan bidra till att uppfylla det jämställdhetspolitiska målet att kvinnor och män ska ha samma makt att forma samhället och sina egna liv och delmålet att mäns våld mot kvinnor ska upphöra.

Sedan den 1 januari 2020 gäller Förenta nationernas konvention om barnets rättigheter som lag i Sverige. All lagstiftning som rör barn ska utformas i överensstämmelse med barnkonventionens bestämmelser, se propositionen inkorporering av FN:s konvention om barnets rättigheter (prop. 2017/18:186 s. 94). Genom artikel 34 har konventionsstaterna åtagit sig att skydda barn från alla former av sexuellt utnyttjande och sexuella övergrepp. Förslagen innebär förbättrade möjligheter för de brottsbekämpande myndigheterna att förebygga, förhindra, utreda och lagföra brott. Särskilt förslagen om skyldigheter för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster kan ha betydelse för utredning av bl.a. sexualbrott mot barn.

Några remissinstanser lyfter frågor om möjligheten att kommunicera på ett säkert sätt samt frågor om informationssäkerhetsaspekter och riskhanteringsåtgärder. Det finns en risk att tillhandahållare av nummeroberoende interpersonella kommunikationstjänster, i syfte att genomföra den föreslagna anpassningsskyldigheten, väljer att försvaga cybersäkerheten i sina tjänster för användare specifikt i Sverige. Det skulle skapa sårbarheter för svenska företag, organisationer och privatpersoner. Det finns vidare en risk att sådana tillhandahållare, för att undvika att försvaga cybersäkerheten i sina tjänster, väljer att upphöra med verksamheten i Sverige. Utredningen anger dock att det är möjligt för tillhandahållarna att utforma sina tjänster så att kraven på säkerhet och skyddet för kommunikationen tillgodoses. Det är av vikt att exempelvis totalsträckskrypterade tjänster

alltjämt kan användas. Det kan också konstateras att förslagen bl.a. innebär att tillhandahållare av nummeroberoende interpersonella kommunikationstjänster, utöver de krav på skyddsåtgärder som de redan omfattas av, kommer att åläggas krav på att vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda lagrade uppgifter vid behandling. Genom det samlade regelverket bör frågor om informationssäkerhet och riskhantering kunna hanteras på ett tillförlitligt sätt i tillämpningen.

Reglerna om åtkomst till information från elektronisk kommunikation är avgränsade och definierade i lag. Reglerna är inte avsedda att tillämpas på ett annat sätt i förhållande till nummeroberoende interpersonella kommunikationstjänster än för andra tjänster. Åtkomsten till lagrade uppgifter är vidare omgärdat av rättssäkerhetsgarantier och det grundlagsskyddade efterforskningsförbudet vad gäller den som är meddelare till en viss uppgift är alltjämt tillämpligt på myndigheternas verksamhet (3 kap. 5 § tryckfrihetsförordningen och 2 kap. 5 § yttrandefrihetsgrundlagen). Förslagen som rör nummeroberoende interpersonella kommunikationstjänster bedöms därför inte i sig innebära några tillkommande risker för källskyddet i förhållande till nuvarande regler, vilket *TU* och *Journalistförbundet* anser.

Vad gäller *Sveriges advokatsamfunds* påpekande om reglernas förhållande till andra EU-regelverk kan konstateras att regelverket om elektronisk kommunikation tar avstamp i EU-rätten. De nu aktuella förändringarna bedöms inte ge upphov till några konflikter med andra EU-rättsakter. *Kommerskollegium* lyfter frågan om förslagen medför en anmälningsplikt enligt Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster. Utredningen anger att någon sådan anmälningsskyldighet inte kommer att uppkomma med anledning av de aktuella förslagen. Det görs i denna del inte någon annan bedömning än den utredningen har gjort.

Förslagen bedöms i övrigt inte få några ekonomiska eller andra konsekvenser för kommuner eller regioner eller för några andra områden som bör redovisas.

10.2 Konsekvenser för företagen

Utkastets bedömning: Förslagen leder till ett mer konkurrensneutralt regelverk, men det kan inte uteslutas att de kan ha viss påverkan på konkurrensen mellan företagen. De tekniska anpassningar som förslagen medför leder till kostnadsökningar för tillhandahållarna. Konsekvenserna får vid en samlad bedömning anses vara godtagbara i förhållande till förslagens förväntade fördelar.

Utredningens bedömning överensstämmer med utkastets.

Remissinstanserna: Merparten av remissinstanserna yttrar sig inte i denna del. *Bahnhof AB* menar att det kommer behövas väsentligt ökade lagringsresurser om förslagen genomförs i sin helhet. Även kostnaderna och behovet av personella resurser kommer att öka. *TechSverige*, *Hi3G Access AB*, *Telenor Sverige AB* och *Telia Sverige AB* för fram liknande synpunkter. TechSverige påtalar att den

nationella säkerhetslagringen riskerar att leda till extremt omfattande lagring. Samtidigt kan antalet verkställigheter förväntas bli mycket lågt. Att vidhålla dagens modell för ersättning, dvs. att ersätta kostnad för utlämning men inte investeringar och förvaltningskostnader, blir därför ohållbart. Även Hi3G Access AB och Telenor Sverige AB gör gällande att den nuvarande modellen för kostnadsfördelning mellan staten och tillhandahållarna behöver omprövas. Vidare för *TechSverige*, *Hi3G Access AB*, *Telenor Sverige AB* och *Telia Sverige AB* fram att reglering på EU-nivå med harmoniserade regler skulle underlätta marknadsinträde, säkerställa effektivitet och främja konkurrensen på området. Det skulle även säkerställa en harmoniserad och långsiktigt hållbar lösning på datalagringsfrågorna. Hi3G Access AB pekar särskilt på ökade kostnader för lagring av lokaliseringsuppgifter som inte är trafikuppgifter. *Tele2 Sverige AB* menar att lagring av lokaliseringsuppgifterna innebär att den totala lagringskapaciteten behöver mångdubblas. Även *Sveriges advokatsamfund* och *Stockholms universitet (Juridiska fakulteten)* ifrågasätter kostnadsfördelningen. Sveriges advokatsamfund påpekar därutöver att kostnader kan uppkomma för myndigheter och tillhandahållare med anledning av säkerhetsskyddsavtal och krav som följer av EU-rättsakter. *Dataskydd.net Sverige*, *Föreningen för Digitala fri- och rättigheter* och *ISOC-SE* för fram att förslaget om anpassningsskyldighet för nummeroberoende interpersonella kommunikationstjänster kan leda till att vissa tillhandahållare slutar tillhandahålla sina tjänster i Sverige.

Skälen för utkastets bedömning

Konkurrens

I utredningen förs fram att de företag som berörs av förslagen består av två grupper av tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster, de traditionella mobiloperatörerna och tillhandahållare av nummeroberoende interpersonella kommunikationstjänster. Vidare påtalas, vad gäller såväl mobila tjänster som för fast bredband och nummeroberoende interpersonella kommunikationstjänster, att det finns en handfull företag som har den största andelen av marknaden för respektive tjänst.

Som utredningen för fram är det svårt att dra några säkra slutsatser i fråga om hur förslagen påverkar konkurrensen mellan stora och små aktörer. Å ena sidan kan det antas att de brottsbekämpande myndigheterna i första hand kommer att vända sig till de större aktörerna för att få tillgång till uppgifter eftersom de har den större delen av marknaden. Detta skulle innebära en större belastning för de stora aktörerna. Å andra sidan har de aktörerna jämfört med de mindre också större möjlighet att bära de ökade kostnader som det kan medföra.

Tillhandahållare av nummeroberoende interpersonella kommunikationstjänster kommer enligt förslagen att omfattas av bl.a. lagringsskyldighet för uppgifter om abonnemang, anpassningsskyldigheten och reglerna om nationell säkerhetslagring. Det innebär att regelverket blir mer konkurrensneutralt än tidigare eftersom flera av reglerna nu kommer att gälla såväl de traditionella operatörerna som tillhandahållarna av nummeroberoende interpersonella kommunikationstjänster. Reglerna om nationell säkerhetslagring kan sägas vara konkurrensneutrala i den

meningen att lagringsskyldigheten kommer att gälla för alla tillhandahållare. Att förslagen skulle kunna ha viss påverkan på konkurrensen kan dock inte uteslutas.

Som *TechSverige*, *Hi3G Access AB*, *Telenor Sverige AB* och *Telia Sverige AB* för fram är det möjligt att en harmoniserad EU-reglering skulle underlätta bland annat marknadsinträde, säkerställa effektivitet och främja konkurrensen på området. Sverige arbetar aktivt med frågorna på EU-nivå. Under Sveriges ordförandeskap i Europeiska unionens råd första halvåret 2023 initierade Sverige bland annat inrättandet av högnivågruppen för tillgång till data för en effektiv brottsbekämpning. Med hänsyn till brottsutvecklingen och det allvarligt försämrade säkerhetsläget kan det inte anses möjligt att avvakta åtgärder på EU-nivå. Någon EU-harmonisering av frågorna i dess helhet kan inte heller förväntas i närtid.

Dataskydd.net Sverige, *Föreningen för Digitala fri- och rättigheter* och *ISOC-SE* gör gällande att det finns en risk att vissa tillhandahållare slutar tillhandahålla sina tjänster i Sverige på grund av de krav som följer av förslagen om anpassningsskyldighet för nummeroberoende interpersonella kommunikationstjänster. Enbart den omständighet att en kommunikationstjänst är uppbyggd på ett visst sätt rent tekniskt är dock inte skäl att låta andra regler gälla för tjänsten. Förslaget innebär inte någon materiell ändring av anpassningsskyldigheten, utan endast att den utvidgas till att omfatta fler tillhandahållare och därmed blir mer teknikneutral, vilket inte torde vara negativt för konkurrensen.

Kostnader och finansiering

Som bl.a. *Bahnhof*, *TechSverige* och *Telia Sverige AB* för fram innebär lagringsskyldigheten och anpassningsskyldigheten kostnader för de aktörer som ska verkställa lagringen och anpassa sina it-stöd så att beslut om hemliga tvångsmedel kan verkställas.

Förslaget om att uppgifter om abonnemang ska lagras i ett år i stället för sex eller tio månader innebär att sådana uppgifter behöver lagras under längre tid, vilket medför behov av mer lagringsutrymme. Detsamma gäller för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster som åläggs en skyldighet att lagra uppgifter om abonnemang. Uppgifter om abonnemang bör dock i förhållande till andra uppgifter vara mindre resurskrävande att lagra och torde också redan lagras i större omfattning för andra ändamål.

Tillhandahållare av nummeroberoende interpersonella kommunikationstjänster kommer också att omfattas av anpassningsskyldigheten. Det innebär att tillhandahållarna kommer att behöva anpassa sina system så att tvångsmedelsbeslut kan verkställas. Verkställigheten kräver också en organisation och bemanning som gör att tvångsmedel kan verkställas utan dröjsmål. Detta gäller också förslaget som innebär att även tillhandahållare av vissa allmänt tillgängliga elektroniska kommunikationstjänster till fast nätanslutningspunkt omfattas av anpassningsskyldigheten (avsnitt 5.2).

Ett annat förslag som kan vara kostnadsdrivande är förslaget om nationell säkerhetslagring, där såväl de som är lagringsskyldiga enligt nuvarande regler som tillhandahållare av nummeroberoende interpersonella kommunikationstjänster kan bli skyldiga att lagra uppgifter i upp till två år. *TechSverige* för fram att det kan bli fråga om en extremt omfattande lagring som blir kostsam. Lagringsskyldigheten kan även innebära en lagring av uppgifter som inte lagras annars och

antalet uppgifter som lagras skulle kunna öka avsevärt. Detta innebär även att tillhandahållarna kommer att behöva skilja ut de uppgifter som lagras enligt ett sådant beslut från annan lagring och ta höjd för behovet av ytterligare lagringsmedia. Av utredningen framgår bl.a. att teleoperatörerna har uppgett att lagring av lokaliseringsuppgifter som inte är trafikuppgifter medför mycket stora kostnader för bolagen, sett till mängden uppgifter som kan behöva lagras enligt ett beslut om nationell säkerhetslagring. Detta har även förts fram av remissinstanser. Kostnaden avser bl.a. inköp av lagringsmedia och den praktiska hanteringen av beslut om nationell säkerhetslagring.

Hur stora kostnaderna för de olika förslagen kommer att bli är svårt att uppskatta. När det gäller ett beslut om nationell säkerhetslagring kan dock konstateras att ett sådant bara får beslutas under förhållanden som utgör ett allvarligt hot mot Sveriges säkerhet. Även om regleringen i sig innebär att företagen behöver ha beredskap för lagringen oaktat om en sådan beslutas är förhoppningen att en sådan lagringsskyldighet inte kommer att vara vanligt förekommande och att det, sett över tid, rör sig om en hanterbar kostnad. Det har särskilt framhållits att lagring av lokaliseringsuppgifter kommer att vara kostnadsdrivande då det rör sig om en stor mängd uppgifter som genereras med hög frekvens. Med anledning av dessa synpunkter är förslaget i den delen att uppgifterna ska lagras under ett års tid i stället för utredningens förslag om två år. I det sammanhanget ska även beaktas att vad som ska lagras enligt 9 kap. 19 b § lagen om elektronisk information är uppgifter som är nödvändiga. Det innebär alltså inte per automatik att samtliga uppgifter behöver lagras. I enlighet med upplysningsbestämmelsen i 9 kap. 23 § kan det också meddelas närmare föreskrifter på lägre nivå än lag. Sådana föreskrifter kan underlätta för frågan om vad som närmare ska lagras och kan bidra till att mängden uppgifter står i rimlig proportion till syftet med lagringen. Det ska därutöver betonas att den tillkommande lagringsskyldigheten, till skillnad mot vad *Tele2 Sverige AB* för fram, inte innebär att leverantörerna blir skyldiga att lagra uppgifter som annars inte förekommer i deras verksamhet.

En fråga som uppkommer med anledning av de tillkommande kostnaderna är hur dessa ska fördelas. Den nuvarande kostnadsfördelningen mellan det allmänna och operatörerna innebär att operatörerna står för kostnader för anpassning, drift och underhåll och att de brottsbekämpande myndigheterna utger ersättning till operatörerna vid varje uppgiftsutlämnande. Denna ordning har sin utgångspunkt i ställningstagandet att det finns verksamhetsområden där samhället, som en förutsättning för att tillåta ett företag att driva näringsverksamhet, kräver att vissa samhälleliga intressen beaktas, se propositionen Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG (prop. 2010/11:46 s. 67). Modellen har även samhällsekonomiska fördelar, genom att den part som har möjlighet att påverka kostnaderna har ett ansvar för dem. Operatörernas tekniska och administrativa kompetens nyttjas, samtidigt som de har ett tydligt incitament att hålla nere kostnader för anpassning och drift. Ett flertal remissinstanser för fram att kostnadsfördelningen behöver ses över.

Ett delvis förändrat regelverk kan uppfattas som betungande. Som utredningen för fram finns det dock starka skäl för att den gällande modellen för kostnadsfördelning inte ska frångås. Frågan om en översyn av kostnadsansvaret ligger även utanför detta lagstiftningsärende. Det innebär att tillhandahållarna alltjämt ska stå

för anpassningskostnader, drift och underhåll. Det innebär även att det allmänna fortsättningsvis ska ersätta operatörerna för de kostnader som hänför sig till utlämnande av uppgifter i enskilda ärenden.

Förslaget i avsnitt 5.1 om att uppgifter om abonnemang som omfattas av lagringsskyldigheten bör få behandlas även i andra syften än att lämnas ut till brottsbekämpande myndigheter bör underlätta hanteringen för företagen. Vidare bör förslaget om ändring av anpassningsskyldigheten i avsnitt 5.2, där kretsen av aktörer som omfattas av skyldigheten knyts till de som är lagringsskyldiga, leda till ökad tydlighet och förutsägbarhet. Tillhandahållare av nummeroberoende interpersonella kommunikationstjänster kommer att omfattas av fler delar av regelverket och fler skyldigheter än tidigare, men kommer också att omfattas av reglerna om ersättning för kostnader som uppstår när uppgifter lämnas ut till brottsbekämpande myndigheter.

Konsekvenserna för företagen får vid en samlad bedömning anses vara godtagbara i förhållande till förslagens förväntade fördelar.

10.3 Konsekvenser för myndigheter

Utkastets bedömning: De föreslagna ändringarna medför ökade kostnader för Säkerhetspolisen och kontrollorganet för nationell säkerhetsprövning, Försvarsunderrättelsedomstolen. I enlighet med budgetpropositionen för 2024 tillförs Säkerhetspolisen och kontrollorganet medel från och med 2025 för att finansiera kostnaderna för förslagen. I övrigt bedöms de kostnadsökningar som förslagen kan medföra för berörda myndigheter kunna hanteras inom befintliga ekonomiska ramar.

Utredningens bedömning överensstämmer delvis med utkastets. Utredningen bedömer att förslagen medför att Säkerhetspolisen behöver ytterligare ekonomiska tillskott. Utredningen bedömer vidare att förslagen medför att Polismyndigheten och Tullverket behöver ekonomiska tillskott.

Remissinstanserna: Merparten av remissinstanserna yttrar sig inte i denna del. *Förvaltningsrätten i Stockholm* påpekar att förslagen kan medföra att antalet överklaganden av Post- och telestyrelsens beslut ökar, vilket leder till fler processer i de allmänna förvaltningsdomstolarna. *Kammarrätten i Stockholm* för fram en liknande synpunkt. *Post- och telestyrelsen (PTS)* lyfter att vägledning, tillsyn och övriga uppgifter som ankommer på PTS i sin roll som tillsynsmyndighet kommer leda till ökade kostnader hos myndigheten. Vidare anförs att det kan finnas svårigheter vid myndighetens kontroll av lagringsskyldigheten vid den nationella säkerhetslagringen.

Skälen för utkastets bedömning

Konsekvenser för Säkerhetspolisen

Genom förslaget om nationell säkerhetslagring får Säkerhetspolisen en ny uppgift med tillhörande administration. Förslaget innebär även kostnader för utbildning och genomförande. Säkerhetspolisens medverkan krävs även när ett beslut om

nationell säkerhetslagring överprövas. Även om det, som utredningen för fram, kan förväntas bli fråga om ett begränsat antal ärenden så torde det krävas en inte obetydlig arbetsinsats varje gång ett ärende om nationell säkerhetslagring aktualiseras. Förslaget om nationell säkerhetslagring medför sannolikt även en ökning av antalet framställningar om verkställighet av beslut om tillstånd till hemliga tvångsmedel och beslut enligt inhämtningslagen. Omfattningen av ökningen är dock svår att bedöma.

Förslaget om lagringsskyldighet för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster och förändringen i inhämtningslagen medför, tillsammans med förtydligandet av anpassningsskyldigheten, att uppgifter kan inhämtas från fler tillhandahållare. Det medför vissa initiala kostnader för att upprätta kontaktvägar och kommunikationskanaler för inhämtning av uppgifter från tillhandahållare som inte tidigare har omfattats av skyldigheterna. Det innebär också att en ökad mängd uppgifter kan komma in till Säkerhetspolisen. Därmed uppkommer en viss ökning av kostnader för att kunna omhänderta och hantera dessa uppgifter. För användning av hemliga tvångsmedel i realtid krävs även säkra förbindelser mellan Säkerhetspolisen och tillhandahållare av nummeroberoende interpersonella kommunikationstjänster. Sådana lösningar finns redan i drift för de teleoperatörer som i dag har motsvarande anpassningsskyldighet. Utredningen, som även för fram att en exakt bedömning är svår att göra, uppskattar att cirka 20 miljoner kronor kommer att krävas årligen. Kostnaderna bör dock, i vart fall delvis, kunna fördelas mellan de brottsbekämpande myndigheterna.

Säkerhetspolisen tillsköts, till skillnad från bl.a. Polismyndigheten, Åklagarmyndigheten, Tullverket och Ekobrottsmyndigheten, inte medel för användningen av hemliga tvångsmedel i budgetpropositionen för 2023. Förslagen förväntas medföra kostnadsökningar som inte kan hanteras inom ramen för befintliga anslag. Samtidigt föreslås nu att regeringen inte ska gå vidare med samtliga av de förslag som utredningen bedömt förväntas leda till kostnader för Säkerhetspolisen, vilka utredningen också fört fram är behäftade med viss osäkerhet. Bedömningen är att den kostnadsökning som förslagen medför kommer att täckas av de medel som myndigheten tillförs fr.o.m. 2025 i enlighet med budgetpropositionen för 2024 och att tillkommande kostnader därmed kan hanteras inom myndighetens befintliga ekonomiska ramar.

Konsekvenser för Försvarsunderrättelsedomstolen

Förslagen förväntas medföra kostnadsökningar som inte kan hanteras inom ramen för befintliga anslag. Den kostnadsökning som förslagen medför för Försvarsunderrättelsedomstolen kommer att täckas av de medel som tilldelas det tidigare aktuella kontrollorganet Säkerhets- och integritetsskyddsnämnden fr.o.m. 2025 i enlighet med budgetpropositionen för 2024.

Konsekvenser för Polismyndigheten och Tullverket

Utredningen bedömer att förslagen kommer att leda till ett ökat resursbehov hos Polismyndigheten och Tullverket. Det handlar dels om teknikanpassningar och andra utvecklingskostnader, dels om ytterligare resursbehov för att hantera den

förväntade ökade mängden elektronisk information som kan väntas komma in till myndigheterna.

I utkastet behandlas inte utredningens förslag om riktad lagring för bekämpning av allvarlig brottslighet, vilket svarar mot delar av Polismyndighetens och Tullverkets förväntade kostnader. De delar av utredningens förslag som nu behandlas innebär kostnader för tekniska anpassningar, främst utifrån förslagen om att låta bl.a. lagrings- och anpassningsskyldigheterna gälla tillhandahållare av nummeroberoende interpersonella kommunikationstjänster. Tillämpningen av förslagen förutsätter bl.a. investeringar i teknik och kan också leda till kostnader för hantering av tillkommande information. Samtidigt förväntas förslagen också förbättra förutsättningarna för myndigheterna att utföra sitt brottsbekämpande uppdrag. En effektivare tillgång till elektronisk information kan också leda till resursbesparingar eftersom andra, mer resurskrävande, utredningsmetoder inte längre behöver användas i samma utsträckning. Polismyndigheten och Tullverket tillfördes medel för användningen av hemliga tvångsmedel i budgetpropositionen för 2023. Mot bakgrund av detta görs bedömningen att kostnaderna ryms inom myndigheternas befintliga ekonomiska ramar.

Konsekvenser för andra myndigheter

I enlighet med utredningens bedömning bedöms de kostnader som kan antas uppstå för andra myndigheter, inklusive domstolarna, rymmas inom ramen för deras befintliga ekonomiska anslag. *PTS* för fram att det av sekretesskäl kan finnas svårigheter för planlagd tillsyn på eget initiativ när det gäller lagring enligt ett beslut om nationell säkerhetslagring. Tillsyn bör i dessa fall kunna ske efter påtalande av Säkerhetspolisen.

11 Författningskommentar

11.1 Förslaget till lag om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet

Lagens innehåll

1 § Denna lag innehåller bestämmelser om när uppgifter om elektronisk kommunikation får lagras och lämnas ut för att skydda Sveriges säkerhet.

Paragrafen anger lagens innehåll. Övervägandena finns i avsnitt 6.1.

Med uttrycket uppgifter om elektronisk kommunikation avses uppgift om abonnemang samt trafikuppgifter och lokaliseringsuppgifter som inte är trafikuppgifter, dvs. de uppgifter som framgår av 9 kap. 31 § första stycket 1, 3 och den nya punkten 4 lagen (2022:482) om elektronisk kommunikation.

Nationell säkerhetslagring

2 § Säkerhetspolisen får besluta att den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § lagen (2022:482) om elektronisk kommunikation eller den som tillhandahåller en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst enligt samma lag ska lagra uppgifter i enlighet med vad som följer av denna lag (beslut om nationell säkerhetslagring). Ett sådant beslut får endast fattas om det finns ett allvarligt hot mot Sveriges säkerhet och det är absolut nödvändigt.

Ett beslut får gälla i högst ett år och omfattningen ska begränsas till vad som är absolut nödvändigt. Säkerhetspolisen får genom ett nytt beslut förlänga lagringsskyldigheten om hotet mot Sveriges säkerhet består. Om det inte längre finns skäl för nationell säkerhetslagring, ska Säkerhetspolisen upphäva beslutet.

I 9 kap. 19 b och 22 §§ lagen om elektronisk kommunikation anges vilka uppgifter som får omfattas av ett beslut om nationell säkerhetslagring respektive hur länge uppgifterna ska lagras.

Ett beslut om nationell säkerhetslagring får verkställas omedelbart.

Paragrafen innehåller bestämmelser som anger förutsättningarna för ett beslut om nationell säkerhetslagring och giltighetstiden för ett sådant beslut. Paragrafen innehåller också bestämmelser som ger uttryck för den proportionalitetsprincip som gäller vid nationell säkerhetslagring. Paragrafen innehåller därutöver en hänvisning till lagen om elektronisk kommunikation. Övervägandena finns i avsnitt 6.2 och 6.5.

Av *första stycket* framgår att Säkerhetspolisen ska bedöma hotet mot den nationella säkerheten och, under vissa förutsättningar, får besluta att den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § lagen (2022:482) om elektronisk kommunikation eller den som tillhandahåller en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst enligt samma lag ska lagra uppgifter för att skydda Sveriges säkerhet. En sådan lagring kallas nationell säkerhetslagring. Det avser en lagring som sker i syfte att skydda den nationella säkerheten och är mer omfattande än vad som annars gäller enligt lagen om elektronisk kommunikation.

För lagring krävs att det finns ett allvarligt hot mot Sveriges säkerhet. Omständigheter som kan vara av betydelse vid bedömningen av hotet mot den nationella säkerheten är t.ex. om det inträffar ett terrordåd, förhöjd terrorhotsnivå i Sverige, hot om ett väpnat angrepp mot Sverige eller om det finns andra jämförbara allvarliga hot mot Sveriges inre eller yttre säkerhet. Av EU-domstolens praxis framgår att det ska föreligga tillräckligt konkreta omständigheter för att anse att staten står inför ett allvarligt hot mot nationell säkerhet som visat sig vara verkligt och aktuellt eller förutsebart (EU-domstolens dom den 6 oktober 2020 i de förenade målen C-511/18, C-512/18 och C-520/18 La Quadrature du Net m.fl.).

Ett beslut får endast fattas när det är absolut nödvändigt. Vad som är absolut nödvändigt beror på omständigheterna i det enskilda fallet. Exempelvis har det betydelse vilken typ av hot det är fråga om och vilka alternativ till nationell säkerhetslagring som finns tillgängliga.

Andra stycket reglerar dels hur lång tid ett beslut om nationell säkerhetslagring får gälla, dels att det ska göras en proportionalitetsbedömning när omfattningen av lagringsskyldigheten bestäms. I stycket regleras även när ett beslut kan förlängas eller ska upphävas.

Ett beslut får gälla i högst ett år. Tiden tar sikte på giltigheten av beslutet. Regleringen avser alltså inte tiden som de lagrade uppgifterna ska finnas kvar (se tredje stycket). När det gäller beslutets omfattning kan det exempelvis begränsas i fråga om, utöver beslutets giltighetstid, vilka tillhandahållare som ska omfattas av lagringsskyldigheten och vilka typer av uppgifter som ska omfattas av lagringsskyldigheten. Om Säkerhetspolisen gör bedömningen att hotet mot den nationella säkerheten kvarstår efter ett år, får myndigheten förlänga lagringsskyldigheten genom ett nytt beslut. Förfaranderegelerna och reglerna om kontroll gäller även för det nya beslutet. Säkerhetspolisen ska enligt bestämmelsen löpande ompröva om hotet består och upphäva beslutet om det inte längre finns skäl för nationell säkerhetslagring.

Tredje stycket hänvisar till bestämmelser i lagen om elektronisk kommunikation. Där finns bestämmelser om lagringsskyldighetens omfattning och hur lång tid uppgifterna ska lagras.

Av *fjärde stycket* framgår att ett beslut om nationell säkerhetslagring får verkställas omedelbart.

Offentligt ombud för nationell säkerhetslagring

3 § Ett offentligt ombud för nationell säkerhetslagring ska bevaka enskildas intressen i ärenden om nationell säkerhetslagring.

Paragrafen anger att det i ärenden om nationell säkerhetslagring ska finnas ett ombud som ska bevaka enskildas intressen. Övervägandena finns i avsnitt 6.4.1.

Med enskilda åsyftas inte bara enskilda fysiska personer utan även bl.a. tillhandahållare av elektroniska kommunikationstjänster. Uttrycket enskildas intressen kan avse personliga, ekonomiska och andra förhållanden.

4 § Regeringen förordnar för högst tre år i sänder en person som ska tjänstgöra som ordinarie offentligt ombud för nationell säkerhetslagring och två personer som ska vara det ordinarie ombudets ställföreträdare.

Ombudet ska vara svensk medborgare och ska

– ha varit ordinarie domare, eller

– vara eller ha varit advokat eller ha motsvarande juridisk erfarenhet.

Ombudet får inte vara i konkurstillstånd eller ha förvaltare enligt 11 kap. 7 § föräldrabalken.

Regeringen ska inhämta förslag på lämpliga kandidater från Domarnämnden och Sveriges advokatsamfund.

Ombudet får trots att regeringens förordnande har upphört slutföra pågående uppdrag.

Paragrafen innehåller bestämmelser om offentliga ombud för nationell säkerhetslagring. Övervägandena finns i avsnitt 6.4.1.

Av *första stycket* framgår att regeringen ska förordna en person som ska tjänstgöra som ordinarie offentligt ombud för nationell säkerhetslagring under högst tre år. Förordnandetiden kan vara kortare än tre år. Regeringen ska även förordna två personer som ska vara det ordinarie ombudets ställföreträdare.

Av *andra och tredje styckena* framgår de krav som ställs på ombudet. Kraven motsvarar i huvudsak vad som gäller för offentliga ombud enligt 27 kap. 27 §

rättegångsbalken. Med att ett ombud ska ha motsvarande juridisk erfarenhet som en advokat avses att också personer omfattas som genom utbildning, meriter och erfarenhet har tillräckliga kvalifikationer i frågor som uppkommer i angelägenheter som rör nationell säkerhetslagring.

Enligt *fjärde stycket* ska regeringen hämta in förslag på lämpliga kandidater från Domarnämnden och Sveriges advokatsamfund. Detta hindrar inte att regeringen inhämtar förslag och relevant information om lämpliga kandidater även från annat håll.

Femte stycket innebär att ombudet får slutföra ett uppdrag i ett ärende som är pågående när förordandet upphör.

5 § Den som har förordnats som offentligt ombud för nationell säkerhetslagring får inte obehörigen röja vad han eller hon har fått kännedom om i ett ärende om nationell säkerhetslagring.

Paragrafen reglerar tystnadsplikt för ombudet. Övervägandena finns i avsnitt 6.8.

Med uttrycket obehörigen avses att ombudet inte får röja sådant som ombudet fått kännedom om i ärendet om nationell säkerhetslagring. Däremot hindrar bestämmelsen inte att ombudet redogör för uppgifterna hos Försvarsunderrättelsedomstolen i samband med överprövningen. Bestämmelsen omfattar alla uppgifter som ombudet får kännedom om i ärendet om nationell säkerhetslagring.

Underställning av beslutet hos Försvarsunderrättelsedomstolen

6 § När ett beslut om nationell säkerhetslagring har fattats ska beslutet omedelbart underställas Försvarsunderrättelsedomstolen.

Försvarsunderrättelsedomstolen ska så snart som möjligt hålla ett sammanträde. Vid sammanträdet ska Säkerhetspolisen och det offentliga ombudet för nationell säkerhetslagring närvara. Försvarsunderrättelsedomstolen har vid sammanträdet rätt att ta del av de omständigheter som ligger till grund för beslutet om nationell säkerhetslagring. Vid sammanträdet ska Säkerhetspolisen redogöra för beslutet och ombudet har rätt att yttra sig.

Paragrafen reglerar tillsammans med 7 § förfarandet vid överprövningen av Säkerhetspolisens beslut. Övervägandena finns i avsnitt 6.4.2.

Av *första stycket* framgår att ett beslut om nationell säkerhetslagring omedelbart ska underställas Försvarsunderrättelsedomstolen.

Av *andra stycket* framgår att Försvarsunderrättelsedomstolen ska överpröva Säkerhetspolisens beslut vid ett sammanträde i närvaro av företrädare för Säkerhetspolisen och av det offentliga ombudet för nationell säkerhetslagring. Företrädare för Säkerhetspolisen ska vid sammanträdet redogöra för myndighetens beslut liksom ett underlag som redovisar de omständigheter som ligger till grund för beslutet. Försvarsunderrättelsedomstolens ledamöter och ombudet får ställa frågor vid sammanträdet. Det ankommer på domstolen att bestämma formerna för sammanträdet.

7 § Försvarsunderrättelsedomstolen ska pröva om Säkerhetspolisens beslut om nationell säkerhetslagring ska fortsätta att gälla. Domstolen ska även besluta om ersättning till det offentliga ombudet för nationell säkerhetslagring. I fråga om ersättning till ombudet tilläm-

pas bestämmelserna i 21 kap. 10 § första och andra styckena rättegångsbalken. Försvarsunderrättelsedomstolens beslut om nationell säkerhetslagring och ersättning får inte överklagas.

Paragrafen reglerar tillsammans med 6 § förfarandet vid överprövningen av Säkerhetspolisens beslut. Övervägandena finns i avsnitt 6.4.2.

Försvarsunderrättelsedomstolen ska pröva om Säkerhetspolisens beslut ska fortsätta att gälla. Domstolen kan inte göra ändringar av ett beslut om nationell säkerhetslagring. Prövningen omfattar om det finns ett hot mot den nationella säkerheten enligt 2 § och om beslutet är författningsenligt och proportionerligt. Att Försvarsunderrättelsedomstolen upphäver ett beslut om nationell säkerhetslagring hindrar inte att Säkerhetspolisen fattar ett nytt beslut om lagring avseende samma förhållanden.

Försvarsunderrättelsedomstolens beslut om nationell säkerhetslagring får inte överklagas. Överklagandeförbudet omfattar även ersättning till ombudet.

Tillgång till lagrade uppgifter

8 § Uppgifter som har lagrats enligt ett beslut enligt 2 § får endast hämtas in efter ett tillstånd till hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation enligt 27 kap. 18 eller 19 § rättegångsbalken eller ett tillstånd till inhämtning enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Uppgifter får endast hämtas in enligt första stycket om det i tillståndet har angetts att inhämtningen får avse uppgifter som har lagrats med stöd av denna lag.

Paragrafen reglerar tillsammans med 9 § tillgång till uppgifter som lagrats enligt ett beslut om nationell säkerhetslagring. Övervägandena finns i avsnitt 6.6.

För tillgång till uppgifterna krävs att vissa villkor är uppfyllda. I *första stycket* anges att ett villkor för tillgång till uppgifterna är att det finns ett beslut om hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation eller inhämtning enligt lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. Det omfattar även hemliga tvångsmedel enligt 27 kap. rättegångsbalken då andra författningar tillämpas, såsom lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott och lagen (2022:700) om särskild kontroll av vissa utlänningar.

Av *andra stycket* framgår att uppgifter endast får hämtas in om det i tillståndsbeslutet om hemliga tvångsmedel enligt första stycket har angetts att inhämtningen får avse uppgifter som lagrats för den nationella säkerheten.

9 § Uppgifter får hämtas in enligt 8 § endast i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott som anges i andra stycket eller för att utreda och beivra sådana brott.

De brott som ger rätt till inhämtning av uppgifter som lagrats enligt ett beslut enligt 2 § är:

1. sabotage eller grovt sabotage enligt 13 kap. 4 eller 5 § brottsbalken,

2. mordbrand, grov mordbrand, allmänfarlig ödeläggelse, kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 1, 2, 3, 5 a eller 5 b § brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,

3. uppror, väpnat hot mot laglig ordning eller brott mot medborgerlig frihet enligt 18 kap. 1, 3 eller 5 § brottsbalken,

4. högförräderi, krigsanstiftan, spionerі, grovt spionerі, utlandsspionerі, grovt utlandsspionerі, obehörig befattning med hemlig uppgift, grov obehörig befattning med hemlig uppgift eller olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person enligt 19 kap. 1, 2, 5, 6, 6 a, 6 b, 7, 8, 10, 10 a eller 10 b § brottsbalken,

5. företagsspionerі enligt 26 § lagen (2018:558) om företagshemligheter, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning,

6. terroristbrott, deltagande i en terroristorganisation, samröre med en terroristorganisation, finansiering av terrorism eller särskilt allvarlig brottslighet, offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet, rekrytering till terrorism eller särskilt allvarlig brottslighet, utbildning för terrorism eller särskilt allvarlig brottslighet eller resa för terrorism eller särskilt allvarlig brottslighet enligt 4, 4 a, 5, 6, 7, 8, 9 eller 10 § terroristbrottslagen (2022:666),

7. andra brott än de som anges i 1–6 och som på grund av sin omfattning eller karaktär utgör ett allvarligt hot mot Sveriges säkerhet, om det för brottet inte är föreskrivet lindrigare straff än fängelse i två år, eller

8. försök, förberedelse eller stämpling till brott som avses i 1–7, om en sådan gärning är belagd med straff.

Paragrafen reglerar tillsammans med 8 § tillgång till uppgifter som lagrats enligt ett beslut om nationell säkerhetslagring. Övervägandena finns i avsnitt 6.6.

Genom *första stycket* begränsas tillgången till uppgifter som lagrats för nationell säkerhet till bekämpning av brott och brottslighet som kan innebära ett hot mot Sveriges säkerhet.

I *andra stycket* finns en brottskatalog som syftar till att definiera vilka brott eller vilka typer av brottslighet som, sett till fara eller effekt, kan få påverkan på Sveriges säkerhet och för vilket de lagrade uppgifterna får hämtas in enligt 8 §.

Punkterna 1–6 motsvarar de brott och den brottsliga verksamhet som Säkerhetspolisen har i uppgift att bekämpa och för vilken inhämtning av uppgifter kan ske efter beslut enligt inhämtningslagen, eller efter tillstånd till hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation enligt rättegångsbalken och lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

Punkten 7 är en s.k. ventil som medger tillgång till uppgifter som lagrats för den nationella säkerheten för andra brott än de som Säkerhetspolisen har i uppgift att bekämpa under förutsättning att det är fråga om brott som på grund av sin omfattning eller karaktär utgör ett allvarligt hot mot Sveriges säkerhet. Dessutom gäller att det för brottet är stadgat minst två års fängelse. Som exempel på brottslighet som avses kan nämnas grov brottslig verksamhet som blivit så allvarlig att den riskerar att slå ut eller försvaga viktiga funktioner i samhället.

Punkten 8 rör försök, förberedelse och stämpling till brott som avses i 1–7, förutsatt att en sådan gärning är belagd med straff.

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

10 kap.

10 § Sekretess hindrar inte att den som är knuten till en myndighet på det sätt som anges i 2 kap. 1 § andra stycket och som är misstänkt för brott eller mot vilken rättegång eller annat jämförbart rättsligt förfarande har inletts, lämnar uppgift till sitt ombud eller biträde i saken eller till någon annan enskild, om det behövs för att han eller hon ska kunna ta till vara sin rätt.

Sekretess hindrar inte att uppgift i ett ärende hos domstol eller i ett beslut i ett sådant ärende lämnas till ett offentligt ombud enligt rättegångsbalken eller till ett integritetsskyddsombud enligt lagen (2009:966) om Försvarsunderrättelsedomstol.

Sekretess hindrar inte att uppgift i ett ärende om nationell säkerhetslagring lämnas till ett offentligt ombud för nationell säkerhetslagring enligt lagen (2025:000) om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

Paragrafen innehåller sekretessbrytande bestämmelser. Övervägandena finns i avsnitt 6.8.

Genom ett nytt tredje stycke införs en sekretessbrytande regel för uppgifter som lämnas till ett offentligt ombud för nationell säkerhetslagring i ett ärende om nationell säkerhetslagring.

Regleringen motsvarar vad som gäller i domstol för ett offentligt ombud enligt rättegångsbalken och ett integritetsskyddsombud enligt lagen om Försvarsunderrättelsedomstol. Bestämmelsen omfattar förfarandet hos Försvarsunderrättelsedomstolen.

18 kap.

19 § Den tystnadsplikt som följer av 5–7, 8, 9 och 10 §§, 11 § första stycket, 12, 12 a och 13 §§ inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning, hemlig dataavläsning på grund av beslut av domstol, undersökningsledare eller åklagare, inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet *eller nationell säkerhetslagring enligt lagen (2025:000) om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.*

Den tystnadsplikt som följer av 17 § inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning på grund av beslut av domstol eller åklagare.

Att den tystnadsplikt som följer av 1–3 §§ i vissa fall inskränker rätten att meddela och offentliggöra uppgifter utöver det som anges i andra stycket följer av 7 kap. 10 §, 12–18 §§,

20 § 3 och 22 § första stycket 1 och andra stycket tryckfrihetsförordningen samt 5 kap. 1 § och 4 § första stycket 1 och andra stycket yttrandefrihetsgrundlagen.

I paragrafen regleras vilka tystnadsplikter enligt 18 kap. offentlighets- och sekretesslagen som har företräde framför rätten att meddela och offentliggöra uppgifter. Övervägandena finns i avsnitt 6.8.

I *andra stycket* införs nationell säkerhetslagring i uppräkningen av de åtgärder där tystnadsplikten inskränker rätten att meddela och offentliggöra uppgifter enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen.

29 kap.

2 § Sekretess gäller hos en myndighet som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst för uppgift om innehållet i ett elektroniskt meddelande eller *en trafikuppgift*. Om sekretess inte följer av någon annan bestämmelse, får dock *en* sådan uppgift lämnas till den som har tagit del i utväxlingen av ett elektroniskt meddelande eller som på något annat sätt har sänt eller tagit emot ett sådant meddelande. Detsamma gäller innehavaren av ett abonnemang som använts för ett elektroniskt meddelande när det är fråga om uppgift om något annat än innehållet i meddelandet.

Paragrafen innehåller bestämmelser om sekretess hos en myndighet som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Övervägandena finns i avsnitt 5.3.

Paragrafen ändras på så sätt att uttrycket annan uppgift som angår ett särskilt elektroniskt meddelande ersätts med begreppet trafikuppgift. Motsvarande ändring föreslås i bestämmelsen om tystnadsplikt i 9 kap. 31 § första stycket 3 lagen om elektronisk kommunikation, se författningskommentaren till den paragrafen. Någon ändring i sak är inte avsedd.

35 kap.

1 § Sekretess gäller för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i

1. utredning enligt bestämmelserna om förundersökning i brottmål,
2. angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott eller i ärende enligt lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder,
3. angelägenhet som avser säkerhetsprövning enligt säkerhetsskyddslagen (2018:585),
4. annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott eller verkställa uppbörd och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen,
5. register som förs av Polismyndigheten enligt 5 kap. lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas med stöd av de bestämmelserna, eller uppgifter som behandlas av Säkerhetspolisen eller Polismyndigheten med stöd av lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter,
6. register som förs enligt lagen (1998:621) om misstankeregister,

7. register som förs av Skatteverket enligt lagen (2018:1696) om Skatteverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag,

8. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 5 kap. 1 §,

9. register som förs av Tullverket enligt lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag,

10. utredning om självständigt förverkande, *eller*

11. angelägenhet som avser nationell säkerhetslagring enligt lagen (2025:000) om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

Sekretessen enligt första stycket 2 gäller hos domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till honom eller henne lider skada eller men om uppgiften röjs. Vid förhandling om användning av tvångsmedel gäller sekretess för uppgift om vem som är misstänkt endast om det kan antas att fara uppkommer för att den misstänkte eller någon närstående till honom eller henne utsätts för våld eller lider annat allvarligt men om uppgiften röjs.

Första stycket gäller inte om annat följer av 2, 6 eller 7 §.

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

Paragrafen reglerar sekretess för uppgift om en enskilds personliga och ekonomiska förhållanden om uppgiften förekommer i verksamhet som bl.a. syftar till att förebygga, uppdaga, utreda eller beivra brott. Övervägandena finns i avsnitt 6.8.

I listan i *första stycket* införs en ny punkt 11, angelägenhet som avser nationell säkerhetslagring. Ändringen innebär att sekretess gäller för uppgift om en enskilds personliga och ekonomiska förhållanden i angelägenhet om nationell säkerhetslagring. Av uttrycket *angelägenhet som avser nationell säkerhetslagring* följer att det är fråga om en s.k. primär sekretessbestämmelse, vars räckvidd inte är begränsad. Bestämmelsen riktar sig alltså direkt till alla myndigheter som är involverade i angelägenheten.

24 § Den tystnadsplikt som följer av *1 § 11,* 11, 12 a § och den tystnadsplikt som följer av ett förbehåll som har gjorts med stöd av 9 § andra stycket inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Den tystnadsplikt som följer av 15 och 16 §§ inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift vars röjande kan antas medföra fara för att någon utsätts för våld eller lider annat allvarligt men.

I paragrafen regleras vilka tystnadsplikter enligt 35 kap. som har företräde framför rätten att meddela och offentliggöra uppgifter. Övervägandena finns i avsnitt 6.8.

I *första stycket* görs ett tillägg som innebär att även en uppgift som förekommer i en angelägenhet om nationell säkerhetslagring omfattas av den tystnadsplikt som inskränker rätten att meddela och offentliggöra uppgifter enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen (35 kap. 1 § 11 offentlighets- och sekretesslagen).

44 kap.

4 § Rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter inskränks av den tystnadsplikt som följer av

1. 5 kap. 1 § första stycket 1 samt 2 och 3 §§ postlagen (2010:1045),
2. 1 kap. 15 § lagen (2022:482) om elektronisk kommunikation, när det är fråga om uppgift om förhållanden av betydelse för att förebygga eller hantera fredstida krissituationer,
3. 9 kap. 31 § lagen om elektronisk kommunikation, när det är fråga om uppgift om innehållet i ett elektroniskt meddelande eller som annars rör ett särskilt sådant meddelande, och
4. 9 kap. 32 § lagen om elektronisk kommunikation, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation på grund av beslut av domstol, undersökningsledare eller åklagare, om inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet *eller om nationell säkerhetslagring enligt lagen (2025:000) om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.*

I paragrafen regleras när vissa tystnadsplikter som följer av postlagen och lagen om elektronisk kommunikation inskränker rätten enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter. Övervägandena finns i avsnitt 6.8.

Punkt 4 ändras till följd av att det införs bestämmelser om tystnadsplikt för tillhandahållarna i 9 kap. 32 § lagen om elektronisk kommunikation. Tystnadsplikten gäller i angelägenhet om nationell säkerhetslagring. Genom tillägget i punkten 4 får tystnadsplikten företräde framför meddelarfriheten. Punkten motsvarar det meddelarförbud som gäller för myndigheter enligt 18 kap. 19 § och 35 kap. 24 § offentlighets- och sekretesslagen.

5 § Rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter inskränks av den tystnadsplikt som följer

1. av beslut som har meddelats med stöd av 7 § lagen (1999:988) om förhör m.m. hos kommissionen för granskning av de svenska säkerhetstjänsternas författningsskyddande verksamhet,
2. av 7 kap. 1 § 1 lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap,
3. av 4 kap. 16 § försäkringsrörelselagen (2010:2043),
4. av 5 kap. 15 § lagen (1998:293) om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige,
5. av 32 § lagen (2020:62) om hemlig dataavläsning,
6. av 4 § lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter, *och*
7. *av 5 § lagen (2025:000) om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet*.

I paragrafen regleras när den tystnadsplikt som följer av vissa bestämmelser i annan lagstiftning än offentlighets- och sekretesslagen inskränker rätten enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter. Övervägandena finns i avsnitt 6.8.

I uppräkningen införs en ny punkt, 7. Den innebär att ett offentligt ombud för nationell säkerhetslagring enligt 5 § lagen om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet inte får meddela eller offentliggöra uppgifter som han eller hon har fått kännedom om i angelägenhet om nationell säkerhetslagring.

11.3 Förslaget till lag om ändring i lagen (2009:966) om Försvarsunderrättelsedomstol

1 § Försvarsunderrättelsedomstolen ska pröva frågor om tillstånd till signalspaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet. *Försvarsunderrättelsedomstolen ska även överpröva Säkerhetspolisens beslut om nationell säkerhetslagring enligt lagen (2025:000) om lagring av och tillgång till uppgifter om elektronisk information i syfte att skydda Sveriges säkerhet.*

I paragrafen anges Försvarsunderrättelsedomstolens uppgifter. Övervägandena finns i avsnitt 6.3.

Ändringen innebär att det i lagen anges att domstolen även ska överpröva Säkerhetspolisens beslut om nationell säkerhetslagring.

5 § Ett integritetsskyddsombud ska bevaka enskildas integritetsintresse i mål vid domstolen *om tillstånd till signalspaning.* Ombudet har rätt att ta del av det som förekommer i målet och att yttra sig.

Paragrafen innehåller bestämmelser om integritetsskyddsombud. Övervägandena finns i avsnitt 6.4.2.

Ändringen innebär ett förtydligande om att regleringen om integritetsskyddsombud avser mål som rör tillstånd till signalspaning och inte mål som rör nationell säkerhetslagring.

11.4 Förslaget till lag om ändring i säkerhetsskyddslagen (2018:585)

3 kap.

1 § Den som genom en anställning eller på något annat sätt ska delta i säkerhetskänslig verksamhet ska säkerhetsprövas. Säkerhetsprövning ska dock inte göras när det gäller

1. uppdrag som statsråd *eller som* ledamot av Europaparlamentet, riksdagen eller kommun- och regionfullmäktige, eller

2. annat uppdrag som offentlig försvarare eller ombud inför domstol än sådant som avser offentligt ombud enligt 27 kap. 27 § rättegångsbalken, integritetsskyddsombud enligt 6 § lagen (2009:966) om Försvarsunderrättelsedomstol *eller ombud för nationell säkerhetslag-*

ring enligt lagen (2025:000) om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

I paragrafen anges krav på säkerhetsprövning när en person genom anställning eller på något annat sätt ska delta i säkerhetskänslig verksamhet. Övervägandena finns i avsnitt 6.4.1.

Ändringen innebär att säkerhetsprövning ska göras när det gäller ombud för nationell säkerhetslagring enligt lagen om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

11.5 Förslaget till lag om ändring i lagen (2022:482) om elektronisk kommunikation

8 kap.

5 § Den som enligt 9 kap. 19*, 19 a eller 19 b §* är skyldig att lagra uppgifter ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling.

Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § *eller tillhandahåller en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst* och som har förelagts enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift ska avseende den uppgiften vidta sådana åtgärder som anges i första stycket.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om sådana skyddsåtgärder.

I paragrafen regleras en skyldighet för den som ska lagra uppgifter för brottsbekämpande ändamål att vidta åtgärder för att säkerställa att behandlade uppgifter skyddas mot integritetsintrång. Övervägandena finns i avsnitt 7.7.

I *första stycket* görs ett tillägg som innebär att även tillhandahållare av allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster omfattas av kraven på skyddsåtgärder.

I *andra stycket* görs ett tillägg som innebär att tillhandahållare av allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster även omfattas av kraven på skyddsåtgärder för uppgifter som bevarats med stöd av ett s.k. bevarandeföreläggande enligt 27 kap. 16 § rättegångsbalken.

9 kap.

1 § Den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst ska utplåna eller avidentifiera trafikuppgifter som har lagrats eller behandlats på något annat sätt när de inte längre behövs för överföring av ett elektroniskt meddelande. Detta gäller under förutsättning att uppgifterna avser användare som är fysiska personer eller abonnenter.

Första stycket *gäller* inte uppgifter som sparas för sådan behandling som anges i 2, 15, 19*, 19 b* eller 21 § eller om uppgifterna behövs för en sådan behandling som är tillåten enligt Europaparlamentets och rådets förordning (EU) 2021/1232 av den 14 juli 2021 om ett tillfälligt undantag från vissa bestämmelser i direktiv 2002/58/EG vad gäller användning av teknik hos tillhandahållare av nummeroberoende interpersonella kommunikationstjänster för

behandling av personuppgifter och andra uppgifter i syfte att bekämpa sexuella övergrepp mot barn på nätet.

Paragrafen innehåller huvudregeln om behandling av trafikuppgifter. Övervägandena finns i avsnitt 6.7.

Andra stycket ändras på så sätt att undantaget från huvudregeln i första stycket utvidgas till att även omfatta uppgifter som sparas för sådan behandling av uppgifter som avses i 19 b § som innehåller bestämmelser om lagring på grund av ett beslut enligt lagen om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

10 § Lokaliseringsuppgifter som omfattas av ett beslut om inhämtning av uppgifter enligt 27 kap. rättegångsbalken eller lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet får behandlas trots 7–9 §§.

Lokaliseringsuppgifter som lagras enligt 19 b § får behandlas trots 7–9 §§.

Paragrafen innehåller undantag från 7–9 §§ där det finns begränsningar för hur lokaliseringsuppgifter som inte är trafikuppgifter får behandlas av tillhandahållarna. Övervägandena finns i avsnitt 6.7.

I *andra stycket*, som är nytt, regleras att tillhandahållarna får behandla lokaliseringsuppgifter vid nationell säkerhetslagring enligt 19 b §.

19 § Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § ska lagra sådana uppgifter som avses i 31 § första stycket 1 och 3 som är nödvändiga för att spåra och identifiera kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning vid kommunikationens början och slut.

Lagringsskyldigheten omfattar uppgifter som genereras eller behandlas vid

1. telefonitjänst eller meddelandehantering via mobil nätanslutningspunkt, eller
2. internetåtkomst.

Även vid misslyckad uppringning gäller skyldigheten att lagra uppgifter som genereras eller behandlas. För telefonitjänst gäller lagringsskyldigheten inte uppgift om nummer som ett samtal styrts till.

Paragrafen regleras en skyldighet att lagra trafikuppgifter för brottsbekämpande ändamål. Ändringen innebär att paragrafens hittillsvarande fjärde stycke flyttas till en ny paragraf, den nya 19 c §, i samma kapitel. Övervägandena finns i avsnitt 7.2.

19 a § *Den som tillhandahåller en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst ska lagra sådana uppgifter som avses i 31 § första stycket 1 som kan användas för att identifiera en abonnent och registrerad användare.*

Lagringsskyldigheten som gäller för allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster omfattar uppgifter som genereras eller behandlas vid tjänster som tillhandahåller samtal och meddelandehantering vid kommunikation som sker till, från eller inom Sverige.

Vid lagring enligt 19 b § av uppgifter som avses i 31 § första stycket 4 omfattar lagringsskyldigheten endast uppgifter som avser lokalisering i Sverige.

Även vid misslyckad uppringning gäller skyldigheten att lagra uppgifter som genereras eller behandlas.

Paragrafen, som är ny, innehåller bestämmelser om att tillhandahållare av allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster ska lagra uppgifter om abonnemang. Den innehåller också vissa generella bestämmelser som gäller när de är lagringsskyldiga. Övervägandena finns i avsnitt 7.2.

Av *första stycket* framgår att den som tillhandahåller en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst ska lagra uppgifter som avses i 31 § första stycket 1, dvs. uppgifter om abonnemang som kan användas för att identifiera en abonnent och registrerad användare.

Av *andra stycket* följer att lagringsskyldigheten för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster gäller kommunikation som sker till, från eller inom Sverige. Detta kan exempelvis fastställas genom att kommunikation skickas från eller tas emot till en ip-adress i Sverige. Det finns även andra sätt att lokalisera en användares kommunikationsutrustning, exempelvis genom lokaliseringsuppgifter som genereras i utrustningen. Om tillhandahållaren behandlar sådana uppgifter, exempelvis för felsökning eller i syfte att kunna rikta reklam, kan uppgifterna användas för att fastställa var kommunikationen har ägt rum. Bestämmelsen gäller både när tillhandahållarna lagrar uppgifter om abonnemang enligt första stycket och vid nationell säkerhetslagring enligt 19 b §.

I *tredje stycket* anges genom hänvisningen till 31 § första stycket 4 att lagring av lokaliseringsuppgifter som inte är trafikuppgifter endast omfattar uppgifter i Sverige. Lagringsskyldigheten för sådana uppgifter finns endast vid lagring som följer av ett beslut om nationell säkerhetslagring enligt 19 b §, se författningskommentaren till den paragrafen.

I *fjärde stycket* föreskrivs att lagringsskyldigheten gäller även vid misslyckad uppringning, dvs. en uppringning som kopplas fram utan att nå en mottagare, såsom när mottagaren inte svarar. Även lagringsskyldigheten för dessa uppgifter gäller endast vid ett beslut om nationell säkerhetslagring (se 19 b §).

19 b § *Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § och den som tillhandahåller en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst ska lagra de uppgifter som framgår av ett beslut enligt lagen (2025:000) om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.*

Beslutet får omfatta sådana uppgifter som avses i 31 § första stycket 1, 3 och 4 som är nödvändiga för att spåra och identifiera kommunikationskällan och slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning, lokalisering av kommunikationsutrustning vid kommunikationen samt lokaliseringsuppgifter som inte är trafikuppgifter.

Paragrafen, som är ny, innehåller bestämmelser om lagringsskyldighet vid nationell säkerhetslagring. Övervägandena finns i avsnitt 6.5.

I *första stycket* anges att lagringsskyldigheten kan avse uppgifter om abonnemang, trafikuppgifter och lokaliseringsuppgifter som inte är trafikuppgifter enligt 31 § första stycket 1, 3 och 4. Förutsättningarna för lagringen framgår i övrigt av lagen om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet. För en kommentar om de förutsättningarna, se författningskommentaren till 2 och 3 §§ den lagen.

I *andra stycket* föreskrivs att bestämmelsen utöver vad som omfattas av 19 § även avser lokaliseringsuppgifter som inte är trafikuppgifter.

19 c § *Den som ska lagra uppgifter enligt 19, 19 a eller 19 b § får ge någon annan i uppdrag att utföra lagringen.*

I paragrafen, som är ny, föreskrivs att den som ska lagra uppgifter får ge någon annan i uppdrag att utföra lagringen. Övervägandena finns i avsnitt 7.2.

Paragrafen motsvarar i sak hittillsvarande 19 § fjärde stycket.

20 § Tillsynsmyndigheten får i enskilda fall besluta om undantag från skyldigheten enligt 19 *eller 19 a §* att lagra uppgifter, om det finns synnerliga skäl för det. Beslutet får förenas med villkor.

Beslutet om undantag får återkallas om villkoren i beslutet inte har följts eller det finns andra särskilda skäl för återkallelse.

I paragrafen regleras möjligheten för tillsynsmyndigheten att i enskilda fall besluta om undantag från lagringsskyldigheten i 19 och 19 a §§. Övervägandena finns i avsnitt 7.2.

I *första stycket* läggs 19 a § till i hänvisningen till vilka bestämmelser om lagringsskyldighet som tillsynsmyndigheten får meddela undantag från. Det innebär att undantag också får meddelas från skyldigheten för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster att lagra uppgifter om abonnemang.

21 § *Trafikuppgifter som avses i 31 § första stycket 3 och* som har lagrats enligt 19 § får behandlas endast för att lämnas ut enligt

1. 33 § första stycket 2 eller 5,
2. 27 kap. 19 § rättegångsbalken, eller
3. lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Uppgifter som har lagrats enligt 19 b § får behandlas enbart för att lämnas ut enligt 8 § lagen (2025:000) om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

Paragrafen innehåller bestämmelser om i vilka fall uppgifter som har lagrats enligt 19 och 19 b §§ får behandlas. Övervägandena finns i avsnitt 5.1 och 6.7.

I *första stycket* görs en ändring som innebär att begränsningen för behandling av uppgifter som lagrats enligt 19 § inte längre gäller uppgifter om abonnemang utan gäller endast trafikuppgifter.

I *andra stycket*, som är nytt, föreskrivs att uppgifter som lagrats vid nationell säkerhetslagring endast får behandlas för att lämnas ut enligt 8 § lagen om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet. Den som är lagringsskyldig har därigenom rätt att lämna ut uppgifter som lagrats i syfte att skydda den nationella säkerheten i enlighet med de villkor som gäller i lagen om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

22 § Uppgifter som avses i 19 § ska lagras enligt följande:

– Uppgifter som genereras eller behandlas vid telefonitjänst och meddelandehantering via mobil nätanslutningspunkt ska lagras i sex månader. Lokaliseringsuppgifter ska dock lagras i endast två månader. *Uppgifter som avses i 31 § första stycket 1 ska lagras i ett år.*

– Uppgifter som genereras eller behandlas vid internetåtkomst ska lagras i tio månader. Om uppgifterna identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten, ska de dock lagras i endast sex månader. *Uppgifter som avses i 31 § första stycket 1 ska lagras i ett år.*

Uppgifter som avses i 19 a § första stycket ska lagras i ett år.

Uppgifter som avses i 19 b § ska lagras enligt följande:

– Uppgifter i 31 § första stycket 1 och 3 ska lagras i två år.

– Uppgifter i 31 § första stycket 4 ska lagras i ett år.

När lagringstiden har löpt ut ska den lagringsskyldige genast utplåna uppgifterna. Om en begäran om utlämnande i fall som avses i 21 § har kommit in eller ett föreläggande enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift har meddelats innan lagringstiden löpt ut, ska den lagringsskyldige dock fortsätta lagra uppgifterna till dess att de har lämnats ut eller tiden för bevarande har löpt ut. Därefter ska uppgifterna genast utplånas.

Paragrafen innehåller bestämmelser om lagringstid och åtgärder som ska vidtas vid lagringstidens slut. Övervägandena finns i avsnitt 5.1, 6.5 och 7.3.

I *första stycket* anges lagringstiderna. Genom tillägg i första och andra strecksatserna ändras lagringstiden för uppgifter om abonnemang till ett år. Det gäller oavsett om uppgifterna genereras eller behandlas vid telefonitjänst via mobil nätanslutningspunkt eller vid internetåtkomst.

Andra stycket, som är nytt, reglerar lagringstiden för uppgifter om abonnemang som lagras av tillhandahållare av nummeroberoende interpersonella kommunikationstjänster enligt 19 a §. Samma lagringstid för uppgifter om abonnemang gäller för sådana tillhandahållare som för tillhandahållare av telefonitjänst via mobil nätanslutningspunkt och vid internetåtkomst enligt första stycket, dvs. ett år.

Tredje stycket, som är nytt, reglerar lagringstiden vid nationell säkerhetslagring. Uppgifter som omfattas av ett sådant beslut ska lagras i två år när det gäller uppgifter om abonnemang och trafikuppgifter som avses 31 § första stycket 1 och 3. Lokaliseringsuppgifter som inte är trafikuppgifter som avses i 31 § första stycket 4 ska lagras i ett år.

Fjärde stycket motsvarar det hittillsvarande tredje stycket.

22 a § *Lagringstiden enligt 22 § räknas från den dag kommunikationen avslutades. Om uppgift saknas om när kommunikationen avslutades räknas lagringstiden från den dag uppgifterna genererades.*

För uppgifter som avses i 31 § första stycket 1 räknas lagringstiden från den dag abonnemanget eller tilldelningen av en tillfällig identifierare upphörde.

För lokaliseringsuppgifter som inte är trafikuppgifter räknas lagringstiden från den dag uppgifterna genererades.

Vid meddelandehantering via en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst räknas lagringstiden från den dag meddelandet skickades.

Paragrafen, som är ny, innehåller bestämmelser som anger hur lagringstiden i 22 § ska beräknas. Övervägandena finns i avsnitt 5.1, 6.5 och 7.3.

Första stycket anger hur lagringstiden för trafikuppgifter ska beräknas. Första meningen motsvarar det hittillsvarande andra stycket i 22 §. I andra meningen görs ett tillägg som innebär att i de fall uppgift om när kommunikationen avslutades saknas, ska lagringstiden i stället räknas från den dag uppgifterna genererades.

Andra stycket anger hur lagringstiden för uppgifter om abonnemang ska beräknas. Lagringstiden räknas från det att abonnemanget upphörde eller att tilldelningen av en tillfällig identifierare upphörde hos användaren. Med tillfälliga identifierare avses exempelvis dynamiska ip-adresser och uppgift om kopplingen mellan permanenta och tillfälliga identifierare i 5G-nätet. Att en användare avregistrerar sig från en nummeroberoende interpersonell kommunikationstjänst kan likställas med att ett abonnemang upphör.

Tredje stycket reglerar hur lagringstiden för lokaliseringsuppgifter som inte är trafikuppgifter ska beräknas. Lagringstiden för sådana uppgifter räknas från den dag uppgiften genererades.

Fjärde stycket innehåller en bestämmelse om lagringstid för meddelanden som skickas via en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst. För meddelanden skickade genom en sådan tjänst räknas lagringstiden från den dag meddelandet skickades.

23 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om

1. vilka uppgifter som ska lagras enligt 19*, 19 a och 19 b §§*, och
2. lagringstiden enligt 22 § *första–tredje styckena och 22 a §*.

Paragrafen innehåller en upplysning om möjligheten att meddela närmare föreskrifter på lägre normgivningsnivå än lag. Övervägandena finns i avsnitt 6.5 och 7.3.

I *punkten 1* görs ett tillägg som innebär att det upplyses om att möjligheten att meddela närmare föreskrifter även omfattar skyldigheten för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster att lagra uppgifter om abonnemang enligt 19 a §. Det görs också ett tillägg som innebär att det upplyses om möjligheten att meddela sådana föreskrifter för nationell säkerhetslagring enligt 19 b §.

Genom tilläggen i *punkten 2* upplyses det om att möjligheten att meddela närmare föreskrifter om lagringstiden även avser när tillhandahållare av nummeroberoende interpersonella kommunikationstjänster lagrar enligt 19 a § och vid nationell säkerhetslagring enligt 19 b §.

29 § *Den som är skyldig att lagra uppgifter enligt 19, 19 a eller 19 b § ska bedriva sin verksamhet* så att beslut om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation *och inhämtning enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet* kan verkställas och så att verkställandet inte röjs.

Första stycket gäller inte vid tillhandahållande av maskin-till-maskin-tjänster.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om frågor som avses i första stycket samt får i enskilda fall besluta om undantag från kravet i första stycket.

Paragrafen innehåller bestämmelser som bl.a. innebär en skyldighet för tillhandahållare att anpassa sin verksamhet så att hemliga tvångsmedel kan verkställas och så att verkställandet inte röjs. Övervägandena finns i avsnitt 5.2 och 7.4.

I *första stycket* görs en ändring som innebär att anpassningsskyldigheten omfattar de som är lagringsskyldiga. Vidare görs en ändring som innebär att även tillhandahållare av nummeroberoende interpersonella kommunikationstjänster omfattas av paragrafen. Det görs också ett förtydligande om att anpassningsskyldigheten även gäller vid beslut om inhämtning med stöd av inhämtningslagen. Ändringarna innebär inte någon ändring av anpassningsskyldigheten i materiellt hänseende.

I *andra stycket*, som är nytt, införs ett undantag från anpassningsskyldigheten för tillhandahållare av maskin-till-maskin-tjänster. Det avser tjänster som omfattar automatisk överföring av data och information mellan enheter och mjukvarubaserade tillämpningar med liten eller ingen mänsklig medverkan. Det gäller exempelvis övervakning, mätning, styrning, transport och logistik i bl.a. bilar, tåg, elmätare, hemlarm och gräsklippare.

Tredje stycket motsvarar det hittillsvarande andra stycket.

29 a § Den som *är skyldig att lagra uppgifter enligt 19, 19 a eller 19 b §* har rätt till ersättning för kostnader som uppstår när uppgifter som avses i 31 § första stycket lämnas ut till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott. I de fall det är särskilt föreskrivet ska ersättningen beräknas enligt schablon. Ersättningen ska betalas av den myndighet som har begärt uppgifterna.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om ersättningen och schablonberäkningen.

Paragrafen innehåller bestämmelser om ersättning vid utlämnande av uppgifter till brottsbekämpande myndigheter. Övervägandena finns i avsnitt 6.6 och 7.5.

Första stycket ändras så att ersättningsrätten även omfattar tillhandahållare av nummeroberoende interpersonella kommunikationstjänster enligt 19 a §. Ändringarna innebär även att utlämning av uppgifter som lagrats enligt ett beslut om nationell säkerhetslagring enligt 19 b § ger rätt till ersättning.

Det tidigare andra stycket, där det stadgades att ersättning även skulle utgå för lokaliseringsuppgifter som inte är trafikuppgifter, utgår som en följd av att sådana uppgifter nu omfattas av tystnadsplikten i 31 § första stycket och därmed av huvudregeln i det nu aktuella första stycket.

Andra stycket motsvarar det hittillsvarande tredje stycket.

29 b § När den som *är skyldig att lagra uppgifter enligt 19, 19 a eller 19 b §* lämnar ut uppgifter som avses i 31 § första stycket till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott, ska utlämnandet, om uppgifterna gäller brottslig verksamhet eller misstanke om brott, göras utan dröjsmål och på ett sådant sätt att utlämnandet inte röjs.

Uppgifterna ska ordnas och göras tillgängliga i ett format som gör att de enkelt kan tas om hand.

Tillsynsmyndigheten får i enskilda fall besluta om undantag från kravet i andra stycket, om det finns särskilda skäl för det.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om hur uppgifterna ska lämnas ut.

Paragrafen innehåller bestämmelser om hur uppgifter ska lämnas ut till brottsbekämpande myndigheter. Övervägandena finns i avsnitt 5.2 och 7.4.

I *första stycket* görs en ändring som innebär att bestämmelsen avser de som är lagringsskyldiga, i stället för de som enligt hittillsvarande ordning är anmälningspliktiga enligt 2 kap. 1 §. Vidare görs en ändring som innebär att även tillhandahållare av nummeroberoende interpersonella kommunikationstjänster omfattas av paragrafen.

Det hittillsvarande tredje stycket, där det stadgades att ersättning även skulle utgå för lokaliseringsuppgifter som inte är trafikuppgifter, tas bort. Uppgifterna omfattas nu av tystnadsplikten i 31 § första stycket och omfattas därmed av huvudregeln i det nu aktuella första stycket.

Tredje och fjärde styckena motsvarar de hittillsvarande fjärde respektive femte styckena.

31 § Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst får inte obehörigen föra vidare eller utnyttja det som han eller hon i samband med tillhandahållandet har fått del av eller tillgång till i form av

1. en uppgift om abonnemang,
2. innehållet i ett elektroniskt meddelande,
3. en *trafikuppgift, eller*
4. *en lokaliseringsuppgift som inte är en trafikuppgift och som rör användare som är fysiska personer eller abonnenter.*

För tillhandahållare av nummeroberoende interpersonella kommunikationstjänster gäller tystnadsplikten enligt första stycket endast vid sådan kommunikation som sker till, från eller inom Sverige samt för lokaliseringsuppgifter som inte är trafikuppgifter och som avser lokalisering i Sverige.

Tystnadsplikt som följer av första stycket gäller inte i förhållande till den som har tagit del i utväxlingen av ett elektroniskt meddelande eller som på något annat sätt har sänt eller tagit emot ett sådant meddelande.

Tystnadsplikt som följer av första stycket 1, 3 *och 4* gäller inte heller i förhållande till innehavaren av *abonnemanget*.

Paragrafen innehåller bestämmelser om tystnadsplikt och undantag från tystnadsplikten. Övervägandena finns i avsnitt 5.3, 6.8 och 7.5.

I *första stycket* tas undantaget för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster bort. Tystnadsplikten gäller därmed även för sådana tillhandahållare, med de begränsningar som framgår av andra till fjärde styckena.

I första stycket 3 ersätts begreppet annan uppgift som angår ett särskilt elektroniskt meddelande med begreppet trafikuppgift. Ändringen innebär inte någon ändring i sak. Begreppet inbegriper liksom hittillsvarande uttryck även lokaliseringsuppgifter som är trafikuppgifter.

Genom den nya *punkten 4* i första stycket omfattas lokaliseringsuppgifter som inte är trafikuppgifter av tystnadsplikten. Sådana lokaliseringsuppgifter får lagras enligt 19 b §.

I *andra stycket* stadgas en särskild begränsning för tystnadsplikten i förhållande till tillhandahållare av nummeroberoende interpersonella kommunikationstjänster. För sådana tillhandahållare gäller tystnadsplikten vid kommunikation som till någon del sker i Sverige samt för lokaliseringsuppgifter som inte är trafikuppgifter och som avser lokalisering i Sverige.

Genom att första stycket punkt 4, som avser lokaliseringsuppgifter som inte är trafikuppgifter, läggs till i *fjärde stycket* gäller inte tystnadsplikt för sådana uppgifter i förhållande till innehavaren av abonnemanget.

Övriga ändringar är språkliga.

32 § Tystnadsplikt som följer av 31 § första stycket gäller även för en uppgift som hänför sig till

1. en åtgärd att med stöd av 27 kap. 9 § rättegångsbalken hålla kvar försändelser,
2. en angelägenhet som avser användning av hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation enligt 27 kap. 18 eller 19 § rättegångsbalken eller som gäller tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation eller med hemlig övervakning av elektronisk kommunikation enligt 4 kap. 25 b § lagen (2000:562) om internationell rättslig hjälp i brottmål,
3. en angelägenhet som avser inhämtning av signaler i elektronisk form enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet,
4. inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet,
5. en begäran enligt 33 § första stycket 2 om att en uppgift om abonnemang ska lämnas,
6. ett föreläggande enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift,
7. en begäran enligt 33 § första stycket 5 om att en uppgift om tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster ska lämnas*, eller*

8. en angelägenhet som avser nationell säkerhetslagring enligt lagen (2025:000) om lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

Paragrafen innehåller ytterligare bestämmelser om tystnadsplikt. Övervägandena finns i avsnitt 6.8.

Punkten 8, som är ny, innebär att tystnadsplikt gäller för en angelägenhet som avser nationell säkerhetslagring. Av 44 kap. 4 § offentlighets- och sekretesslagen framgår att denna tystnadsplikt har företräde framför meddelarfriheten.

33 § Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och som har fått del av eller tillgång till en uppgift som avses i 31 § första stycket ska på begäran lämna

1. en uppgift som avses i 31 § första stycket 1 till

a) en myndighet som i ett särskilt fall behöver en sådan uppgift för delgivning enligt delgivningslagen (2010:1932), om myndigheten bedömer att det kan antas att den som söks för delgivning håller sig undan eller att det annars finns synnerliga skäl,

b) Finansinspektionen, om inspektionen bedömer att uppgiften är av väsentlig betydelse för utredningen av en misstänkt överträdelse av Europaparlamentets och rådets förordning (EU) nr 596/2014 av den 16 april 2014 om marknadsmissbruk (marknadsmissbruksförordning) och om upphävande av Europaparlamentets och rådets direktiv 2003/6/EG och kommissionens direktiv 2003/124/EG, 2003/125/EG och 2004/72/EG,

c) Finansinspektionen, om inspektionen bedömer att uppgiften är av väsentlig betydelse i ett ärende om tillsyn när det gäller någon av bestämmelserna i 4 a kap. 1–8 §§ lagen (2010:751) om betaltjänster eller 1 kap. 5 § eller 4 kap. 7, 8, 9, 10, 11 eller 14 § lagen (2016:1024) om verksamhet med bostadskrediter,

d) Konsumentombudsmannen, om ombudsmannen bedömer att uppgiften är av väsentlig betydelse i ett ärende om tillsyn enligt lagen (1994:1512) om avtalsvillkor i konsumentförhållanden eller marknadsföringslagen (2008:486), när det är fråga om en misstänkt överträdelse av unionslagstiftning som skyddar konsumenternas intressen enligt bilagan till Europaparlamentets och rådets förordning (EU) 2017/2394 av den 12 december 2017 om samarbete mellan de nationella myndigheter som har tillsynsansvar för konsumentskyddslagstiftningen och om upphävande av förordning (EG) nr 2006/2004,

e) Konsumentverket, om verket bedömer att uppgiften är av väsentlig betydelse i ett ärende om tillsyn enligt lagen (2019:59) med kompletterande bestämmelser till EU:s geoblockeringsförordning,

f) Kronofogdemyndigheten, om myndigheten behöver uppgiften i exekutiv verksamhet och myndigheten bedömer att uppgiften är av väsentlig betydelse för handläggningen av ett ärende,

g) Läkemedelsverket, om verket bedömer att uppgiften är av väsentlig betydelse i ett ärende om tillsyn när det gäller bestämmelserna om marknadsföring i 12 kap. läkemedelslagen (2015:315),

h) Polismyndigheten, om myndigheten bedömer att uppgiften behövs i samband med underrättelse, efterforskning eller identifiering vid olyckor eller dödsfall eller för att myndigheten ska kunna fullgöra en uppgift som avses i 12 § polislagen (1984:387),

i) Polismyndigheten, om myndigheten bedömer att uppgiften behövs i ett särskilt fall för att myndigheten ska kunna lokalisera en person som är dömd till fängelse, rättspsykiatrisk vård eller sluten ungdomsvård i syfte att möjliggöra verkställighet av påföljden,

j) Polismyndigheten eller en åklagarmyndighet, om myndigheten bedömer att uppgiften behövs i ett särskilt fall för att myndigheten ska kunna fullgöra en underrättelseskyldighet enligt 33 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare,

k) Skatteverket, om verket bedömer att uppgiften är av väsentlig betydelse för handläggningen av ett ärende som avser kontroll av skatt eller avgift eller rätt folkbokföringsort enligt folkbokföringslagen (1991:481), och

l) Säkerhetspolisen, om myndigheten bedömer att uppgiften behövs i ett särskilt fall för att myndigheten ska kunna lokalisera en utlänning som inte har fullgjort sin anmälningsskyldighet enligt lagen (2022:700) om särskild kontroll av vissa utlänningar,

2. en uppgift som avses i 31 § första stycket 1 och som gäller brottslig verksamhet eller misstanke om brott till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brottet eller den brottsliga verksamheten,

3. en uppgift som avses i 31 § första stycket 1 eller 3 till en regional alarmeringscentral som avses i lagen (1981:1104) om verksamheten hos vissa regionala alarmeringscentraler,

4. en uppgift som avses i 31 § första stycket 1 eller 3 samt uppgift om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits till Polismyndigheten, om myndigheten bedömer att uppgiften behövs i samband med efterforskning av personer som har försvunnit under sådana omständigheter att det kan antas att det då fanns eller fortfarande finns fara för deras liv eller allvarlig risk för deras hälsa, och

5. en uppgift som avses i 31 § första stycket 3 om vilka övriga tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster som har deltagit vid överföringen av ett meddelande som omfattas av ett föreläggande enligt 27 kap. 16 § rätte-

gångsbalken att bevara en viss lagrad uppgift till den myndighet som meddelat föreläggandet.

Ersättning för att lämna ut andra uppgifter enligt första stycket 3 än lokaliseringsuppgifter ska vara skälig med hänsyn till kostnaderna för utlämnandet.

Paragrafen innehåller bestämmelser om en skyldighet att på begäran lämna ut vissa uppgifter som enligt 31 § första stycket omfattas av tystnadsplikt. Övervägandena finns i avsnitt 7.6.

I *första stycket* tas undantaget för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster bort. Skyldigheterna att lämna ut uppgift om abonnemang m.m. med stöd av paragrafen gäller därmed även för sådana tillhandahållare.

12 kap.

1 § Tillsynsmyndigheten ska besluta att ta ut en sanktionsavgift av den som

1. inte tillhandahåller en sammanfattning av avtalet i enlighet med 7 kap. 1 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 102.3 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,
2. inte tillämpar villkor om bindningstid eller uppsägningstid i enlighet med 7 kap. 8, 13 eller 14 §,
3. inte uppfyller kraven på nummerportabilitet i enlighet med 7 kap. 19 och 20 §§ eller föreskrifter om nummerportabilitet som har meddelats med stöd av 7 kap. 21 § första stycket,
4. inte vidtar åtgärder för att hantera risker som hotar säkerheten i nät och tjänster i enlighet med 8 kap. 1 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,
5. inte rapporterar om säkerhetsincidenter i enlighet med 8 kap. 3 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,
6. inte informerar om hot om säkerhetsincidenter i enlighet med 8 kap. 4 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,
7. inte vidtar skyddsåtgärder enligt 8 kap. 5 § eller föreskrifter som har meddelats med stöd av den paragrafen,
8. inte vidtar åtgärder för att säkerställa skydd av uppgifter som behandlas i samband med tillhandahållandet av en tjänst i enlighet med 8 kap. 6 § eller föreskrifter som har meddelats med stöd av den paragrafen,
9. inte informerar abonnenten om särskilda risker för bristande skydd av behandlade uppgifter i enlighet med 8 kap. 7 §,
10. inte underrättar om integritetsincidenter i enlighet med 8 kap. 8 § eller kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets direktiv 2002/58/EG vad gäller personlig integritet och elektronisk kommunikation,

11. inte behandlar uppgifter i ett elektroniskt meddelande eller trafikuppgifter som hör till detta meddelande i enlighet med 9 kap. 27 §,

12. inte bedriver sin verksamhet så att beslut om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation *och inhämtning enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet* kan verkställas och så att verkställandet inte röjs i enlighet med 9 kap. 29 § första stycket eller föreskrifter som har meddelats i anslutning till det stycket,

13. inte ordnar uppgifter och gör dem tillgängliga i ett format som gör att de enkelt kan tas om hand i enlighet med 9 kap. 29 b § andra stycket eller föreskrifter som har meddelats i anslutning till det stycket,

14. inte överför signaler till samverkanspunkter i enlighet med 9 kap. 30 § eller föreskrifter som har meddelats med stöd av den paragrafen,

15. inte lämnar ut en uppgift i enlighet med 9 kap. 33 §*, eller*

16. inte lagrar uppgifter i enlighet med 9 kap. 19, 19 a, 19 b, 22 och 22 a §§ eller föreskrifter som har meddelats i anslutning till de paragraferna.

En sanktionsavgift enligt första stycket 2 ska, när det är fråga om ett paket enligt 7 kap. 26 §, tas ut endast om överträdelsen avser en allmänt tillgänglig elektronisk kommunikationstjänst som inte är en nummeroberoende interpersonell kommunikationstjänst eller en överföringstjänst som används för tillhandahållande av maskin-till-maskin-tjänster.

Paragrafen innehåller bestämmelser om vilka överträdelser som tillsynsmyndigheten ska besluta om sanktionsavgift för. Övervägandena finns i avsnitt 8.

I *första stycket 12* görs ett tillägg som innebär att en sanktionsavgift ska tas ut av den som inte bedriver sin verksamhet så att beslut om inhämtning enligt inhämtningslagen kan verkställas.

Genom *första stycket 16*, som är ny, ska en sanktionsavgift tas ut även av den som inte lagrar uppgifter om elektronisk kommunikation på föreskrivet sätt. Bestämmelsen omfattar dels de som enligt hittillsvarande ordning är lagringsskyldiga enligt 9 kap. 19 §, dels tillhandahållare av allmänt tillgängliga nummeroberoende kommunikationstjänster i 9 kap. 19 a §. Den omfattar även när dessa aktörer är lagringsskyldiga vid nationell säkerhetslagring enligt 9 kap. 19 b §. Möjligheten att ta ut en sanktionsavgift omfattar vidare åsidosättande av skyldigheterna i bestämmelserna om lagringstid enligt 9 kap. 22 och 22 a §§. Slutligen omfattar bestämmelsen också bristande efterlevnad av föreskrifter som har meddelats i anslutning till paragraferna.

Sammanfattning av betänkandet Datalagring och åtkomst till elektronisk information (SOU 2023:22)

Utredningens uppdrag och arbete

Vi har haft i uppdrag att analysera och utvärdera nuvarande reglering om lagring av och tillgång till uppgifter om elektronisk kommunikation för brottsbekämpande syften, bl.a. i förhållande till ny praxis från EU-domstolen. I uppdraget har också ingått att analysera förutsättningar för att leverantörer av s.k. OTT-tjänster ska kunna omfattas av skyldigheten att lagra och ge tillgång till uppgifter om elektronisk information. Uppdraget har även omfattat att analysera och föreslå moderniseringar när det gäller tillhandahållarnas skyldighet att se till att hemliga tvångsmedel kan verkställas på ett effektivt sätt. Vi har också haft i uppdrag att se över vissa frågor om svenska myndigheters tillgång till elektroniska uppgifter, när de finns utanför Sveriges gränser (exekutiv jurisdiktion).

Syftet med uppdraget har varit att säkerställa att de brottsbekämpande myndigheternas tillgång till information förbättras och inte försämras över tid på grund av teknikutveckling och förändrade kommunikationsvanor, samtidigt som respekten för mänskliga rättigheter säkerställs.

EU-rätten och datalagring

Förslag om ändring av svensk datalagringsreglering bör lämnas i anledning av ny domstolspraxis från EU-domstolen

Datalagring innebär en skyldighet för tillhandahållare av elektroniska kommunikationsnät och kommunikationstjänster, t.ex. mobiloperatörer, att lagra uppgifter om elektronisk kommunikation. Begreppet uppgifter om elektronisk kommunikation omfattar information om kommunikationen men inte själva innehållet. Information om kommunikation kan exempelvis vara vem som kommunicerade med vem, när kommunikationen skedde och var de parter som kommunicerade med varandra befann sig.

I Sverige har datalagring för brottsbekämpande ändamål funnits sedan 1990-talet. I dag spelar EU-rätten en stor roll för lagstiftningen om datalagring för brottsbekämpande ändamål.

Europaparlamentets och rådets direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (e-dataskyddsdirektivet) anger bl.a. att medlemsstaterna ska säkerställa konfidentialitet vid elektronisk kommunikation och därmed förbundna trafikuppgifter. Uppgifter som inte längre behövs ska enligt direktivet utplånas eller avidentifieras. Medlemsstaterna får dock göra undantag från dessa skyldigheter om det behövs för bl.a. brottsbekämp-

ande verksamhet. Direktivet är genomfört i svensk rätt främst genom bestämmelser i lagen (2022:482) om elektronisk kommunikation (LEK).

De svenska bestämmelserna om datalagring prövades av EU-domstolen i de förenade målen C-203/15 och C-698/15 (Tele2-domen). Lagringsskyldigheten vid tiden för domen var generell och obegränsad i den meningen att den omfattade alla telefoni-, meddelande- och bredbandstjänster som tillhandahölls av de traditionella teleoperatörerna. I Tele2-domen slog EU-domstolen fast att sådan lagringsskyldighet överskred gränserna för vad som är strängt nödvändigt och att den inte, i enlighet med e-dataskyddsdirektivet, kunde anses motiverad i ett demokratiskt samhälle.

Den svenska lagstiftningen sågs därför över och den 1 oktober 2019 trädde nya regler om datalagring i kraft (prop. 2018/19:86). Anpassningarna till EU-rätten innebar bl.a. att lagringsskyldigheten begränsades och lagringstiderna differentierades.

Efter Tele2-domen har ny praxis kommit från EU-domstolen i flera mål som rör datalagring. Till följd av domarna har bl.a. Tyskland, Frankrike, Belgien och Danmark anpassat sina regler om datalagring till EU-rätten.

Vår analys visar att det kan finnas anledning att ändra den svenska regleringen med anledning av EU-domstolens praxis från senare tid. Vi har gjort bedömningen att förslag bör lämnas om datalagring för att skydda den nationella säkerheten. Vi har även kommit till slutsatsen att det finns anledning att lämna förslag om s.k. riktad lagring för att bekämpa grov brottslighet. Med begreppet riktad lagring avses normalt en lagring av uppgifter som är avgränsad, antingen till ett visst geografiskt område, till en viss personkrets eller med hjälp av något annat särskiljande kriterium, exempelvis tekniska kriterier.

Nationell säkerhetslagring

Vi har föreslagit regler om nationell säkerhetslagring. En sådan ska vara tillåten, om den bedöms vara absolut nödvändig för att bekämpa ett allvarligt hot mot nationell säkerhet som är verkligt och aktuellt eller förutsebart. Säkerhetspolisen ska bedöma hotet mot den nationella säkerheten och får, om ett säkerhetshot finns, besluta om en generell och odifferentierad lagringsskyldighet.

Ett beslut om nationell säkerhetslagring ska kunna bli föremål för en effektiv kontroll. Ett offentligt ombud ska bevaka enskildas intressen och kunna överklaga Säkerhetspolisens beslut till ett kontrollorgan. Kontrollorganet ska pröva om förutsättningarna för lagringsskyldigheten är uppfyllda och om lagringsskyldigheten är proportionell. Kontrollorganet ska kunna fastställa eller upphäva Säkerhetspolisens beslut om lagring. Vi föreslår att ett nytt särskilt beslutsorgan inom Säkerhets- och integritetsskyddsnämnden (SIN), Datalagringsdelegationen, ska vara kontrollorgan.

Lagringsskyldigheten, vid nationell säkerhetslagring, är mer omfattande än dagens lagringsskyldighet, både vad gäller vilka slags uppgifter som kan lagras och själva lagringstiden. Exempelvis ska lokaliseringsuppgifter som inte är trafikuppgifter kunna omfattas av nationell säkerhetslagring. Med lokaliseringsuppgifter som inte är trafikuppgifter avses exempelvis gps-positioner som genereras i en mobiltelefon. Lagringstiden ska vara två år och som huvudregel räknas från den dag kommunikationen avslutades.

Tillgången genom straffprocessuella tvångsmedel till uppgifter som har lagrats för att skydda den nationella säkerheten ska vara begränsad till bekämpning av brott och brottslighet som kan innebära ett allvarligt hot mot Sveriges säkerhet. De lagringsskyldiga, dvs. tillhandahållarna, måste därför kunna särskilja uppgifter som lagras på denna grund från andra lagrade uppgifter.

Beslut om nationell säkerhetslagring ska omfattas av sekretess och tystnadsplikt ska gälla för tillhandahållarna.

Lagring för att bekämpa grov brottslighet som inte utgör ett hot mot den nationella säkerheten

Vi har vidare lämnat förslag på två former av riktad lagring i syfte att bekämpa grov brottslighet, geografiskt riktad lagring och utökad riktad lagring. Dessa förslag skulle kunna ersätta dagens lagringsregler rörande uppgifter om elektronisk kommunikation i brottsbekämpande syfte.

Geografiskt riktad lagring

Geografiskt riktad lagring ska ske i områden där det utifrån objektiva kriterier går att konstatera att det finns en jämförelsevis större sannolikhet för förekomst av grov brottslighet än i andra områden. Geografiskt riktad lagring ska grunda sig på den officiella statistiken över anmälda brott som redovisas av Brottsförebyggande rådet (Brå) och med kommunerna som geografiska enheter. Post- och telestyrelsen (PTS) ska årligen föreskriva vilka kommuner som ska omfattas av den geografiskt riktade lagringen.

Utökad riktad lagring

Utökad riktad lagring ska komplettera den geografiskt riktade lagringen. Utökad riktad lagring kan avse

ett begränsat geografiskt område där grov brottslighet har förekommit eller där det är sannolikt att grov brottslighet kommer att äga rum,

en skyddsvärd plats,

en person som dömts för grova brott,

en person som har varit föremål för hemliga tvångsmedel, eller

en utrustnings- eller abonnemangsidentitet som använts vid eller skäligen kan antas komma till användning vid ett grovt brott eller vid grov brottslig verksamhet.

Polismyndigheten, Säkerhetspolisen och Tullverket ska få besluta om utökad riktad lagring och SIN ska utöva tillsyn över tillämpningen.

Geografiskt riktad lagring ska omfatta fler uppgiftstyper än den lagringsskyldighet som gäller i dag. Lagringsskyldigheten omfattar samma typer av uppgifter som får lagras vid nationell säkerhetslagring. Även ett beslut om utökad riktad lagring får omfatta samma uppgiftstyper. Lagringstiden för såväl geografiskt riktad lagring som utökad riktad lagring ska vara ett år, som huvudregel räknat från den dag kommunikationen avslutades.

Beslut om utökad riktad lagring ska omfattas av sekretess och för tillhandahållarna gäller tystnadsplikt.

Tillhandahållare av OTT-tjänster

De s.k. OTT-tjänsterna har i hög grad påverkat enskildas kommunikationsvanor. Det är i dag mycket vanligt att kommunikation sker genom internetbaserade tjänster som vissa e-posttjänster eller tjänster som Apple Imessage, Apple Facetime, Discord, Snapchat, Google Messages, Google Meet, Kik Messenger, Line, Messenger from Meta, Skype, Slack, Telegram, Viber och Whatsapp, för att nämna några bland många. Inom den EU-rättsliga regleringen används begreppet allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster (Noik) som ett samlingsbegrepp för dessa tjänster.

Tillhandahållare av Noik har i dag inte någon lagringsskyldighet motsvarande den som de traditionella teleoperatörerna har. Det sker således ingen datalagring för brottsbekämpande ändamål vid användning av Noik-tjänsterna. Vår analys visar att den tekniska utvecklingen och ändrade kommunikationsvanor har inneburit försämrade möjligheter för de brottsbekämpande myndigheternas arbete. De brottsbekämpande myndigheterna har stor nytta och ett påtagligt behov av uppgifter om elektronisk kommunikation, även när kommunikationen sker i andra kanaler än via de traditionella teleoperatörerna. Vi har gjort bedömningen att nyttan och behovet av tillgång till uppgifter om elektronisk kommunikation från tillhandahållare av Noik väger tyngre än de motstående intressen som talar emot en sådan tillgång.

Skyldigheter för tillhandahållare av Noik

Vi har föreslagit att lagringsskyldighet ska gälla även för den som tillhandahåller allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster (Noik) i Sverige.

Lagringsskyldigheten ska omfatta kommunikation som till någon del sker i Sverige. Detta kan exempelvis fastställas genom att kommunikation skickas från eller mottas via en ip-adress i Sverige.

Lagringsskyldigheten och lagringstiden ska som huvudregel motsvara det vi föreslår för övriga lagringsskyldiga, dvs. enligt våra förslag om nationell säkerhetslagring, geografiskt riktad lagring och utökad riktad lagring.

Tillhandahållare av Noik ska omfattas av sådan tystnadsplikt som gäller för tillhandahållare av andra elektroniska kommunikationstjänster.

Uppdraget att modernisera anpassningsskyldigheten

De som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster enligt LEK spelar en viktig roll när brottsbekämpande myndigheter hämtar in elektronisk kommunikation och uppgifter om sådan. För att underlätta för de brottsbekämpande myndigheterna har tillhandahållarna ålagts en viss anpassningsskyldighet. Skyldigheten innebär att verksamheten ska bedrivas så att hemliga tvångsmedel kan verkställas och att det ska kunna ske utan att verkställandet röjs.

Den teknikutveckling som skett och fortfarande pågår har dock medfört att regleringen av anpassningsskyldighet har blivit oklar och ålderdomlig. Med hänsyn till våra förslag om lagringsskyldighet för tillhandahållare av Noik finns ytterligare behov av förändring av anpassningsskyldigheten. Vi föreslår därför en modernisering av bestämmelserna om anpassningsskyldighet för att åstadkomma en reglering som är tydlig, enhetlig och teknikneutral.

En modernisering av anpassningsskyldigheten

Vi har förslagit att anpassningsskyldigheten ska omfatta samma aktörer som enligt våra förslag ska omfattas av lagringsskyldighet enligt LEK. Ett undantag ska dock gälla för tillhandahållare av s.k. maskin-till-maskin-tjänster. Med maskin-till-maskin-tjänster avses tjänster som omfattar automatisk överföring av data mellan enheter eller mjukvarubaserade tillämpningar, med liten eller ingen mänsklig medverkan. Tjänsterna kan exempelvis användas för övervakning, mätning, styrning, transport och logistik i bl.a. bilar, tåg, elmätare, hemlarm och gräsklippare.

Även tillhandahållare av Noik ska alltså vara skyldiga att bedriva sin verksamhet så att beslut om hemliga tvångsmedel kan verkställas och så att verkställandet inte röjs. Det omfattar även de fall en tillhandahållare för sina kunder möjliggör totalsträckskryptering, dvs. när bara sändare och mottagare har tillgång till meddelandena i läsbar form. I dessa fall innebär anpassningsskyldigheten att tillhandahållaren ska kunna göra uppgifterna tillgängliga för brottsbekämpande myndigheter i läsbar form.

Vid ett utlämnande av uppgifter ska tillhandahållare av Noik även omfattas av rätten till ersättning.

Exekutiv jurisdiktion

Rätten för en stat att vidta åtgärder och verkställa beslut som har fattats inom ramen för lagstiftning och rättskipning kallas exekutiv jurisdiktion. Utgångspunkten i folkrätten är att det råder ett förbud för stater att vidta verkställighetsåtgärder, t.ex. att använda hemliga tvångsmedel, inom andra staters territorier. Detta baseras på den s.k. territorialitetsprincipen, som är en grundläggande folkrättslig princip om staters suveränitet.

Elektroniskt lagrade uppgifter kan finnas i flera stater samtidigt eller ständigt förflyttas mellan olika stater. I många fall är det inte ens för den som tillhandahåller tjänsten möjligt att klargöra var uppgifterna finns i varje givet ögonblick. Även när detta är möjligt kan förhållandena ändras på bråkdelen av en sekund.

För en effektiv brottsbekämpning är det viktigt att reglerna om tillgång till elektronisk kommunikation och annan elektronisk bevisning också kan tillämpas i praktiken, även när informationen finns utanför Sverige eller när det är okänt var den finns.

Vi har sett över förutsättningarna, inklusive de folkrättsliga aspekterna, för att införa en särskild lagreglering för exekutiv jurisdiktion i förhållande till elektronisk information som finns utanför Sverige vid användning av straffprocessuella tvångsmedel.

Vi har gjort bedömningen att det under vissa förutsättningar inte finns några folkrättsliga hinder mot att de brottsbekämpande myndigheterna inhämtar elektronisk information som är eller kan vara lagrad utanför Sverige. Högsta domstolen har den 30 mars 2023 avseende exekutiv jurisdiktion meddelat beslut om att genomsökning på distans får ske även om den eftersökta informationen kan vara lagrad i utlandet.[15]

Mot bakgrund av det har vi föreslagit en lagreglering som förtydligar vad som gäller för viss inhämtning av elektronisk information som lagras utanför Sverige.

Inhämtning av elektronisk information som lagras utanför Sverige

Vi har föreslagit en lagreglering avseende möjligheten för brottsbekämpande myndigheter att inhämta elektronisk information som lagras eller kan vara lagrad utanför Sverige, t.ex. information på användarkonton till olika molntjänster.

För detta ska krävas

- att de brottsbekämpande myndigheterna utan bistånd kan skaffa sig tillgång till uppgifterna,
- att inhämtningen inte bedöms innebära mer än ett obetydligt intrång i en annan stats suveränitet, och
- att inhämtningen inte bedöms kunna orsaka någon skada på det avläsningsbara informationssystem som tvångsmedlet avser.

Konsekvenser och genomförande

Förslagen om nationell säkerhetslagring, lagringsskyldighet också för tillhandahållare av Noik, modernisering av anpassningsskyldigheten och om exekutiv jurisdiktion kommer att vara klart positiva för brottsbekämpningen. Förslagen om riktad lagring kan ibland komma att försvåra det brottsbekämpande arbetet. Sammantaget kommer dock förslagen att vara till fördel för brottsbekämpningen.

Våra förslag om nationell säkerhetslagring kan öka risken för intrång i den personliga integriteten jämfört med i dag. Det gör inte förslagen om en modernisering av anpassningsskyldigheten. Inte heller förslaget till reglering om exekutiv jurisdiktion kan sägas öka risken för intrång i den personliga integriteten. Förslagen om riktad lagring kan leda till en minskad risk för intrång i den personliga integriteten. De tekniska anpassningar som behövs för en förändrad lagringsskyldighet leder till kostnadsökningar för tillhandahållarna och förslagen kan ha en viss påverkan på konkurrensen mellan företag. Polismyndigheten, Säkerhetspolisen, Tullverket och SIN kommer att behöva ytterligare resurser.

De föreslagna reglerna om inhämtning av elektronisk information som är lagrad utanför Sverige föreslås träda i kraft den 1 juli 2024. Övriga författningsförslag föreslås träda i kraft den 1 juli 2025.

[15] Se Högsta domstolens beslut den 30 mars 2023 i mål Ö 5686-22.

Betänkandets lagförslag

Förslag till lag (2024:000) om inhämtning av elektronisk information som är lagrad utanför Sverige vid användning av straffprocessuella tvångsmedel

Härigenom föreskrivs följande.

1 § Med de begränsningar som följer av 2 och 3 §§ denna lag får brottsbekämpande myndigheter genom straffprocessuella tvångsmedel inhämta elektronisk information som är lagrad utanför Sverige.

2 § Inhämtning enligt 1 § får avse endast sådan information som de brottsbekämpande myndigheterna utan bistånd kan skaffa sig tillgång till i det informationssystem som tvångsmedlet avser.

3 § Inhämtning enligt 1 § får inte innebära mer än ett obetydligt intrång i en annan stats suveränitet. Information får inte inhämtas, om inhämtningen bedöms kunna orsaka någon skada på det informationssystem som tvångsmedlet avser.

Denna lag träder i kraft den 1 juli 2024.

Förslag till lag (2025:000) om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet

Härigenom föreskrivs följande.

1 § Denna lag innehåller bestämmelser om när uppgifter om elektronisk kommunikation får lagras och lämnas ut för att skydda Sveriges säkerhet.

Föreläggande om nationell säkerhetslagring

2 § Säkerhetspolisen får, om det föreligger ett allvarligt hot mot Sveriges säkerhet som är verkligt och aktuellt eller förutsebart, förelägga den som är skyldig att lagra uppgifter enligt 9 kap. 19 § lagen (2022:482) om elektronisk kommunikation att lagra uppgifter om elektronisk kommunikation i enlighet med vad som följer av denna lag (nationell säkerhetslagring). Säkerhetspolisen ska inför sin bedömning av hotet mot Sveriges säkerhet samråda med Försvarsmakten.

Ett föreläggande enligt första stycket får gälla i högst ett år. Säkerhetspolisen får genom ett nytt föreläggande förlänga lagringsskyldigheten om hotet mot Sveriges säkerhet består. Om det inte längre finns skäl för nationell säkerhetslagring, ska Säkerhetspolisen upphäva föreläggandet.

Av 9 kap. 19 b och 22 §§ lagen om elektronisk kommunikation framgår vilka uppgifter som får omfattas av ett föreläggande enligt första stycket respektive hur länge uppgifterna ska lagras.

3 § Ett föreläggande enligt 2 § får meddelas endast när det är absolut nödvändigt för att skydda Sveriges säkerhet. Föreläggandet ska begränsas till vad som är absolut nödvändigt för syftet med lagringen i fråga om

1. vilka tillhandahållare som ska omfattas av lagringsskyldigheten,
2. beslutets giltighetstid, och
3. vilka typer av uppgifter som ska omfattas av lagringsskyldigheten.

Offentligt ombud

4 § Ett offentligt ombud ska bevaka enskildas intressen i ärenden om nationell säkerhetslagring.

5 § Regeringen förordnar för en period om högst tre år en person som ska tjänstgöra som ordinarie offentligt ombud samt en person som i första hand ska vara det ordinarie ombudets ställföreträdare och en annan person som i andra hand ska vara det ordinarie ombudets ställföreträdare.

Ett offentligt ombud ska vara svensk medborgare och ska ha varit ordinarie domare, vara eller ha varit advokat eller ha motsvarande juridisk erfarenhet. Ett offentligt ombud får inte vara i konkurstillstånd eller ha förvaltare enligt 11 kap. 7 § föräldrabalken.

Regeringen ska inhämta förslag på lämpliga personer från Domarnämnden och Sveriges advokatsamfund.

Ett offentligt ombud får trots att regeringens förordnande har upphört slutföra uppdraget i ett specifikt ärende om nationell säkerhetslagring.

6 § I fråga om ersättning till ett offentligt ombud tillämpas bestämmelserna i 21 kap. 10 § första och andra styckena rättegångsbalken. Säkerhetspolisen beslutar om ersättning till det offentliga ombudet. Om Säkerhetspolisens beslut om nationell säkerhetslagring överklagas, ska Säkerhets- och integritetsskyddsnämnden besluta om ersättning till det offentliga ombudet. Om beslutet om nationell säkerhetslagring inte överklagas, får det offentliga ombudet överklaga Säkerhetspolisens beslut om ersättning till Säkerhets- och integritetsskyddsnämnden.

7 § Den som förordnats som offentligt ombud får inte obehörigen röja vad han eller hon har fått kännedom om i ett ärende om nationell säkerhetslagring.

Beslut och överklagande

8 § När Säkerhetspolisen avser att fatta ett beslut om nationell säkerhetslagring ska myndigheten så snart som möjligt hålla ett sammanträde till vilket det offentliga ombudet ska kallas. Det offentliga ombudet har vid sammanträdet rätt att ta del av det tilltänkta beslutet om nationell säkerhetslagring och de omständigheter som ligger till grund för detta. Vid sammanträdet ska Säkerhetspolisen redogöra för beslutet och det offentliga ombudet har rätt att ställa frågor. Säkerhetspolisen får därefter besluta om nationell säkerhetslagring.

Det offentliga ombudet har rätt att inom en vecka från beslutet om nationell säkerhetslagring överklaga detta till Säkerhets- och integritetsskyddsnämnden. Det offentliga ombudet får avge en skriftlig förklaring om att beslutet inte kommer att överklagas.

9 § Säkerhetspolisen ska underrätta Säkerhets- och integritetsskyddsnämnden om att ett beslut om nationell säkerhetslagring har överklagats. Säkerhets- och integritetsskyddsnämnden ska så snart som möjligt därefter hålla ett sammanträde. Vid sammanträdet ska Säkerhetspolisen och det offentliga ombudet närvara. Säkerhets- och integritetsskyddsnämnden har vid sammanträdet rätt att ta del av de omständigheter som ligger till grund för beslutet om nationell säkerhetslagring. Vid sammanträdet ska Säkerhetspolisen redogöra för beslutet och det offentliga ombudet har rätt att yttra sig.

10 § Säkerhets- och integritetsskyddsnämnden ska pröva om Säkerhetspolisens beslut om nationell säkerhetslagring ska fastställas eller upphävas. Säkerhets- och integritetsskyddsnämndens beslut får inte överklagas.

Säkerhetspolisens beslut om nationell säkerhetslagring får verkställas om det inte har överklagats inom föreskriven tid, om det offentliga ombudet har avgett en förklaring enligt 8 § andra stycket eller om det har fastställts av Säkerhets- och integritetsskyddsnämnden.

Bilaga 2

Tillgång till lagrade uppgifter

11 § Uppgifter som har lagrats med stöd av ett föreläggande enligt 2 § får endast inhämtas efter ett tillstånd till hemlig avlyssning av elektronisk kommunikation eller till hemlig övervakning av elektronisk kommunikation enligt 27 kap. 18 § eller 19 § rättegångsbalken eller ett tillstånd till inhämtning enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Inhämtning enligt första stycket får ske endast om det i tillståndet har angetts att inhämtningen får avse uppgifter som har lagrats med stöd av denna lag.

12 § Inhämtning av uppgifter enligt 11 § får endast ske i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott som anges i andra stycket eller för att utreda och beivra sådana brott.

De brott som ger rätt till inhämtning av uppgifter som lagrats med stöd av ett föreläggande enligt 2 § är:

1. sabotage eller grovt sabotage enligt 13 kap. 4 eller 5 § brottsbalken,
2. mordbrand, grov mordbrand, allmänfarlig ödeläggelse, kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 1, 2, 3, 5 a eller 5 b § brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
3. uppror, väpnat hot mot laglig ordning eller brott mot medborgerlig frihet enligt 18 kap. 1, 3 eller 5 § brottsbalken,
4. högförräderi, krigsanstiftan, spionieri, grovt spionieri, obehörig befattning med hemlig uppgift, grov obehörig befattning med hemlig uppgift eller olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person enligt 19 kap. 1, 2, 5, 6, 7, 8, 10, 10 a eller 10 b § brottsbalken,
5. företagsspionieri enligt 26 § lagen (2018:558) om företagshemligheter, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning,
6. terroristbrott, samröre med en terroristorganisation, finansiering av terrorism eller särskilt allvarlig brottslighet, offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet, rekrytering till terrorism eller särskilt allvarlig brottslighet, utbildning för terrorism eller särskilt allvarlig brottslighet eller resa för terrorism eller särskilt allvarlig brottslighet enligt 4, 5, 6, 7, 8, 9 eller 10 § terroristbrottslagen (2022:666),
7. andra brott än de som anges i 1–6 och som på grund av sin omfattning eller karaktär utgör ett allvarligt hot mot Sveriges säkerhet, om det för brottet inte är föreskrivet lindrigare straff än fängelse i två år, eller
8. försök, förberedelse eller stämpling till brott som avses i 1–7, om en sådan gärning är belagd med straff.

Denna lag träder i kraft den 1 juli 2025.

Förslag till lag (2025:000) om lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet

Härigenom föreskrivs följande.

1 § Denna lag innehåller bestämmelser om när uppgifter om elektronisk kommunikation får lagras för att bekämpa grov brottslighet.

Geografiskt riktad lagring

2 § Uppgifter om elektronisk kommunikation får lagras i vissa kommuner för att bekämpa grov brottslighet (geografiskt riktad lagring). Bestämmelser om sådan lagringsskyldighet finns, förutom i denna lag, i 9 kap. 19 c § lagen (2022:482) om elektronisk kommunikation.

3 § Lagring enligt 2 § ska avse de kommuner där antalet brottsanmälningar är samma eller högre än genomsnittet i landet.

Beräkningen enligt första stycket ska grunda sig på den slutliga årsstatistiken över anmälda brott som tas fram enligt lagen (2001:99) om den officiella statistiken och ska göras utifrån ett genomsnitt av anmälda brott delat med befolkningsmängden under den treårsperiod som föregår lagringsskyldigheten.

4 § Post- och telestyrelsen ska årligen, senast den 1 juni, föreskriva vilka kommuner som omfattas av geografiskt riktad lagring enligt 3 §.

Utökad riktad lagring

5 § Geografiskt riktad lagring får kompletteras med utökad riktad lagring enligt 9 kap. 19 d § lagen (2022:482) om elektronisk kommunikation avseende

1. ett begränsat geografiskt område där brott som avses i 27 kap. 19 § tredje stycket rättegångsbalken har förekommit eller där det är sannolikt att sådant brott kommer att äga rum,
2. en skyddsvärd plats,
3. en person som är eller har varit föremål för
   – hemliga tvångsmedel som avses i rättegångsbalken,
   – hemlig dataavläsning enligt lagen (2020:62) om hemlig dataavläsning, eller
   – beslut enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet,
4. en person som genom lagakraftvunnen dom eller godkänt strafföreläggande ålagts påföljd för brott som avses i 1, eller
5. sådan utrustnings- eller abonnemangsidentitet som använts vid eller skäligen kan antas komma till användning vid brott som avses i 1 eller vid brottslig verksamhet som innefattar sådana brott.

Ett beslut om lagring enligt första stycket 3 får inte grunda sig på ett tvångsmedelsbeslut som är äldre än tre år. Ett beslut om lagring enligt första stycket 4 får inte grunda sig på en dom eller ett godkänt strafföreläggande senare än tre år efter det att den ålagda påföljden till fullo har verkställts.

6 § Vid bedömningen av vad som är en skyddsvärd plats enligt 5 § första stycket 2 ska särskilt beaktas om

1. platsen är ett skyddsobjekt enligt skyddslagen (2010:305),
2. det bedrivs säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585) på platsen, eller
3. platsen annars bedöms vara särskilt betydelsefull från brottsbekämpningssynpunkt.

7 § Polismyndigheten, Säkerhetspolisen och Tullverket får besluta om utökad riktad lagring enligt 5 §. Ett sådant beslut ska innehålla de skäl som beslutet grundas på. Innan beslut fattas ska myndigheterna samråda med varandra om behovet av utökad riktad lagring. I brådskande fall, eller om samråd är olämpligt av sekretesskäl, får beslut fattas utan samråd. Om det behövs, ska samråd äga rum även med andra myndigheter.

Den beslutande myndigheten ska underrätta Säkerhets- och integritetsskyddsnämnden om beslutet och skälen för detta senast en vecka efter det att beslutet fattades.

8 § Ett beslut om utökad riktad lagring får gälla

1. högst ett år om beslutet avser ett område enligt 5 § första stycket 1,
2. högst tre år om beslutet avser en skyddsvärd plats enligt 5 § första stycket 2,
3. högst ett år om beslutet avser en person enligt 5 § första stycket 3 och 4, och
4. högst ett år om beslutet avser utrustnings- eller abonnemangsidentitet enligt 5 § första stycket 5.

Om det föreligger ett fortsatt behov av lagring, får lagringsskyldigheten förlängas genom ett nytt beslut. Beslut om lagring enligt 5 § första stycket 3 och 4, får inte fattas senare än tre år efter det tvångsmedelsbeslutet meddelades eller den ålagda påföljden till fullo har verkställts.

9 § Ett beslut om utökad riktad lagring får fattas endast när det är absolut nödvändigt för att bekämpa grov brottslighet. Beslutet ska begränsas till vad som är absolut nödvändigt för syftet med lagringen i fråga om

1. vilka tillhandahållare som ska omfattas av lagringsskyldigheten,
2. beslutets giltighetstid, och
3. vilka typer av uppgifter som ska omfattas av lagringsskyldigheten.

10 § Om det inte längre finns skäl för utökad riktad lagring, ska beslutet upphävas av den myndighet som har fattat beslutet.

11 § Polismyndighetens, Säkerhetspolisens och Tullverkets beslut enligt denna lag får inte överklagas.

Bilaga 2

Förslag till lag om ändring i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet

Härigenom föreskrivs i fråga om lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet att 1 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

1 §[1]

Säkerhets- och integritetsskyddsnämnden (nämnden) ska utöva tillsyn över

1. brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter,
2. Säkerhetspolisens användning av hemliga tvångsmedel vid särskild kontroll av vissa utlänningar, och
3. därmed sammanhängande verksamhet.

Nämnden ska även utöva tillsyn över den behandling av personuppgifter som utförs av Polismyndigheten, Säkerhetspolisen och Ekobrottsmyndigheten enligt brottsdatalagen (2018:1177) och lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område för de syften som anges i 1 kap. 1 § i den sistnämnda lagen, och lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter. Tillsynen ska särskilt avse behandling enligt 2 kap. 11 § brottsdatalagen och 2 kap. 9 § lagen om Säkerhetspolisens behandling av personuppgifter.

Nämnden ska också utöva tillsyn över Polismyndighetens och Säkerhetspolisens tillämpning av lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott.	Nämnden ska också utöva tillsyn över Polismyndighetens och Säkerhetspolisens tillämpning av lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott *samt Polismyndighetens, Säkerhetspolisens och Tullverkets tillämpning av bestämmelserna om utökad riktad lagring enligt lagen (2025:000) om lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet.*

Tillsynen ska särskilt syfta till att säkerställa att verksamhet enligt första-tredje styckena bedrivs i enlighet med lag eller annan författning.

Denna lag träder i kraft den 1 juli 2025.

[1] Senaste lydelse 2022:707.

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

Härigenom föreskrivs i fråga om offentlighets- och sekretesslagen (2009:400) att 10 kap. 10 §, 18 kap. 19 §, 29 kap. 2 §, 35 kap. 1 och 24 §§, och 44 kap. 4 och 5 §§ ska ha följande lydelse.

Nuvarande lydelse *Föreslagen lydelse*

10 kap.

10 §[1]

Sekretess hindrar inte att den som är knuten till en myndighet på det sätt som anges i 2 kap. 1 § andra stycket och som är misstänkt för brott eller mot vilken rättegång eller annat jämförbart rättsligt förfarande har inletts, lämnar uppgift till sitt ombud eller biträde i saken eller till någon annan enskild, om det behövs för att han eller hon ska kunna ta till vara sin rätt.

Sekretess hindrar inte att uppgift i ett ärende hos domstol eller i ett beslut i ett sådant ärende lämnas till ett offentligt ombud enligt rättegångsbalken eller till ett integritetsskyddsombud enligt lagen (2009:966) om Försvarsunderrättelsedomstol.

Sekretess hindrar inte att uppgift i ett ärende om nationell säkerhetslagring lämnas till ett offentligt ombud enligt lagen (2025:000) om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

18 kap.

19 §[2]

Den tystnadsplikt som följer av 5–8, 9 och 10 §§, 11 § första stycket och 12 och 13 §§ inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning *eller* hemlig dataavläsning på grund av beslut av domstol, undersökningsledare eller åklagare *eller* in-

Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att meddela och offentliggöra upp- gifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning, hemlig dataavläsning på grund av beslut av domstol, undersökningsledare eller åklagare eller inhämtning av upp-

[1] Senaste lydelse 2009:1020.
[2] Senaste lydelse 2020:66.

hämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.	gifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*, nationell säkerhetslagring enligt lagen (2025:000) om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet, eller utökad riktad lagring enligt lagen (2025:000) om lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet.*

Den tystnadsplikt som följer av 17 § inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning på grund av beslut av domstol eller åklagare.

Att den tystnadsplikt som följer av 1–3 §§ i vissa fall inskränker rätten att meddela och offentliggöra uppgifter utöver det som anges i andra stycket följer av 7 kap. 10 §, 12–18 §§, 20 § 3 och 22 § första stycket 1 och andra stycket tryckfrihetsförordningen samt 5 kap. 1 § och 4 § första stycket 1 och andra stycket yttrandefrihetsgrundlagen.

29 kap.

2 §[3]

Sekretess gäller hos en myndighet som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst för uppgift om innehållet i ett elektroniskt meddelande eller *annan uppgift som angår ett särskilt elektroniskt meddelande*. Om sekretess inte följer av någon annan bestämmelse, får dock sådan uppgift lämnas till den som har tagit del i utväxlingen av ett elektroniskt meddelande eller som på något annat sätt har sänt eller tagit emot ett sådant meddelande. Detsamma gäller innehavaren av ett abonnemang som använts för ett elektroniskt meddelande när det är fråga om uppgift om något annat än innehållet i meddelandet.	Sekretess gäller hos en myndighet som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst för uppgift om innehållet i ett elektroniskt meddelande eller *trafikuppgift*. Om sekretess inte följer av någon annan bestämmelse, får dock sådan uppgift lämnas till den som har tagit del i utväxlingen av ett elektroniskt meddelande eller som på något annat sätt har sänt eller tagit emot ett sådant meddelande. Detsamma gäller innehavaren av ett abonnemang som använts för ett elektroniskt meddelande när det är fråga om uppgift om något annat än innehållet i meddelandet.

[3] Senaste lydelse 2012:288.

35 kap.

1 §[4]

Sekretess gäller för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i

1. utredning enligt bestämmelserna om förundersökning i brottmål,

2. angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott,

3. angelägenhet som avser säkerhetsprövning enligt säkerhetsskyddslagen (2018:585),

4. annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott eller verkställa uppbörd och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen,

5. register som förs av Polismyndigheten enligt 5 kap. lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas med stöd av de bestämmelserna, eller uppgifter som behandlas av Säkerhetspolisen eller Polismyndigheten med stöd av lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter,

6. register som förs enligt lagen (1998:621) om misstankeregister,

7. register som förs av Skatteverket enligt lagen (2018:1696) om Skatteverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag,

8. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 5 kap. 1 §, *eller*

9. register som förs av Tullverket enligt lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag.

8. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 5 kap. 1 §,

9. register som förs av Tullverket enligt lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag,

10. angelägenhet som avser nationell säkerhetslagring enligt lagen (2025:000) om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet, eller

11. angelägenhet som avser utökad riktad lagring lagen (2025:000) om lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet.

Sekretessen enligt första stycket 2 gäller hos domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till honom eller henne lider skada eller men om uppgiften röjs. Vid förhandling om användning av tvångsmedel gäller

[4] Senaste lydelse 2019:1184.

sekretess för uppgift om vem som är misstänkt endast om det kan antas att fara uppkommer för att den misstänkte eller någon närstående till honom eller henne utsätts för våld eller lider annat allvarligt men om uppgiften röjs.

Första stycket gäller inte om annat följer av 2, 6 eller 7 §.

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

24 §[5]

Den tystnadsplikt som följer av *11 §* och den tystnadsplikt som följer av ett förbehåll som har gjorts med stöd av 9 § andra stycket inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.	Den tystnadsplikt som följer av *1 § 10 och 11,* 11 § och den tystnadsplikt som följer av ett förbehåll som har gjorts med stöd av 9 § andra stycket inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Den tystnadsplikt som följer av 15 och 16 §§ inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift vars röjande kan antas medföra fara för att någon utsätts för våld eller lider annat allvarligt men.

44 kap.

4 §[6]

Rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter inskränks av den tystnadsplikt som följer av

1. 2 kap. 14 § första stycket 1 och 3–5 postlagen (2010:1045),

2. 9 kap. 31 § lagen (2022:482) om elektronisk kommunikation, när det är fråga om uppgift om innehållet i ett elektroniskt meddelande eller som annars rör ett särskilt sådant meddelande, och

3. 9 kap. 32 § lagen om elektronisk kommunikation, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation på grund av beslut av domstol, undersökningsledare eller åklagare *eller* om inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.	3. 9 kap. 32 § lagen om elektronisk kommunikation, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation på grund av beslut av domstol, undersökningsledare eller åklagare*,* om inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, *om nationell säkerhetslagring enligt lagen (2025:000) om lagring av och åtkomst till uppgifter om elektronisk*

[5] Senaste lydelse 2018:1919.

[6] Senaste lydelse 2022:1495.

	kommunikation i syfte att skydda Sveriges säkerhet, eller om utökad riktad lagring enligt lagen (2025:000) om lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet.

5 §[7]

Rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter inskränks av den tystnadsplikt som följer

1. av beslut som har meddelats med stöd av 7 § lagen (1999:988) om förhör m.m. hos kommissionen för granskning av de svenska säkerhetstjänsternas författningsskyddande verksamhet,

2. av 7 kap. 1 § 1 lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap,

3. av 4 kap. 16 § försäkringsrörelselagen (2010:2043),

4. av 5 kap. 15 § lagen (1998:293) om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige,

5.av 32 § lagen (2020:62) om hemlig dataavläsning,

6. av 11 a § lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen, *och*	6. av 11 a § lagen (1996:701) om Tullverkets befogenheter vid Sveriges gräns mot ett annat land inom Europeiska unionen,
7. av 4 kap. 23 a § tullagen (2016:253).	7. av 4 kap. 23 a § tullagen (2016:253), *och*
	8. av 7 § lagen (2025:000) om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

Denna lag träder i kraft den 1 juli 2025.

[7] Senaste lydelse 2022:1495.

Bilaga 2

Förslag till lag om ändring i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet

Härigenom föreskrivs att 1 § lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 §[1]	
Polismyndigheten, Säkerhetspolisen eller Tullverket får, under de förutsättningar som anges i denna lag, i underrättelseverksamhet i hemlighet från den som enligt lagen (2022:482) om elektronisk kommunikation tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst *som inte är en nummeroberoende interpersonell kommunikationstjänst* hämta in uppgifter om	Polismyndigheten, Säkerhetspolisen eller Tullverket får, under de förutsättningar som anges i denna lag, i underrättelseverksamhet i hemlighet från den som enligt lagen (2022:482) om elektronisk kommunikation tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst hämta in uppgifter om

1. meddelanden som i ett elektroniskt kommunikationsnät har överförts till eller från ett telefonnummer eller annan adress,
2. vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område, eller
3. i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits.

Denna lag träder i kraft den 1 juli 2025.

[1] Senaste lydelse 2022:501.

Förslag till lag om ändring i lagen (2022:482) om elektronisk kommunikation

Härigenom föreskrivs i fråga om lagen (2022:482) om elektronisk kommunikation

dels att 9 kap. 20 §[1] ska upphöra att gälla,

dels att 8 kap. 5 §, 9 kap. 1, 10, 19, 21–23, 29–29 b, 31–33 §§ och 12 kap. 1 § ska ha följande lydelse,

dels att det ska införas fem nya paragrafer, 9 kap. 19 a–e §§ och närmast före 9 kap. 19–23 §§ nya rubriker av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
8 kap.	
5 §[2]	
Den som enligt 9 kap. 19 § är skyldig att lagra uppgifter ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling.	
Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § och som har förelagts enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift ska avseende den uppgiften vidta sådana åtgärder som anges i första stycket.	*Den som* enligt 27 kap. 16 § rättegångsbalken har förelagts att bevara en viss lagrad uppgift ska avseende den uppgiften vidta sådana åtgärder som anges i första stycket.
Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om sådana skyddsåtgärder.	
9 kap.	
1 §[3]	
Den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst ska utplåna eller avidentifiera trafikuppgifter som har lagrats eller behandlats på något annat sätt när de inte längre behövs för överföring av ett elektroniskt meddelande. Detta gäller under förutsättning att uppgifterna avser användare som är fysiska personer eller abonnenter.	
Första stycket avser inte uppgifter som sparas för sådan behandling som anges i 2, 15, *19* eller 21 § eller om uppgifterna behövs för en sådan behandling som är tillåten enligt Europaparlamentets och rådets förordning (EU) 2021/1232 av den 14 juli 2021 om ett tillfälligt undantag från vissa bestämmelser i direktiv 2002/58/EG vad gäller användning av teknik hos tillhanda-	Första stycket avser inte uppgifter som sparas för sådan behandling som anges i 2, 15, *19 b– 19 d* eller 21 § eller om uppgifterna behövs för en sådan behandling som är tillåten enligt Europaparlamentets och rådets förordning (EU) 2021/1232 av den 14 juli 2021 om ett tillfälligt undantag från vissa bestämmelser i direktiv 2002/58/EG vad gäller användning av teknik hos tillhanda-

[1] Senaste lydelse av 20 § 2022:482
[2] Senaste lydelse 2022:1086.
[3] Senaste lydelse 2022:482.

hållare av nummeroberoende interpersonella kommunikationstjänster för behandling av personuppgifter och andra uppgifter i syfte att bekämpa sexuella övergrepp mot barn på nätet	hållare av nummeroberoende interpersonella kommunikationstjänster för behandling av personuppgifter och andra uppgifter i syfte att bekämpa sexuella övergrepp mot barn på nätet.
	10 §[4]
	Lokaliseringsuppgifter som ska lagras enligt 19 b–19 d §§ får behandlas trots 7–9 §§.
Lokaliseringsuppgifter som omfattas av ett beslut om inhämtning av uppgifter enligt 27 kap. rättegångsbalken, eller lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet får behandlas trots 7–9 §§.	
Lagring och annan behandling av trafikuppgifter m.m. för brottsbekämpande ändamål	***Lagringsskyldiga och tjänster som omfattas av lagringsskyldighet***
	19 §[5]
Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § ska lagra sådana uppgifter som avses i 31 § första stycket 1 och 3 *som är nödvändiga för att spåra och identifiera kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning* vid *kommunikationens början och slut.*	Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § *och den som tillhandahåller en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst* ska *utan dröjsmål lagra uppgifter enligt vad som anges i 19 a–19 d §§.*
Lagringsskyldigheten omfattar uppgifter som genereras eller behandlas vid	*För den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § omfattar lagringsskyldigheten* uppgifter som genereras eller behandlas vid *tjänster som tillhandahåller*
1. telefonitjänst eller meddelandehantering *via mobil nätanslutningspunkt*, eller	1. telefonitjänst eller meddelandehantering, eller
2. internetåtkomst.	
Även vid misslyckad uppringning gäller skyldigheten att lagra uppgifter som genereras eller behand-	*För den som tillhandahåller en allmänt tillgänglig nummeroberoende interpersonell kommunika-*

[4] Senaste lydelse 2022:482.
[5] Senaste lydelse 2022:482.

las. För telefonitjänst gäller lagringsskyldigheten inte uppgift om nummer som ett samtal styrts till.

tionstjänst omfattar lagringsskyldigheten uppgifter som genereras eller behandlas vid tjänster som tillhandahåller samtal och meddelandehantering vid sådan kommunikation som sker till, från eller inom Sverige.

Den som enligt denna paragraf ska lagra uppgifter får uppdra åt någon annan att utföra lagringen.

Lagring av uppgift om abonnemang

19 a §

Den som är skyldig att lagra uppgifter enligt 19 § ska lagra sådana uppgifter som avses i 31 § första stycket 1 som kan användas för att identifiera en abonnent och registrerad användare.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vilka uppgifter som ska lagras enligt första stycket.

Nationell säkerhetslagring

19 b §

Den som är skyldig att lagra uppgifter enligt 19 § ska lagra de uppgifter som framgår av ett föreläggande enligt 2 § lagen (2025:000) om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet. Ett sådant föreläggande får omfatta sådana uppgifter som avses i 31 § första stycket 1, 3 och 4 som är nödvändiga för att spåra och identifiera kommunikationskällan och slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning, lokalisering av kommunikationsutrustning vid kommunikationen samt lokaliseringsuppgifter som inte är trafikuppgifter.

Geografiskt riktad lagring

19 c §

Den som är skyldig att lagra uppgifter enligt 19 § ska i de kommuner som föreskrivs enligt 4 § lagen (2025:000) om lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet lagra sådana uppgifter som anges i 19 b §.

Utökad riktad lagring

19 d §

Den som är skyldig att lagra uppgifter enligt 19 § ska lagra de uppgifter som framgår av ett beslut enligt 5 § lagen (2025:000) om lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet. Ett sådant beslut får omfatta sådana uppgifter som anges i 19 b §.

Lagringsskyldighet vid misslyckad uppringning

19 e §

Lagringsskyldigheten enligt 19 c § ska även omfatta uppgifter som genereras eller behandlas vid misslyckad uppringning. Sådana uppgifter får även lagras enligt 19 b och 19 d §§.

21 §[6]

Behandling av trafik- och lokaliseringsuppgifter

Uppgifter som har lagrats enligt *19 §* får behandlas endast för att lämnas ut enligt

Uppgifter som har lagrats enligt *19 c och d §§* får behandlas endast för att lämnas ut enligt

1. 33 § första stycket 2 eller 5,
2. 27 kap. 19 § rättegångsbalken, eller
3. lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

[6] Senaste lydelse 2022:482.

	Uppgifter som har lagrats enligt 19 b § får behandlas enbart för att lämnas ut enligt 11 § lagen (2025:000) om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

22 §[7]

Lagringstider

Uppgifter som avses *i 19 §* ska lagras enligt följande:	Uppgifter som avses *i 19 a–d §§* ska lagras enligt följande.
– Uppgifter som genereras eller behandlas vid telefonitjänst och meddelandehantering via mobil nätanslutningspunkt ska lagras i sex månader. Lokaliseringsuppgifter ska dock lagras i endast två månader.	*– Uppgifterna som avses i 19 a § ska lagras till dess att ett år har förflutit sedan abonnemanget upphörde eller tilldelningen av en tillfällig identifierare upphörde.*
	– Uppgifter som avses i 19 b § ska lagras i två år.
– Uppgifter som genereras eller behandlas vid internetåtkomst ska lagras i tio månader. Om uppgifterna identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten, ska de dock lagras i endast sex månader.	*– Uppgifter som avses i 19 c och 19 d §§ ska lagras i ett år.*
Lagringstiden räknas från den dag kommunikationen avslutades.	Lagringstiden räknas från den dag kommunikationen avslutades. *Om uppgift saknas om när kommunikationen avslutades, ska lagringstiden räknas från den dag då uppgifterna genererades. Beträffande lokaliseringsuppgift som inte är trafikuppgift räknas lagringstiden från den dag då uppgiften genererades.*
	Vid meddelandehantering via en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst räknas lagringstiden från den dag meddelandet skickades.

När lagringstiden har löpt ut ska den lagringsskyldige genast utplåna uppgifterna. Om en begäran om utlämnande i fall som avses i 21 § har kommit in eller ett föreläggande enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift har meddelats innan lagringstiden löpt ut, ska den lagringsskyldige dock fortsätta lagra uppgifterna till dess att de har lämnats ut eller tiden för bevarande har löpt ut. Därefter ska uppgifterna genast utplånas.

[7] Senaste lydelse 2022:482.

23 §[8]

Upplysning om verkställighetsföreskrifter

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om

1. vilka uppgifter som ska lagras enligt *19 §, och*

2. lagringstiden enligt 22 § första *stycket*.

1. vilka uppgifter som ska lagras enligt *19 b–19 d §§, och*

2. lagringstiden enligt 22 § första, *andra och tredje stycket*.

29 §[9]

En verksamhet *ska bedrivas* så att beslut om hemlig avlyssning av elektronisk kommunikation *och* hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs*, om verksamheten avser tillhandahållande av*

1. ett allmänt elektroniskt kommunikationsnät som inte enbart är avsett för utsändning till allmänheten av program som avses i 1 kap. 2 § yttrandefrihetsgrundlagen, eller

2. tjänster inom ett allmänt elektroniskt kommunikationsnät som består av

a) en allmänt tillgänglig telefonitjänst till en fast nätanslutningspunkt som medger överföring av lokala, nationella och internationella samtal, telefax och datakommunikation med en sådan lägsta datahastighet som medger funktionell tillgång till internet, eller

b) en allmänt tillgänglig elektronisk kommunikationstjänst till en mobil nätanslutningspunkt.

Den som är skyldig att lagra uppgifter enligt 19 § ska bedriva sin verksamhet så att beslut om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation *och inhämtning enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet* kan verkställas och så att verkställandet inte röjs.

Första stycket gäller inte vid tillhandahållande av maskin-till-maskin-tjänster.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om frågor

[8] Senaste lydelse 2022:1086.
[9] Senaste lydelse 2022:1086.

som avses i första stycket samt får i enskilda fall besluta om undantag från kravet i första stycket.

29 a §[10]

Den som bedriver verksamhet *som ska anmälas enligt 2 kap. 1 §* har rätt till ersättning för kostnader som uppstår när uppgifter som avses i 31 § första stycket lämnas ut till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott. I de fall det är särskilt föreskrivet ska ersättningen beräknas enligt schablon. Ersättningen ska betalas av den myndighet som har begärt uppgifterna.

Första stycket gäller även lokaliseringsuppgifter som inte är trafikuppgifter.

Den som *är skyldig att lagra uppgifter enligt 19 §* har rätt till ersättning för kostnader som uppstår när uppgifter som avses i 31 § första stycket lämnas ut till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott. I de fall det är särskilt föreskrivet ska ersättningen beräknas enligt schablon. Ersättningen ska betalas av den myndighet som har begärt uppgifterna.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om ersättningen och schablonberäkningen.

29 b §[11]

När den som bedriver verksamhet som *ska anmälas enligt 2 kap. 1 §* lämnar ut uppgifter som avses i 31 § första stycket till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott, ska utlämnandet, om uppgifterna gäller brottslig verksamhet eller misstanke om brott, göras utan dröjsmål och på ett sådant sätt att utlämnandet inte röjs.

Uppgifterna ska ordnas och göras tillgängliga i ett format som gör att de enkelt kan tas om hand.

Första och andra styckena gäller även lokaliseringsuppgifter som inte är trafikuppgifter.

När den som *är skyldig att lagra uppgifter enligt 19 §* lämnar ut uppgifter som avses i 31 § första stycket till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott, ska utlämnandet, om uppgifterna gäller brottslig verksamhet eller misstanke om brott, göras utan dröjsmål och på ett sådant sätt att utlämnandet inte röjs.

Tillsynsmyndigheten får i enskilda fall besluta om undantag från kravet i andra stycket, om det finns särskilda skäl för det.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om hur uppgifterna ska lämnas ut.

[10] Senaste lydelse 2022:1086.
[11] Senaste lydelse 2022:1086.

31 §[12]

Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst *som inte är en nummeroberoende interpersonell kommunikationstjänst,* får inte obehörigen föra vidare eller utnyttja det som han eller hon i samband med tillhandahållandet har fått del av eller tillgång till i form av

1. en uppgift om abonnemang,
2. innehållet i ett elektroniskt meddelande, *eller*
3. en *annan uppgift som angår ett särskilt elektroniskt meddelande.*

Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, får inte obehörigen föra vidare eller utnyttja det som han eller hon i samband med tillhandahållandet har fått del av eller tillgång till i form av

2. innehållet i ett elektroniskt meddelande,
3. en trafikuppgift, eller
4. en lokaliseringsuppgift som inte är en trafikuppgift och som rör användare som är fysiska personer eller abonnenter.

För tillhandahållare av nummeroberoende interpersonella kommunikationstjänster gäller tystnadsplikten enligt första stycket endast vid sådan kommunikation som sker till, från eller inom Sverige samt för lokaliseringsuppgifter i Sverige som inte är trafikuppgifter.

Tystnadsplikt som följer av första stycket gäller inte i förhållande till den som har tagit del i utväxlingen av ett elektroniskt meddelande eller som på något annat sätt har sänt eller tagit emot ett sådant meddelande.

Tystnadsplikt som följer av första stycket 1 *och* 3 gäller inte heller i förhållande till innehavaren av *ett abonnemang som har använts för ett elektroniskt meddelande*.

Tystnadsplikt som följer av första stycket 1, *3 och 4* gäller inte heller i förhållande till innehavaren av *abonnemanget*.

32 §[13]

Tystnadsplikt som följer av 31 § första stycket gäller även för en uppgift som hänför sig till

1. en åtgärd att med stöd av 27 kap. 9 § rättegångsbalken hålla kvar försändelser,
2. en angelägenhet som avser användning av hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation enligt 27 kap. 18 eller 19 § rättegångsbalken eller som gäller tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation eller med hemlig övervakning av elektronisk kommunikation enligt 4 kap. 25 b § lagen (2000:562) om internationell rättslig hjälp i brottmål,

[12] Senaste lydelse 2022:482.
[13] Senaste lydelse 2022:482.

3. en angelägenhet som avser inhämtning av signaler i elektronisk form enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet,

4. inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet,

5. en begäran enligt 33 § första stycket 2 om att en uppgift om abonnemang ska lämnas,

6. ett föreläggande enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift, *eller*

7. en begäran enligt 33 § första stycket 5 om att en uppgift om tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster ska lämnas.

6. ett föreläggande enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift,

7. en begäran enligt 33 § första stycket 5 om att en uppgift om tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster ska lämnas,

8. en angelägenhet som avser nationell säkerhetslagring enligt lagen (2025:000) om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet, eller

9. en angelägenhet som avser utökad riktad lagring enligt lagen (2025:000) om lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet.

33 §[14]

Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst *som inte är en nummeroberoende interpersonell kommunikationstjänst* och som har fått del av eller tillgång till en uppgift som avses i 31 § första stycket ska på begäran lämna

Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och som har fått del av eller tillgång till en uppgift som avses i 31 § första stycket ska på begäran lämna

1. en uppgift som avses i 31 § första stycket 1 till

a) en myndighet som i ett särskilt fall behöver en sådan uppgift för delgivning enligt delgivningslagen (2010:1932), om myndigheten bedömer att det kan antas att den som söks för delgivning håller sig undan eller att det annars finns synnerliga skäl,

b) Finansinspektionen, om inspektionen bedömer att uppgiften är av väsentlig betydelse för utredningen av en misstänkt överträdelse av Europaparlamentets och rådets förordning (EU) nr 596/2014 av den 16 april 2014 om marknadsmissbruk (marknadsmissbruksförordning) och om upphävande av Europaparlamentets och rådets direktiv 2003/6/EG och kommissionens direktiv 2003/124/EG, 2003/125/EG och 2004/72/EG,

[14] Senaste lydelse 2022:1086.

c) Finansinspektionen, om inspektionen bedömer att uppgiften är av väsentlig betydelse i ett ärende om tillsyn när det gäller någon av bestämmelserna i 4 a kap. 1–8 §§ lagen (2010:751) om betaltjänster eller 1 kap. 5 § eller 4 kap. 7, 8, 9, 10, 11 eller 14 § lagen (2016:1024) om verksamhet med bostadskrediter,

d) Konsumentombudsmannen, om ombudsmannen bedömer att uppgiften är av väsentlig betydelse i ett ärende om tillsyn enligt lagen (1994:1512) om avtalsvillkor i konsumentförhållanden eller marknadsföringslagen (2008:486), när det är fråga om en misstänkt överträdelse av unionslagstiftning som skyddar konsumenternas intressen enligt bilagan till Europaparlamentets och rådets förordning (EU) 2017/2394 av den 12 december 2017 om samarbete mellan de nationella myndigheter som har tillsynsansvar för konsumentskyddslagstiftningen och om upphävande av förordning (EG) nr 2006/2004,

e) Konsumentverket, om verket bedömer att uppgiften är av väsentlig betydelse i ett ärende om tillsyn enligt lagen (2019:59) med kompletterande bestämmelser till EU:s geoblockeringsförordning,

f) Kronofogdemyndigheten, om myndigheten behöver uppgiften i exekutiv verksamhet och myndigheten bedömer att uppgiften är av väsentlig betydelse för handläggningen av ett ärende,

g) Läkemedelsverket, om verket bedömer att uppgiften är av väsentlig betydelse i ett ärende om tillsyn när det gäller bestämmelserna om marknadsföring i 12 kap. läkemedelslagen (2015:315),

h) Polismyndigheten, om myndigheten bedömer att uppgiften behövs i samband med underrättelse, efterforskning eller identifiering vid olyckor eller dödsfall eller för att myndigheten ska kunna fullgöra en uppgift som avses i 12 § polislagen (1984:387),

i) Polismyndigheten eller en åklagarmyndighet, om myndigheten bedömer att uppgiften behövs i ett särskilt fall för att myndigheten ska kunna fullgöra en underrättelseskyldighet enligt 33 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare, och

j) Skatteverket, om verket bedömer att uppgiften är av väsentlig betydelse för handläggningen av ett ärende som avser kontroll av skatt eller avgift eller rätt folkbokföringsort enligt folkbokföringslagen (1991:481),

2. en uppgift som avses i 31 § första stycket 1 och som gäller brottslig verksamhet eller misstanke om brott till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brottet eller den brottsliga verksamheten,

3. en uppgift som avses i 31 § första stycket 1 eller 3 till en regional alarmeringscentral som avses i lagen (1981:1104) om verksamheten hos vissa regionala alarmeringscentraler,

4. en uppgift som avses i 31 § första stycket 1 eller 3 samt uppgift om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits till Polismyndigheten, om myndigheten bedömer att uppgiften behövs i samband med efterforskning av personer som har försvunnit under sådana omständigheter att det kan antas att det då fanns eller fortfarande finns fara för deras liv eller allvarlig risk för deras hälsa, och

5. en uppgift som avses i 31 § första stycket 3 om vilka övriga tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommuni-

kationstjänster som har deltagit vid överföringen av ett meddelande som omfattas av ett föreläggande enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift till den myndighet som meddelat föreläggandet.

Ersättning för att lämna ut andra uppgifter enligt första stycket 3 än lokaliseringsuppgifter ska vara skälig med hänsyn till kostnaderna för utlämnandet.

12 kap.

1 §[15]

Tillsynsmyndigheten ska ta ut en sanktionsavgift av den som

1. inte tillhandahåller en sammanfattning av avtalet i enlighet med 7 kap. 1 §, föreskrifter som har meddelats med stöd av den paragrafen och genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 102.3 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,

2. inte tillämpar villkor om bindningstid och uppsägningstid i enlighet med 7 kap. 8, 13 eller 14 §,

3. inte uppfyller kraven på nummerportabilitet i enlighet med 7 kap. 19 och 20 §§ och föreskrifter om nummerportabilitet som har meddelats med stöd av 7 kap. 21 § första stycket,

4. inte vidtar åtgärder för att hantera risker som hotar säkerheten i nät och tjänster i enlighet med 8 kap. 1 §, föreskrifter som har meddelats med stöd av den paragrafen och genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,

5. inte rapporterar om säkerhetsincidenter i enlighet med 8 kap. 3 §, föreskrifter som har meddelats med stöd av den paragrafen och genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,

6. inte informerar om hot om säkerhetsincidenter i enlighet med 8 kap. 4 §, föreskrifter som har meddelats med stöd av den paragrafen och genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,

7. inte vidtar skyddsåtgärder enligt 8 kap. 5 § och föreskrifter som har meddelats med stöd av den paragrafen,

8. inte vidtar åtgärder för att säkerställa skydd av uppgifter som behandlas i samband med tillhandahållandet av en tjänst i enlighet med 8 kap. 6 § och föreskrifter som har meddelats med stöd av den paragrafen,

9. inte informerar abonnenten om särskilda risker för bristande skydd av behandlade uppgifter i enlighet med 8 kap. 7 §,

10. inte underrättar om integritetsincidenter i enlighet med 8 kap. 8 § och föreskrifter som har meddelats med stöd av den paragrafen,

11. inte behandlar uppgifter i ett elektroniskt meddelande eller trafikuppgifter som hör till detta meddelande i enlighet med 9 kap. 27 §,

12. inte bedriver sin verksamhet så att beslut om hemlig avlyssning av elektronisk kommunikation *och* hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs i en-

12. inte bedriver sin verksamhet så att beslut om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation *och inhämtning enligt lagen (2012:278) om inhämt-*

[15] Senaste lydelse 2022:1086.

lighet med 9 kap. 29 § första stycket och föreskrifter som har meddelats i anslutning till det stycket,	*ning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet* kan verkställas och så att verkställandet inte röjs i enlighet med 9 kap. 29 § första stycket och föreskrifter som har meddelats i anslutning till det stycket,

13. inte ordnar uppgifter och gör dem tillgängliga i ett format som gör att de enkelt kan tas om hand i enlighet med 9 kap. 29 b § andra stycket och föreskrifter som har meddelats i anslutning till det stycket,

14. inte överför signaler till samverkanspunkter i enlighet med 9 kap. 30 § och föreskrifter som har meddelats med stöd av den paragrafen, *eller*	14. inte överför signaler till samverkanspunkter i enlighet med 9 kap. 30 § och föreskrifter som har meddelats med stöd av den paragrafen,
15. inte lämnar ut en uppgift i enlighet med 9 kap. 33 §.	15. inte lämnar ut en uppgift i enlighet med 9 kap. 33 §, *eller*
	16. inte lagrar uppgifter i enlighet med 9 kap. 19 a–d och 22 §§ och föreskrifter som har meddelats i anslutning till dessa paragrafer.

En sanktionsavgift enligt första stycket 2 ska, när det är fråga om ett paket enligt 7 kap. 26 §, tas ut endast om överträdelsen avser en allmänt tillgänglig elektronisk kommunikationstjänst som inte är en nummeroberoende interpersonell kommunikationstjänst eller en överföringstjänst som används för tillhandahållande av maskin-till-maskin-tjänster.

---

1. Denna lag träder i kraft den 1 juli 2025.

2. Uppgifter som lagrats enligt 9 kap. 19 § ska lagras enligt 9 kap. 22 § efter ikraftträdandet av denna lag.

Förteckning över remissinstanserna

Efter remiss av betänkandet Datalagring och åtkomst till elektronisk information (SOU 2023:22) har yttranden lämnats av Apple Aktiebolag, Bahnhof AB, Brottsförebyggande rådet, Brottsofferjouren Sverige, Brottsoffermyndigheten, Dataskydd.net Sverige, Diskrimineringsombudsmannen, Domarnämnden, Domstolsverket, ECPAT Sverige, Ekobrottsmyndigheten, Föreningen för Digitala fri- och rättigheter, Försvarets radioanstalt, Försvarsmakten, Försvarsunderrättelsedomstolen, Förvaltningsrätten i Stockholm, Göteborgs tingsrätt, Göteborgs universitet (Juridiska institutionen), Helsingborgs tingsrätt, HI3G Access AB, Hovrätten för Västra Sverige, Institutet för mänskliga rättigheter, Integritetsskyddsmyndigheten, ISOC-SE, Justitiekanslern, Kammarrätten i Stockholm, Kommerskollegium, Kriminalvården, Kustbevakningen, Myndigheten för samhällsskydd och beredskap, Netnod AB, Polismyndigheten, Post- och telestyrelsen, Riksdagens ombudsmän, Skatteverket, Statens inspektion för försvarsunderrättelseverksamheten, Stiftelsen för Internetinfrastruktur, Stockholms tingsrätt, Stockholms universitet (juridiska fakulteten), Svea hovrätt, Svenska Journalistförbundet, Sveriges advokatsamfund, Sveriges Domareförbund, Säkerhets- och integritetsskyddsnämnden, Säkerhetspolisen, Södertörns tingsrätt, TechSverige, Tele2 Sverige AB, Telenor Sverige AB, Telia Sverige AB, Tidningsutgivarna, Tullverket, Uppsala universitet (juridiska fakulteten) och Åklagarmyndigheten.

Amnesty international, Centrum för rättvisa, Civil Rights Defenders, Facebook Sweden AB, Google Sweden AB, Microsoft AB, RISE Research Institutes of Sweden AB, Rädda barnen, Rättighetsalliansen, Svenska stadsnätsföreningen och Utgivarna har inte hörts av.