Datalagring och åtkomst till elektronisk information

2021 års datalagringsutredning

Stockholm 2023

STATENS OFFENTLIGA UTREDNINGAR

SOU 2023:22

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

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

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck och remisshantering: Elanders Sverige AB, Stockholm 2023

ISBN 978-91-525-0611-0 (tryck)
ISBN 978-91-525-0612-7 (pdf)
ISSN 0375-250X

Till statsrådet och chefen för Justitiedepartementet

Regeringen beslutade den 5 augusti 2021 att tillkalla en särskild utredare med uppdraget 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). Till särskild utredare förordnades samma dag f.d. lagmannen Sigurd Heuman.

Rättssakkunniga Staffan Uhlmann (Justitiedepartementet) samt kanslirådet Felisa Krzyzanski och Susanna Mattsson (Infrastrukturdepartementet, numera Finansdepartementet) förordnades som sakkunniga att biträda utredningen från och med den 23 september 2021. Som experter förordnades från och med samma dag advokaten Johanna Björkman (Advokatsamfundet), enhetschefen Cecilia Agnehall (Säkerhets- och integritetsskyddsnämnden), vice chefsåklagaren Måns Biörklund (Åklagarmyndigheten), kammaråklagaren Johan Lengholm (Åklagarmyndigheten), vice chefsåklagaren Ted Murelius (Ekobrottsmyndigheten), juristen Peder Cristvall (Post- och telestyrelsen), rådmannen Christofer Gatenheim (Göteborgs tingsrätt), juristerna Sofie Klahr och Anna Olander Selldén (Polismyndigheten), enhetschefen Robert Nygren och verksjuristen Carl Rundström Frödén (Säkerhetspolisen), verksjuristen Micaela Nordberg (Tullverket) och juristen Lisa Zettervall (Integritetsskyddsmyndigheten).

Måns Biörklund entledigades från och med den 24 februari 2022 och ersattes av kammaråklagaren Christoffer Östlind (Åklagarmyndigheten). Cecilia Agnehall entledigades från och med den 8 juli 2022 och ersattes av verksjuristen Jessica Öhlund Andersson (Säkerhets- och integritetsskyddsnämnden). Carl Rundström Frödén entlediga-

des från och med den 21 oktober 2022 och ersattes av verksjuristen Maria Sertcanli (Säkerhetspolisen).

Som sekreterare anställdes från och med den 16 augusti 2021 rättschefen Eva Melander Tell. Från och med den 25 juli 2022 anställdes rättsutvecklaren Soheil Roshanbin som sekreterare varvid Eva Melander Tell blev huvudsekreterare. Eva Melander Tell entledigades från uppdraget från och med den 6 februari 2023.

Utredningen har antagit namnet 2021 års datalagringsutredning. Sigurd Heuman svarar som utredare ensam för innehållet i betänkandet även om också experterna har ställt sig bakom det, i den mån inte annat framgår av ett särskilt yttrande. Särskilda uppfattningar i enskildheter och i formuleringar kan dock förekomma utan sådant yttrande. Härmed överlämnas betänkandet *Datalagring och åtkomst till elektronisk information* (SOU 2023:22).

Stockholm i maj 2023

Sigurd Heuman

/ Eva Melander Tell
Soheil Roshanbin

Innehåll

Förkortningar

anmälnings-direktivet	Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster
Brå	Brottsförebyggande rådet
datalagrings-direktivet	Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät
dataskydds-direktivet	Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter
E.164-nummer	Den internationella nummerplanen för telefoni
e-dataskydds-direktivet	Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktivet om integritet och elektronisk kommunikation) (EGT L 201, 2002, s. 37), i dess lydelse enligt Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009

e-handels-direktivet	Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden
e-kodexen	Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation
eSIM	Embedded Subscriber Identity Module (inbyggt simkort)
EU:s dataskydds-förordning	Europaparlamentet och rådet 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)
EU-domstolen	Europeiska unionens domstol
EUO	lagen (2017:1000) om en europeisk utredningsorder
Europadomstolen	europeiska domstolen för de mänskliga rättigheterna
Europa-konventionen	den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna, med de tillägg och ändringar som gjorts genom de protokoll som Sverige ratificerat
FEUF	fördraget om Europeiska unionens funktionssätt
FL	förvaltningslagen (2017:900)
Gamla FEK	förordningen (2003:396) om elektronisk kommunikation
Gamla LEK	lagen (2003:389) om elektronisk kommunikation

Gps	Global Positioning System (satellitbaserat system för positioner)
HAK	hemlig avlyssning av elektronisk kommunikation
HDA eller HDA-lagen	hemlig dataavläsning eller lagen (2020:62) om hemlig dataavläsning
HÖK	hemlig övervakning av elektronisk kommunikation
ICCID	Integrated Circuit Card Identifier (serienummer för sim-kort)
IMEI	International Mobile Equipment Identity (en form av utrustningsidentitet)
IMSI	International Mobile Subscriber Identity (en form av abonnemangsidentitet)
inhämtningslagen	lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet
IP	Internet Protocol (kommunikationsprotokoll för internet)
IPv4	Internet Protocol version 4 (kommunikationsprotokoll för internet version 4)
IPv6	Internet Protocol version 6 (kommunikationsprotokoll för internet version 6)
JK	Justitiekanslern
JO	Riksdagens ombudsmän
LIRB	lagen (2000:562) om internationell rättslig hjälp i brottmål
LSU	lagen (2022:700) om särskild kontroll av vissa utlänningar
MAC-adress	Media Access Control Address (en form av utrustningsidentitet)

MMS	Multimedia Messaging Service (meddelandetjänst)
NAT	Network Address Translation (adressöversättning)
Noik	nummeroberoende interpersonella kommunikationstjänster
Nya FEK	förordning (2022:511) om elektronisk kommunikation
Nya LEK	lagen (2022:482) om elektronisk kommunikation
OSL	offentlighets- och sekretesslagen (2009:400)
OTT-tjänster	Over-the-top (operatörsoberoende tjänster)
preventivlagen	lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott
Prop.	regeringens proposition
PTS	Post och telestyrelsen
ramdirektivet	Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster
RB	rättegångsbalken
RF	regeringsformen
rättighetsstadgan eller stadgan	Europeiska unionens stadga om de grundläggande rättigheterna (2012/c 326/02)
SFS	svensk författningssamling
sim	Subscriber Identity Module
SIN	Säkerhets- och integritetsskyddsnämnden
sms	Short Message Service
SOU	Statens offentliga utredningar
SUCI	Subscription Concealed Identifier (tillfällig identifierare i 5G-nätet)

SUPI	Subscription Permanent Identifier (permanent identifierare i 5G-nätet)
Tele2-domen	EU-domstolens dom den 21 december 2016 i de förenade målen C-203/15 och C-698/15
TF	tryckfrihetsförordningen
UTC (SP)	Coordinated Universal Time (den tillämpning av den internationella tidsskalan UTC som används i Sverige)
WLAN	Wireless Local Area Network (trådlöst lokalt nätverk)
xDSL	Digital Subscriber Line (en form av bredbands-uppkoppling)
YGL	yttrandefrihetsgrundlagen
3G (UMTS)	Universal Mobile Telecommunications System (tredje generationens mobilkommunikation)
4G (LTE)	Long Term Evolution (fjärde generationens mobilkommunikation)
5G	femte generationens mobilkommunikation

Sammanfattning

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 kom-

munikation 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. brottsbekämpande 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

1. ett begränsat geografiskt område där grov brottslighet har förekommit eller där det är sannolikt att grov brottslighet kommer att äga rum,
2. en skyddsvärd plats,
3. en person som dömts för grova brott,
4. en person som har varit föremål för hemliga tvångsmedel, eller
5. 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.[1]

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

[1] Se Högsta domstolens beslut den 30 mars 2023 i mål Ö 5686-22.

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.

Summary

The Commission's mandate and work

The Commission's mandate involved analysing and evaluating the current regulations on retention of and access to electronic communications data for law enforcement purposes, including in relation to new case law from the Court of Justice of the European Union. The mandate also included analysing the conditions under which providers of OTT services could be covered by the obligation to retain and provide access to electronic data. It also included analysing and proposing modernisations relating to the obligation for providers to ensure that secret coercive measures can be implemented effectively. The Commission also had a mandate to review certain issues concerning Swedish authorities' access to electronic data when it is located outside Sweden's borders (executive jurisdiction).

The aim of the mandate was to ensure that law enforcement authorities' access to information is improved and does not deteriorate over time on account of technological developments and changes in communication habits, while ensuring respect for human rights.

EU law and data retention

A proposal to amend Swedish data retention rules should be submitted in the light of new case law from the Court of Justice of the European Union

Data retention is an obligation for providers of electronic communications networks and services, such as mobile operators, to retain electronic communications data. The term electronic communications data includes data about the communication but not the content itself. Data on communication may, for example, be who communicated with

whom, when the communication took place and the location of the parties communicating with each other.

In Sweden, data retention for law enforcement purposes has existed since the 1990s. Today, EU law plays a major role in legislation on data retention for law enforcement purposes.

Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) states, among other things, that Member States must ensure the confidentiality of electronic communications and related traffic data. Data that is no longer needed must, under the Directive, be erased or made anonymous. However, the Member States may make exceptions to these obligations if they are necessary for purposes such as law enforcement activities. The Directive has been implemented in Swedish law mainly through provisions in the Electronic Communications Act (2022:482).

The Swedish provisions on data retention were examined by the Court of Justice of the European Union in Joined Cases C-203/15 and C-698/15 (the Tele2 judgment). The retention obligation at the time of the judgment was general and unlimited in the sense that it covered all telephony, messaging and broadband services provided by the traditional telecoms operators. In the Tele2 judgment, the Court of Justice of the European Union ruled that such retention obligations exceeded the limits of strict necessity and could not, in accordance with the Directive on privacy and electronic communications, be considered justified in a democratic society.

The Swedish legislation was therefore reviewed and, on 1 October 2019, new rules on data retention entered into force (Govt. Bill 2018/19:86). The adaptations to EU law included limiting the retention obligation and differentiating between the retention periods.

Following the Tele2 judgment, the Court of Justice of the European Union has issued new case law in several cases related to data retention. As a result of the judgments, Member States including Germany, France, Belgium and Denmark have adapted their data retention rules to EU law.

Our analysis shows that there may be reason to amend the Swedish rules in the light of recent case law from the Court of Justice of the European Union. We have concluded that proposals on data retention should be submitted to protect national security. We have also

come to the conclusion that there is reason to submit proposals on targeted retention to combat serious crime. The term targeted retention normally refers to retention of data that is limited to a specific geographical area, to a specific group of people or by some other distinguishing criterion, such as technical criteria.

National security retention

We have proposed rules on national security retention. This should be permitted if it is deemed strictly necessary to combat a serious threat to national security that is real and present or foreseeable. The Swedish Security Service must assess the threat to national security and may, if a security threat exists, decide to introduce a general, undifferentiated retention obligation.

A decision on national security retention must be subject to effective supervision. A public representative must protect the interests of individuals and be able to appeal against the decisions of the Swedish Security Service to a supervisory body. The supervisory body must examine whether the conditions for the retention obligation are met and whether the retention obligation is proportionate. The supervisory body must be able to confirm or revoke the decision by the Swedish Security Service on retention. We propose that a new specialist decision-making body within the Swedish Commission on Security and Integrity Protection (SIN), the Data Retention Delegation, be the supervisory body.

The retention obligation, in the case of national security retention, is more extensive than the current retention obligation, both in terms of the types of data that can be retained and the duration of the retention. For example, it must be possible for location data that is not traffic data to be subject to national security retention. Location data that is not traffic data means, for example, GPS positions generated on a mobile phone. The retention period should be two years and, as a general rule, be counted from the date on which the communication ended.

Access to data retained by means of coercive measures for the purpose of protecting national security must be limited to combating offences and crime that may pose a serious threat to Sweden's security. The persons responsible for retention, i.e. the providers, must

therefore be able to distinguish between data retained on this basis and other data retained.

Decisions on national security retention must be subject to confidentiality, and professional secrecy must apply to the providers.

Retention to combat serious crime that does not constitute a threat to national security

We have also proposed two forms of targeted retention to combat serious crime: geographically targeted retention and extended targeted retention. These proposals could replace the current retention rules for electronic communications data for law enforcement purposes.

Geographically targeted retention

Geographically targeted retention must take place in areas in which objective criteria indicate that there is a comparatively higher probability of serious crime than in other areas. Geographically targeted retention must be based on the official statistics on reported crimes presented by the Swedish National Council for Crime Prevention (Brå) and with the municipalities as geographical units. The Swedish Post and Telecom Authority (PTS) must annually prescribe the municipalities that are to be subject to geographically targeted retention.

Extended targeted retention

Extended targeted retention is designed to complement geographically targeted retention. Extended targeted retention may concern

1. a limited geographical area in which serious crime has occurred or in which it is probable that serious crime will occur,
2. a site worthy of protection,
3. a person convicted of serious offences,
4. a person that has been subject to secret coercive measures, or

5. an equipment or subscription identity that has been used in a serious crime or serious criminal activity or that it may reasonably be assumed may be used in a serious crime or serious criminal activity.

The Swedish Police Authority, the Swedish Security Service and Swedish Customs will be able to decide on extended targeted retention, and SIN will supervise its application.

Geographically targeted retention will cover more types of data than the current retention obligation. The retention obligation covers the same types of data as those that may be stored in national security retention. A decision on extended targeted retention may also cover the same types of data. The retention period for both geographically targeted retention and extended targeted retention should be one year, as a general rule from the date on which the communication ended.

Decisions on extended targeted retention must be subject to confidentiality, and professional secrecy must apply to the providers.

Providers of OTT services

OTT services have greatly influenced the communication habits of individuals. It is now very common for communication to take place through internet-based services such as certain email services or services like Apple iMessage, Apple FaceTime, Discord, Snapchat, Google Messages, Google Meet, Kik Messenger, Line, Messenger from Meta, Skype, Slack, Telegram, Viber and Whatsapp, to name just a few. The EU regulatory framework uses the concept of publicly available number-independent interpersonal communications services (NI-ICS) as an umbrella term for these services.

NI-ICS providers do not currently have a retention obligation equivalent to that of traditional telecoms operators. Consequently, there is no data retention for law enforcement purposes when using NI-ICS services. Our analysis shows that technological developments and changing communication habits have had a negative impact on the possibilities for law enforcement authorities to do their work. Law enforcement authorities benefit greatly from and have a great need for electronic communications data, even when the communication takes place via channels other than the traditional telecoms oper-

ators. We have concluded that the benefit from and need for access to electronic communications data from NI-ICS providers outweighs the opposing interests against such access.

Obligations of NI-ICS providers

We have proposed that a retention obligation should also apply to providers of publicly available number-independent interpersonal communications services (NI-ICS) in Sweden.

The retention obligation must cover communications that take place to some extent in Sweden. This can be established, for example, by verifying that communications are sent from or received via an IP address in Sweden.

As a general rule, the retention obligation and the duration of retention should correspond to what we propose for other parties obliged to retain data, i.e. according to our proposals for national security retention, geographically targeted retention and extended targeted retention.

Providers of NI-ICS must be subject to the same professional secrecy obligation as providers of other electronic communications services.

Mandate to modernise the adaptation obligation

Providers of public electronic communications networks or publicly available electronic communications services as defined in the Electronic Communications Act play an important role when law enforcement authorities obtain electronic communications and related data. To facilitate the work of law enforcement authorities, a certain adaptation obligation has been imposed on providers. The obligation means that activities must be conducted in such a way that secret coercive measures can be implemented, and that it must be possible to do so without such implementation being disclosed.

However, the technological developments that have taken place and are still ongoing have meant that the rules on the adaptation obligation have become unclear and outdated. In view of our proposals on the retention obligation for NI-ICS providers, there is a further need to change the adaptation obligation. We therefore propose to

modernise the provisions on the adaptation obligation to provide clear, consistent and technology-neutral regulation.

Modernisation of the adaptation obligation

We have proposed that the adaptation obligation should cover the same actors as those who, according to our proposals, should be subject to the retention obligation under the Electronic Communications Act. However, an exemption should apply to providers of machine-to-machine services. Machine-to-machine services are services involving the automatic transfer of data between devices or software-based applications, with little or no human intervention. The services can be used, for example, for monitoring, measurement, control, transport and logistics in cars, trains, electricity meters, home alarms and lawnmowers.

Consequently, providers of NI-ICS should also be obliged to conduct their activities in such a way that decisions on secret coercive measures can be implemented and such implementation is not disclosed. This also covers cases in which a provider enables its customers to use end-to-end encryption, i.e. where only the sender and the recipient have access to the messages in readable form. In these cases, the adaptation obligation means that the provider must be able to make the data available to law enforcement authorities in readable form.

If data is made available, NI-ICS providers should also be entitled to compensation.

Executive jurisdiction

The right of a state to take action and enforce decisions made in the context of legislation and the administration of justice is called executive jurisdiction. The basic premise of international law is that states are prohibited from implementing enforcement measures, such as the use of secret coercive measures, in the territory of other states. This is based on the principle of territoriality, which is a fundamental principle of international law on state sovereignty.

Electronically stored data may exist in several states at the same time or be constantly moving between different states. In many cases,

it is not even possible for the service provider to establish where the data is at any given moment. Even when this is possible, conditions may change in a fraction of a second.

For effective law enforcement, it is important that the rules on access to electronic communications and other electronic evidence can also be applied in practice, even when the information is located outside Sweden or when its location is unknown.

We have reviewed the conditions, including the aspects of international law, for introducing a special legal regulation for executive jurisdiction in relation to electronic information located outside Sweden when using coercive measures.

We have concluded that, under certain conditions, there are no obstacles under international law to the law enforcement authorities obtaining electronic information that is or may be stored outside Sweden. On 30 March 2023, regarding executive jurisdiction, the Swedish Supreme Court ruled that remote searches may be carried out even if the information sought may be stored abroad.[1]

Against this background, we have proposed legislation that clarifies what applies to obtaining electronic information stored outside Sweden in certain cases.

Obtaining electronic information stored outside Sweden

We have proposed a legal regulation regarding the possibility for law enforcement authorities to obtain electronic information that is stored or may be stored outside Sweden, such as information in user accounts for various cloud services.

This presupposes:

- that law enforcement authorities can access the data without assistance,
- that obtaining the data is judged to involve no more than insignificant infringement of the sovereignty of another state, and
- that obtaining the data is not expected to cause any damage to the scannable information system to which the coercive measure relates.

[1] See the Supreme Court decision of 30 March 2023 in case Ö 5686-22.

Impact and implementation

The proposals on national security retention, a retention obligation that also applies to NI-ICS providers, modernisation of the adaptation obligation and executive jurisdiction will clearly have a positive impact on law enforcement. The proposals on targeted retention may sometimes complicate the work of law enforcement. Overall, however, the proposals will be beneficial to law enforcement.

Our proposals on national security retention may increase the risk of invasion of privacy compared to today. The proposals on modernisation of the adaptation obligation do not. Nor can the proposed regulation on executive jurisdiction be said to increase the risk of invasion of privacy. The proposals on targeted retention may lead to a lower risk of invasion of privacy.

The technical adaptations needed for a change in the retention obligation entail cost increases for providers, and the proposals may have some impact on competition between companies. The Swedish Police Authority, the Swedish Security Service, Swedish Customs and SIN will need additional resources.

The proposed rules on obtaining electronic information that is stored outside Sweden are proposed to enter into force on 1 July 2024. It is proposed that other statutory proposals enter into force on 1 July 2025.

1 Författningsförslag

1.1 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.

1.2 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.

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, spionerі, grovt spionerі, 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. 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, 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.

1.3 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.

Denna lag träder i kraft den 1 juli 2025.

1.4 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 kom-*

[1] Senaste lydelse 2022:707.

munikation 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.

1.5 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	Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att

[1] Senaste lydelse 2009:1020.
[2] Senaste lydelse 2020:66.

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 inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.	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 eller inhämtning av uppgifter 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.

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),

[3] Senaste lydelse 2012:288.
[4] Senaste lydelse 2019:1184.

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 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

[5] Senaste lydelse 2018:1919.
[6] Senaste lydelse 2022:1495.

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 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),

[7] Senaste lydelse 2022:1495.

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*

7. av 4 kap. 23 a § tullagen (2016:253).

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), *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.

1.6 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.

1.7 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.	

[1] Senaste lydelse av 20 § 2022:482.
[2] Senaste lydelse 2022:1086.
[3] Senaste lydelse 2022:482.

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 tillhandahållare av nummeroberoende interpersonella kommunikationstjänster för behandling av personuppgifter och andra uppgifter i syfte att bekämpa sexuella övergrepp mot barn på nätet

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 tillhandahållare 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 §§.

[4] Senaste lydelse 2022:482.

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 behandlas. För telefonitjänst gäller lagringsskyldigheten inte uppgift om nummer som ett samtal styrts till.	*För den som tillhandahåller en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst omfattar lagringsskyldigheten uppgifter som genereras eller behandlas vid tjänster som tillhandahåller samtal och meddelandehantering vid sådan kom-*

[5] Senaste lydelse 2022:482.

munikation 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 miss-

lyckad 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

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 c och d §§* får behandlas endast för att lämnas ut enligt

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 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 internetåtkomst ska

Uppgifter som avses *i 19 a–d §§* ska lagras enligt följande.

– 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.

[6] Senaste lydelse 2022:482.
[7] Senaste lydelse 2022:482.

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.

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

[8] Senaste lydelse 2022:1086.

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 som avses i första stycket samt får i enskilda fall besluta om undantag från kravet i första stycket.

[9] Senaste lydelse 2022:1086.

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.

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.

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 §[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.

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.

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

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 §[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.

[12] Senaste lydelse 2022:482.

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,

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 elektro-

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 elektro-

[13] Senaste lydelse 2022:482.

niska kommunikationstjänster ska lämnas.	niska 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, Åklagarmyn-

digheten 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 §[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

[15] Senaste lydelse 2022:1086.

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 enlighet med 9 kap. 29 § första stycket och 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 och föreskrif-

	ter 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.

1.8 Förslag till förordning om ändring i förordningen (2007:951) med instruktion för Post- och telestyrelsen

Härigenom föreskrivs i fråga om förordning om ändring i förordningen (2007:951) med instruktion för Post- och telestyrelsen att 4 § ska ha följande lydelse

Nuvarande lydelse	*Föreslagen lydelse*

4 §[1]

Post- och telestyrelsen har till uppgift att

1. främja tillgången till säkra och effektiva elektroniska kommunikationer, inbegripet att se till att samhällsomfattande tjänster finns tillgängliga, och att främja tillgången till ett brett urval av elektroniska kommunikationstjänster,

2. främja utbyggnaden av och följa tillgången till bredband och mobiltäckning i alla delar av landet, inbegripet att skapa förutsättningar för samverkan mellan myndigheter som kan bidra till utbyggnaden av bredband,

3. svara för att möjligheterna till radiokommunikation och andra användningar av radiovågor utnyttjas effektivt,

4. svara för att nummer ur nationella nummerplaner utnyttjas på ett effektivt sätt,

5. främja en effektiv konkurrens,

6. övervaka pris- och tjänsteutvecklingen,

7. bedriva informationsverksamhet riktad till konsumenter,

8. följa utvecklingen när det gäller säkerhet vid elektronisk kommunikation och uppkomsten av eventuella miljö- och hälsorisker,

9. pröva frågor om tillstånd och skyldigheter, fastställa och analysera marknader samt utöva tillsyn och pröva tvister enligt lagen (2022:482) om elektronisk kommunikation,

10. meddela föreskrifter enligt förordningen (2022:511) om elektronisk kommunikation,

11. upprätta och offentliggöra planer för frekvensfördelning till ledning för radioanvändningen samt offentliggöra information av all-

[1] Senaste lydelse 2022:515.

mänt intresse om rättigheter, villkor, förfaranden och avgifter som rör radiospektrumanvändningen,

12. tillhandahålla information om frekvensanvändning till Europeiska radiokommunikationskontorets frekvensinformationssystem (EFIS),

13. vara marknadskontrollmyndighet enligt radioutrustningslagen (2016:392),

14. vara tillsynsmyndighet enligt lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering och ge stöd och information till myndigheter och enskilda när det gäller betrodda tjänster,

15. följa utvecklingen när det gäller toppdomäner med geografiska namn som har anknytning till Sverige,

16. vara tillsynsmyndighet enligt lagen (2006:24) om nationella toppdomäner för Sverige på internet samt meddela föreskrifter enligt förordningen (2006:25) om nationella toppdomäner för Sverige på internet,

17. verka för robusta elektroniska kommunikationer och minska risken för störningar, inbegripet att upphandla förstärkningsåtgärder, och verka för ökad krishanteringsförmåga,

18. verka för ökad nät- och informationssäkerhet i fråga om elektronisk kommunikation, genom samverkan med myndigheter som har särskilda uppgifter inom informationssäkerhets-, säkerhetsskydds- och integritetsskyddsområdet samt med andra berörda aktörer,

19. lämna råd och stöd till myndigheter, kommuner och regioner och till företag, organisationer och andra enskilda i frågor om nätsäkerhet,

20. vara tvistlösnings- och tillsynsmyndighet enligt lagen (2016:534) om åtgärder för utbyggnad av bredbandsnät och ansvara för informationstjänsten för utbyggnad av bredbandsnät enligt samma lag, *och*

21. vara tillsynsmyndighet enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

20. vara tvistlösnings- och tillsynsmyndighet enligt lagen (2016:534) om åtgärder för utbyggnad av bredbandsnät och ansvara för informationstjänsten för utbyggnad av bredbandsnät enligt samma lag,

21. vara tillsynsmyndighet enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, *och*

22. meddela föreskrifter om vilka kommuner som omfattas av geografiskt riktad lagring enligt 4 § lagen (2025:000) om lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet.

Denna förordning träder i kraft den 1 juli 2025.

1.9 Förslag till förordning om ändring i förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden

Härigenom föreskrivs i fråga om förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden

dels att 1, 8, och 13 §§ ska ha följande lydelse,

dels att det ska införas tre nya paragrafer, 3 a §, 26 a och 26 b §§, och närmast före 26 a § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 §[1]
Säkerhets- och integritetsskyddsnämnden är en myndighet som ansvarar för de uppgifter som framgår av 1 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet och av 2 *och 3* §§ denna förordning.	Säkerhets- och integritetsskyddsnämnden är en myndighet som ansvarar för de uppgifter som framgår av 1 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet och av *2–3 a §§* denna förordning.
	3 a §
	Myndigheten har till uppgift att överpröva Säkerhetspolisens beslut om nationell säkerhetslagring enligt lagen (2025:000) om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.
	8 §[2]
Inom myndigheten ska det finnas *två* särskilda beslutsorgan, som benämns Registerkontrolldelegationen *och* Skyddsregistreringsdelegationen.	Inom myndigheten ska det finnas *tre* särskilda beslutsorgan, som benämns Registerkontrolldelegationen, Skyddsregistreringsdelegationen *och Datalagringsdelegationen.*

[1] Senaste lydelse 2007:1141.
[2] Senaste lydelse 2009:1516.

Registerkontrolldelegationen har till uppgift att besluta i frågor som avses i 2 §.

Skyddsregistreringsdelegationen har till uppgift att besluta i frågor som avses i 3 §.

Datalagringsdelegationen har till uppgift att besluta i frågor som avses i 3 a.

Varje delegation består av en ordförande, en vice ordförande samt högst tre andra ledamöter.

13 §[3]

Ledamöterna i Registerkontrolldelegationen *och* Skyddsregistreringsdelegationen utses av regeringen för en bestämd tid. Ordföranden och vice ordföranden ska vara eller ha varit ordinarie domare eller ha annan motsvarande juridisk erfarenhet.

Ledamöterna i Registerkontrolldelegationen, Skyddsregistreringsdelegationen *och Datalagringsdelegationen* utses av regeringen för en bestämd tid. Ordföranden och vice ordföranden ska vara eller ha varit ordinarie domare eller ha annan motsvarande juridisk erfarenhet.

Av de övriga ledamöterna i Skyddsregistreringsdelegationen ska en av dem ha särskild erfarenhet av verksamhet som avser folkbokföring.

Bland de övriga ledamöterna i Datalagringsdelegationen ska det finnas personer med särskild erfarenhet av integritetsskyddsfrågor, frågor som avser elektronisk kommunikation och verksamhet som rör nationell säkerhet.

[3] Senaste lydelse 2009:1516.

Handläggning av ärenden i Datalagringsdelegationen

26 a §

När Säkerhetspolisens beslut om nationell säkerhetslagring har överklagats ska Datalagringsdelegationen sammanträda så snart som möjligt.

26 b §

Datalagringsdelegationen är beslutför när ordföranden och minst två andra ledamöter är närvarande.

Om både ordföranden och vice ordföranden i delegationen har förhinder får nämndens ordförande träda in som delegationens ordförande.

Denna förordning träder i kraft den 1 juli 2025.

1.10 Förslag till förordning om ändring i förordningen (2022:511) om elektronisk kommunikation

Härigenom föreskrivs i fråga om förordningen (2022:511) om elektronisk kommunikation

dels att 9 kap. 10 §[1] ska upphöra att gälla,

dels att 9 kap. 6, 7 och 8 § ska ha följande lydelse,

dels att det ska införas tre nya paragrafer, 9 kap. 6 a–c §§ och närmast före 6, 7–9 §§ nya rubriker av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	9 kap.
	6 §[2]
	Lagring av uppgift om abonnemang
För att uppfylla lagringsskyldigheten i 9 kap. 19 § lagen (2022:482) om elektronisk kommunikation ska den lagringsskyldige lagra de uppgifter som anges i 7 och 8 §§.	*Lagringsskyldigheten enligt 9 kap. 19 a § lagen (2022:482) om elektronisk kommunikation omfattar uppgifter som är nödvändiga för att identifiera abonnent och registrerad användare och som är uppgift om* *1. abonnent och registrerad användare,* *2. användares ip-adress och andra uppgifter,* *3. användares abonnemangs- och utrustningsidentiteter samt* *4. koppling mellan tillfälliga och permanenta identifierare för utrustning och abonnemang.* *Post- och telestyrelsen får meddela ytterligare föreskrifter om vilka uppgifter som ska lagras enligt första stycket.*

[1] Senaste lydelse av 10 § 2022:511.
[2] Senaste lydelse 2022:511.

Nationell säkerhetslagring

6 a §

Lagringsskyldigheten i 9 kap. 19 b § lagen (2022:482) om elektronisk kommunikation får omfatta de uppgifter som anges i 6 b och 6 c §§.

6 b §

När det gäller telefonitjänst, samtal och meddelandehantering får följande lagras:

1. i fråga om telefonitjänst och samtal, uppringande och uppringt nummer, ip-adress eller annan meddelandeadress, abonnemangs- och utrustningsidentitet,

2. i fråga om meddelanden, avsändares och mottagares

nummer, ip-adress eller annan meddelandeadress,

abonnemangs-, konto- eller utrustningsidentitet,

3. nummer, ip-adress eller andra meddelandeadresser som kommunikationen styrts till vid överflyttning, vidareförmedling eller transport av 1 och 2,

4. uppgifter om abonnent och registrerad användare som uppgifterna i 1–3 kan hänföras till,

5. kopplingen mellan tillfälliga och permanenta identifierare för utrustning eller abonnemang,

6. uppgifter om den eller de tjänster som använts,

7. datum och spårbar tid för då kommunikationen påbörjades

och avslutades eller ett meddelande skickades och togs emot,

8. lokaliseringsuppgifter vid kommunikationen,

9. lokaliseringsuppgifter som inte är trafikuppgifter samt lokaliseringsuppgifter som genererats i användares utrustning, och

10. uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten.

Om den som slutligt avskiljer kommunikationen till den enskilda abonnenten inte omfattas av lagringsskyldighet, ska första stycket 10 gälla för den som avskiljer kommunikationen till den som slutligt avskiljer kommunikationen till den enskilda abonnenten.

6 c §

När det gäller internetåtkomst får följande lagras:

1. användares ip-adress och andra uppgifter som är nödvändiga för att identifiera abonnent och registrerad användare,

2. uppgifter om abonnent och registrerad användare,

3. användares abonnemangs- och utrustningsidentiteter,

4. koppling mellan tillfälliga och permanenta identifierare för utrustning och abonnemang,

5. den typ av kapacitet för överföring som har använts,

När det gäller telefonitjänst och meddelandehantering via mobil nätanslutningspunkt ska följande lagras:

1. uppringande och uppringt nummer, avsändares och mottagares nummer eller annan meddelandeadress,

2. i fråga om telefonitjänst, uppringandes och uppringds abonnemangsidentitet och utrustningsidentitet,

6. datum och spårbar tid för åtkomsten,

7. lokaliseringsuppgifter vid åtkomsten,

8. lokaliseringsuppgifter som inte är trafikuppgifter samt lokaliseringsuppgifter som genererats i användares utrustning,

9. uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten.

Om den som slutligt avskiljer kommunikationen till den enskilda abonnenten inte omfattas av lagringsskyldighet, ska första stycket 9 gälla för den som avskiljer kommunikationen till den som slutligt avskiljer kommunikationen till den enskilda abonnenten.

7 §[3]

Geografiskt riktad lagring

Lagringsskyldigheten i 9 kap. 19 c § lagen (2022:482) om elektronisk kommunikation ska omfatta de uppgifter som anges i 6 b och 6 c §§.

[3] Senaste lydelse 2022:511.

3. uppgifter om abonnent och registrerad användare som uppgifterna i 1 och 2 kan hänföras till,

4. datum och spårbar tid då kommunikationen påbörjades och avslutades eller ett meddelande skickades och togs emot,

5. lokaliseringsuppgifter då kommunikationen påbörjades och avslutades eller ett meddelade skickades och togs emot, och

6. datum, spårbar tid och lokaliseringsuppgifter för den första aktiveringen av en förbetald anonym tjänst.

8 §[4]

Utökad riktad lagring

När det gäller internetåtkomst ska följande lagras:

1. användares ip-adress och andra uppgifter som är nödvändiga för att identifiera abonnent och registrerad användare,

2. uppgifter om abonnent och registrerad användare,

3. datum och spårbar tid för på- och avloggning i tjänsten som ger internetåtkomst, och

4. uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten.

Om den som slutligt avskiljer kommunikationen till den enskilda abonnenten inte omfattas av 9 kap. Lagringsskyldigheten i 9 kap. 19 d § lagen (2022:482) om elektronisk kommunikation får omfatta de uppgifter som anges 7 §.

[4] Senaste lydelse 2022:511.

19 § lagen (2022:482) om elektronisk kommunikation, ska första stycket 4 gälla för den som avskiljer kommunikationen till den som slutligt avskiljer kommunikationen till den enskilda abonnenten.	

9 §[5]

Föreskriftsrätt

Post- och telestyrelsen får meddela närmare föreskrifter om vilka uppgifter som ska lagras enligt *7 och 8 §§*.	Post- och telestyrelsen får meddela närmare föreskrifter om vilka uppgifter som ska lagras enligt *6 b och 6 c §§*.

Denna förordning träder i kraft den 1 juli 2025.

[5] Senaste lydelse 2022:511.

2 Utredningens uppdrag och arbete

2.1 Utredningens uppdrag

Regeringen beslutade den 5 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. Uppdraget syftar till att säkerställa att de brottsbekämpande myndigheternas tillgång till information förbättras och upprätthålls över tid i takt med teknikutvecklingen och förändrade kommunikationsvanor, samtidigt som respekten för mänskliga rättigheter säkerställs.

Enligt utredningens direktiv ska nuvarande reglering om lagring av och tillgång till uppgifter om elektronisk kommunikation analyseras och utvärderas i förhållande till bl.a. ny praxis från EU-domstolen och ställning tas till om regelverket behöver förändras. Vi ska också analysera förutsättningarna för och ta ställning till om leverantörer av s.k. OTT-tjänster (dvs. nummeroberoende interpersonella kommunikationstjänster, Noik) ska omfattas av denna reglering.

Vi ska vidare analysera och föreslå moderniseringar av regleringen när det gäller tjänsteleverantörers skyldighet att anpassa sin verksamhet så att hemliga tvångsmedel kan verkställas på ett effektivt sätt.

Slutligen ska vi analysera vissa frågor om jurisdiktion, inklusive folkrättsliga överväganden, i förhållande till elektronisk information som finns eller kan finnas utanför Sverige och ta ställning till om det bör införas en särskild lagreglering för exekutiv jurisdiktion.

Det ingår i uppdraget att noga väga behovet av en effektiv brottsbekämpning mot den enskildes rätt till skydd för sin personliga integritet, analysera förslagens påverkan på skyddet för mänskliga rättigheter, inklusive rätten till respekt för privatlivet, ta ställning till om

skyddet för privat- och familjelivet respektive den personliga integriteten bör stärkas, och se till att de förslag som lämnas uppfyller högt ställda krav på rättssäkerhet.

Uppdraget innefattar också att säkerställa att en välfungerande systematik i regelverket kring hemliga tvångsmedel upprätthålls. Det innebär att vi även ska bedöma behovet av följdändringar i rättegångsbalken, lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen), lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen), lagen (2022:700) om särskild kontroll av vissa utlänningar (LSU), lagen (2020:62) om hemlig dataavläsning (HDA) och lagen (2022:482) om elektronisk kommunikation (nya LEK). Vi ska även bedöma behovet av följdändringar i lagen (2000:562) om internationell rättslig hjälp i brottmål (LIRB) och lagen (2017:1000) om en europeisk utredningsorder.

2.2 Utredningsarbetet

Uppdraget har inrymt överväganden inom ett mycket komplext område, både juridiskt och tekniskt. Utredningen har haft elva expertgruppssammanträden. Därutöver har företrädare för utredningen haft flera separata möten med experter från Polismyndigheten, Säkerhetspolisen och Post- och telestyrelsen (PTS). Företrädare har även även haft sammanträden med branchorganisationen TechSverige (tidigare IT & Telekomföretagen) tillsammans med företrädare för Meta (tidigare Facebook), Microsoft, Google, Internetstiftelsen, Hi3G, Tele2, Telenor och Telia. Utredningen har också haft separata möten med Apple, Meta, Microsoft, Hi3G, Tele2, Telenor och Telia. Företrädare för utredningen har också haft separata möten med Apple, Meta, Microsoft, Hi3G, Tele2, Telenor och Telia.

Företrädare har haft underhandskontakter med bl.a. Brottsförebyggande rådet (Brå), Säkerhets- och integritetsskyddsnämnden (SIN), Internetstiftelsen, Netnod och ISOC-SE. Utredningen har haft kontakt med personer som arbetar med motsvarande frågor i andra länder. Därtill har utredningen samrått med bl.a. Utredningen om utökade möjligheter att använda hemliga tvångsmedel (Ju 2020:20) och Utredningen om preventiva tvångsmedel (Ju 2021:15).

Vi har inte kunnat beakta material som tillkommit efter den 31 mars 2023.

2.3 Betänkandets disposition

Fortsättningen av betänkandet inleds med avsnitt 3, om enskildas grundläggande rättigheter. Därefter beskrivs i avsnitt 4 relevant gällande rätt kring elektronisk kommunikation. Avsnitt 5 utgör en översiktlig beskrivning av de brottsbekämpande myndigheternas utredande verksamhet och underrättelseverksamhet. I avsnitt 6 gör vi en översyn av reglerna om lagring och tillgång till uppgifter om elektronisk kommunikation. I samma avsnitt finns våra överväganden och förslag om lagring av abonnemangsuppgifter och behovet av anpassning av den svenska datalagringsregleringen. I avsnitt 7–9 finns våra överväganden och förslag om nationell säkerhetslagring, riktad lagring och om lagring av och tillgång till elektroniska uppgifter om elektronisk kommunikation från tillhandahållare av Noik. I avsnitt 10 och 11 finns överväganden och förslag om modernisering av anpassningsskyldigheten och frågor om exekutiv jurisdiktion. Den sista delen av betänkandet utgörs av förslag på ikraftträdande, avsnitt 12, en beskrivning av förslagens konsekvenser, avsnitt 13 och en författningskommentar, avsnitt 14. Våra författningsförslag finns i avsnitt 1.

3 Grundläggande rättigheter

3.1 Rätten till personlig integritet

Svensk rätt innehåller ingen allmängiltig definition av begreppet personlig integritet. Någon enhetlig definition finns inte heller i internationell rätt.[1] Begreppet personlig integritet har beskrivits som att kränkningar av den personliga integriteten utgör intrång i den fredade sfär som den enskilde bör vara tillförsäkrad och där intrång bör kunna avvisas. Det har vidare inte ansetts nödvändigt att formulera en allmängiltig definition av begreppet personlig integritet för att kunna bedöma vilka intressen som har ett sådant skyddsvärde att de bör omfattas av ett särskilt starkt skydd mot omotiverade ingrepp.[2] Utformningen av integritetsskyddet i svensk rätt har kommit att bestämmas av summan av ett stort antal skyddsregler av varierande slag.[3]

I Integritetsskyddsmyndighetens integritetsrapport 2020 analyseras begreppet och myndigheten konstaterar bl.a. följande.[4]

> Även om någon fast definition inte slås fast och även om rättigheten inte är absolut, bör personlig integritet i det digitala samhället sammanfattningsvis kunna förstås som den enskildes rätt till
>
> **Privatliv.** Rätten att få vara ifred, ha privata tankar och kunna kommunicera förtroligt med andra utan att bli kartlagd, spårad eller övervakad.
>
> **Självbestämmande.** Att själv kunna kontrollera personuppgifter som rör en själv, vem som använder uppgifterna och för vilka syften. Detta är särskilt angeläget när det handlar om vem som ska få ta del av känsliga uppgifter som rör till exempel hälsa eller sexualliv.

[1] Se SOU 2016:65 s. 34.
[2] Se bl.a. prop. 2009/10:80 s. 175.
[3] Se bl.a. SOU 2015:31 s. 51 och SOU 2017:75 s. 59.
[4] Se Integritetsskyddsmyndighetens integritetsrapport 2020, IMY rapport 2021:1, s. 27 f.

3.2 Skyddet för privatlivet

3.2.1 FN:s konventioner

Förenta nationernas (FN) allmänna förklaring om de mänskliga rättigheterna antogs 1948. Ingen får utsättas för godtyckligt ingripande i fråga om privatliv, familj, hem eller korrespondens (artikel 12). En person får endast underkastas sådana inskränkningar som har fastställts i lag och enbart i syfte att trygga tillbörlig hänsyn till och respekt för andras fri- och rättigheter samt för att tillgodose ett demokratiskt samhälles berättigade krav på moral, allmän ordning och allmän välfärd (artikel 29). Motsvarande skydd för den personliga integriteten finns i FN:s konvention om medborgerliga och politiska rättigheter, som antogs 1966. Även FN:s konvention om ekonomiska, sociala och kulturella rättigheter, som antogs 1966, innehåller regler om skydd för bl.a. privat- och familjelivet.

FN:s konvention om barns rättigheter (barnkonventionen) antogs 1989 och artiklarna 1–42 är sedan den 1 januari 2020 inkorporerad i svensk lag.[5] Inget barn får utsättas för godtyckliga eller olagliga ingripanden i sitt privat- eller familjeliv, sitt hem eller sin korrespondens och inte heller för olagliga angrepp på sin heder och sitt anseende (artikel 16). I artikel 40 (b) (vii) nämns särskilt att ett barn som misstänks eller åtalas för brott ska få sitt privatliv till fullo respekterat under alla stadier av förfarandet. Vid samtliga åtgärder som rör barn ska i första hand beaktas vad som bedöms vara barnets bästa (artikel 3). Barn ska skyddas från alla former av fysiskt eller psykiskt våld, narkotika, sexuella övergrepp och annat utnyttjande. Det ska finnas effektiva medel för bl.a. förebyggande, identifiering, undersökning och uppföljning samt förfaranden för rättsligt ingripande om barn farit illa (se artiklarna 19 och 32–36).

3.2.2 Europakonventionen

Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) är inkorporerad i svensk rätt och gäller som svensk lag.[6] Enligt 2 kap. 19 § RF

[5] Se lagen (2018:1197) om Förenta nationernas konvention om barnets rättigheter.
[6] Se lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.

får lag eller annan föreskrift inte meddelas i strid med Sveriges åtaganden på grund av Europakonventionen. Genom att underteckna Europakonventionen har staten garanterat var och en, som befinner sig under dess jurisdiktion, de fri- och rättigheter som anges i konventionen. Var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens (artikel 8). Rätten till respekt för privat- och familjeliv omfattar bl.a. kommunikation via telefon. Rätten innefattar även skyddet av personuppgifter. Offentlig myndighet får inte inskränka dessa rättigheter annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter. Det innebär att en inskränkning måste ha stöd i inhemsk lag som i sin tur måste uppfylla rimliga anspråk på rättssäkerhet, såsom att skydda mot godtycke, vara tillgänglig för allmänheten och vara förutsebar. Att inskränkningen måste vara nödvändig i ett demokratiskt samhälle för något av de i artikeln skyddade intressena innebär i huvudsak att det ska finnas ett angeläget samhälleligt behov av åtgärden och att den måste stå i rimlig proportion till det syfte som ska tillgodoses.[7] Konventionsstaterna har ett visst handlingsutrymme att själva avgöra om begränsningarna är nödvändiga för ett givet syfte. Europadomstolen förbehåller sig dock rätten att överpröva denna bedömning inom ramen för prövningen av någons enskilda klagomål hos domstolen.

Europadomstolen har utarbetat en minimistandard som ställer följande krav på lagstiftning om hemliga övervakningsåtgärder.[8]

- Arten av de brott som skulle kunna leda till en begäran om åtgärden måste framgå.
- Det ska finnas en definition av de personkategorier som skulle kunna riskera att bli föremål för åtgärden.
- Åtgärdens varaktighet ska vara begränsad.
- Det måste finnas förfaranderegler för undersökning, användning och lagring av de uppgifter som inhämtas.

[7] Se Danelius, Mänskliga rättigheter i europeisk praxis, 5 uppl. 2015, s. 369 f.
[8] Se t.ex. Roman Zakharov mot Ryssland (nr 47143/06), 4 december 2015, § 231 med hänvisningar.

- Försiktighetsåtgärder vid överföring av information till andra parter ska vidtas.
- De omständigheter under vilka inhämtade uppgifter (t.ex. inspelningar) kan eller måste raderas ska anges.

De viktigaste punkterna har bedömts vara de två förstnämnda. Det kan konstateras att den grad av förutsebarhet som krävs varierar beroende på vilken typ av åtgärd som lagstiftningen avser och hur ingripande åtgärden är. Europadomstolen har också slagit fast att nationell lagstiftning om dolda spaningsåtgärder måste innehålla kontrollmekanismer för att skydda mot missbruk. Vad som krävs i det avseendet beror på omständigheter som åtgärdernas karaktär, räckvidd och varaktighet, vilka motiv som krävs för att besluta, utföra och övervaka dem samt vilken typ av rättsmedel som finns i den nationella lagstiftningen.

Artikel 8 i Europakonventionen ger enligt praxis inte bara upphov till en negativ förpliktelse för det allmänna att avhålla sig från omotiverade inskränkningar i denna rättighet utan även en positiv skyldighet för det allmänna att se till att enskilda tillförsäkras en rätt till skydd för privat- och familjeliv. Ett sådant skydd tillförsäkras bl.a. genom kriminalisering av olika åtgärder som innefattar intrång i den personliga integriteten. En förutsättning för att staten ska kunna leva upp till kraven på att upprätthålla rättstryggheten för enskilda är att staten har en väl fungerande och effektiv brottsbekämpning.[9] Att ha en väl fungerande brottsbekämpning innebär t.ex. att myndigheterna ska ha tillgång till effektiva utredningsverktyg, även i den elektroniska miljön. När så inte varit fallet har staten ansetts kränka de rättigheter som följer av Europakonventionen. Ett exempel på detta var när en person som gjort sig skyldig till förtal eller möjligen sexuellt ofredande av ett 12-årigt barn i Finland inte kunde identifieras på grund av att den nationella lagstiftningen inte möjliggjorde att uppgift om vem som använt en ip-adress kunde hämtas in från operatören. I det aktuella fallet uttalade Europadomstolen att konfidentialitet för kommunikation och yttrandefrihet ibland måste få ge vika för brottsbekämpande ändamål.[10]

[9] Se t.ex. SOU 2015:31 s. 52 f. och SOU 2017:75 s. 60 f.
[10] Se Europadomstolens dom den 2 december 2008 i mål K.U. mot Finland, mål nr 2872/02.

3.2.3 EU:s rättighetsstadga

En bestämmelse om rätt till respekt för bl.a. privatlivet finns också i artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna. Av artikel 52.3 i stadgan följer att i den mån stadgan omfattar rättigheter som motsvarar sådana som garanteras av Europakonventionen, ska de ha samma innebörd och räckvidd som enligt konventionen eller ett mer långtgående skydd. Varje begränsning i utövandet av de fri- och rättigheter som erkänns i stadgan 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). Rättighetsstadgan riktar sig till medlemsstaterna endast när de tillämpar unionsrätten (artikel 51.1). Av EU-domstolens praxis framgår att detta innebär att rättigheterna i stadgan måste iakttas inte bara vid tillämpningen av nationell lagstiftning som genomför EU-rätt utan så snart nationell lagstiftning omfattas av unionens tillämpningsområde.[11] Ingen bestämmelse i stadgan får tolkas som att den inskränker eller inkräktar på de mänskliga rättigheter och grundläggande friheter som inom respektive tillämpningsområde erkänns i unionsrätten, internationell rätt och de internationella konventioner i vilka unionen eller samtliga medlemsstater är parter, särskilt europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, samt i medlemsstaternas författningar (artikel 53).

3.2.4 Regeringsformen

Grundläggande bestämmelser som har betydelse för det allmännas ansvar att skydda enskildas privatliv och integritet finns bl.a. i regeringsformen (RF). Av 1 kap. 2 § RF framgår att den offentliga makten ska utövas med respekt bl.a. för den enskilda människans frihet och värdighet samt att det allmänna ska värna den enskildes privatliv och familjeliv. Enligt 2 kap. 6 § första stycket RF är var och en gentemot det allmänna skyddad mot bl.a. husrannsakan och liknande intrång, undersökning av brev eller annan förtrolig försändelse samt hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt

[11] Se t.ex. Åkerberg Fransson, mål C-617/10.

meddelande. Vidare gäller enligt paragrafens andra stycke ett skydd mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Dessa grundläggande fri- och rättigheter får begränsas endast genom lag och endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningarna får aldrig gå utöver vad som är nödvändigt eller utgöra ett hot mot den fria åsiktsbildningen (2 kap. 20 och 21 §§ RF). För utländska medborgare som är bofasta i riket gäller att särskilda begränsningar i dessa rättigheter får göras genom lag (2 kap. 25 § RF).

3.3 Skyddet för personuppgifter

3.3.1 Dataskyddskonventionen

De dataskyddsregler som har antagits inom ramen för Europarådet finns i första hand i Europarådets konvention till skydd för enskilda vid automatisk behandling av personuppgifter (den s.k. dataskyddskonventionen). Konventionen trädde i kraft i oktober 1985. Sverige har, liksom övriga EU-medlemsstater, anslutit sig till konventionen. Dataskyddskonventionen innehåller principer för dataskydd som de konventionsanslutna staterna måste iaktta i sin nationella lagstiftning. Syftet med konventionen är att säkerställa respekten för grundläggande fri- och rättigheter, särskilt den enskildes rätt till personlig integritet i samband med automatiserad behandling av personuppgifter. Konventionen kompletteras av ett antal icke-bindande rekommendationer om hur personuppgifter bör behandlas inom olika områden. I syfte att modernisera konventionen antogs i maj 2018 ett ändringsprotokoll till konventionen. Sverige har undertecknat men inte ratificerat protokollet. Ändringarna träder i kraft när alla parter till dataskyddskonventionen har ratificerat ändringsprotokollet eller den 11 oktober 2023 om 38 parter då har ratificerat protokollet.

3.3.2 EU-rättslig reglering

Bestämmelser om behandling av personuppgifter finns i unionsrättens primärrätt och sekundärrätt. I artikel 8 i rättighetsstadgan föreskrivs att var och en har rätt till skydd av de personuppgifter som rör honom

eller henne. Sådana uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem.

Den allmänna regleringen om behandling av personuppgifter inom EU fanns tidigare i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter. Direktivet genomfördes i Sverige i huvudsak genom personuppgiftslagen (1998:204).

Den 27 april 2016 antog Europaparlamentet och rådet 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), i det följande EU:s dataskyddsförordning. EU:s dataskyddsförordning är tillämplig i medlemsstaterna sedan den 25 maj 2018. Det huvudsakliga syftet med EU:s dataskyddsförordning är att ytterligare harmonisera och effektivisera skyddet för personuppgifter för att förbättra den inre marknadens funktion och öka enskildas kontroll över sina personuppgifter. EU:s dataskyddsförordning utgör numera den generella regleringen för personuppgiftsbehandling inom EU. Den gäller dock inte för behandlingen av personuppgifter i myndigheters brottsförebyggande eller brottsutredande verksamhet. För den brottsbekämpande sektorn har i stället Europaparlamentet och rådet antagit 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, i det följande dataskyddsdirektivet. Viss behandling av personuppgifter undantas från både EU:s dataskyddsförordning och dataskyddsdirektivets tillämpningsområden. Det gäller personuppgiftsbehandling i verksamhet som inte omfattas av unionsrätten, däribland området nationell säkerhet.

För att säkerställa rätten till skydd för uppgifter 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 (e-dataskyddsdirektivet, se också avsnitt 4.2).

3.3.3 Nationell lagstiftning

EU:s dataskyddsförordning började tillämpas den 25 maj 2018. Samma dag trädde lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, (nedan kallad dataskyddslagen) i kraft. I dataskyddslagen finns kompletterande bestämmelser till EU:s dataskyddsförordning. Lagen är subsidiär i förhållande till andra lagar och förordningar och ska inte heller tillämpas i den utsträckning det skulle strida mot grundlagsbestämmelserna om tryck- och yttrandefrihet. Genom dataskyddslagen upphävdes den tidigare gällande personuppgiftslagen.

Dataskyddsdirektivet har i huvudsak genomförts genom en ny ramlag, brottsdatalagen (2018:1177), som trädde i kraft den 1 augusti 2018. Brottsdatalagen är generellt tillämplig inom det område som direktivet reglerar. Lagen är subsidiär i förhållande till annan lag eller förordning, vilket möjliggör avvikande bestämmelser i s.k. registerförfattningar. Brottsdatalagen gäller vid behandling av personuppgifter som utförs av myndigheter som har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Lagen gäller också för behandling av personuppgifter vid upprätthållande av allmän ordning och säkerhet.

I särskilda registerförfattningar finns bestämmelser som innebär preciseringar, undantag eller avvikelser från bestämmelserna i brottsdatalagen. Som exempel kan nämnas lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område, lagen (2018:1697) om åklagarväsendets behandling av personuppgifter inom brottsdatalagens område och lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område. För Säkerhetspolisen gäller lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter vid sådan behandling av personuppgifter som rör nationell säkerhet i Säkerhetspolisens brottsbekämpande och lagförande verksamhet.

Registerförfattningar förekommer också inom andra områden. Författningarna har till sitt huvudsakliga syfte att reglera hanteringen av register eller andra samlingar av personuppgifter.

Särskilda bestämmelser om behandling i personuppgifter finns även i 9 kap. nya LEK.

3.4 Yttrandefrihet

EU:s rättighetsstadga skyddar yttrandefriheten (artikel 11). I artikeln föreskrivs att var och en har rätt till yttrandefrihet. Denna rätt innefattar åsiktsfrihet samt frihet att ta emot och sprida uppgifter och tankar utan någon offentlig myndighets inblandning och oberoende av territoriella gränser. Motsvarande skydd finns i artikel 10 i Europakonventionen, artikel 19 i FN:s konvention om medborgerliga och politiska rättigheter och artikel 13 i barnkonventionen. FN:s råd för mänskliga rättigheter (UNHCR) antog i juni 2012 en resolution om yttrandefrihet på Internet (HRC44). I resolutionen anges bl.a. att ”samma rättigheter som folk har offline måste även skyddas online, i synnerhet yttrandefriheten”.

I regeringsformen föreskrivs att var och en är gentemot det allmänna tillförsäkrad yttrandefrihet, dvs. frihet att i tal, skrift eller bild eller på annat sätt meddela upplysningar samt uttrycka tankar, åsikter och känslor (2 kap. 1 § RF).

Tryckfriheten innebär en frihet för var och en att i tryckt skrift uttrycka tankar, åsikter och känslor samt att offentliggöra allmänna handlingar och i övrigt lämna uppgifter i vilket ämne som helst samt en rätt att ge ut skrifter utan att en myndighet eller ett annat allmänt organ hindrar detta i förväg (1 kap. 1 § TF).

Vidare är var och en gentemot det allmänna tillförsäkrad rätt att i ljudradio, tv och vissa liknande överföringar, offentliga uppspelningar ur en databas samt filmer, videogram, ljudupptagningar och andra tekniska upptagningar offentligen uttrycka tankar, åsikter och känslor och i övrigt lämna uppgifter i vilket ämne som helst (1 kap. 1 § Yttrandefrihetsgrundlagen, YGL).

4 Elektronisk kommunikation

4.1 Allmänt om elektronisk kommunikation

Elektronisk kommunikation innebär överföring av signaler i elektronisk form. Elektronisk kommunikation omfattar telefoni, datakommunikation och utsändningar till allmänheten via radio eller tv. Den tekniska utvecklingen har medfört att dessa delar gradvis vuxit samman. Dessutom har de tjänster som används i kommunikationssyfte utvecklats på så sätt att traditionell taltelefoni, sms och e-posttjänster har ersatts med funktionsmässigt likvärdiga onlinetjänster, där överföring av signaler inte ingår i tjänsten.

Uppgifter om elektronisk kommunikation har i svensk rätt delats in i tre olika och delvis överlappande grupper, nämligen

- uppgifter om abonnemang,
- trafikuppgifter, och
- lokaliseringsuppgifter.

Någon definition av begreppet *uppgift om abonnemang* finns varken i EU-rätten eller i nationell rätt. Med uppgifter om abonnemang avses främst uppgifter om abonnentens nummer, namn, titel och adress, men även uppgifter om exempelvis avtal och fakturering. Vidare anses såväl fasta som dynamiska ip-adresser vara uppgifter om abonnemang, eftersom det huvudsakliga syftet med sådana adresser kan sägas vara att identifiera abonnenten. Vi återkommer till frågan om ip-adresser i avsnitt 6.6.1.

Även IMSI-nummer (nummer som är kopplade till abonnentens simkort och telefonnummer) och IMEI-nummer (nummer som är kopplade till själva kommunikationsenheten) kan vara uppgift om abonnemang. PTS har inom ramen för sin tillsyn av skyldigheten att lämna ut uppgifter till brottsbekämpande myndigheter bedömt att

uppgifter om IMEI-nummer är att anse som uppgift om abonnemang, när det tydligt framgår av begäran att syftet är att identifiera ett abonnemang eller en abonnent.[1]

Uppgifter om abonnemang anses typiskt sett vara mindre integritetskänsliga än trafik- och lokaliseringsuppgifter. Regeringen har anfört att det kan ifrågasättas om det är lämpligt eller ens möjligt att definiera uppgifter om abonnemang endast utifrån vilken uppgift det är fråga om. Det har i stället ansetts mer relevant att som utgångspunkt definiera uppgifter om abonnemang som uppgifter som identifierar abonnenten eller den registrerade användaren bakom ett visst nummer eller en viss adress, i motsats till uppgifter som redogör för hur numret eller adressen har använts.[2]

En *trafikuppgift* definieras i 1 kap. 7 § nya LEK som en uppgift som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande. De trafikuppgifter som genereras vid elektronisk kommunikation kan avslöja t.ex. vilken typ av kommunikation som förekommit (telefoni, sms, etc.), vilken utrustning som använts, vilka nummer eller adresser som kommunicerat med varandra samt när och hur länge kommunikationen har pågått. Utanför begreppet trafikuppgifter faller information som avslöjar meddelandets innehåll. Vi återkommer till begreppet trafikuppgift i avsnitt 6.6.2.

En *lokaliseringsuppgift* definieras i nya LEK som en uppgift som behandlas i ett allmänt mobilt elektroniskt kommunikationsnät och som anger den geografiska positionen för en slutanvändares terminalutrustning eller en uppgift i ett allmänt fast elektroniskt kommunikationsnät om nätanslutningspunktens fysiska adress (1 kap. 7 §). Det kan t.ex. vara fråga om vilken cell (antenn på basstation) som utrustningen kopplat upp sig mot, eller en gps-position.[3]

[1] Se PTS beslut den 17 mars 2021 i ärende dnr 20-3144 m.fl. Jfr SOU 2017:75 s. 98 och prop. 2018/19:86 s. 93.
[2] Se prop. 2018/19:86 s. 93.
[3] Se vidare om dessa begrepp exempelvis SOU 2017:75, avsnitt 6.2.

4.2 Integritetsskydd och tystnadsplikt vid elektronisk kommunikation

Som anförs ovan skyddas mellanmänsklig kommunikation av EU:s rättighetsstadga, som föreskriver att var och en har rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer (artikel 7). Rättighetsstadgan föreskriver även ett skydd för personuppgifter (artikel 8). I syfte att säkerställa full respekt för de rättigheter som följer av artikel 7 och 8 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), det s.k. e-dataskyddsdirektivet. E-dataskyddsdirektivet syftar även till att säkerställa fri rörlighet för sådana uppgifter samt för utrustning och tjänster avseende elektronisk kommunikation inom unionen.

E-dataskyddsdirektivet definierar trafikuppgifter och lokaliseringsuppgifter (artikel 2) men inte abonnemangsuppgifter.

Bestämmelser om säkerhet vid behandlingen av uppgifter finns i artikel 4 i direktivet. Enligt artikel 4.1 ska leverantören av en allmänt tillgänglig elektronisk kommunikationstjänst vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa säkerheten i sina tjänster, om nödvändigt tillsammans med leverantören av det allmänna kommunikationsnätet när det gäller nätsäkerhet. Dessa åtgärder ska säkerställa en säkerhetsnivå som är anpassad till den risk som föreligger, med beaktande av dagens tillgängliga teknik och kostnaderna för att genomföra åtgärderna. Enligt artikel 4.1 a i e-dataskyddsdirektivet ska, utan att det påverkar tillämpningen av dataskyddsförordningen, de åtgärder som avses i punkt 1 minst

- säkerställa att endast auktoriserad personal, och endast i lagligen tillåtna syften, får tillgång till personuppgifter,
- skydda personuppgifter som lagrats eller överförts mot oavsiktlig eller olaglig förstörelse, oavsiktlig förlust eller ändring samt mot icke auktoriserad eller olaglig lagring och behandling eller icke auktoriserat eller olagligt tillträde eller offentliggörande, och
- säkerställa införandet av en strategi för behandling av personuppgifter.

De behöriga nationella myndigheterna ska kunna granska de åtgärder som vidtas av leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster och utfärda rekommendationer om bästa praxis beträffande den säkerhetsnivå som bör uppnås med hjälp av dessa åtgärder.

Enligt artikel 5 ska medlemsstaterna genom nationell lagstiftning säkerställa konfidentialitet vid kommunikation och därmed förbundna trafikuppgifter via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster. Medlemsstaterna ska särskilt förbjuda avlyssning, uppfångande med tekniskt hjälpmedel, lagring eller andra metoder som innebär att kommunikationen och de därmed förbundna trafikuppgifterna kan fångas upp eller övervakas av andra personer än användarna utan de berörda användarnas samtycke, utom när de har laglig rätt att göra så i enlighet med direktivet.

I artikel 6 finns bestämmelser om för vilka ändamål trafikuppgifter får behandlas och krav på begränsningar i fråga om tillgången till uppgifter för dem som behöver det för att utföra vissa närmare angivna arbetsuppgifter. Som huvudregel ska trafikuppgifter om abonnenter och användare som behandlas och lagras av en leverantör utplånas eller avidentifieras när de inte längre behövs för sitt syfte att överföra kommunikation. Trafikuppgifter som krävs för abonnentfakturering och betalning av samtrafikavgifter får dock behandlas. Om abonnenten har samtyckt till det, får uppgifter också behandlas för vissa marknadsföringsändamål.

I artikel 9 finns bestämmelser om andra lokaliseringsuppgifter än trafikuppgifter. Om sådana uppgifter kan behandlas, får dessa uppgifter endast behandlas sedan de har avidentifierats eller om användarna eller abonnenterna gett sitt samtycke.

Vidare finns i artikel 15 ett stöd för medlemsstaterna att – för vissa närmare specificerade ändamål – föreskriva undantag från de skyddsregler som finns i bl.a. artiklarna 5, 6 och 9. Undantag får bl.a. göras om det i ett demokratiskt samhälle är nödvändigt, lämpligt och proportionerligt för att skydda nationell säkerhet, försvaret och allmän säkerhet samt för förebyggande, undersökning, avslöjande av och åtal för brott.

E-dataskyddsdirektivet genomfördes i svensk rätt främst genom bestämmelser som togs in i lagen (2003:389) om elektronisk kommunikation (gamla LEK), se nedan.

Europeiska kommissionen har lämnat ett förslag till en ny förordning om respekt för privatlivet och skydd för personuppgifter i samband med elektronisk kommunikation (förordning om integritet och elektronisk kommunikation (COM(2017) 10 final)). Förordningen ska ersätta e-dataskyddsdirektivet och utgöra en specialreglering i förhållande till dataskyddsförordningen. Det är i dagsläget oklart när förordningen kan antas och vilket innehåll den kommer att få.

4.3 Nya lagen om elektronisk kommunikation

Gamla LEK trädde i kraft i juli 2003. Genom den lagen genomfördes i huvudsak den EU-rättsliga regleringen på området för elektronisk kommunikation.

Den 11 december 2018 antogs Europaparlamentets och rådets direktiv (EU) 2018/1972 om inrättande av en europeisk kodex för elektronisk kommunikation (e-kodexen). E-kodexen utgör en omarbetning av och ersätter

- Europaparlamentets och rådets direktiv 2002/21/EG om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektivet),
- Europaparlamentets och rådets direktiv 2002/19/EG om tillträde till och samtrafik mellan elektroniska kommunikationsnät och tillhörande faciliteter (tillträdesdirektivet),
- Europaparlamentets och rådets direktiv 2002/20/EG om auktorisation för elektroniska kommunikationsnät och kommunikationstjänster (auktorisationsdirektivet), och
- Europaparlamentets och rådets direktiv 2002/22/EG om samhällsomfattande tjänster och användares rättigheter (USO-direktivet).

Medlemsstaterna skulle senast den 21 december 2020 anta och offentliggöra de lagar och andra författningar som är nödvändiga för att genomföra kodexen.

Den 3 juni 2022 trädde nya LEK i kraft. Nya LEK, som ersatte gamla LEK, genomförde e-kodexen. I sak motsvarar nya LEK i stora delar gamla LEK, med de ändringar och tillägg som är föranledda av

e-kodexen. Bland förändringarna kan noteras att definitionen av elektronisk kommunikationstjänst har fått en delvis annan utformning. Definitionen har ändrats så att den är funktionellt baserad snarare än baserad på enbart tekniska parametrar. Överföringen av signaler är fortfarande det centrala momentet för att fastställa vilka tjänster som omfattas av definitionen, men den omfattar även andra tjänster som möjliggör kommunikation. Vidare har sanktionsavgifter införts för vissa överträdelser av lagen.

Nya LEK syftar dels till att enskilda och myndigheter ska få tillgång till säkra och effektiva elektroniska kommunikationer, dels till största möjliga utbyte för alla av elektroniska kommunikationstjänster sett till urvalet samt till deras pris, kvalitet och kapacitet. Syftet ska uppnås främst genom att konkurrens, innovation, internationell harmonisering samt säkerhet i nät och tjänster främjas. Samhällsomfattande tjänster ska därutöver alltid finnas tillgängliga på för alla likvärdiga villkor i hela landet till överkomliga priser. Vid tillämpningen av lagen ska särskilt Sveriges säkerhet liksom elektroniska kommunikationers betydelse för yttrandefrihet och informationsfrihet beaktas (1 kap. 1 §).

Lagen gäller elektroniska kommunikationsnät och elektroniska kommunikationstjänster med tillhörande faciliteter och tjänster samt annan radioanvändning (1 kap. 2 §).

I 1 kap. 7 § nya LEK definieras bl.a. följande begrepp.

Ett *elektroniskt kommunikationsnät* definieras som ett system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt passiva nätdelar och andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs.

Med en *elektronisk kommunikationstjänst* avses en tjänst som vanligen tillhandahålls mot ersättning via elektroniska kommunikationsnät och som – med undantag för dels tjänster i form av tillhandahållande av innehåll som överförs med hjälp av elektroniska kommunikationsnät och elektroniska kommunikationstjänster, dels tjänster som innebär utövande av redaktionellt ansvar över sådant innehåll – är en

1. internetanslutningstjänst enligt artikel 2.2 i Europaparlamentets och rådets förordning (EU) 2015/2120 av den 25 november 2015 om åtgärder rörande en öppen internetanslutning och slutkunds-

avgifter för reglerad kommunikation inom EU och om ändring av direktiv 2002/22/EG och förordning (EU) nr 531/2012,

2. interpersonell kommunikationstjänst, eller
3. tjänst som utgörs helt eller huvudsakligen av överföring av signaler, såsom överföringstjänster som används för tillhandahållande av maskin-till-maskin-tjänster eller för rundradio.

En *interpersonell kommunikationstjänst* definieras som en tjänst som vanligen tillhandahålls mot ersättning och som möjliggör ett direkt interpersonellt och interaktivt informationsutbyte via elektroniska kommunikationsnät mellan ett begränsat antal personer, varigenom de personer som inleder eller deltar i kommunikationen bestämmer vem eller vilka som ska vara mottagare av denna, dock inte en tjänst som möjliggör interpersonell och interaktiv kommunikation enbart som en extrafunktion av mindre betydelse som är direkt kopplad till en annan tjänst.

Det finns alltså inget krav på att interpersonella kommunikationstjänster helt eller huvudsakligen ska utgöras av överföring av signaler.

De interpersonella kommunikationstjänsterna kan vara antingen nummerbaserade eller nummeroberoende. En *nummerbaserad interpersonell kommunikationstjänst* etablerar en förbindelse till nummer i nationella eller internationella nummerplaner eller möjliggör kommunikation med sådana nummer. En *nummeroberoende interpersonell kommunikationstjänst* etablerar inte en förbindelse till nummer i nationella eller internationella nummerplaner och möjliggör inte heller kommunikation med sådana nummer. En sådan tjänst använder alltså inte telefonnummer för att ställa upp kommunikationen utan andra identifierare som normalt bara fungerar mellan den aktörens kunder.

Bestämmelser om säkerhet i nät och tjänster finns i 8 kap. 1–4 §§ nya LEK. Här anges bl.a. att den som tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att på lämpligt sätt hantera risker som hotar säkerheten i nät och tjänster. Det kan i detta sammanhang noteras att en revidering av det s.k. NIS-direktivet har antagits i november 2022 genom det s.k. NIS2-direktivet. NIS2-direktivet, som syftar till att ytterligare harmonisera medlemsstaternas arbete med informationssäkerhet, omfattar även tillhandahållare av allmänna

elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster.

Vidare finns bestämmelser om skydd av uppgifter vid tillhandahållande av tjänster i 8 kap. 6–9 §§ nya LEK. Den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst ska bl.a. vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av tjänsten skyddas.

Nya LEK innehåller vidare bestämmelser om under vilka förutsättningar trafikuppgifter och lokaliseringsuppgifter får behandlas (9 kap. 1–10 §§). Generellt gäller att trafikuppgifter, och däribland uppgifter som behandlas för att fakturera elektroniska meddelanden, ska utplånas eller avidentifieras så snart de inte längre behövs. En leverantör får dock lagra sådana uppgifter för vissa specifika ändamål. Så är fallet t.ex. för abonnentfakturering och – om den som uppgifterna gäller har samtyckt till det – för marknadsföring.

Den centrala bestämmelsen om lagringsskyldighet finns i 9 kap. 19 § nya LEK. Lagringsskyldiga enligt den bestämmelsen är de som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § samma lag. Allmänna elektroniska kommunikationsnät som vanligen tillhandahålls mot ersättning eller allmänt tillgängliga elektroniska kommunikationstjänster får tillhandahållas endast efter anmälan till tillsynsmyndigheten. Någon skyldighet att anmäla verksamheten gäller dock inte för nummeroberoende interpersonella kommunikationstjänster eller för verksamhet som består enbart i överföring av signaler via tråd för utsändning till allmänheten av program som avses i 1 kap. 2 § YGL.

Som en följd av EU-domstolens praxis ändrades de svenska reglerna om datalagring. Ändringarna, som trädde i kraft den 1 oktober 2019, innebär bl.a. att lagringens omfattning har begränsats och att lagringstiderna har differentierats. Lagringens omfattning är nu begränsad till uppgifter som genereras eller behandlas vid telefonitjänst och meddelandehantering via mobil nätanslutningspunkt samt vid internetåtkomst. Det betyder att det inte ska lagras några uppgifter om telefonitjänster eller meddelandehantering som sker inom det fasta telefonnätet eller genom fasta internetanslutningar. Med nätanslutningspunkt avses den fysiska punkt vid vilken en slutanvändare ansluts till ett allmänt elektroniskt kommunikationsnät (1 kap. 7 § nya LEK). En mobil nätanslutningspunkt är t.ex. där en mobiltelefon

kopplar upp sig mot en mast eller mot ett trådlöst lokalt nätverk (wifi) som tillhandahålls av någon som omfattas av lagringsskyldigheten.

Lagringsskyldigheten omfattar uppgifter som anges som nödvändiga för vissa preciserade syften. Dessa är formulerade som uppgifter 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.

Skyldigheten att lagra uppgifter omfattar uppgifter som genereras eller behandlas i leverantörens verksamhet. Det innebär att leverantören inte har någon skyldighet att införskaffa uppgifter som inte genereras eller behandlas i verksamheten. Däremot ska en uppgift lagras så fort den har funnits hos leverantören, även om det bara rör sig om en ytterst kort tid.[4]

Lagringsskyldighetens längd regleras i 9 kap. 22 § nya LEK och varierar från två månader upp till tio månader beroende på uppgiftsslag. Lagringstiden räknas från den dag kommunikationen avslutades.

I 9 kap. 7 och 8 §§ förordningen (2022:511) om elektronisk kommunikation (nya FEK) anges på en mer detaljerad nivå vilka uppgifter som ska lagras när det gäller telefonitjänst och meddelandehantering via mobil nätanslutningspunkt respektive när det gäller internetåtkomst.

Uppgifter som har lagrats enligt 9 kap. 19 § nya LEK får behandlas endast för att lämnas ut för brottsbekämpande ändamål enligt 9 kap. 33 § nya LEK, 27 kap. 19 § RB (hemlig övervakning av elektronisk kommunikation) eller inhämtningslagen (9 kap. 21 § nya LEK).

När lagringstiden har löpt ut ska uppgifterna omedelbart utplånas. Om en begäran om utlämnande har kommit in eller ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § RB har meddelats innan lagringstiden löpt ut, ska den lagringsskyldige fortsätta att lagra uppgifterna till dess de har lämnats ut respektive när tiden för bevarande har löpt ut. Därefter ska uppgifterna genast utplånas (9 kap. 22 § tredje stycket nya LEK).

I 9 kap. 29 och 29 b §§ nya LEK regleras den s.k. anpassningsskyldigheten. Den innebär att vissa verksamheter ska bedrivas så att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas under

[4] Se prop. 2010/11 :46 s. 77.

sådana former att verkställandet inte röjs (9 kap. 29 § nya LEK). Anpassningsskyldigheten innebär också ett krav på skyndsamhet och format vid utlämnandet av uppgifter (9 kap. 29 b § nya LEK).

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. I de fall det är särskilt föreskrivet ska ersättningen beräknas enligt schablon. Ersättningen ska betalas av den myndighet som har begärt uppgifterna (9 kap. 29 a § nya LEK).

I 9 kap. 31 § nya LEK föreskrivs att den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst som inte är en nummeroberoende interpersonell kommunikationstjänst (Noik) har fått del av eller tillgång till vissa närmare angivna uppgifter inte obehörigen får föra vidare eller utnyttja det han eller hon har fått del av eller tillgång till. Tystnadsplikten omfattar uppgift om abonnemang, innehållet i ett elektroniskt meddelande eller annan uppgift som angår ett särskilt elektroniskt meddelande (dvs. en trafikuppgift, se avsnitt 6.6.2).

Dessutom finns för nyss nämnda tillhandahållare en tystnadsplikt för uppgift som hänför sig till användning av vissa hemliga tvångsmedel. Tystnadsplikt gäller även bl.a. för uppgift som hänför sig till en begäran om utlämnande av uppgifter för brottsbekämpande verksamhet enligt 9 kap. 31 § första stycket 2 och 5 (se 9 kap. 32 § nya LEK). Ett obehörigt röjande eller utnyttjande av sådana uppgifter i strid med aktuella bestämmelser är straffsanktionerat som brott mot tystnadsplikten enligt 20 kap. 3 § brottsbalken.

I lagen finns dessutom bestämmelser som föreskriver en skyldighet för nämnda tillhandahållare att i vissa fall på begäran lämna ut bl.a. uppgift om abonnemang (9 kap. 33 § första stycket nya LEK).

Regeringen bestämmer vilken myndighet som ska vara regleringsmyndighet respektive tillsynsmyndighet (1 kap. 6 § nya LEK). Regleringsmyndigheten ska pröva ansökningar, besluta om skyldigheter och i övrigt pröva frågor och handlägga ärenden enligt nya LEK och enligt föreskrifter meddelade i anslutning till den lagen. Tillsynsmyndigheten ska ta emot anmälningar och utöva tillsyn enligt vad som framgår av nya LEK. PTS är regleringsmyndighet och tillsynsmyndighet enligt nya LEK (1 kap. 5 § nya FEK).

5 Uppgifter om elektronisk kommunikation i brottsbekämpande verksamhet

5.1 Brottsbekämpande verksamhet

Brottsbekämpande verksamhet innefattar främst åtgärder för att dels förebygga, förhindra och upptäcka brottslig verksamhet, dels för att utreda och lagföra brott. Polismyndigheten och Säkerhetspolisen har en brottsbekämpande funktion. Även Åklagarmyndigheten, Ekobrottsmyndigheten, Tullverket, Kustbevakningen, Skatteverket och Försvarsmakten (militärpolisen) är brottsbekämpande myndigheter. Verksamhet för att utreda och beivra brott omfattar framför allt åtgärder inom ramen för förundersökningar. Förfarandet vid en förundersökning regleras framför allt i rättegångsbalken och i förundersökningskungörelsen (1947:948). En förundersökning ska, enligt 23 kap. 1 § RB, inledas så snart det på grund av angivelse eller av annat skäl finns anledning att anta att ett brott som hör under allmänt åtal har förövats. Förundersökningen har huvudsakligen två syften (se 23 kap. 2 §). Det ena är att utröna om brott föreligger, vem som skäligen kan misstänkas för brottet och att skaffa tillräckligt material för bedömning av om åtal ska väckas. Det andra syftet är att bereda målet så att bevisningen kan läggas fram i ett sammanhang vid en huvudförhandling i domstol. Under förundersökningen får straffprocessuella tvångsmedel enligt 24–28 kap. RB användas.

Verksamhet för att förebygga, förhindra och upptäcka brottslig verksamhet bedrivs i ett skede där det inte finns någon konkret uppgift om att ett bestämt brott har begåtts. Med underrättelseverksamhet avses verksamhet som består i att samla in, bearbeta och analysera information för att klarlägga om brottslig verksamhet har utövats,

eller kan komma att utövas, och som inte utgör förundersökning enligt 23 kap. rättegångsbalken.[1]

Underrättelseverksamheten är alltså i huvudsak inriktad på att upptäcka om en viss, inte närmare specificerad brottslighet har ägt rum, pågår eller kan antas komma att begås. Ett övergripande mål är att förse de brottsutredande myndigheterna med kunskap som kan omsättas i operativ verksamhet.

Polismyndigheten och Säkerhetspolisen bedriver underrättelseverksamhet. Sådan verksamhet bedrivs också vid vissa andra myndigheter, såsom Ekobrottsmyndigheten, Skatteverket och Tullverket.

Underrättelseverksamhet bedrivs enligt en viss process. Det första ledet i processen är planeringsfasen. I planeringsfasen tar man ställning till t.ex. vilka områden som är prioriterade och vilka uppgifter som ska hämtas in. Nästa steg är inhämtningen, som kan ske på flera olika sätt. Trots att det ännu inte är fråga om verksamhet för att utreda brott finns det vissa möjligheter att använda tvångsmedel. När information har hämtats in bearbetas den genom att struktureras, systematiseras och värderas, t.ex. genom jämförelser med sedan tidigare kända uppgifter. Därefter vidtar analysen, som är den avgörande fasen i underrättelseprocessen. Det kan handla om t.ex. hot- och riskanalys, analys av brottsmönster och kartläggning av kriminella nätverk och grupperingar. Efter inhämtning, bearbetning och analys är ambitionen att det framtagna underrättelsematerialet ska kunna användas i operativt arbete. Det framtagna underrättelsematerialet kan t.ex. läggas till grund för beslut om att inleda förundersökning eller beslut om att vidta särskilda åtgärder för att förebygga, förhindra eller upptäcka brott. Det kan också användas för att gå ut i media för att förebygga ett visst brottsligt tillvägagångssätt. En annan form av förebyggande verksamhet innebär att berörda personer kontaktas och därigenom blir medvetna om den brottsbekämpande myndighetens intresse, vilket många gånger leder till att den planerade brottsliga verksamheten aldrig kommer till stånd.[2]

[1] Se prop. 2017/18:232 s. 430 och jämför med legaldefinitionen i 1 kap. 3 § i den numera upphävda Polisdatalagen (1998:622)
[2] Se SOU 2017:75 s. 84 f., Ds 2018:35 s. 34, prop. 2018/19:96 s. 14 och Ds 2020:12 s. 38.

5.2 Allmänt om straffprocessuella tvångsmedel

Straffprocessuella tvångsmedel är åtgärder som företas i myndighetsutövning och innebär intrång i en persons rättssfär utan att personen har lämnat sitt samtycke.[3] Exempel på tvångsmedel är husrannsakan, kroppsvisitation, kroppsbesiktning, beslag, gripande, anhållande och häktning. En grundläggande förutsättning för att använda straffprocessuella tvångsmedel är normalt att en förundersökning har inletts. Användningen ska då ytterst ha till syfte att utreda eller lagföra ett visst brott. Regleringen ger dock stöd även för att i vissa fall använda hemliga tvångsmedel för att förebygga, förhindra eller upptäcka brottslig verksamhet utan att förundersökning har inletts, dvs. i underrättelseverksamhet.

Bland de straffprocessuella tvångsmedlen intar de hemliga tvångsmedlen en särställning. Dessa är hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, kvarhållande (och kontroll) av försändelse, hemlig rumsavlyssning och hemlig dataavläsning. Till dessa kommer de s.k. osjälvständiga tvångsmedlen, dvs. tvångsmedlen enligt LSU och preventivlagen, som har sin tillämpning utanför en förundersökning. Även inhämtning av uppgifter enligt inhämtningslagen anses vara ett hemligt tvångsmedel.[4] Den berörde är inte medveten om dessa åtgärder, men det antas att de äger rum mot hans eller hennes vilja. Inhämtning av uppgifter om abonnemang enligt nya LEK anses inte som ett hemligt tvångsmedel.[5]

De hemliga tvångsmedlen omgärdas av särskilda garantier och mekanismer som ska säkerställa att reglerna och tillämpningen av dem lever upp till högt ställda krav på rättssäkerhet och att intrånget i den personliga integriteten minimeras. För tillstånd till hemliga tvångsmedel krävs normalt prövning i domstol. Vid domstolsprövningen av flertalet av tvångsmedlen ska ett offentligt ombud närvara för att bevaka enskildas integritetsintressen. Det offentliga ombudet ska ha tillgång till allt material som ligger till grund för domstolens prövning och rätt att överklaga domstolens beslut. Till rättssäkerhetsgarantierna räknas också bl.a. en skyldighet att i efterhand underrätta vissa personer om att hemliga tvångsmedel har använts samt

[3] Lindberg, Straffprocessuella tvångsmedel, 5:e uppl., 2022, s. 47.
[4] Se prop. 2011/12:55 s. 111.
[5] Se a. prop. s. 110–111.

SIN:s tillsyn över de brottsbekämpande myndigheternas användning av tvångsmedlen.

När lagstiftaren har preciserat i vilka fall en viss myndighet ska ha rätt att få tillgång till en viss typ av uppgifter kan regleringen inte kringgås genom att myndigheten väljer att tillämpa andra tvångsmedel. Exempelvis regleras de brottsbekämpande myndigheternas tillgång till innehållet i ett särskilt elektroniskt meddelande som finns hos en teleoperatör[6] exklusivt av reglerna om hemlig avlyssning av elektronisk kommunikation. Beslag, husrannsakan och edition får därför inte användas för att få fram sådana uppgifter. När ett meddelande har nått fram till mottagaren är det däremot åtkomligt med stöd av reglerna om husrannsakan och beslag.[7]

Principerna om ändamål, behov och proportionalitet

För all användning av tvångsmedel gäller tre allmänna principer: ändamålsprincipen, behovsprincipen och proportionalitetsprincipen.

Enligt ändamålsprincipen får ett tvångsmedel användas endast för det ändamål som framgår av lagstiftningen. En ändamålsprövning bör ske före behovs- och proportionalitetsprövningen. Om tvångsmedlet inte ska användas för det ändamål det är till för, spelar det ingen roll om det finns ett påtagligt behov och åtgärden framstår som proportionerlig. I reglerna om hemliga tvångsmedel anges dock inte uttryckligen för vilket specifikt ändamål tvångsmedlen får användas. Ändamålet får i stället sökas i de allmänna ändamålen med förundersökning.[8]

Behovsprincipen innebär att ett tvångsmedel får användas endast om det finns ett påtagligt behov och en mindre ingripande åtgärd inte är tillräcklig. När det inte längre finns skäl för åtgärden ska den upphävas. Åtgärder som huvudsakligen har till syfte att underlätta för myndigheten anses strida mot principen.

Enligt proportionalitetsprincipen ska en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet stå i rimlig proportion till vad som står att vinna med åtgärden. Proportionalitetsprincipen finns

[6] Med teleoperatör menar vi i detta betänkande sådana tillhandahållare som omfattas av skyldigheten att anmäla sin verksamhet enligt 2 kap. 1 § nya LEK.
[7] Se prop. 2002/03:74 s. 45 och 46 och Lindberg, Straffprocessuella tvångsmedel, 5:e uppl. 2022, s. 600 och 601.
[8] Se Lindberg, Straffprocessuella tvångsmedel, 5:e uppl. 2022, s. 569 och SOU 2017:75 s. 90–92.

lagstadgad i t.ex. 27 kap. 1 § RB och 2 § inhämtningslagen, men anses gälla vid all tvångsanvändning även utan lagstöd. Vid bedömningen om åtgärden är proportionerlig ska det intrång eller annat men som tvångsmedlet innebär för den misstänkte eller för något annat motstående intresse beaktas. Härmed inbegrips, förutom direkta följder för den som utsätts för tvångsmedlet, även indirekta verkningar av tvångsmedelsanvändningen. Det kan t.ex. röra sig om intrång i tredje mans rättsligt skyddade intressen. Det ska alltid ske en prövning huruvida tvångsmedlet över huvud taget är påkallat med hänsyn till förhållandena i det enskilda fallet och om syftet kan tillgodoses genom någon mindre ingripande åtgärd. Utgångspunkten bör vara att pröva om alternativa spaningsåtgärder kan användas och om det kan räcka med att exempelvis tillgripa hemlig övervakning av elektronisk kommunikation i stället för hemlig avlyssning. Personlig frihet och integritet ska också beaktas. Ingrepp i dessa intressen är till sin art allvarligare än ingrepp mot egendom eller andra ekonomiska intressen.[9] Det är särskilt viktigt att proportionalitet iakttas vid långtgående intrång i den privata sfären.

När begränsningar görs i rättigheter som följer av Europakonventionen eller EU-stadgan ska alltid proportionalitetsprincipen beaktas. Endast om det finns ett rimligt förhållande mellan behovet av det som ska tillgodoses och ingreppet i den enskildes rätt kan ingreppet vara proportionerligt och därmed nödvändigt i ett demokratiskt samhälle.[10]

5.3 Tillgången till uppgifter om elektronisk kommunikation

5.3.1 Tillgången till uppgift om abonnemang, m.m.

Som nämnts i avsnitt 4.3 har den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst som inte är en nummeroberoende interpersonell kommunikationstjänst (Noik) en tystnadsplikt för bl.a. uppgifter om abonnemang (9 kap. 31 § förstastycket 1 nya LEK). Trots tystnadsplikten har Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brottet

[9] Se SOU 1979:6 s. 294 och SOU 1984:54 s. 78.
[10] Se Hans Danelius, Mänskliga rättigheter i europeisk praxis, 5:e uppl., 2015, s. 57 och 58.

eller den brottsliga verksamheten rätt att få tillgång till abonnemangsuppgifter från dessa tillhandahållare, om uppgiften gäller brottslig verksamhet eller misstanke om brott som myndigheten ska ingripa mot (9 kap. 33 § förstastycket 2 nya LEK). Regleringen innebär att de brottsbekämpande myndigheterna i princip har rätt att hämta in abonnemangsuppgifter för att beivra alla typer av brott utom sådana som åtalas enbart av målsäganden.[11] Uppgifter om abonnemang får hämtas in även i underrättelseverksamhet.[12] Det saknas närmare regler om vem inom de brottsbekämpande myndigheterna som har rätt att hämta in abonnemangsuppgifterna och formen för hur uppgifterna ska hämtas in. Det kan noteras att Utredningen om utökade möjligheter att använda hemliga tvångsmedel (Ju 2020:20) i sitt slutbetänkande *Bättre möjligheter att verkställa frihetsberövanden* (SOU 2022:50) bl.a. har föreslagit en skyldighet för nämnda tillhandahållare att på begäran lämna ut uppgifter om abonnemang dels till Polismyndigheten om myndigheten bedömer att uppgiften behövs för att den ska kunna lokalisera personer i syfte att möjliggöra verkställighet av frihetsberövande påföljder, dels till Säkerhetspolisen om myndigheten bedömer att uppgiften behövs för att myndigheten ska kunna lokalisera en utlänning som inte har fullgjort sin anmälningsskyldighet enligt LSU.

Uppgifter om abonnemang anses typiskt sett vara mindre integritetskänsliga än t.ex. trafik- och lokaliseringsuppgifter eftersom de endast ger uppgift om att personen är abonnent eller användare av en viss tjänst eller av en ip-adress vid en viss tidpunkt. Som nämnts ovan anses tillgången till abonnemangsuppgifter inte heller utgöra ett hemligt tvångsmedel.

Bestämmelserna om uppgiftsskyldighet i gamla LEK ändrades den 1 juli 2012. Tidigare gällde att tystnadsplikten för uppgifter om abonnemang bara bröts om fängelse var föreskrivet för brottet och det enligt myndighetens bedömning kunde föranleda annan påföljd än böter. I förarbetena till 2012 års ändring i gamla LEK konstaterade regeringen att det skett en betydande teknisk utveckling och förändring av i vilken omfattning enskilda använder bl.a. datorer och mobiltelefoner.[13] Trakasserier över internet och vuxnas kontakter med barn i sexuellt syfte bedömdes ha blivit ett allt vanligare feno-

[11] Se SOU 2015:31 s. 198 f. och SOU 2017:75 s. 101.
[12] Se prop. 2021/22 :183 s. 61.
[13] Se prop. 2011/12 :55 s. 102.

men. Regeringen fann att intresset av att lämna ut abonnemangsuppgifter för att bekämpa brott vägde tyngre än det motstående intresset av att skydda enskildas integritet och föreslog därför att kravet på fängelse i straffskalan och det särskilda kravet i fråga om brottets straffvärde togs bort.[14]

Vidare finns det en skyldighet i 9 kap. 33 § förstastycket 5 nya LEK för den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst som inte är en Noik att lämna ut uppgifter som angår ett särskilt elektroniskt meddelande 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 § RB till den myndighet som meddelat föreläggandet. Denna skyldighet och möjligheten i rättegångsbalken att meddela ett sådant s.k. bevarandeföreläggande infördes i maj 2021 i samband med att Sverige skulle tillträda Europarådets konvention om it-relaterad brottslighet (den s.k. Budapestkonventionen).[15] Budapestkonventionen ställer nämligen krav på att lagrade datorbehandlingsbara uppgifter ska kunna säkras oavsett om en eller flera tjänsteleverantörer har deltagit i överföringen. Konventionsstaterna ska därför garantera att en tillräcklig mängd sådana trafikuppgifter ska kunna röjas för myndigheterna så att tjänsteleverantörerna, och den väg meddelandet överförts, ska kunna identifieras (artikel 17). Det är genom bestämmelsen i 9 kap. 33 § förstastycket 5 nya LEK möjligt att ta reda på från vilken tillhandahållare som meddelandet sändes och, för det fall det har vidaresänts, till vilken tillhandahållare det vidaresändes. Det ankommer på tillhandahållaren att ta fram de uppgifter som begärs. Om leverantören inte har någon uppgift om vilka de övriga aktörerna är kan någon information inte lämnas ut. Bestämmelsen innebär inte heller något krav på att spara eller lagra uppgifter.[16]

Bestämmelserna i 9 kap. 33 § första stycket nya LEK omfattar även skyldigheter för tillhandahållarna att lämna ut uppgifter såväl till brottsbekämpande som till vissa andra myndigheter och till regionala alarmeringscentraler i annat än brottsbekämpande syfte.

För att uppgifter om en fysisk person ska tas in i en allmänt tillgänglig abonnentförteckning krävs att personen har samtyckt till det

[14] Se a. prop. s. 103.
[15] Se prop. 2020/21:72.
[16] Se a. prop. s. 38 f.

(se 9 kap. 17 och 18 §§ nya LEK). I den utsträckning uppgifter finns tillgängliga i sådana allmänt tillgängliga förteckningar omfattas de, på grund av abonnentens samtycke, i praktiken inte av tystnadsplikten. Bestämmelserna om skyldighet att lämna ut uppgifter om abonnenter får därför betydelse i första hand i fråga om uppgifter som rör abonnenter som inte har lämnat sitt samtycke till att uppgifterna offentliggörs och när det gäller sådana uppgifter som normalt inte offentliggörs, såsom t.ex. ip-adresser.[17]

5.3.2 Tillgången till trafik- och lokaliseringsuppgifter inom en förundersökning

Hemlig avlyssning av elektronisk kommunikation

Hemlig avlyssning av elektronisk kommunikation (HAK) innebär att meddelanden, som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress, i hemlighet avlyssnas eller tas upp genom ett tekniskt hjälpmedel för återgivning av innehållet i meddelandet (27 kap. 18 § första stycket RB). Definitionen omfattar alla former av kommunikation genom elektroniska kommunikationsnät, såväl muntlig som skriftlig, och avser t.ex. telefontrafik, e-posttrafik och överföring av datafiler. Avlyssning kan, med vissa begränsningar, ske även utanför allmänt tillgängliga telenät, t.ex. inom större företagsnät.

HAK får användas vid förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år. Därutöver får HAK användas vid förundersökning om vissa samhällsfarliga brott som bekämpas av Säkerhetspolisen, t.ex. sabotage, spioneri och vissa brott enligt terroristbrottslagen (2022:666). HAK får också användas vid förundersökning om försök, förberedelse eller stämpling till nu nämnd brottslighet i den mån sådana förstadier till brott är straffbelagda. Tvångsmedlet får också användas vid förundersökning i fråga om annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde skulle överstiga fängelse i två år. Ett tillstånd till HAK ger också rätt att vidta åtgärder som avses i 27 kap. 19 § RB, dvs. att inhämta sådana uppgifter som omfattas av hemlig övervakning av elektronisk kommunikation.

[17] Se prop. 2018/19:86 s. 94.

En förutsättning för att HAK ska få användas vid förundersökning är att någon är skäligen misstänkt för brottet. Åtgärden ska vidare vara av synnerlig vikt för utredningen (27 kap. 20 § första stycket RB). Avlyssning får avse ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning som under den tid som tillståndet avser innehas eller har innehafts av den misstänkte eller annars kan antas ha använts eller komma att användas av den misstänkte. Avlyssningen får också avse ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Hemlig övervakning av elektronisk kommunikation

Hemlig övervakning av elektronisk kommunikation (HÖK) innebär att uppgifter i hemlighet hämtas in om meddelanden (både samtal och skriftliga meddelanden) som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress. Även uppgifter om vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område (s.k. basstationstömning) eller i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits kan hämtas in med stöd av hemlig övervakning av elektronisk kommunikation (27 kap. 19 § första stycket RB). Tvångsmedlet kan även användas för att hindra meddelanden som överförs i ett elektroniskt kommunikationsnät från att nå fram (27 kap. 19 § andra stycket RB).

Tvångsmedlet ger inte tillgång till innehållet i utväxlade meddelanden. Det som kan hämtas in är trafikuppgifter och lokaliseringsuppgifter. HÖK omfattar såväl inhämtning av uppgifter från teleoperatörer som inhämtning genom egna tekniska medel som de brottsbekämpande myndigheterna förfogar över.

HÖK får användas vid förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader, vid förundersökning som avser dataintrång, barnpornografibrott som inte är att anse som ringa eller narkotikabrott och narkotikasmuggling av normalgraden. Därutöver får tvångsmedlet användas vid förundersökning om vissa samhällsfarliga brott som bekämpas av Säkerhetspolisen, t.ex. sabotage, spionerі och brott enligt terroristbrottslagen.

HÖK får också användas vid förundersökning om försök, förberedelse eller stämpling till nu nämnd brottslighet i den mån sådana förstadier till brott är straffbelagda (27 kap. 19 § andra stycket RB). HÖK får användas när någon är skäligen misstänkt för brottet eller, med vissa begränsningar, för att utreda vem som skäligen kan misstänkas för brottet (27 kap. 20 § andra stycket RB).

Utredningen om utökade möjligheter att använda hemliga tvångsmedel

Utredningen om utökade möjligheter att använda hemliga tvångsmedel (Ju 2020:20) har i delbetänkandet *Utökade möjligheter att använda hemliga tvångsmedel* (SOU 2022:19) föreslagit vissa ändringar i reglerna om hemliga tvångsmedel. Bl.a. föreslås att straffvärdeventiler ska införas som gör det möjligt att i vissa situationer beakta en flerfaldig brottslighets samlade straffvärde vid bedömningen av om hemliga tvångsmedel ska få användas. Vidare föreslås att bl.a. HAK och HÖK ska få användas vid förundersökningar om grovt dataintrång, sexualbrott mot barn och barnpornografibrott, utpressning och grov utpressning, mened, övergrepp i rättssak, grovt jaktbrott och grovt insiderbrott. Dessutom föreslås att HAK i vissa fall ska få användas för att utreda vem som skäligen kan misstänkas för brottet.

I slutbetänkandet *Bättre möjligheter att verkställa frihetsberövanden* (SOU 2022:50) har utredningen bl.a. förslagit att det ska införas en möjlighet att använda HÖK i syfte att eftersöka en person som är anhållen eller häktad men inte frihetsberövad. Vidare föreslås att det ska införas en ny lag med tillhörande förordning med bestämmelser som möjliggör användning av bl.a. HÖK i syfte att lokalisera personer som håller sig undan från en frihetsberövande påföljd.

5.3.3 Tillgången till trafik- och lokaliseringsuppgifter utanför en förundersökning

Lagen om åtgärder för att förhindra vissa särskilt allvarliga brott

Lagen om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen) ger myndigheterna en möjlighet att använda hemliga tvångsmedel för att förhindra brott. Tillstånd till bl.a. HAK och

HÖK får meddelas om det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva brottslig verksamhet som innefattar bl.a. sabotage, spionerі och terroristbrott (1 § första stycket). Tillstånd får också meddelas om det finns en påtaglig risk för att det inom en organisation eller grupp kommer att utövas sådan brottslig verksamhet och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet. HAK och HÖK får enligt lagen enbart avse

- ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning som under den tid tillståndet avser innehas eller har innehafts av den för tvångsmedlet aktuella personen, eller som annars kan antas ha använts eller komma att användas av honom eller henne, eller
- ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning som det finns synnerlig anledning att anta att personen under den tid tillståndet avser har kontaktat eller kommer att kontakta.

Även om lagen främst rör brottslig verksamhet inom Säkerhetspolisens område kan också Polismyndigheten använda lagen. Frågan om tillstånd till tvångsmedel enligt lagen prövas av Stockholms tingsrätt efter ansökan av åklagare. Tillstånd får meddelas endast om åtgärden är proportionerlig och av synnerlig vikt för att förhindra brottslig verksamhet.

Den 2 november 2021 tillsatte regeringen en utredning om preventiva tvångsmedel för att förhindra allvarlig brottslighet (dir. 2021:102). Utredningen om preventiva tvångsmedel (Ju 2021:15) har i delbetänkandet *Utökande möjligheter att använda preventiva tvångsmedel* (SOU 2022:52) övervägt i vilken utsträckning det ska införas utökade möjligheter att använda preventiva tvångsmedel för att förhindra allvarlig brottslighet som förekommer inom ramen för kriminella nätverk. Utredningen har föreslagit ett utökat tillämpningsområde som avgränsas till brottslig verksamhet som utövas inom en organisation eller grupp och att tvångsmedelsanvändningen endast får riktas mot en person som tillhör eller verkar för organisationen eller gruppen och kan befaras medvetet främja den brottsliga verksamheten. Det utökade tillämpningsområdet föreslås omfatta brottslig verksamhet

innefattande bl.a. mord, människorov, narkotikabrott, vapenbrott, sprängningsbrott och olovlig hantering av explosiva varor.

Genom tilläggsdirektiv den 7 juli 2022 (dir. 2022:104) ska utredningen även ta ställning till om, och i så fall vilka, ytterligare tvångsmedel och verkställighetsåtgärder som bör få användas av de brottsbekämpande myndigheterna för att förhindra allvarlig brottslighet, till exempel hemlig rumsavlyssning, hemlig dataavläsning avseende rumsavlyssningsuppgifter, genomsökning på distans, biometrisk autentisering och kopiering. Utredaren ska dessutom ta ställning till om tillstånd till hemlig kameraövervakning och hemlig dataavläsning avseende kameraövervakningsuppgifter utanför en förundersökning bör kunna knytas till en person. Uppdraget ska i denna del redovisas senast den 31 maj 2023.

Lagen om särskild kontroll av vissa utlänningar

Den 1 juli 2022 trädde lagen (2022:700) om särskild kontroll av vissa utlänningar (LSU) i kraft.[18] Enligt 2 kap. 1 § LSU får en utlänning utvisas ur Sverige om utlänningen

1. med hänsyn till vad som är känt om hans eller hennes tidigare verksamhet och övriga omständigheter kan antas komma att begå eller på annat sätt medverka till ett brott enligt terroristbrottslagen (2022:666), eller
2. kan utgöra ett allvarligt hot mot Sveriges säkerhet.

Vissa tvångsmedel får användas om ett beslut om sådan utvisning tills vidare inte ska verkställas på grund av ett beslut om inhibition eller ett tidsbegränsat uppehållstillstånd. Detsamma gäller om ett beslut om utvisning enligt 8 eller 8 a kap. utlänningslagen (2005:716) inte kan verkställas och utlänningen skulle kunna utvisas enligt 2 kap. 1 § LSU (5 kap. 1 § LSU).

Om det finns särskilda skäl får tillstånd till vissa hemliga tvångsmedel meddelas om det är av betydelse för att klarlägga om

[18] Genom lagen upphävdes lagen (1991:572) om särskild utlänningskontroll.

1. utlänningen tillhör eller verkar för en organisation eller grupp som planlägger eller förbereder brott enligt terroristbrottslagen (2022:666) eller om det finns en risk för att utlänningen kan komma att engagera sig i en sådan organisation eller grupp,
2. det finns risk för att utlänningen själv planlägger eller förbereder brott som avses i 1, eller
3. det finns risk för att utlänningen själv eller tillsammans med andra medverkar i eller på annat sätt främjar ett allvarligt brott som rör Sveriges säkerhet.

Säkerhetspolisen får hos Migrationsverket ansöka om godkännande att ansöka om tillstånd de hemliga tvångsmedlen (5 kap. 8 § andra stycket 2 LSU). I samband med att regeringen beslutar om inhibition eller tidsbegränsat uppehållstillstånd får regeringen godkänna att Säkerhetspolisen får ansöka om tillstånd till de hemliga tvångsmedlen (5 kap. 9 § förstastycket 2 LSU).

Säkerhetspolisen får, efter godkännande enligt ovan, hos Stockholms tingsrätt ansöka om ett tillstånd till HAK, HÖK, hemlig kameraövervakning eller postkontroll (5 kap. 11 § LSU).

Det kan slutligen nämnas att det i slutbetänkandet *Bättre möjligheter att verkställa frihetsberövanden* (SOU 2022:50) har förslagits att det ska införas en möjlighet att använda HÖK i syfte att kunna lokalisera en utlänning som inte har fullgjort sin anmälningsskyldighet.

Inhämtningslagen

Enligt lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) får Polismyndigheten, Säkerhetspolisen eller Tullverket i sin underrättelseverksamhet i hemlighet hämta in uppgifter om meddelanden som i ett elektroniskt kommunikationsnät har överförts till eller från ett telefonnummer eller annan adress, om vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område eller uppgifter om inom vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits (1 §). Lagen reglerar enbart inhämtning från den som enligt lagen om elektronisk kommunikation tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommuni-

kationstjänst som inte är en nummeroberoende interpersonell kommunikationstjänst. Lagen ger alltså inte stöd för de brottsbekämpande myndigheterna att hämta in uppgifter med hjälp av egna tekniska hjälpmedel.

Uppgifter får enligt lagen hämtas in om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott som har minst två års fängelse i straffskalan. Inhämtning av uppgifter är också möjlig vid brottslig verksamhet som innefattar vissa särskilt angivna samhällsfarliga brott inom Säkerhetspolisens ansvarsområde med lägre straffminimum, t.ex. sabotage och spioneri (2 §). Genom rekvisitet ”brottslig verksamhet” framgår att det inte ställs krav på att det ska finnas en misstanke om ett specifikt brott.[19]

Beslut om inhämtning av uppgifter fattas av åklagare vid Åklagarmyndigheten efter ansökan av Polismyndigheten, Säkerhetspolisen eller Tullverket.

Enligt tilläggsdirektiv den 28 april 2022 (dir. 2022:32) ska Utredningen om preventiva tvångsmedel ta ställning till om, och i så fall på vilket sätt, tillämpningsområdet för inhämtningslagen bör utvidgas och till hur beslutsordningen bör se ut vid en eventuell utvidgning av inhämtningslagens tillämpningsområde. Uppdraget i denna del ska redovisas senast den 31 maj 2023.

5.3.4 Hemlig dataavläsning

Hemlig dataavläsning (HDA) är ett relativt nytt tvångsmedel som innebär att uppgifter, som är avsedda för automatiserad behandling, i hemlighet och med ett tekniskt hjälpmedel läses av eller tas upp i ett avläsningsbart informationssystem (1 § lagen om hemlig dataavläsning). Tvångsmedlet ger Polismyndigheten, Säkerhetspolisen, Tullverket och Ekobrottsmyndigheten möjligheter att avlyssna och övervaka personer som är misstänkta för eller förväntas begå allvarliga brott.

HDA kan användas såväl under en förundersökning som utanför. Med stöd av tvångsmedlet kan myndigheterna i hemlighet installera mjuk- eller hårdvara i en teknisk utrustning (till exempel en dator, mobiltelefon eller läsplatta) och med hjälp av mjuk- eller hårdvaran

[19] Se prop. 2011/12:55 s. 121.

läsa av uppgifter som finns i utrustningen. Det kan till exempel handla om att installera en trojan för att läsa av meddelanden och avlyssna samtal i krypterade program och appar eller skaffa sig tillgång till ett konto i sociala medier. Det kan också handla om att aktivera mikrofonen eller kameran i en utrustning och på så sätt hämta in tal och rörliga bilder. Det kan också handla om att myndigheterna, med tillgång till inloggningsuppgifter, kan logga in från sina egna datorer på ett användarkonto för att t.ex. ta del av e-postmeddelanden.

Om hårdvara behöver installeras i t.ex. någons dator, kan myndigheterna få tillstånd att i hemlighet ta sig in i utrymmet där utrustningen finns för att installera hårdvaran.

Frågor om hemlig dataavläsning prövas av domstol. Lagen om hemlig dataavläsning är tidsbegränsad och upphör att gälla vid utgången av mars 2025. En särskild utredare har fått i uppdrag att utvärdera lagen inför ett ställningstagande till om den bör permanentas och om den i så fall bör ändras i något avseende (dir. 2022:82). Uppdraget ska redovisas senast den 1 december 2023.

I delbetänkandet *Utökade möjligheter att använda hemliga tvångsmedel* (SOU 2022:19) föreslås vissa ändringar i lagen om hemlig dataavläsning. Bl.a. föreslås en straffvärdeventil som gör det möjligt att i vissa situationer beakta en flerfaldig brottslighets samlade straffvärde vid bedömning av om hemlig dataavläsning ska få användas.

Som nämnts ovan ska Utredningen om preventiva tvångsmedel ta ställning till om hemlig dataavläsning avseende rumsavlyssningsuppgifter bör få användas av de brottsbekämpande myndigheterna för att förhindra allvarlig brottslighet.

5.3.5 Genomsökning på distans

Den 1 juni 2022 infördes tvångsmedlet genomsökning på distans. Tvångsmedlet innebär en möjlighet för de brottsbekämpande myndigheterna att söka efter handlingar som finns lagrade i ett avläsningsbart informationssystem utanför den elektroniska kommunikationsutrustning som används för att utföra genomsökningen (28 kap. 10 a § RB). Genomsökning på distans får ske endast i syfte att söka efter handlingar som kan ha betydelse för utredning av brott eller om förverkande av utbyte av brottslig verksamhet enligt 36 kap. 1 b § brottsbalken. För att genomsökning på distans ska få utföras krävs

att det finns anledning att anta att brott har begåtts på vilket fängelse kan följa. Vidare krävs att det informationssystem som genomsökningen ska utföras i kan ha använts av den som skäligen kan misstänkas för brottet eller, i annat fall, om det finns synnerlig anledning att anta att det går att påträffa handlingar som kan vara av betydelse för utredning av brottet eller om förverkande av utbyte av brottslig verksamhet. Till skillnad mot HDA får genomsökningen endast utföras genom autentisering i det informationssystem som åtgärden avser (28 kap. 10 b § RB).

Om det finns anledning att anta att någon har möjlighet att öppna informationssystemet genom biometrisk autentisering, är han eller hon skyldig att på tillsägelse av en polisman medverka till detta under förutsättning att genomsökningen annars försvåras. Vid vägran att medverka vid sådan autentisering får en polisman genomföra autentiseringen (27 kap. 17 f § RB). Vad som nu sagts gäller även för tjänstemän vid Tullverket och kustbevakningstjänstemän i fråga om vissa brott (se 26 och 29 a §§ lagen [2000:1225] om straff för smuggling).

Genomsökning på distans får beslutas av undersökningsledaren, åklagaren eller rätten. En polisman får dock vidta åtgärden utan ett sådant beslut om det är fara i dröjsmål och genomsökningen inte kan antas bli av stor omfattning eller medföra synnerlig olägenhet för den som drabbas av åtgärden (28 kap. 10 d § RB). Den misstänktes samtycke får inte åberopas som stöd för genomsökningen, om inte den misstänkte själv har begärt att åtgärden ska utföras (28 kap. 1 § tredje stycket RB). Genomsökning på distans får beslutas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller något annat motstående intresse (28 kap. 3 a och 10 i §§ RB).

5.4 Svensk jurisdiktion och internationell rättslig hjälp

5.4.1 Svensk jurisdiktion

Ordet jurisdiktion används främst för att hänvisa till en stats maktutövning över personer och egendom inom dess eget territorium. En stats jurisdiktion kan utövas genom rätten att stifta lagar och andra regler (legislativ jurisdiktion), rätten att tillämpa lagstiftningen eller skipa rätt (judiciell jurisdiktion) och rätten att verkställa åtgärder

eller förverkliga beslut som fattats inom ramen för lagstiftning och rättskipning (exekutiv jurisdiktion).

I det s.k. Lotus-målet från år 1927 (som avgjordes av den Fasta mellanfolkliga domstolen, Permanent Court of International Justice, PCIJ, Ser. A, no. 10) slog domstolen fast att den viktigaste inskränkningen som folkrätten ålägger en stat är att inte utöva makt inom en annan stats territorium. Samtidigt konstaterade domstolen att det inte finns något hinder för en stat att utöva jurisdiktion inom sitt eget territorium över något som har inträffat utomlands om det inte finns ett uttryckligt folkrättsligt förbud mot det. Domstolen menade att en stat kan utöva lagstiftande och dömande makt över personer och egendom som befinner sig utomlands och över händelser som äger rum utanför statens territorium, så länge det handlar om egna medborgare eller egendom som har en länk till staten och förutsatt att det inte råder något folkrättsligt förbud mot ett sådant utövande av jurisdiktion. Verkställigheten av nationella lagar och domar (t.ex. gripande eller beslag) kan dock äga rum endast inom det egna territoriet.

Domstolens avgörande i Lotus-målet har gett upphov till den s.k. Lotus-principen, som innebär att det som inte uttryckligen är förbjudet i folkrätten är tillåtet. Principen handlar både om rätten att stifta nationella lagar och om rätten att verkställa nationella lagar.

En stats maktmonopol inom det egna territoriet vad gäller verkställande åtgärder har ett undantag. Sådana åtgärder får inte tillämpas på andra länders diplomatiska eller politiska företrädare, vilka åtnjuter immunitet.

När det gäller utövande av lagstiftande eller dömande straffrättslig jurisdiktion har en stat rätt att lagföra brott inom sitt eget territorium samt över egna medborgare, även om brottet i fråga begåtts i en annan stat. När det gäller utövningen av en stats straffrättsliga jurisdiktion mot en annan stats medborgare är folkrättsliga regler om jurisdiktion relevanta. Nationella domstolars behörighet att tillämpa sina egna strafflagar bygger på ett antal principer som har stöd i statspraxis och i folkrättsdoktrinen, och som kan hänföras till ett antal anknytningspunkter, t.ex. om territoriet, nationalitet, skyddet av statens vitala intressen samt det universella intresset.[20]

I avsnitt 11 avhandlas vissa frågor om exekutiv jurisdiktion.

[20] Se Bring m.fl., Sverige och folkrätten, JUNO, version 6, s. 107 ff.

5.4.2 Internationell rättslig hjälp

Eftersom svenska brottsbekämpande myndigheter saknar exekutiv jurisdiktion för att verkställa beslut om utredningsåtgärder i en annan stat, får de i stället begära hjälp från den aktuella staten för att få åtgärden utförd. Svenska brottsbekämpande myndigheters möjlighet till rättslig hjälp när det gäller straffprocessuella tvångsmedel regleras främst i lagen (2000:562) om internationell rättslig hjälp i brottmål och i lagen (2017:1000) om en europeisk utredningsorder. Nedan redogörs för dessa lagar (se även avsnitt 11.4).

Lagen om internationell rättslig hjälp i brottmål

Lagen om internationell rättslig hjälp i brottmål (LIRB) är tillämplig på samarbete som tar sikte på rättsliga förfaranden som gäller utredning om och lagföring för brott. Lagen gäller inte om lagen om en europeisk utredningsorder är tillämplig (se nedan). Enligt 1 kap. 2 § LIRB kan rättslig hjälp omfatta bl.a. HAK, HÖK och hemlig dataavläsning (HDA).

Tillstånd till nämnda tvångsmedel lämnas under samma förutsättningar som gäller för motsvarande åtgärder under en svensk förundersökning, enligt rättegångsbalken eller annan lag eller författning, med beaktande av de särskilda bestämmelser som finns i LIRB (2 kap. 1 §). Vid prövningen om åtgärden kan vidtas i Sverige ska gärningen bedömas enligt svensk rätt och de svenska strafftrösklarna gäller. Det föreligger ett krav på dubbel straffbarhet (2 kap. 2 § LIRB).

Det finns vissa allmänna regler som gäller för samtliga prövningar av ansökningar från andra länder. En ansökan ska enligt dessa bestämmelser avslås om ett bifall till ansökan skulle kränka Sveriges suveränitet, medföra fara för rikets säkerhet eller strida mot svenska allmänna rättsprinciper eller andra väsentliga intressen. Ansökan får vidare avslås bl.a. om gärningen har karaktär av ett politiskt eller militärt brott, eller omständigheterna annars är sådana att ansökan inte bör bifallas. Om åklagaren eller domstolen finner att ansökan bör avslås på någon av de nu angivna grunderna ska ansökan överlämnas till regeringen som beslutar i frågan (2 kap. 14 och 15 §§ LIRB).

Svenska åklagares möjligheter att begära rättslig hjälp utomlands är i huvudsak oreglerad, eftersom möjligheterna att få rättslig hjälp

av andra stater främst styrs av dessa staters internationella åtaganden och nationella lagstiftning.

Lagen om en europeisk utredningsorder

Med en europeisk utredningsorder avses antingen

1. ett beslut i Sverige som innebär att en utredningsåtgärd ska vidtas i en annan medlemsstat i syfte att inhämta bevisning och som har meddelats av en åklagare eller domstol under en förundersökning eller rättegång i brottmål, eller
2. ett beslut i en annan medlemsstat som innebär att en utredningsåtgärd ska vidtas i Sverige i syfte att inhämta bevisning och som har meddelats eller godkänts av en domare, domstol, undersökningsdomare eller allmän åklagare i ett straffrättsligt förfarande eller i ett annat förfarande avseende straffbara gärningar som inleds vid en administrativ eller rättslig myndighet, när ett beslut i ett sådant annat förfarande kan leda till ett förfarande inför en domstol som är behörig att handlägga brottmål (1 kap. 3 § lagen om en europeisk utredningsorder).

I 1 kap. 4 § lagen om en europeisk utredningsorder anges vad en utredningsåtgärd enligt lagen ska avse eller motsvara. Där framgår att bl.a. HAK, HÖK och HDA är utredningsåtgärder som avses i lagen.

En europeisk utredningsorder får utfärdas i Sverige av åklagare om de förutsättningar som gäller för att vidta utredningsåtgärden under en svensk förundersökning är uppfyllda och åtgärden är nödvändig och proportionerlig. Dessutom krävs, när det är fråga om hemliga tvångsmedel, att domstol har lämnat tillstånd till att utfärda ordern (se 2 kap. samma lag).

När det gäller erkännande och verkställighet i Sverige av en europeisk utredningsorder gäller att en utredningsorder som sänds över från en annan medlemsstat ska erkännas och verkställas i Sverige om vissa särskilda förutsättningar enligt lagen är uppfyllda och inte annat följer av lagen (3 kap. 1 § lagen om en europeisk utredningsorder). För hemliga tvångsmedel ställs som en särskild förutsättning upp att en utredningsorder får erkännas och verkställas endast om den gärning som avses i utredningsordern motsvarar ett brott enligt svensk lag

och om övriga förutsättningar som gäller för en motsvarande åtgärd i en svensk förundersökning är uppfyllda (3 kap. 4 § samma lag).

Bland de obligatoriska vägransgrunderna nämns att utredningsordern skulle medföra fara för Sveriges säkerhet. Även att utredningsåtgärden inte motsvarar en åtgärd som anges i 1 kap. 4 § lagen om en europeisk utredningsorder utgör en obligatorisk vägransgrund, dock inte om en annan utredningsåtgärd kan vidtas som ger motsvarande resultat som den åtgärd som utredningsordern avser (3 kap. 5 § samma lag).

5.5 Nyttan och behovet av uppgifter om elektronisk kommunikation

För att de brottsbekämpande myndigheterna ska kunna fullgöra sina uppgifter att förebygga, förhindra, upptäcka, utreda och lagföra brott har myndigheterna behov av information. Detta behov kan vara olika stort beroende på vilken brottslighet och vilken sorts aktörer det är fråga om. Myndigheterna kan använda olika metoder för att skaffa relevant information, t.ex. spaning, förhör och kontakter med anmälare och tipsare. Behovet av information i såväl utrednings- som underrättelseverksamhet innefattar också ett behov av uppgifter om elektronisk kommunikation.

I utredningar om allvarlig brottslighet är tillgången till uppgifter om elektronisk kommunikation ofta avgörande för att utredningarna ska kunna föras framåt. Trafik- och lokaliseringsuppgifter har med tiden blivit ett allt viktigare verktyg i brottsbekämpningen och används i princip i varje utredning rörande grova brott. Uppgifterna är ofta den första och enda ingången i ärenden som rör grov brottslighet. I många fall är uppgifterna också helt avgörande för att utredningarna ska nå det stadium där andra insatser kan sättas in.[21] Uppgifter om elektronisk kommunikation kan svara på frågor bl.a. om vilka nummer som har haft kontakt med varandra, när kommunikationen skett, hur intensiv kommunikationen har varit och var användare av t.ex. mobiltelefoner har befunnit sig. Inhämtade uppgifter kan i många fall också få till följd att personer avförs från en utredning, eftersom misstankarna mot dem visar sig sakna substans.

[21] Se t.ex. SOU 2017:75 s. 120 f.

Genom tillgången till historiska trafik- och lokaliseringsuppgifter kan de brottsbekämpande myndigheterna kartlägga händelser som anknyter såväl till själva brottstillfället som till planläggning och flykt. Det är inte möjligt att ersätta sådan inhämtning med t.ex. fysisk spaning, eftersom inhämtningen avser historiska uppgifter. Uppgifter om användning av kommunikationstjänster går inte heller att inhämta på annat sätt då det sker i en miljö som de brottsbekämpande myndigheterna inte har tillgång till. De brottsbekämpande myndigheterna är därför beroende av att tillhandahållaren lagrar uppgifter och att dessa uppgifter kan hämtas in när sådana behov uppstår i den brottsbekämpande verksamheten. Vid utredning av internetrelaterad brottslighet är uppgifter om elektronisk kommunikation ofta helt avgörande för att identifiera en misstänkt gärningsman och för att i övrigt driva utredningen framåt. Trafikuppgifternas betydelse i brottsutredningar hänger också samman med att den information som kommer fram vid HÖK och HAK ofta bedöms ha ett betydande bevisvärde i rättegångar som rör grov och organiserad brottslighet.[22]

Uppgifter om elektronisk kommunikation kan även vara av största vikt för att i underrättelseverksamhet förebygga, förhindra och upptäcka brottslig verksamhet. 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 förundersökning. Uppgifterna är också väsentliga för en effektiv planering av fysisk spaning, som är resurskrävande och därför viktig att använda på rätt plats och vid rätt tillfälle.[23]

Lagringsskyldigheten i 9 kap. 19 § nya LEK syftar till att säkerställa tillgången till vissa uppgifter om elektronisk kommunikation för brottsbekämpande ändamål.

[22] Se a.a. s. 121 f.
[23] Se skr. 2020/21:59 s. 39.

6 Lagring och tillgång till uppgifter i syfte att bekämpa brott

6.1 Inledning

Den 1 oktober 2019 trädde nya regler om datalagring för brottsbekämpande ändamål i Sverige i kraft. Ändringarna var föranledda av den s.k. Tele2-domen. Ändringarna innebär bl.a. att lagringens omfattning har begränsats och att lagringstiderna har differentierats i jämförelse med hur det var tidigare. I förarbetena uttalade regeringen att det senast inom fyra år efter ikraftträdandet kunde finnas anledning att se över regleringen, bl.a. mot bakgrund av den tekniska utvecklingen, ändrade kommunikationsvanor och nya mål om datalagring i EU-domstolen.[1] Den tekniska utvecklingen har fortsatt i snabb takt och kommunikationsvanorna har förändrats. Det finns också ny praxis på området.

I samband med att de nya reglerna antogs tillkännagav Riksdagen för regeringen att den skyndsamt ska återkomma med förslag som dels innebär en mer omfattande skyldighet att lagra uppgifter med koppling till nationell säkerhet, dels innebär en mer omfattande lagringsskyldighet generellt.[2] Vidare har riksdagen i ett tillkännagivande den 31 mars 2022 understrukit vikten av att denna utrednings arbete bedrivs skyndsamt och att regeringen så snart som möjligt därefter återkommer till riksdagen med ett förslag i enlighet med det tidigare tillkännagivandet.[3]

Enligt våra direktiv ska vi analysera hur dagens regler om lagring och tillgång till uppgifter om elektronisk kommunikation förhåller sig till ny praxis, överväga och ta ställning till vilka möjligheter som finns till förändringar av reglerna om lagring och tillgång till uppgifter

[1] Se prop. 2018/19:86 s. 38 och 108.
[2] Se bet. 2018/19: JuU27 punkt 6, rskr. 2018/19:296.
[3] Se bet. 2021/22:JuU24 punkt 5, rskr. 2021/22:216.

om elektronisk kommunikation i syfte att tillgodose de brottsbekämpande myndigheternas möjligheter att upprätthålla och stärka sin förmåga, samtidigt som skyddet för de mänskliga rättigheterna säkerställs, och lämna förslag på de författningsändringar och andra åtgärder som bedöms nödvändiga.

6.2 Bakgrunden till nuvarande reglering

Den nu gällande lagringsskyldigheten regleras i 9 kap. 19 och 22 §§ nya LEK och i 9 kap. 7 och 8 §§ nya FEK. Bestämmelserna motsvarar fullt ut vad som tidigare reglerades i 6 kap. 16 a och 16 d §§ gamla LEK och 39 och 40 §§ gamla FEK. Eftersom de ändringar som trädde i kraft den 1 oktober 2019 var föranledda av den s.k. Tele2-domen finns det anledning att här sammanfatta den domen och de överväganden som regeringen gjorde med anledning av den.

6.2.1 Tele2-domen

I Tele2-domen den 21 december 2016 (förenade målen C-203/15 och C-698/15) besvarade EU-domstolen bl.a. en begäran om förhandsavgörande från Kammarrätten i Stockholm avseende tolkningen av artikel 15.1 i e-dataskyddsdirektivet jämförd med artiklarna 7, 8 och 52.1 i rättighetsstadgan. EU-domstolen uttalade att direktivet omfattade både lagstiftning som reglerar lagringen av uppgifter och lagstiftning som reglerar tillgången till dessa uppgifter (p. 75 och 76 i domen). Artikel 15.1 i direktivet, som i viss utsträckning tillåter datalagring, ska enligt domstolen tolkas strikt och mot bakgrund av rättighetsstadgan (p. 91 i domen). Att proportionalitetsprincipen ska iakttas framgår av domstolens fasta praxis, enligt vilken skyddet av den grundläggande rätten till respekt för privatlivet på unionsnivå kräver att undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt (p. 96 i domen). De svenska reglerna om datalagring bedömdes utgöra inskränkningar i rättigheterna enligt stadgans artiklar 7 (rätten till respekt för privatlivet), 8 (skyddet för personuppgifter) och 11 (yttrandefriheten). Inskränkningar i rättigheterna får enligt EU-domstolen endast göras under vissa förutsättningar, däribland att de är proportionella och strängt nödvändiga. EU-domstolen uttalade vidare att en generell och

odifferentierad lagring aldrig kan vara strängt nödvändig, inte ens för att bekämpa grov brottslighet. EU-domstolen konkluderade att den svenska lagstiftningen överskred gränserna för vad som är strängt nödvändigt och att den inte kan anses motiverad i ett demokratiskt samhälle, såsom krävs enligt artikel 15.1 i e-dataskyddsdirektivet jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan (p. 107 i domen).

När det gäller tillgång till uppgifterna fastslog EU-domstolen att precisa krav måste föreskrivas, att tillgång endast får ges för att bekämpa grov brottslighet och att tillgången i princip bara får avse personer som på något sätt är inblandade i grov brottslighet. I särskilda fall, som när vitala intressen för nationell säkerhet, försvar eller allmän säkerhet hotas av terrorism, skulle dock tillgång kunna ges även till uppgifter om andra personer när det finns objektiva omständigheter som ger skäl att anta att de uppgifterna i ett konkret fall effektivt skulle kunna bidra till att bekämpa terrorism (p. 115–119 i domen). Tillgång ska enligt EU-domstolen som huvudregel ges först efter förhandskontroll av domstol eller annan oberoende myndighet och berörda ska informeras, så snart det inte längre skadar myndighetens utredningar (p. 120 och 121 i domen). Därutöver uttalade domstolen att leverantörerna av elektroniska kommunikationstjänster måste garantera en särskilt hög skydds- och säkerhetsnivå genom lämpliga tekniska och organisatoriska åtgärder, att uppgifterna måste förstöras när lagringstiden gått ut och att lagringen måste ske inom unionen (p. 122 i domen).

EU-domstolens slutsatser i Tele2-domen var att EU-rätten utgör hinder för (1) en nationell lagstiftning som i brottsbekämpande syfte föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel och för (2) en nationell lagstiftning som inte begränsar tillgången till trafik- och lokaliseringsuppgifter till enbart åtgärder som syftar till att bekämpa grov brottslighet, inte föreskriver att tillgången ska vara underkastad förhandskontroll av en domstol eller en oberoende myndighet och inte kräver att uppgifterna ska lagras inom unionen.

EU-domstolens uttalanden om riktad lagring

Domstolen anförde att det inte finns något hinder mot att en medlemsstat antar lagstiftning som i förebyggande syfte tillåter en riktad lagring av trafikuppgifter och lokaliseringsuppgifter, i syfte att bekämpa grov brottslighet. Förutsättningen för detta är att lagringen av uppgifterna, vad gäller vilka slags uppgifter som ska lagras, vilka kommunikationsmedel som avses, vilka personer som berörs och hur länge lagringen ska ske, begränsas till vad som är strängt nödvändigt (p. 108 i domen). För att en riktad lagring ska vara förenlig med EU-rätten måste den nationella lagstiftningen, enligt EU-domstolen, föreskriva tydliga och precisa bestämmelser som reglerar omfattningen och tillämpligheten av en sådan lagringsåtgärd och som slår fast minimikrav. De personer vars uppgifter har lagrats ska ha tillräckliga garantier som möjliggör ett effektivt skydd av deras personuppgifter mot riskerna för missbruk. Lagstiftningen måste särskilt precisera under vilka omständigheter och villkor en sådan lagringsåtgärd får vidtas i förebyggande syfte, vilket säkerställer att lagringen begränsas till vad som är strängt nödvändigt (p. 109 i domen). Domstolen påpekade att även om villkoren kan variera utifrån vilka åtgärder som vidtas för att förebygga, undersöka, avslöja och väcka åtal för grov brottslighet, måste lagringen av uppgifterna alltid uppfylla objektiva kriterier, som fastställer ett samband mellan de uppgifter som ska lagras och det eftersträvade syftet. I synnerhet måste villkoren vara sådana att de klart avgränsar omfattning och följaktligen den berörda personkretsen (p. 110 i domen). Vad gäller avgränsningen av den personkrets och de situationer som kan komma att beröras av riktad lagring gjorde EU-domstolen följande bedömning. Den nationella lagstiftningen ska grunda sig på objektiva omständigheter som gör det möjligt att ta sikte på en personkrets vars uppgifter kan avslöja en, åtminstone indirekt, koppling till grov brottslighet och på ett eller annat sätt kan bidra till att bekämpa grov brottslighet eller förhindra en allvarlig risk för den allmänna säkerheten. En sådan avgränsning kan säkerställas genom en bedömning att det i ett eller flera geografiska områden finns en förhöjd risk för förberedelse eller genomförande av sådana handlingar (p. 111 i domen).

6.2.2 Tolkningen av Tele2-domen i Sverige

Regeringens uttalanden om riktad lagring

I förarbetena till de ändringar i datalagringsregleringen som gjordes efter Tele2-domen uttalade regeringen bl.a. följande.[4]

Mot bakgrund av EU-domstolens slutsatser i Tele2-domen behöver svensk rätt anpassas för att vara förenlig med EU-rätten. Att upphäva de bestämmelser som föreskriver att operatörerna ska lagra uppgifter om elektronisk kommunikation är uteslutet av både brottsbekämpande och folkrättsliga skäl. Uppgifter om elektronisk kommunikation och andra elektroniska spår är i dag helt nödvändiga för brottsbekämpningen. Om de brottsbekämpande myndigheterna inte skulle ha tillgång till adekvata utredningsverktyg i den elektroniska miljön, skulle brotten i vissa fall vara omöjliga att klara upp och brottsoffer i motsvarande omfattning vara rättslösa. Vissa brott skulle i praktiken kunna bli straffria. Utöver detta måste hänsyn tas till Sveriges internationella åtaganden enligt t.ex. Europakonventionen. Staten har en skyldighet att skydda enskildas privatliv och personliga integritet mot intrång som begås av andra enskilda och, om intrång görs, se till att brotten utreds. En förutsättning för att staten ska kunna leva upp till kraven på att upprätthålla rättstryggheten för enskilda är att staten har en välfungerande och effektiv brottsbekämpning vilket t.ex. innebär att myndigheterna ska ha tillgång till effektiva utredningsverktyg – även i den elektroniska miljön.

När det gäller nyttan och behovet av en riktad lagring är det komplicerat att i förväg ringa in vissa personer eller vissa områden som lagringen skulle riktas in mot, eftersom det inte på förhand går att veta av vem, var eller när ett brott kommer att begås. Europadomstolen har i ett mål om bl.a. avlyssning av mängddata (eng. bulk interception) i underrättelseverksamhet uttalat att det vore fel att automatiskt förutsätta att avlyssning av mängddata skulle innebära ett större intrång i privatlivet än en riktad avlyssning mot misstänkta personer, eftersom den senare till sin natur mer sannolikt skulle resultera i inhämtning och undersökning av stora mängder data gällande den ifrågavarande personens kommunikationer.[5]

[4] Se prop. 2018/19:86 s. 26–36.
[5] Se Big Brother Watch m.fl. mot Förenade Kungariket, 13 september 2018, mål nr 58170/13, 62322/14 och 24960/15, punkterna 316–317. Målet har därefter prövats i stor sammansättning i en dom den 25 maj 2021.

När det gäller en riktad lagring som begränsar sig till vissa geografiska områden skulle det innebära att förutsättningarna för att lösa allvarlig brottslighet blir olika för olika delar av landet, vilket skulle vara mycket problematiskt. Att införa ett regelverk som får till följd att allvarliga brott skulle bli väsentligt svårare, och i vissa fall kanske omöjliga, att klara upp beroende på var själva brottet begicks eller planerades är enligt regeringens mening oacceptabelt. Det skulle också kunna innebära att viss brottslighet anpassar sig till detta och förläggs på en plats där lagring inte sker, i syfte att förhindra eller försvåra upptäckt. En geografisk avgränsning är också problematisk vid sådan brottslighet som inte kan sägas vara kopplad till geografiska förhållanden över huvud taget, t.ex. internetrelaterad brottslighet. I vissa fall kan brottsrisken öka i ett visst område vid speciella händelser, varför en riktad lagring kring den platsen skulle vara tänkbar. Värdet av en sådan lagring skulle dock inte vara särskilt stort eftersom planering och kontakter mellan gärningsmän med största säkerhet inte äger rum enbart på själva brottsplatsen och inte sällan under en längre tid. En lagring som bara riktar sig mot personer som använder vissa specifika tekniker, t.ex. vissa mjukvaror för anonymisering, skulle bara fånga in en försvinnande liten del av de uppgifter som är nödvändiga för brottsbekämpningen. Dessutom skulle integritetsintrånget för den enskilde öka eftersom man skulle behöva ta del av vilken mjukvara som personen använder för kommunikationen.

Regeringen kunde mot bakgrund av det anförda inte se någon större praktisk nytta eller något större behov av riktad lagring. Dessutom menade regeringen att det inte är säkert att en riktad lagring skulle innebära integritetsvinster. Att rikta lagringen mot en viss person eller krets av personer (exempelvis i ett visst område), utan att det finns någon konkret misstanke mot dessa personer, innebär rimligen en än större rättighetskränkning mot dessa människor och skulle riskera att vara diskriminerande mot vissa grupper. Det är svårt att se hur en sådan urvalsprocess i praktiken ska kunna ske på objektiva grunder. Tvärtom torde risken för diskriminering eller i övrigt stötande effekter vara stor.

Dessutom är riktad lagring förknippad med problem, eftersom ett stort antal operatörer skulle behöva underrättas om lagringsbeslutet. Det skulle bli en praktiskt utmanande uppgift, samtidigt som uppgiften om att ett visst område eller vissa personer är av intresse för

den brottsbekämpande verksamheten skulle spridas till en alltför stor krets. Sammantaget ansåg regeringen att en riktad lagring till en viss personkrets, ett visst geografiskt område eller till personer som använder vissa specifika tekniker varken är en ändamålsenlig, proportionerlig eller lämplig lösning. Regeringen ansåg inte heller att lagring i form av bevarandeföreläggande, kryptering eller lagring av senaste abonnemangsaktivitet skulle vara en framkomlig väg i detta sammanhang. Den enda rimliga kvarvarande modellen var enligt regeringen en lagringsskyldighet som inte omfattar alla kommunikationssätt, som är mindre omfattande än i dag och som är anpassad efter vad som är strängt nödvändigt för att bekämpa grov brottslighet.

Ändringarna i lagringsskyldigheten

Den lagstiftning som infördes 2019 innebär att vissa typer av uppgifter inte längre omfattas av lagringsskyldigheten och att lagringstiden har differentierats. När det gäller telefonitjänster och meddelandehantering gäller lagringsskyldigheten i dag enbart kommunikation via mobil nätanslutningspunkt. Tidigare omfattades uppgifter från såväl fast telefoni som fast ip-telefoni av lagringsskyldigheten. Lagringsskyldigheten omfattade tidigare också flera slags uppgifter vid kommunikation via mobil nätanslutningspunkt än vad som i dag är fallet. När det gäller internetåtkomst omfattades tidigare uppgifter om den typ av kapacitet för överföring som hade använts. Dessa uppgifter omfattas inte av dagens lagringsskyldighet (se jämförelsetabell i bilaga 3 för en översiktlig beskrivning av lagringsskyldigheten).

Vidare infördes en differentierad lagringstid beroende på vilken typ av uppgift det är fråga om. Uppgifter som gäller telefonitjänst och meddelandehantering via mobil nätanslutningspunkt ska lagras i sex månader medan lokaliseringsuppgifter ska lagras endast i två månader. Uppgifter om internetåtkomst ska lagas i tio månader, men om uppgifterna identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilde abonnenten, ska de dock lagras endast i sex månader.

6.3 EU-domstolens praxis efter Tele2-domen

EU-domstolen har, efter Tele2-domen, meddelat ett antal domar som rör lagring och åtkomst till uppgifter om elektronisk kommunikation. De mest relevanta domarna redovisas nedan i kronologisk ordning.

6.3.1 Ministerio Fiscal-domen

Den 2 oktober 2018 meddelade EU-domstolen den s.k. Ministerio Fiscal-domen (mål C-207/16) angående en begäran om förhandsavgörande från Provinsdomstolen i Tarragona i Spanien.

EU-domstolen prövade huruvida artikel 15.1 i e-dataskyddsdirektivet jämförd med artiklarna 7 och 8 i stadgan, ska tolkas på så sätt att myndigheters tillgång till identitetsuppgifter för innehavare av sim-kort som aktiverats med en stulen mobiltelefon, såsom för- och efternamn och eventuellt adress, utgör ett ingrepp i dessa personers grundläggande rättigheter enligt stadgan. Vidare prövades frågan om de eventuella ingreppen var av en sådan betydelse att denna tillgång i samband med förebyggande, utredning, upptäckt och lagföring av brott bör begränsas till kampen mot allvarlig brottslighet.

Domstolen konstaterade inledningsvis att den nationella lagstiftningsåtgärden omfattas av tillämpningsområdet för e-dataskyddsdirektivet. Artikel 15.1 i direktivet förutsätter nämligen med nödvändighet att de där avsedda nationella åtgärderna omfattas av direktivets tillämpningsområde, eftersom direktivet uttryckligen tillåter medlemsstaterna att vidta sådana åtgärder endast under förutsättning att de däri angivna villkoren är uppfyllda. De lagstiftningsåtgärder som avses i artikel 15.1 i direktiv 2002/58 reglerar dessutom – för de syften som anges i bestämmelsen – verksamheten för leverantörer av elektroniska kommunikationstjänster (p. 34 i domen). Lagstiftning som ålägger leverantörer av elektronisk kommunikation att lagra personuppgifter eller ge de behöriga nationella myndigheterna tillgång till dessa uppgifter medför med nödvändighet behandling av personuppgifter från leverantörernas sida (p. 37 i domen). Identitetsuppgifter för innehavare av sim-kort ingår bland trafikuppgifter såsom de definieras i artikel 2 andra stycket b e-dataskyddsdirektivet och uppgifterna omfattas följaktligen av tillämpningsområdet för direktivet (p. 42 i domen).

Domstolen konstaterade vidare att begäran i det aktuella fallet syftade enbart till att identifiera innehavarna av de sim-kort som aktiverats med den stulna mobiltelefonens IMEI-kod. Begäran avsåg enbart tillgång till de telefonnummer som svarar mot sim-korten samt identitetsuppgifter för innehavarna av dessa kort. Dessa uppgifter rör inte den kommunikation som ägt rum med den stulna mobiltelefonen eller telefonens geografiska position. Dessa uppgifter gör det inte möjligt att dra några mer precisa slutsatser om privatlivet för de personer vars uppgifter berörs. Tillgång till endast de uppgifter som avses med begäran kan inte anses som ett ”allvarligt” ingrepp i de grundläggande rättigheterna för de personer som uppgifterna avser. Det ingrepp som tillgång till sådana uppgifter innebär kan således vara motiverat av syftet att förebygga, utreda, upptäcka och lagföra brott i allmänhet, såsom nämns i artikel 15.1 första meningen i direktiv 2002/58, utan att dessa brott behöver kvalificeras som ”allvarliga” (p. 59–62 i domen).

6.3.2 La Quadrature du Net-domen

I den s.k. La Quadrature du Net-domen den 6 oktober 2020 (de förenade målen C-511/18, C-512/18 och C-520/18) besvarade EU-domstolen en begäran om förhandsavgöranden från Högsta förvaltningsdomstolen i Frankrike och Författningsdomstolen i Belgien. Målen rörde tolkningen dels av artikel 15.1 i e-dataskyddsdirektivet, dels av artiklarna 12–15 i Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (e-handelsdirektivet), jämförda med artiklarna 4, 6–8, 11 och 52.1 i stadgan och artikel 4.2 FEU.

I domen konstaterade domstolen att e-dataskyddsdirektivet är tillämpligt också när det gäller lagring av eller tillgång till uppgifter i elektroniska kommunikationer som syftar till att skydda den nationella säkerheten (p. 104 i domen). Domstolen uttalade bl.a. att en annan tolkning av direktivet skulle innebära att artikel 15.1 i direktivet helt fråntogs sin ändamålsenliga verkan (p. 97 i domen) och att enligt domstolens fasta praxis kan den omständigheten att en åtgärd har vidtagits för att skydda nationell säkerhet inte kan befria medlemsstaterna från skyldigheterna att iaktta unionsrätten (p. 99).

Domstolen uttalade att betydelsen av målet att skydda nationell säkerhet är mer långtgående än betydelsen av de övriga mål som anges i artikel 15.1. Under förutsättning att övriga krav i artikel 51.2 i stadgan iakttas, kan målet att skydda nationell säkerhet motivera åtgärder som innebär mer långtgående ingrepp i de grundläggande rättigheterna än dem som dessa övriga mål skulle kunna motivera (p. 136 i domen). Under sådana förutsättningar utgör EU-rätten i princip inte hinder för en lagstiftning som ger behöriga myndigheter rätt att ålägga tjänsteleverantörer en generell och odifferentierad lagringsskyldighet avseende trafik- och lokaliseringsuppgifter under en begränsad tid. Detta gäller under förutsättning att det föreligger tillräckligt konkreta omständigheter för att anse att den berörda medlemsstaten står inför ett allvarligt hot mot nationell säkerhet som visat sig vara verkligt, aktuellt eller förutsägbart (p. 137 i domen). En sådan lagring kan tillåtas under förutsättning att beslutet kan bli föremål för en effektiv kontroll av en domstol eller av en oberoende myndighet och att den sker under en period som är tidsmässigt begränsad till vad som är strängt nödvändigt, men som kan förlängas om hotet består (p. 138 och 139 i domen).

När det gäller datalagring för bekämpning av grov brottslighet och för att förebygga allvarliga hot mot den allmänna säkerheten stod domstolen fast vid sina uttalanden i Tele2-domen om att en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter om samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel inte är förenlig med EU-rätten (p. 141 i domen). Inte ens medlemsstaternas positiva skyldigheter att införa bestämmelser som möjliggör en effektiv bekämpning av brott kan motivera så allvarliga ingrepp i de grundläggande rättigheterna som en lagstiftning om lagring av praktiskt taget hela befolkningens trafik- och lokaliseringsuppgifter innebär, utan att det finns ett, åtminstone indirekt, samband mellan de berörda personerna och det eftersträvade målet (p. 145 i domen). Däremot kan målen att t.ex. bekämpa grov brottslighet motivera det synnerligen allvarliga ingrepp som en riktad lagring av trafik- och lokaliseringsuppgifter innebär (p. 146 i domen). Domstolen stod vidare fast vid sina tidigare uttalanden om att medlemsstaterna är oförhindrade att föreskriva om en tidsbegränsad riktad lagring vilken, på grundval av objektiva och icke-diskriminerande faktorer, är avgränsad genom de kategorier av personer som berörs eller genom ett geografiskt kriterium.

Samtidigt uttalade domstolen att en generell och odifferentierad lagring av uppgifter om den fysiska identiteten (eng. civil identity) för användare av elektroniska kommunikationsmedel är tillåten utan någon specifik tidsbegränsning, i syfte att förebygga, undersöka, avslöja och åtala för brott i allmänhet samt att skydda allmän säkerhet (p. 159 i domen).

Beträffande ip-adresser anförde domstolen att dessa genereras utan anknytning till en viss kommunikation och huvudsakligen har till syfte att, via leverantörer av elektroniska kommunikationstjänster, identifiera den fysiska personen som äger den terminalutrustning från vilken en kommunikation sker via internet. Ip-adresser har enligt domstolen en lägre grad av känslighet än andra trafikuppgifter (p. 152 i domen). I fråga om brott som begås på internet kan ip-adressen utgöra det enda som gör det möjligt att identifiera den person, till vilken denna adress var tilldelad vid den tidpunkt då brottet begicks. Det kan dessutom bli omöjligt att upptäcka brott som har begåtts på internet utan en lagstiftning enligt artikel 15.1 i e-dataskyddsdirektivet (p. 154 i domen). Domstolen konstaterade att EU-rätten i princip inte utgör ett hinder mot lagstiftning som föreskriver en generell och odifferentierad lagring av ip-adresser som har tilldelats källan för en internetanslutning, om det sker i syfte att skydda den nationella säkerheten, bekämpa grov brottslighet och för att förebygga allvarliga hot mot den allmänna säkerheten, och om lagringen är tidsmässigt begränsad till vad som är strängt nödvändigt (p. 155 och 156 i domen).

Domstolen uttalade sig också om möjligheterna att genom beslut från en behörig myndighet, vilket kan vara föremål för en effektiv domstolsprövning, ålägga tjänsteleverantörer att skyndsamt säkra de trafik- och lokaliseringsuppgifter som de har tillgång till (p. 161–163 i domen). Domstolen noterade att det i Europarådets konvention om it-relaterad brottlighet (Budapestkonventionen) föreskrivs att varje part, för utrednings- och lagföringsändamål, ska vidta vissa åtgärder beträffande redan sparade uppgifter, såsom skyndsamt säkrande av dessa uppgifter. Domstolen uttalade bl.a. att medlemsstaterna i sin lagstiftning måste precisera det ändamål för vilket det får företas ett skyndsamt säkrande av uppgifter och att det endast är bekämpning av grov brottslighet och, i ännu högre grad, skyddet av nationell säkerhet som kan motivera detta ingrepp i de grundläggande rättigheterna. Åtgärderna ska vidare begränsas till uppgifter som kan bidra

till att klarlägga det aktuella grova brottet eller den aktuella handlingen till men för nationell säkerhet. Även lagringstiden för uppgifterna måste begränsas till vad som är strängt nödvändigt (p. 164 i domen). Säkrandet av uppgifter behöver inte vara begränsat till uppgifter om personer som misstänks ha begått ett brott utan kan även t.ex. avse uppgifter om offret, offrets sociala bekantskapskrets eller om geografiska områden.

6.3.3 Privacy International-domen

I den s.k. Privacy International-domen den 6 oktober 2020 (mål C 623/17) besvarade EU-domstolen en begäran om förhandsavgörande från Domstolen för utredningsbefogenheter i Förenade kungariket. Målet rörde lagenligheten av en lagstiftning som tillåter att säkerhets- och underrättelsetjänsterna inhämtar och använder s.k. mängddata (bulk communications data). Domstolen konstaterade, med liknande resonemang som i La Quadrature du Net-domen, att artiklarna 1.3, 3 och 15.1 i e-dataskyddsdirektivet, jämförda med artikel 4.2 FEU, ska tolkas på så sätt att direktivets tillämpningsområde omfattar en nationell lagstiftning som ger en statlig myndighet rätt att ålägga leverantörer av elektroniska kommunikationstjänster att överföra trafikuppgifter och lokaliseringsuppgifter till säkerhets- och underrättelsetjänsterna i syfte att skydda nationell säkerhet (p. 49 i domen). Med hänvisning till den nyss nämnda domen uttalade domstolen att under förutsättning att övriga krav i artikel 52.1 i rättighetsstadgan iakttas, kan målet att skydda nationell säkerhet motivera åtgärder som innebär mer långtgående ingrepp i de grundläggande rättigheterna än dem som dessa övriga mål skulle kunna motivera. För att uppfylla kravet på proportionalitet måste en nationell lagstiftning som innebär ett ingrepp i de grundläggande rättigheterna uppfylla de krav som följer av domstolens praxis.

Beträffande en myndighets åtkomst till personuppgifter fann domstolen att en lagstiftning inte kan vara begränsad till att kräva att myndigheternas åtkomst till uppgifterna svarar mot det ändamål som eftersträvas med lagstiftningen, utan den måste även fastställa de materiella och formella villkor som gäller för sådan användning (p. 76 och 77 i domen). En heltäckande tillgång till samtliga lagrade uppgifter, oberoende av om det finns någon koppling, ens indirekt, till det efter-

strävade syftet, kan inte anses vara begränsad till vad som är strängt nödvändigt. En nationell lagstiftning som reglerar tillgång till trafik- och lokaliseringsuppgifter måste vara grundad på objektiva kriterier som avgör under vilka omständigheter och på vilka villkor behöriga nationella myndigheter ska ges tillgång till de aktuella uppgifterna (p. 78 i domen). Domstolen menade att kraven i ännu högre grad gäller för en lagstiftningsåtgärd, som den som var aktuell i det nationella målet, enligt vilken den behöriga nationella myndigheten får ålägga leverantörer av elektroniska kommunikationstjänster att genom generell och odifferentierad överföring lämna ut trafik- och lokaliseringsuppgifter till säkerhets- och underrättelsetjänsterna. Sådan överföring är således även tillämplig på personer beträffande vilka det inte finns något indicium som ger anledning att tro att deras beteende skulle kunna ha ett samband, inte ens indirekt eller avlägset, med målet att skydda den nationella säkerheten och, i synnerhet, utan att det har visats att det finns ett samband mellan de uppgifter som ska överföras och ett hot mot den nationella säkerheten. Med hänsyn till att överföring av trafik- och lokaliseringsuppgifter till statliga myndigheter motsvarar åtkomst till uppgifterna, fann domstolen att en lagstiftning som tillåter en generell och odifferentierad överföring av uppgifter till statliga myndigheter innebär en allmän åtkomst till uppgifterna. En nationell lagstiftning som ålägger leverantörer av elektroniska kommunikationstjänster att genom generell och odifferentierad överföring lämna ut trafik- och lokaliseringsuppgifter till säkerhets- och underrättelsetjänsterna går utöver vad som är strängt nödvändigt och kan inte anses vara motiverad i ett demokratiskt samhälle, såsom krävs enligt artikel 15.1 i e-dataskyddsdirektivet, jämförd med artikel 4.2 FEU samt artiklarna 7, 8, 11 och 52.1 i stadgan (p. 79–81 i domen).

6.3.4 Prokuratuur-domen

Den 2 mars 2021 meddelande EU-domstolen dom i mål C-746/18, (den s.k. Prokuratuur-domen) angående en begäran om förhandsavgörande från Högsta domstolen i Estland. Begäran framställdes i ett brottmål mot H.K. där hon åtalats för stölder, användning av tredje mans bankkort samt övergrepp i rättssak.

Domstolen erinrade om sin praxis när det gäller brottsbekämpande myndigheters tillgång till trafik- och lokaliseringsuppgifter som leverantörer av elektroniska kommunikationstjänster har lagrat.

Domstolen uttalade bl.a. att endast målen att bekämpa grov brottslighet eller förebygga allvarliga hot mot den allmänna säkerheten kan motivera att offentliga myndigheter får tillgång till ett stort antal trafik- eller lokaliseringsuppgifter, såvida det inte finns andra faktorer för att bedöma huruvida ansökan om tillgång är proportionerlig för målet att bekämpa brott i allmänhet. Sådana faktorer kan vara t.ex. under hur lång tid en myndighet får tillgång till de begärda uppgifterna. En offentlig myndighets tillgång till ett stort antal trafik- eller lokaliseringsuppgifter är dock, enligt domstolen, alltid av allvarlig art om de samlade uppgifterna gör det möjligt att dra specifika slutsatser om den berörda personens privatliv, såsom var fallet i det nationella målet (p. 35–39 i domen). Eftersom det tillstånd till tillgång, som beviljas av domstol eller av en oberoende behörig myndighet, meddelas innan det är möjligt att ta del av uppgifterna och den information som följer därav måste bedömningen av ingreppets allvarlighet göras utifrån den risk för den berörda personens privatliv som normalt sett är knuten till den kategori av uppgifter som begärs utlämnade.

Den hänskjutande domstolen frågade bl.a. om artikel 15.1 i e-dataskyddsdirektivet, jämförd med artiklarna 7, 8, 11 och 52.1 i rättighetsstadgan, ska tolkas så, att den utgör hinder mot nationell lagstiftning som ger en åklagarmyndighet, vars uppdrag är att leda förundersökningar och, i förekommande fall, väcka åtal i samband med ett senare förfarande, behörighet att ge offentliga myndigheter tillgång till trafik- och lokaliseringsuppgifter inom ramen för en brottsutredning. Domstolen besvarade denna fråga jakande och uttalade följande. En allmän tillgång till samtliga lagrade uppgifter, oberoende av om det finns någon koppling till det eftersträvade ändamålet, kan inte anses vara begränsad till vad som är strängt nödvändigt. Den nationella lagstiftningen måste vara grundad på objektiva kriterier som avgör under vilka omständigheter och på vilka villkor behöriga nationella myndigheter ska ges tillgång till de aktuella uppgifterna. För att säkerställa att dessa villkor uppfylls i praktiken, är det väsentligt att tillgången till de lagrade uppgifterna är underkastad förhandskontroll av en domstol eller en oberoende myndighet som meddelar sina beslut efter motiverade framställningar från myndigheterna. En sådan

förhandskontroll innebär bl.a. att den domstol eller det organ som ska utföra kontrollen har alla befogenheter och lämnar alla nödvändiga garantier för att kunna göra en vederbörlig avvägning mellan de olika intressen och rättigheter som är i fråga.

Vad särskilt gäller en brottsutredning kräver en sådan kontroll att denna domstol eller detta organ kan säkerställa en korrekt balans mellan de intressen som gör sig gällande för att svara mot utredningens behov, å ena sidan, och de grundläggande rättigheterna avseende respekt för privatlivet och skydd av personuppgifter, å den andra sidan. När denna kontroll inte utförs av en domstol utan av en oberoende förvaltningsmyndighet måste denna myndighet ha en ställning som innebär att den kan fullgöra sitt uppdrag på ett objektivt och opartiskt sätt, och den måste därför vara fri från all yttre påverkan (p. 50–53 i domen). På det straffrättsliga området innebär kravet på oberoende att den myndighet som ska utföra förhandskontrollen dels inte får vara involverad i den aktuella brottsutredningen, dels ska ha en neutral ställning i förhållande till parterna i det straffrättsliga förfarandet. Så är inte fallet med en åklagarmyndighet som leder utredningsförfarandet och, i förekommande fall, väcker åtal för det allmännas räkning. Åklagarmyndigheten har nämligen inte till uppgift att helt oavhängigt avgöra en tvist utan att, i förekommande fall, hänskjuta tvisten till behörig domstol, i egenskap av part i målet. Den omständigheten att en åklagarmyndighet är skyldig att kontrollera både sådana omständigheter som är till den misstänktes nackdel och sådana som är till dennes fördel, säkerställa att utredningen är lagenlig och endast agera i enlighet med lagen och sin egen övertygelse, är inte tillräcklig för att denna myndighet ska anses vara fristående i förhållande till de intressen som är i fråga (p. 54–56 i domen).

Domstolen erinrade också om att den oberoende kontrollen ska ske innan tillgång till uppgifterna beviljas, förutom i vederbörligen motiverade fall då denna kontroll ska ske utan dröjsmål. En sådan senare kontroll kan nämligen inte uppnå det mål som eftersträvas med en förhandskontroll, det vill säga att förhindra att det beviljas tillgång till de aktuella uppgifterna utöver vad som är strängt nödvändigt.

6.3.5 Garda Síochána-domen

Den 5 april 2022 meddelande EU-domstolen dom i mål C-140/20, (den s.k. Garda Síochána-domen) angående en begäran om förhandsavgörande från Högsta domstolen i Irland. Begäran framställdes i ett mål mellan å ena sidan G.D. och å andra sidan Commissioner of An Garda Síochána (Irlands rikspolischef) angående giltigheten av Communications (Retention of Data) Act 2011.

Domstolen hänvisade i stora delar till den praxis som finns när det gäller lagring av och tillgång till trafik- och lokaliseringsuppgifter. Domstolen erinrade således om att artikel 15.1 i e-dataskyddsdirektivet, jämförd med artiklarna 7, 8 och 11 samt 52.1 i stadgan, inte utgör hinder för en lagstiftningsåtgärd som, för att skydda nationell säkerhet, tillåter att leverantörer av elektroniska kommunikationstjänster åläggs att på ett generellt och odifferentierat sätt lagra trafik- och lokaliseringsuppgifter i situationer där den berörda medlemsstaten står inför ett allvarligt hot mot nationell säkerhet beträffande vilket det är visat att hotet är verkligt och aktuellt eller förutsebart. Beslut om sådant åläggande måste vara tidsmässigt begränsat till vad som är strängt nödvändigt, men som kan förlängas om hotet fortfarande kvarstår och måste kunna bli föremål för effektiv kontroll antingen av en domstol eller av en oberoende myndighet (p. 58 i domen). Domstolen förtydligade, efter ett påstående från Europeiska kommissionen, att särskilt allvarlig brottslighet inte kan likställas med ett hot mot den nationella säkerheten och att det alltså inte finns någon mellanliggande kategori mellan nationell säkerhet och allmän säkerhet (p. 62 och 63 i domen).

Domstolen erinrade också om att artikel 15.1 i e-dataskyddsdirektivet, jämförd med artiklarna 7, 8 och 11 samt 52.1 i stadgan, däremot inte utgör hinder för lagstiftningsåtgärder som, i syfte att bekämpa grov brottslighet och förhindra allvarliga hot mot allmän säkerhet, föreskriver

- en riktad lagring av trafik- och lokaliseringsuppgifter vilken, på grundval av objektiva och icke-diskriminerande faktorer, är avgränsad genom de kategorier av personer som berörs eller genom ett geografiskt kriterium, för en period som är tidsmässigt begränsad till vad som är strängt nödvändigt men som kan förlängas,

- en generell och odifferentierad lagring av ip-adresser som har tilldelats källan för en internetanslutning, för en period som är tidsmässigt begränsad till vad som är strängt nödvändigt,
- en generell och odifferentierad lagring av uppgifter om den fysiska identiteten för användare av elektroniska kommunikationsmedel, och
- som tillåter att leverantörer av elektroniska kommunikationstjänster genom ett beslut från behörig myndighet, vilket är föremål för effektiv domstolskontroll, åläggs att, under en begränsad tidsperiod, skyndsamt säkra (quick freeze) de trafik- och lokaliseringsuppgifter som dessa tjänsteleverantörer har tillgång till,

förutsatt att denna lagstiftning, genom klara och precisa regler, säkerställer att lagringen av uppgifterna i fråga iakttar tillämpliga materiella och formella villkor, och att de berörda personerna förfogar över effektiva garantier mot riskerna för missbruk (p. 67 i domen).

Domstolen bemötte den hänskjutande domstolens uppfattning att endast en allmän lagring av trafik- och lokaliseringsuppgifter gör det möjligt att, på ett effektivt sätt, bekämpa grov brottslighet och erinrade bl.a. om att e-dataskyddsdirektivet inte utgör hinder för en generell lagring av identitetsuppgifter om personer i syfte att bekämpa brottslighet i allmänhet. Domstolen uttalade också bl.a. att det inte finns något hinder för en nationell lagstiftning som syftar till att bekämpa grov brottslighet, enligt vilken förvärv av elektroniska kommunikationsmedel, såsom ett förbetalt sim-kort, förutsätter kontroll av officiella handlingar som visar köparens identitet och att säljaren registrerar den information som följer därav, varvid säljaren i förekommande fall är skyldig att ge behöriga nationella myndigheter tillgång till dessa uppgifter (p. 72 i domen).

Domstolen påtalade vidare när det gäller riktad lagring att medlemsstaterna bl.a. kan vidta lagringsåtgärder avseende personer som är föremål för utredning eller andra aktuella övervakningsåtgärder eller som förekommer i det nationella kriminalregistret på grund av en tidigare fällande dom för allvarliga brott som kan vara en indikation på att det föreligger en hög återfallsrisk (p. 78 i domen). En riktad lagringsåtgärd kan även grundas på ett geografiskt kriterium, såsom bland annat den genomsnittliga graden av brottslighet i ett geografiskt område, utan att det nödvändigtvis finns några konkreta in-

dikationer på att allvarliga brott ska förberedas eller begås i de berörda områdena. En riktad lagring som grundar sig på ett geografiskt kriterium är i princip inte av sådan art att den kan ge upphov till diskriminering, eftersom kriteriet avseende den genomsnittliga graden av allvarlig brottslighet i sig inte har något samband med potentiellt diskriminerande omständigheter (p. 80 i domen).

Domstolen uttalade att det inte kan uteslutas att andra objektiva och icke-diskriminerande kriterier än ett personligt eller geografiskt kriterium kan beaktas för att genomföra en riktad lagring av trafik- och lokaliseringsuppgifter. Det ankommer på medlemsstaterna och inte på EU-domstolen att identifiera sådana kriterier. Eventuella svårigheter att exakt fastställa i vilka situationer och under vilka villkor en riktad lagring kan utföras kan i vilket fall som helst inte motivera att medlemsstaterna gör ett undantag till huvudregel genom att föreskriva en generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter (p. 83 och 84 i domen).

Vad gäller skyndsam lagring av trafik- och lokaliseringsuppgifter kan endast bekämpningen av grov brottslighet, och i ännu högre grad, skyddet av den nationella säkerheten, motivera detta allvarliga ingrepp (p. 87 i domen). En sådan lagringsåtgärd kan utsträckas till uppgifter om andra personer än dem som t.ex. misstänks ha begått ett grovt brott, bl.a. personer som ett offer har haft kontakt med genom sina elektroniska kommunikationsmedel, innan en handling som utgör ett allvarligt hot mot den allmänna säkerheten eller ett allvarligt brott har begåtts. Ett skyndsamt säkrande kan också utsträckas till att avse geografiska områden (p. 88–90 i domen). Ett skyndsamt säkrande av uppgifter kan förordnas redan i första skedet av en utredning av ett allvarligt hot mot den allmänna säkerheten eller av ett eventuellt grovt brott (p. 91 i domen).

Inte ens de positiva skyldigheter för medlemsstaterna som avser införande av bestämmelser som möjliggör en effektiv bekämpning av brott, kan medföra att det anses motiverat med en lagstiftning om lagring av praktiskt taget hela befolkningens trafik- och lokaliseringsuppgifter, utan att det finns ett, åtminstone indirekt, samband mellan de berörda personerna och det eftersträvade målet (p. 95 i domen).

Domstolen klargjorde, efter ett påstående från den danska regeringen, att de nationella brottsbekämpande myndigheterna inom ramen för straffrättsliga förfaranden, inte kan få tillgång till trafik- och lokaliseringsuppgifter som har lagrats i syfte att skydda den nationella

säkerheten mot ett verkligt och aktuellt eller förutsebart hot. Annars skulle förbudet mot en generell och odifferentierad lagring av uppgifter i syfte att bekämpa allvarlig brottslighet förlora sin ändamålsenliga verkan (p. 100 i domen).

6.3.6 SpaceNet-domen

Den 20 september 2022 meddelade EU-domstolen dom i de förenade målen C-793/19 och C-794/19 (SpaceNet-domen) angående en begäran om förhandsavgörande från Federala högsta förvaltningsdomstolen i Tyskland.

SpaceNet AG och Telekom Deutschland GmbH är tillhandahållare av bl.a. allmänt tillgängliga internetanslutningstjänster i Tyskland. Bolagen väckte var för sig talan och bestred skyldigheten i tysk lagstiftning att lagra uppgifter om sina kunders telekommunikationstrafik fr.o.m. den 1 juli 2017.

Förvaltningsdomstolen i Köln biföll de båda bolagens talan. Domarna överklagades till den Federala högsta förvaltningsdomstolen i Tyskland, som beslutade att hänskjuta frågan till EU-domstolen.

Lagringsskyldighetens omfattning i Tyskland

Tyskland har anpassat sin lagstiftning om datalagring till EU-domstolens tidigare praxis och har en reglering som påminner om den svenska. Lagringstiderna är 10 veckor för trafikuppgifter och 4 veckor för lokaliseringsuppgifter. Den tyska lagringsskyldigheten föreskriver följande:

1. i samband med tillhandahållandet av *allmänt tillgängliga telefonitjänster*, inklusive kommunikation via sms, multimediameddelande eller liknande meddelande samt samtal som inte besvaras eller når fram ska följande uppgifter lagras:

   a) telefonnumret eller något annat identifikationsnummer för det uppringande abonnemanget, det uppringda abonnemanget samt för om- och vidarekopplingar,

b) datum och klockslag då kommunikationen inleddes och avslutades eller – om det rör sig om kommunikation via sms, multimediameddelande eller liknande meddelande – tidpunkter för sändande och mottagande av meddelandet, med uppgift om tidszon,

c) uppgifter om vilken tjänst som använts, i de fall då det är möjligt att använda olika tjänster inom ramen för telefonitjänsten,

d) om det rör sig om mobiltelefonitjänster dessutom

e) det internationella identifikationsnumret för mobilabonnenter till det uppringande och det uppringda abonnemanget,

f) det internationella identifikationsnumret för den uppringande och den uppringda terminalutrustningen,

g) datum och klockslag för tjänstens första aktivering, med uppgift om tidszon, när tjänsten har betalats på förhand,

h) beteckningar på de celler som användes via det uppringande och det uppringda abonnemanget i början av kommunikationen,

i) om det rör sig om internettelefonitjänster dessutom ip-adresserna till det uppringande och det uppringda abonnemanget samt tilldelade identifieringsnummer, och

j) i samband med tillhandahållandet av *allmänt tillgängliga internetanslutningstjänster* ska följande uppgifter lagras:

k) den ip-adress som tilldelats abonnenten för internetanvändning,

l) en tydlig identifiering av den förbindelse som möjliggör internetanslutning, samt det tilldelade identifieringsnumret,

m) datum och klockslag då internetanvändningen på den tilldelade ip-adressen inleddes och avslutades, med uppgift om tidszon,

n) vid mobilanvändning, beteckningen på de celler som användes i början av internetanslutningen.

Lagringsskyldigheten omfattar inte kommunikationens innehåll, uppgifter om besökta webbplatser, uppgifter om e-posttjänster eller uppgifter som avser kommunikation till eller från vissa abonnemang som tillhör personer, myndigheter och organisationer inom den sociala eller kyrkliga sfären.

Tolkningsfrågan

Ska artikel 15 i e-dataskyddsdirektivet, jämförd med dels artiklarna 7, 8 och 11 och artikel 52.1 i stadgan, dels artikel 6 i stadgan och artikel 4 i fördraget om Europeiska unionen, tolkas så, att den utgör hinder för en nationell lagstiftning som ålägger operatörer av allmänt tillgängliga elektroniska kommunikationstjänster att lagra trafik- och lokaliseringsuppgifter avseende slutanvändare av nämnda tjänster, när denna skyldighet inte villkoras av särskilda skäl i fråga om geografiska, tidsmässiga eller territoriella aspekter och med det innehåll som den tyska regleringen har (p. 39 i domen).

Domstolens bedömning

Domstolen hänvisade i stora delar till den praxis som finns när det gäller lagring av och tillgång till trafik- och lokaliseringsuppgifter. Domstolen erinrade om att lagring av trafik- och lokaliseringsuppgifter i sig utgör ett ingrepp i de grundläggande rättigheterna till respekt för privatlivet och skydd av personuppgifter, oberoende av om de uppgifter som avser privatlivet är av känslig art eller ej eller om de berörda har fått utstå eventuella olägenheter på grund av ingreppet samt oberoende av om de lagrade uppgifterna senare kommer eller inte kommer att användas (p. 60 i domen). Trafik- och lokaliseringsuppgifter kan avslöja information om ett stort antal aspekter av de berörda personernas privatliv som gör det möjligt att upprätta en profil för de berörda personerna, och denna information är lika känslig ur integritetssynpunkt som själva innehållet i kommunikationerna (p. 61 i domen). Vad gäller den effektiva bekämpningen av brott ska det beaktas att det av artikel 7 i stadgan kan följa positiva skyldigheter för statsmakten att vidta rättsliga åtgärder för att skydda bl.a. privatlivet och familjelivet. Det är därför, enligt domstolen, nödvändigt att göra en avvägning mellan de olika legitima intressen och rättigheter som är i fråga och att inrätta en rättslig ram som möjliggör denna avvägning (p. 65 i domen).

Domstolen uttalade att även om den tyska lagstiftningen undantar innehållet i kommunikationerna och uppgifter om de webbplatser som besökts från lagringsskyldigheten och endast föreskriver lagring av den cellidentifikationskod som använts i början av kommunikationen, så är lagringsskyldigheten i princip densamma som

gällde de nationella bestämmelser som var i fråga i de mål som avgjordes La Quadrature du Net-domen (p. 78 i domen).

Domstolen konstaterade att även om den tyska lagstiftning inte omfattar information om vilka webbplatser som besökts, föreskriver den icke desto mindre att ip-adresserna ska lagras. Eftersom ip-adresser kan användas för att bl.a. på ett uttömmande sätt kartlägga en internetanvändares hela klickström, och därmed dennes onlineaktivitet, är det emellertid möjligt att med användning av dessa uppgifter upprätta en detaljerad profil för internetanvändaren. Den lagring och analys av dessa ip-adresser som krävs för en sådan kartläggning utgör således allvarliga ingrepp i internetanvändarens grundläggande rättigheter enligt artiklarna 7 och 8 i stadgan (p. 79 i domen).

Domstolen konstaterade vidare att endast 1 300 enheter fanns upptagna i den förteckning över personer, myndigheter eller organisationer av social eller kyrklig karaktär vilkas uppgifter om elektronisk kommunikation inte lagras samt att det är uppenbart att detta motsvarar en begränsad andel av de användare i Tyskland vilkas uppgifter omfattas av den tyska lagringsskyldigheten. Sålunda lagras uppgifter om användare som omfattas av tystnadsplikt, såsom advokater, läkare och journalister (p. 82 i domen).

Domstolen uttalade vidare att den tyska lagringsskyldigheten berör nästan alla personer som ingår i befolkningen, även om dessa inte, ens indirekt, befinner sig i en situation som kan leda till straffrättsliga påföljder. Lagringsskyldigheten innebär att merparten av alla trafik- och lokaliseringsuppgifter ska lagras, generellt och utan differentiering i fråga om person, tidpunkt eller geografisk plats, utan krav på skäl. En sådan lagringsskyldighet kan inte anses utgöra en riktad lagring av uppgifterna, i motsats till vad den tyska regeringen har hävdat (p. 83 och 84 i domen).

Domstolen angav att lagringstiden för uppgifterna förvisso är en bland andra relevanta faktorer för att avgöra om unionsrätten utgör hinder mot en generell och odifferentierad lagring samt att den tyska lagstiftningen föreskriver en betydligt kortare lagringstid än de nationella lagstiftningar som prövats i Tele2-domen, La Quadrature du Net-domen och An Garda Síochána-domen (p. 85 och 86 i domen). Enligt domstolen är en lagring av trafik- eller lokaliseringsuppgifter dock alltid av allvarlig art, oberoende av lagringstidens längd och mängden eller arten av de uppgifter som lagras, för det fall att dessa samlade uppgifter gör det möjligt att dra mycket specifika slutsatser om

den eller de berörda personernas privatliv (p. 88 i domen). Enligt den tyska lagstiftningen kan den mängd trafik- och lokaliseringsuppgifter som lagrats under tio respektive fyra veckor göra det möjligt att dra mycket precisa slutsatser om privatlivet för de personer vilkas uppgifter lagrats, såsom deras vanor i vardagslivet, deras stadigvarande och tillfälliga uppehållsorter, deras dagliga förflyttningar och förflyttningar i övrigt, de aktiviteter de utövar, deras sociala relationer och de umgängeskretsar de rör sig i, och i synnerhet göra det möjligt att upprätta en profil för dessa personer (p. 90 i domen).

Den hänskjutande domstolen framhöll att det, på grund av den bristande överensstämmelsen mellan punkterna 155 och 168 i La Quadrature du Net-domen, råder osäkerhet om vad som är förenligt med unionsrätten när det gäller lagring av ip-adresser. Oklarheten består enligt den hänskjutande domstolen i huruvida det för sådan lagring krävs att skälet för lagringen ska vara kopplat till målet att skydda den nationella säkerheten, bekämpa allvarlig brottslighet eller att förhindra allvarliga hot mot den allmänna säkerheten, eller om sådan lagring är tillåten även utan konkret skäl och att kraven avseende nämnda mål endast begränsar användningen av de lagrade uppgifterna. EU-domstolen menade dock att några sådana motsättningar inte finns i La Quadrature du Net-domen eftersom det av denna klart framgår att det endast är bekämpning av grov brottslighet och förebyggande av allvarliga hot mot allmän säkerhet som, i likhet med skyddet av den nationella säkerheten, kan motivera en generell lagring av ip-adresser som tilldelats källan till en internetanslutning, oberoende av om de berörda personerna har en, åtminstone indirekt, koppling till de eftersträvade målen.

EU-domstolen påpekade också att domarna från Europadomstolen av den 25 maj 2021, Big Brother Watch m.fl. mot Förenade kungariket och Centrum för Rättvisa mot Sverige, som vissa regeringar vid förhandlingen åberopade till stöd för att Europakonventionen inte utgör hinder för nationella bestämmelser som i huvudsak föreskriver en generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter, inte påverkar den tolkning av artikel 15.1 i e-dataskyddsdirektivet som följer av resonemanget i den nu aktuella domen. I dessa domar var det nämligen fråga om massavläsning av uppgifter avseende internationell kommunikation. Europadomstolen uttalade sig i nämnda domar således inte om huruvida det var förenligt med Europakonventionen att generellt och odifferentierat lagra trafik-

och lokaliseringsuppgifter på det nationella territoriet eller att göra en omfattande avläsning av dessa uppgifter i syfte att förebygga, upptäcka och utreda allvarliga brott. Under alla omständigheter syftar artikel 52.3 i stadgan till att säkerställa att rättigheterna i stadgan och motsvarande rättigheter enligt Europakonventionen stämmer överens med varandra, enligt vad som är påkallat, utan att undergräva unionsrättens och EU-domstolens autonomi. Detta innebär, enligt EU-domstolen, att det endast är i egenskap av en lägsta skyddsnivå som de motsvarande rättigheterna i Europakonventionen ska beaktas vid tolkningen av stadgan.

Domslut

Domstolen beslutade följande:

Artikel 15.1 i e-dataskyddsdirektivet, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan, ska tolkas på så sätt

att den utgör hinder för nationella lagstiftningsåtgärder som i förebyggande syfte, för att bekämpa grov brottslighet och förhindra allvarliga hot mot allmän säkerhet, föreskriver att det ska ske en generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter,

att den inte utgör hinder för lagstiftning

– som, för att skydda nationell säkerhet, tillåter att leverantörer av elektroniska kommunikationstjänster åläggs att på ett generellt och odifferentierat sätt lagra trafik- och lokaliseringsuppgifter i situationer där den berörda medlemsstaten står inför ett allvarligt hot mot nationell säkerhet som har visat sig vara verkligt och aktuellt eller förutsebart, varvid beslutet om åläggande av nämnda lagringsskyldighet måste kunna bli föremål för effektiv kontroll antingen av en domstol eller av en oberoende myndighet, vars avgörande har bindande verkan, i syfte att kontrollera om någon av dessa situationer föreligger och att de villkor och garantier som måste ställas upp är uppfyllda, och varvid åläggandet endast får meddelas för en period som måste vara tidsmässigt begränsad till vad som är strängt nödvändigt, men som kan förlängas om hotet fortfarande kvarstår,

– som, för att skydda nationell säkerhet, bekämpa grov brottslighet och förhindra allvarliga hot mot allmän säkerhet, föreskriver en riktad lagring av trafik- och lokaliseringsuppgifter vilken, på grundval av objektiva och icke-diskriminerande faktorer, är avgränsad genom de kategorier av personer som berörs eller genom ett geografiskt kriterium, för en period som är tidsmässigt begränsad till vad som är strängt nödvändigt men som kan förlängas,
– som, för att skydda nationell säkerhet, bekämpa grov brottslighet och förhindra allvarliga hot mot allmän säkerhet, föreskriver en generell och odifferentierad lagring av ip-adresser som har tilldelats källan till en internetanslutning, för en period som är tidsmässigt begränsad till vad som är strängt nödvändigt,
– som, för att skydda nationell säkerhet, bekämpa brottslighet och skydda allmän säkerhet, föreskriver en generell och odifferentierad lagring av uppgifter om identiteten beträffande användare av elektroniska kommunikationsmedel, och
– som, för att bekämpa grov brottslighet eller, i ännu högre grad, skydda nationell säkerhet, tillåter att leverantörer av elektroniska kommunikationstjänster genom ett beslut från behörig myndighet, vilket ska kunna bli föremål för en effektiv domstolskontroll, åläggs att, under en begränsad tidsperiod, skyndsamt säkra de trafik- och lokaliseringsuppgifter som dessa tjänsteleverantörer har tillgång till,

förutsatt att denna lagstiftning, genom klara och precisa regler, säkerställer att lagringen av uppgifterna i fråga iakttar tillämpliga materiella och formella villkor, och att de berörda personerna förfogar över effektiva garantier mot riskerna för missbruk.

6.4 Europadomstolens praxis

Europadomstolen har i maj 2021 meddelat två domar som gäller avlyssning av mängddata (eng. bulk interception) i underrättelseverksamhet. Domarna redovisas i korthet nedan.

6.4.1 Domen (2021-05-25) i målet Big Brother Watch m.fl. mot Storbritannien

I Storbritannien regleras avlyssning av mängddata i underrättelseverksamhet i RIPA-regleringen från år 2020. I det aktuella målet lämnade sökandena in ett klagomål mot bl.a. omfattningen och utbredningen av de övervakningsprogram som drivs av den brittiska regeringen enligt tidigare gällande RIPA och att informationen delades med andra stater. Domstolen övervägde om detta system och bestämmelserna i RIPA var förenliga med Europakonventionen. De tre huvudsakliga frågorna som domstolen behandlade var a) inhämtning av mängddata, b) inhämtning av uppgifter från leverantörer av kommunikationstjänster och c) delning av underrättelseinformation med utländska stater.

Domstolen, i stor sammansättning (eng. Grand Chamber), ansåg att inhämtning av mängddata i stor utsträckning kan motiveras av medlemsstaterna utifrån att de måste kunna skydda sig mot potentiella hot mot den nationella säkerheten. Om en stat implementerar en strategi för inhämtning av mängddata, så måste den dock se till att systemet innehåller fullständiga skyddsåtgärder (eng. end-to-end safeguards) mot den potentiella risken för missbruk. Domstolen bedömde att skyddsåtgärderna var otillräckliga och den brittiska regleringen ansågs därför utgöra en kränkning av artikel 8 i Europakonventionen.

Bristerna kan sammanfattas som frånvaro av fristående organ för beviljande av åtgärderna, avsaknad av kategorier av sökord i tillståndet och avsaknad av sökord kopplade till enskilda personer i tillståndet. Bristerna gällde inte bara inhämtning av innehållsuppgifter utan även metadata. Bristerna kunde inte vägas upp av att det fanns en oberoende och effektiv tillsyn och ett robust rättsmedel.

Domstolen fann vidare att ingrepp i skyddet av journalistiska källor inte kan vara förenligt med artikel 10 i konventionen om det inte är motiverat av ett övergripande krav i allmänhetens intresse. Och när det är motiverat med sådant ingrepp så måste lämpliga förfaranden och skyddsåtgärder införas. Sådana skyddsåtgärder bör inkludera kravet på att söka tillstånd från en domstol eller annat oberoende organ när en begäran innehåller specifika söktermer kopplade till en journalist eller till journalistiskt material. Domstolen an-

såg att det saknades lämpliga skyddsåtgärder och att det således hade skett ett åsidosättande av yttrandefriheten enligt artikel 10.

I målet behandlades också bl.a. frågan om inhämtning av uppgifter från leverantörer av kommunikationstjänster och huruvida tillgång till sådana uppgifter utgjorde ett brott mot artiklarna 8 och 10 i Europakonventionen. Domstolen ansåg att tillgången till sådan information bör begränsas till att bekämpa ”allvarlig brottslighet” och betonade behovet av att vidta lämpliga skyddsåtgärder vid åtkomst och behandling av sådana uppgifter. Domstolen fann att det hade skett ett intrång i rätten till privatliv enligt artikel 8 och rätten till yttrandefrihet enligt artikel 10.

6.4.2 Domen (2021-05-25) i målet Centrum för Rättvisa mot Sverige

Den huvudsakliga frågan i målet var om den svenska lagstiftningen om signalspaning i försvarsunderrättelseverksamhet strider mot rätten till skydd för privatliv enligt artikel 8 och rätten till ett effektivt rättsmedel enligt artikel 13 i Europakonventionen.

Europadomstolen i stor sammansättning fann att den svenska lagstiftningen om signalspaning i försvarsunderrättelseverksamhet i vissa delar var i strid med artikel 8 i Europakonventionen. Europadomstolen uttalade att signalspaning i syfte att värna den nationella säkerheten inte i sig står i strid med artikel 8 i Europakonvention. Däremot begränsas staternas bedömningsmarginal då det vid användandet av signalspaning ställs krav på nationella rättssäkerhetsgarantier till skydd för den personliga integriteten.

Europadomstolen framhöll att lagstiftningen innehåller tydliga regler avseende vilka syften som kan rättfärdiga signalspaning och hur förfarandet går till. Däremot identifierade domstolen följande tre brister i det svenska systemet: avsaknad av en tydlig reglering om när inhämtat material som inte innehåller personuppgifter ska förstöras, avsaknad av tydliga riktlinjer i signalspaningslagstiftningen eller annan relevant lagstiftning som anger att den personliga integriteten ska beaktas när beslut fattats om att dela insamlat material med andra stater samt avsaknad av en effektiv efterhandskontroll som ska utföras på begäran av en enskild. Europadomstolen fann därför att Sverige agerat utanför sin bedömningsmarginal och att det således skett en kränkning av artikel 8.

6.5 Internationell utblick

Såvitt vi har kunnat utröna har endast ett fåtal stater inom EU infört regler om generell och odifferentierad lagring i syfte att skydda den nationella säkerheten och om riktad lagring i syfte att bekämpa grov brottslighet. Nedan redovisas vad som gäller i Danmark, Frankrike och Belgien.

6.5.1 Danmark

I Danmark ändrades reglerna om datalagring som en följd av La Quadrature du Net-domen. Med de nya reglerna gäller en tvådelad ordning för datalagring, en riktad lagring samt en generell och odifferentierad lagring. Lagändringarna trädde i kraft den 30 mars 2022.

För det första infördes en ordning med personbestämd och geografiskt riktad lagring för att bekämpa grov brottslighet. Med grov brottslighet avses bl.a. lagöverträdelser som kan straffas med fängelse i tre år eller mer och vissa andra uppräknade brott.

För det andra infördes en ordning med generell och odifferentierad lagring i syfte att skydda den nationella säkerheten.

Riktad lagring

Polismyndigheten (Rigspolitiet) får förelägga tillhandahållare av elektroniska kommunikationsnät- och tjänster (nedan tillhandahållare) att företa riktad lagring beträffande personer och geografiska platser (målrettet registrering og opbevaring).

Den *riktade personbestämda lagringen* kan gälla personer som dömts för grova brott. Skyldigheten att lagra uppgifter om personen ska gälla i tre, fem eller tio år beroende på strafflatituden på det begångna brottet. Lagringstiden räknas i regel från frigivning. Efter en bedömning kan dock lagring ske redan under avtjänande av straff. Uppgifterna ska lagras i ett år från kommunikationen/insamlingen. Dessutom kan lagringen avse personer som varit föremål för hemlig övervakning eller avlyssning av elektronisk kommunikation (teleoplysning og telefonaflytning). Lagringsskyldigheten ska gälla i ett år från det att tvångsmedelsanvändningen avslutats och uppgifterna

ska lagras i ett år från kommunikationen/insamlingen (786 b § retsplejeloven).

Den *geografiskt riktade lagringen* får avse uppgifter från de delar av tillhandahållarens nät som är nödvändigt för att täcka områden på 3 gånger 3 kilometer. Sådan lagring får ske antingen om antalet anmälningar om grova brott begångna i området uppgår till minst 1,5 gånger genomsnittet för landet under de senaste tre åren eller om antalet medborgare dömda för grova brott i området uppgår till minst 1,5 gånger genomsnittet för landet under de senaste tre åren. Uppgifter om vilka områden som omfattas av sådan lagring ska inte vara offentliga.

Polismyndigheten får därutöver få förelägga tillhandahållare en geografiskt riktad lagring som avser särskilt säkerhetskänsliga platser, t.ex. kungahusets residens, statsministerbostaden, ambassader, polisens fastigheter, kriminalvårdsanstalter, trafikknytpunkter, militära områden och offentligt godkända flygplatser. Uppgifterna ska lagras i ett år från kommunikationen/insamlingen (786 c § retsplejeloven).

Slutligen får riktad lagring användas beträffande kommunikationsutrustningar, personer eller bestämda områden om det finns anledning att anta att det finns en anknytning till grov brottslighet (*riktad lagring på konkreta grunder*). Ett sådant föreläggande om riktad lagring kräver domstolsbeslut. Vid geografiskt riktad lagring är storleken på området beroende av hur konkret anknytningen till grov brottslighet är. Är det fråga om en förestående gängkonflikt eller ett terrorbrott kan det vara fråga om mycket stora områden, såsom en landsdel. Domstolen ska ta ställning till under vilken tid lagringsskyldigheten ska gälla. Den tiden ska vara så kort som möjligt och högt sex månader åt gången. Uppgifterna ska lagras i ett år från kommunikationen/insamlingen (786 d § retsplejeloven). Uppgifter om vilka personer, enheter eller områden som omfattas av sådan lagring ska inte vara offentliga.

Generell och odifferentierad lagring

I de fall det föreligger tillräckligt konkreta omständigheter som ger anledning att anta att Danmark står inför ett allvarligt hot mot den nationella säkerheten som kan antas vara reellt, aktuellt eller förutsebart får en generell och odifferentierad lagring ske. Justitieministern

har bemyndigats att, efter förhandling med handels- och industriministern (erhvervsministern), besluta om sådan lagring (genom bekendtgørelse). Beslutet ska grundas på en helhetsbedömning, där bl.a. Center for Terroranalyses årliga ”Vurderingen af Terrortruslen mod Danmark” ska beaktas. Lagringsskyldigheten ska fastställas för en period om ett år åt gången. Uppgifterna ska lagras i ett år från kommunikationen/insamlingen (786 e § retsplejeloven).

Ip-adresser och nummerupplysningsuppgifter m.m.

Lagring ska ske av ip-adresser, portnummer och tidpunkt för tilldelningen. Uppgifterna ska lämnas ut inte enbart i syfte att bekämpa grov brottslighet. Lagringen ska ske i ett år från inhämtningen. Justitieministern får, efter samråd med klimat-, energi- och försörjningsministern, besluta regler om lagring och verifiering av nummerupplysningsuppgifter. Nummerupplysningsdatabasen ska innehålla uppgifter om unikt ID och eventuella uppgifter om användaren, i syfte att stödja polisens möjligheter att identifiera en användare av ett visst kommunikationsmedel (se 786 f, 786 g, 786 h §§ retsplejeloven).

6.5.2 Frankrike

Den 21 april 2021 fattade Högsta förvaltningsdomstolen i Frankrike (Conseil d’État), efter La Quadrature Du Net-domen, beslut om huruvida de franska reglerna om datalagring var i överensstämmelse med EU-rätten.

Domstolen beslutade att det befintliga hotet mot den nationella säkerheten för närvarande motiverar en generell lagring av metadata. Domstolen konstaterade vidare att möjligheten att få tillgång till sådana uppgifter för att bekämpa grov brottslighet för närvarande gör det möjligt att säkerställa de konstitutionella kraven för att förhindra brott mot lag och ordning och spårning av gärningsmän. Domstolen beordrade dock regeringen att regelbundet ompröva hotnivån i Frankrike och som kan motivera en generell lagring av uppgifter och att se till att underrättelsetjänsternas tillgång till dessa uppgifter prövas av en oberoende myndighet.

Enligt fransk lag ska teleoperatörer lagra uppgifter om sina användares metadata i syfte att bekämpa brottslighet och terrorism. Uppgifterna kan indelas i följande tre kategorier:

1. Identitetsuppgifter, som gör det möjligt att identifiera användaren av ett elektroniskt kommunikationssystem (t.ex. för- och efternamn kopplade till ett telefonnummer eller den ip-adress genom vilken en användare är ansluten till internet).
2. Trafikuppgifter, som spårar datum, tid och mottagare av elektronisk kommunikation, eller en förteckning över besökta webbplatser.
3. Platsdata som gör det möjligt att ”märka” en enhet med den basstation som den är ansluten till.

Vid sin kontroll av att genomförandet av EU-rätten inte äventyrar de franska konstitutionella kraven undersökte Högsta författningsdomstolen det franska regelverkets överensstämmelse med EU-rätten. Domstolen klargjorde inledningsvis omfattningen av sin undersökning. Å ena sidan vägrade domstolen att bedöma om EU:s myndigheter, särskilt EU-domstolen, hade överskridit sina befogenheter. Å andra sidan erinrade domstolen om att den franska konstitutionen fortfarande är den högsta normen inom det franska nationella rättssystemet. Följaktligen var domstolen tvungen att se till att tillämpningen av EU-rätten, såsom den har fastställts av EU-domstolen, i praktiken inte äventyrar franska konstitutionella krav som inte garanteras på ett likvärdigt sätt av EU-rätten.

Högsta författningsdomstolen konstaterade att de konstitutionella kraven på att skydda nationens grundläggande intressen, förhindra brott mot lag och ordning, bekämpa terrorism och söka efter brottsförövare inte åtnjuter ett skydd i EU-rätten som motsvarar det som garanteras i den franska konstitutionen. Högsta författningsdomstolen var därför tvungen att se till att de begränsningar som EU-domstolen har infört inte äventyrar dessa konstitutionella krav. Domstolen konstaterade att den generella lagringen av uppgifter, som för närvarande åläggs aktörerna enligt fransk lag, faktiskt är motiverad av ett hot mot den nationella säkerheten, i enlighet med EU-domstolens krav. EU-domstolen kräver att förekomsten av ett sådant hot prövas om med jämna mellanrum. Domstolen beslutade att den generella skyldigheten att lagra uppgifter för andra ändamål än den natio-

nella säkerheten, särskilt lagföring av brott, är olaglig (med undantag för mindre känsliga uppgifter, såsom civilstånd, ip-adress, konton och betalningar). Domstolen konstaterade att den av EU-domstolen föreslagna lösningen med en riktad lagring för ändamålet lagföring av brott varken är möjlig i praktiken eller operativt effektiv. Den metod för ”skyndsamt säkrande” som tillåts enligt EU-rätten kan dock grundas på de uppgifter som generellt lagras för nationella säkerhetsändamål och därmed användas för lagföring av brott. När det gäller EU-domstolens åtskillnad mellan grov brottslighet och vanlig brottslighet erinrade Högsta författningsdomstolen om att proportionalitetsprincipen medför att användningen av metadata är begränsad till lagföring av brott av tillräckligt allvarlig karaktär.

När det slutligen gäller tillgången till lagrade uppgifter i underrättelsesyfte konstaterade Högsta författningsdomstolen att det franska regelverket inte är tillräckligt eftersom yttranden från den nationella kommissionen för kontroll av underrättelseteknik (CNCTR), som måste yttra sig innan ett godkännande ges, inte är bindande. Den franska lagstiftningen bör därför ändras på denna punkt.

Högsta författningsdomstolen beordrade premiärministern att inom sex månader ändra regelverket för att uppfylla dessa krav.

6.5.3 Belgien

I Belgien har ny lagstiftning om datalagring införts. Reglerna gäller såväl riktad lagring för bekämpning av allvarlig brottslighet som generell och odifferentierad lagring i syfte att skydda den nationella säkerheten.

Enligt regleringen får riktad lagring ske baserat på två olika geografiska kriterier. Det första kriteriet är baserat på kriminalstatistik per rättsligt distrikt respektive poliszoner (det finns 12 sådana rättsliga distrikt i Belgien.) För att trafik- och lokaliseringsuppgifter ska få lagras i ett sådant distrikt måste i genomsnitt tre allvarliga brott ha begåtts per 1 000 invånare och år baserat på genomsnittet för de tre föregående kalenderåren. Om ett sådant antal allvarliga brott bara förekommer i en del av distriktet (i en poliszon) får uppgifter lagras inom den zonen. Lagringstiden varierar mellan sex månader och ett år beroende på ”brottslighetens nivå”, dvs. hur många allvarliga brott som begåtts inom distriktet eller zonen. Det finns inget hinder mot

att hela Belgiens territorium omfattas av en sådan lagringsskyldighet, om kriterierna i varje distrikt är uppfyllda. Den riktade lagringen i Belgien omfattar för närvarande hela landet.

Det andra geografiska kriteriet avser strategiska platser, såsom hamnar, flygplatser, tågstationer, polisstationer, fängelser, kraftverk, parlamentet och det kungliga slottet. Ett beslut om riktad lagring gäller i ett år.

En generell och odifferentierad lagringsskyldighet träder i kraft när hotnivån är på nivå 3 på en 4-gradig skala. Uppgifterna ska lagras så länge hotnivån är på lägst nivå 3.

Lagringsskyldigheten gäller även för s.k. OTT-leverantörer (om sådana leverantörer, se avsnitt 9).

Lagändringarna trädde i kraft den 18 augusti 2022. Lagringsskyldigheten avseende strategiska platser träder dock i kraft först den 1 januari 2027, om inte annat bestäms.

Det pågår för närvarande en rättsprocess om giltigheten av den belgiska datalagringsregleringen vid landets konstitutionsdomstol.

6.6 Överväganden och förslag

6.6.1 Lagring av uppgifter om abonnemang för att bekämpa brottslighet

Utredningens bedömning: Begreppet uppgift om abonnemang bör finnas kvar i författning och ha samma innebörd som i dag.

Utredningens förslag: Uppgifter om abonnemang som genereras och behandlas i tillhandahållarnas verksamhet som behövs för att identifiera en abonnent och registrerad användare ska lagras.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vilka uppgifter som ska lagras.

Lagringstiden ska pågå fram till ett år efter det att abonnemanget upphörde att gälla. I fråga om tillfälliga identifierare bör lagringstiden räknas från det att tilldelningen av identifieraren upphörde hos användaren.

Uppgifter som omfattas av lagringsskyldigheten ska få behandlas även för andra syften än brottsbekämpning.

Begreppet uppgift om abonnemang

Som framgår av avsnitt 4 finns det inte någon definition av begreppet uppgift om abonnemang varken i EU-rätten eller i svensk rätt. Regeringen har, som också nämnts i avsnitt 4, uttalat att uppgifter om abonnemang som utgångspunkt är uppgifter som identifierar abonnenten eller den registrerade användaren bakom ett visst nummer eller en viss adress, i motsats till uppgifter som redogör för hur numret eller adressen har använts.[6]

I Sverige anses begreppet uppgifter om abonnemang innefatta uppgifter om abonnentens nummer, namn, titel och adress samt uppgifter om exempelvis avtal och fakturering. Vidare anses fasta, dynamiska eller ip-adresser styrda genom NAT-teknik[7], IMSI-nummer och IMEI-nummer vara uppgifter om abonnemang när syftet med uppgiften är att identifiera ett abonnemang eller en abonnent.

EU-domstolen har, bl.a. i SpaceNet-domen, uttalat att EU-rätten inte utgör ett hinder mot lagstiftning som, för att skydda nationell säkerhet, bekämpa brottslighet och skydda allmän säkerhet, föreskriver en generell och odifferentierad lagring av uppgifter om identiteten beträffande användare av elektroniska kommunikationsmedel. EU-domstolen har dock en annan hållning när det gäller ip-adresser. Ip-adresser som tilldelats källan till en internetanslutning får endast lagras generellt och odifferentierat, för syftet att skydda nationell säkerhet, bekämpa grov brottslighet och förhindra allvarliga hot mot allmän säkerhet, för en tid som är tidsmässigt begränsad till vad som är strängt nödvändigt. Domstolen angav bl.a. följande. Eftersom ip-adresser kan användas för att bl.a. på ett uttömmande sätt kartlägga en internetanvändares hela klickström[8], och därmed dennes onlineaktivitet, är det emellertid möjligt att med användning av dessa uppgifter upprätta en detaljerad profil för internetanvändaren. Den lagring och analys av dessa ip-adresser som krävs för en sådan kartläggning utgör således allvarliga ingrepp i internetanvändarens grundläggande rättigheter enligt artiklarna 7 och 8 i stadgan.[9]

[6] Se prop. 2018/19:86 s. 93. Jfr med prop. 2011/12:55 s. 101–102.
[7] NAT (Network Address Translation) en adressöversättningsteknik som tillåter flera användare att dela på samma ip-adress. Se även PTSFS 2019:2 – Föreskrifter om vilka andra uppgifter som ska lagras för att identifiera abonnent och registrerad användare vid användning av NAT-teknik.
[8] Detta ord används i den svenska översättning av punkt 79 i SpaceNet-domen.
[9] Se SpaceNet-domen p. 79.

Med anledning av EU-domstolens uttalanden finns det skäl att överväga om vi i Sverige bör revidera vår uppfattning om vad som innefattas i begreppet abonnemangsuppgift och om ip-adresser kan innefattas i begreppet. Man kan vidare överväga om man i stället bör använda begreppet uppgift om fysisk identitet.

Ip-adresser kan förenklat beskrivas som en länk mellan å ena sidan en användares enhet (exempelvis en dator eller mobiltelefon) och å andra sidan den som vill kommunicera med enheten. Ip-adressen fyller två huvudsakliga funktioner. Den första funktionen är att identifiera en enhet inom ett nätverk, vilket är förutsättning för att kunna tillhandahålla tjänsten och ta betalt för den från den som äger enheten eller låter andra bruka den. Den andra funktionen är att återge enhetens placering inom ett nätverk för att enheten ska kunna kommunicera med andra enheter, vilket är en förutsättning för internettrafik.[10] En internetleverantör utgör i praktiken en länk mellan en användares privata nätverk och interna ip-adresser (ofta i form av en router som genererar ip-adresser för enheterna i ett hem) och internet. Extern kommunikation blir möjligt genom att användaren får en extern ip-adress av sin internetleverantör. I de flesta fall ändras ip-adressen från gång till annan när enheten kopplar upp sig mot internetleverantörens infrastruktur (dynamiska ip-adresser) och i andra fall, i regel mot extra avgift, kan enheten få en fast ip-adress.

En närmare analys av hur en ip-adress ska kategoriseras bör därför göras med utgångspunkt från att en ip-adress har olika funktioner. Det bör därför göras en skillnad mellan 1) frågan om *vem* som vid viss tidpunkt innehaft en ip-adress, dvs. uppgift om en person, och 2) situationer när en myndighet begär uppgifter om *kommunikation* kopplad till en viss ip-adress och därigenom bl.a. får kunskap om vilken ip-adress som vid en viss tidpunkt kommunicerat med en annan ip-adress.

Isolerat säger en ip-adress, exempelvis 193.11.1.15, inte mer än de uppgifter som kopplas samman med numret (se avsnitt 9.3 för en mer utförligare beskrivning av ip-adress). Det väsentliga är således vad som kopplas till ip-adressen. Om en ip-adress kompletteras med bl.a. information om datapaket, spårbar tid, sändande och mottagande ip-adress, portnummer[11], överföringsprotokoll m.m. kan det ge

[10] Internet Protocol, Darpa Internet Program, Protocol Specification, september 1981, uppdaterad februari 2013, https://www.rfc-editor.org/info/rfc791. Hämtat den 4 april 2023.
[11] Portnummer är ett nummer som tilldelas för att identifiera en slutpunkt för anslutning och för att styra data till en specifik tjänst.

information om kommunikationen, exempelvis att en enhet har varit i förbindelse med en annan enhet. Vem som vid en viss tidpunkt innehaft en ip-adress säger däremot inte något om kommunikationen. Enligt den nuvarande svenska lagringsskyldigheten ska användares ip-adress och andra uppgifter som är nödvändiga för att identifiera abonnent och registrerad användare lagras. Däremot ska uppgifter om kommunikation kopplade till en ip-adress inte lagras. Sådana uppgifter får alltså inte lagras av tjänsteleverantörerna för syftet att bekämpa brottslighet.

De tyska datalagringsbestämmelserna som var föremål för EU-domstolens prövning i SpaceNet-domen, innehöll ett uttryckligt förbud mot lagring av uppgifter som avslöjar trafik till och från webbplatser.

Mot denna bakgrund synes EU-domstolen mena att det med hjälp av *externa källor* går att kartlägga en internetanvändares hela klickström, dvs hos andra än tillhandahållarna eftersom dessa inte fick lagra uppgifter som avslöjar trafik till och från webbplatser. Uttalandet vore annars oförenlig med vad domstolen gav uttryck för i mål C-597/19 M.I.C.M (punkt 121). I denna dom uttalar domstolen att kännedom om en innehavare av en ip-adress normalt inte gör det möjligt att få kännedom om datum, tid, geografisk plats, varaktighet eller mottagare av den kommunikation som ägt rum. Domstolen klargjorde i M.I.C.M. även att ip-adresser inte ger någon information om kommunikationen och därmed inte heller om användarnas privatliv.

Vi anser att det är svårt att utläsa vad EU-domstolen syftar på i SpaceNet-domen när den gör gällande att en ip-adress, trots avsaknad av andra uppgifter om trafik, kan användas för att kartlägga en internetanvändares klickström.

Hur ip-adresser ska bedömas har aktualiserats i ett pågående mål vid EU-domstolen, mål C-470/21, begäran om förhandsavgörande den 30 juli 2021 från den Högsta förvaltningsdomstolen i Frankrike. Den svenska regeringen har i ett yttrande i detta mål anfört som sin inställning att en uppgift om innehavare av en ip-adress i första hand är att betrakta som en uppgift om fysisk identitet. Regeringen anförde också i yttrandet bl.a. följande.

Det är i domstolens praxis inte klarlagt huruvida uppgift om fysisk identitet utgör en egen kategori av uppgifter, skild från trafik- och lokaliseringsuppgifter, eller om den ingår som en underkategori i

begreppet trafikuppgift. Det kan ifrågasättas om uppgifter om fysisk identitet över huvud taget kan anses utgöra trafikuppgifter. Om uppgifter om innehavare av ip-adresser anses utgöra trafikuppgifter, får de anses ha en betydligt lägre känslighetsgrad än andra trafikuppgifter. Eftersom uppgifterna inte är särskilt integritetskänsliga, bör de inte heller vara underkastade krav på förhandskontroll av domstol eller annan oberoende myndighet och vara möjliga att tillgå också för bekämpande av brottslighet i allmänhet, inte enbart grov brottslighet.

Förhandling i mål C-470/21 är planerad den 15–16 maj 2023.

Vår slutsats är att en ip-adress måste kategoriseras utifrån vilka uppgifter som kopplas till ip-adressen, inte bara utifrån numret som sådant. Om frågan avser *vem* som har, eller hade, en ip-adress, utan koppling till trafik- och lokaliseringsuppgift bör numret kategoriseras som en uppgift om abonnemang. Uppgift om den fysiska innehavarens identitet avseende en viss ip-adress är således en uppgift om abonnemang.

Även andra uppgifter kan vara uppgifter om abonnemang, exempelvis uppgift om kopplingen mellan permanenta och tillfälliga identifierare i 5G-nätet. Som framgår av våra överväganden angående utformningen av anpassningsskyldigheten (se avsnitt 10.4.2) kommer möjligheten för de brottsbekämpande myndigheterna att kunna identifiera kommunikationsutrustningar försvinna när permanenta identifierare omvandlas till temporära identifierare i den luftburna delen av 5G-nätet. De permanenta identifierarna i 5G-nätet är motsvarigheten till IMSI-nummer i 4G-nätet. Endast teleoperatören kan koppla ihop de temporära identifierarna med de permanenta. Uppgift om kopplingen mellan dessa identifierare är alltså en uppgift om abonnemang när syftet med uppgiften är att identifiera abonnenten eller den registrerade användaren.

Av våra direktiv framgår att det kan finnas behov av att klarlägga hur vissa EU-rättsliga termer förhåller sig till nationella termer, exempelvis den närmare omfattningen av begreppet abonnemangsuppgifter i förhållande till s.k. NAT-teknik. Som vi redogjort för omfattas i dag NAT-styrda ip-adresser av begreppet abonnemangsuppgift. Vi har inte funnit att EU-rätten ger oss skäl att göra någon annan bedömning än vad som tidigare gjorts. Det väsentliga för bedömningen är inte valet av teknisk lösning. Det saknar för bedömningen betydelse hur en ip-adress tilldelas (fast, dynamiskt eller genom NAT-teknik). Det väsentliga för bedömningen om huruvida en uppgift är

en uppgift om abonnemang är i stället om det med ledning av uppgifterna går att identifiera användaren.

Med denna utgångspunkt ser vi inget behov av att revidera vare sig den svenska innebörden av uppgifter om abonnemang eller begreppet som sådant.

Lagringsskyldighet och lagringstid för abonnemangsuppgifter

Mot bakgrund av våra slutsatser i föregående avsnitt föreslår vi en reglering som anger att den lagringsskyldige ska lagra de uppgifter om abonnemang som genereras eller behandlas i deras verksamhet i syfte att skydda nationell säkerhet, bekämpa grov brottslighet och annan brottslighet samt skydda allmän säkerhet.

Vi menar att lagringstiden för dessa uppgifter rimligen bör sträcka sig till ett år efter det att abonnemanget upphörde att gälla. När det gäller uppgift om innehavare av en dynamisk ip-adress bör dock lagringstiden räknas från att den tilldelade ip-adressen upphör att vara knuten till den aktuella användaren. På samma sätt bör det förhålla sig med lagringstiden för uppgift om kopplingen mellan permanenta och tillfälliga identifierare i 5G-nätet. Det är i båda dessa fall fråga om tillfälliga identifieringsuppgifter.

Vi föreslår att denna lagringsskyldighet ska regleras i en ny paragraf, 9 kap. 19 a § nya LEK. Någon närmare reglering av lagringsskyldigheten bör dock inte finnas i lag. Sådana föreskrifter bör finnas på lägre normnivå. Paragrafen bör därför innehålla ett bemyndigande för regeringen, eller den myndighet som regeringen bestämmer, att få meddela föreskrifter om vilka uppgifter som ska lagras enligt paragrafen. I förordning bör det finnas dels bestämmelser om vilka abonnemangsuppgifter som ska lagras, dels en subdelegation för PTS att meddela ytterligare föreskrifter om vilka uppgifter som ska lagras. Det är lämpligt med en subdelegation till PTS att meddela ytterligare föreskrifter i ämnet. Behovet av ytterligare föreskrifter kan nämligen uppkomma inte minst med hänsyn till den snabba tekniska utvecklingen och ändringar i kommunikationsvanor. På sätt kan PTS bidra till att undanröja eventuella framtida oklarheter om lagringsskyldighetens omfattning.

Lagringstiden bör liksom i dag regleras i 9 kap. 22 § nya LEK.

Tjänsteleverantörernas behandling av abonnemangsuppgifter

Den lagringsskyldighet avseende uppgifter om abonnemang som vi föreslår ovan väcker frågan om det krävs någon särskild reglering avseende tjänsteleverantörernas behandling av dessa uppgifter.

Enligt 9 kap. 21 § nya LEK får uppgifter som har lagrats enligt 9 kap. 19 § nya LEK behandlas endast för att lämnas ut enligt

1. 9 kap. 33 § första stycket 2 och 5 nya LEK,
2. 27 kap. 19 § RB, eller
3. inhämtningslagen.

Utlämnande av abonnemangsuppgifter i brottsbekämpande syfte görs med stöd av 9 kap. 33 § första stycket 2 och 5 nya LEK. Frågan är om uppgifter som har lagrats med stöd av den av oss föreslagna 9 kap. 19 a § nya LEK ska få behandlas endast för att lämnas ut enligt 9 kap. 33 § första stycket 2 och 5. Vi anser att så inte bör vara fallet. Som framgår av övriga delar av 9 kap. 33 § första stycket nya LEK ska uppgifter om abonnemang, trots den tystnadsplikt som gäller för dessa uppgifter enligt 9 kap. 31 § nya LEK, lämnas ut till ett flertal olika myndigheter. Utlämnandet av uppgifter om abonnemang enligt dessa senare bestämmelser har ingenting att göra med lagringsskyldigheten i 9 kap 19 § nya LEK. Uppgifterna kan i dessa fall lämnas ut eftersom de lagras för tjänsteleverantörernas egna syften. Om det föreskrivs att uppgifter om abonnemang som lagras enligt 9 kap. 19 a § nya LEK får behandlas endast för att lämnas ut för brottsbekämpande syften skulle tjänsteleverantörerna behöva lagra sina abonnemangsuppgifter i olika uppgiftssamlingar, en för sina egna syften och en för brottsbekämpande syften. Vi anser att en sådan dubbel lagring av abonnemangsuppgifter är obefogad med hänsyn till att uppgifterna, i jämförelse med trafikuppgifter och lokaliseringsuppgifter, inte är lika integritetskänsliga.

6.6.2 Särskilt om begreppet trafikuppgift

Utredningens förslag: Begreppet *annan uppgift som angår ett särskilt elektroniskt meddelande* i nya LEK ska ersättas med begreppet *trafikuppgift*. Motsvarande ändring ska göras i offentlighets- och sekretesslagen.

Enligt våra direktiv kan det behöva klargöras hur vissa EU-rättsliga termer förhåller sig till nationella termer, exempelvis hur det EU-rättsliga begreppet *trafikuppgift* förhåller sig till begreppet *annan uppgift som angår ett särskilt elektroniskt meddelande*.

Innan förhållandet mellan ovanstående begrepp klargörs bör den närmare definitionen av ett *elektroniskt meddelande* klargöras. Begreppet elektronisk meddelande är hämtat från artikel 2 d i e-dataskyddsdirektivet. I e-dataskyddsdirektivet används begreppet *kommunikation*, men regeringen valde att använda begreppet elektroniskt meddelande av följande skäl.

> Direktivet om integritet och elektronisk kommunikation innehåller en rad definitioner i artikel 2. Av särskilt intresse är definitionen av kommunikation, som i direktivet lyder ”all information som utbyts eller överförs mellan ett begränsat antal parter genom en allmänt tillgänglig elektronisk kommunikationstjänst. Detta inbegriper inte information som överförs som del av en sändningstjänst för rundradio eller TV till allmänheten via ett elektroniskt kommunikationsnät, utom i den mån informationen kan sättas i samband med den enskilde abonnenten eller användaren av informationen”. I ingresspunkt 16 i direktivet förklaras att information som ingår i en sändningstjänst för rundradio eller TV som tillhandahålls via ett allmänt kommunikationsnät är avsedd för en potentiellt obegränsad publik och utgör inte en kommunikation enligt direktivet. I sådana fall där den enskilde abonnenten eller användaren som får sådan information kan identifieras, till exempel när det gäller beställ-TV-tjänster, omfattas emellertid den överförda informationen av vad som i direktivet avses med kommunikation.
>
> Begreppen användare och kommunikation är särpräglade för de bestämmelser som finns i direktivet om integritet och elektronisk kommunikation. Beträffande kommunikation finns risk för begreppsförvirring med hänsyn till termen elektronisk kommunikation. Det föreslås därför det som i direktivet benämns ”kommunikation” i den nya lagen kallas ”elektroniskt meddelande”.

I 1 kap. 7 § nya LEK har ett elektroniskt meddelande därför fått följande definition.

> elektroniskt meddelande: all information som utbyts eller överförs mellan ett begränsat antal parter genom en allmänt tillgänglig elektronisk kommunikationstjänst, utom information som överförs som del av sändningar av ljudradio- och tv-program som är riktade till allmänheten via ett elektroniskt kommunikationsnät om inte denna information kan sättas i samband med den enskilda abonnenten eller användaren av informationen.

Även begreppet *trafikuppgift* är hämtat från e-dataskyddsdirektivet. I artikel 2 i direktivet definieras trafikuppgifter som alla uppgifter som behandlas i syfte att överföra en kommunikation via ett elektroniskt kommunikationsnät eller för att fakturera den. I skäl 15 i e-dataskyddsdirektivet sägs följande:

> (15) En kommunikation kan innehålla alla slags uppgifter om namn, nummer eller adress från sändaren av en kommunikation eller användaren av en förbindelse för att genomföra kommunikationen. Trafikuppgifter kan innefatta varje omvandling av denna information via det nät genom vilket kommunikationen överförs i syfte att utföra överföringen. Trafikuppgifter kan bland annat utgöras av uppgifter om en kommunikations sändningsväg, varaktighet, tid eller volym, vilket protokoll som används, terminalutrustningens, sändarens eller mottagarens placering, det nät där kommunikationen börjar eller slutar samt en förbindelses början, slut eller varaktighet. De kan också bestå av det format i vilket kommunikationen överförs via nätet.

Definitionen finns i 1 kap. 7 § nya LEK. Enligt definitionen är en trafikuppgift en uppgift som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande. Den motsvarar alltså definitionen i direktivet trots användningen av begreppet elektronisk meddelande i lagen. Vid bedömningen av innebörden av begreppet trafikuppgift bör det därför även beaktas definitionen av elektroniskt meddelande i nya LEK.

Frågan är då om det finns någon skillnad mellan begreppet trafikuppgift och annan uppgift som angår ett särskilt elektroniskt meddelande.

Begreppet *annan uppgift som angår ett särskilt elektroniskt meddelande* finns i 9 kap. 31 § nya LEK. I bestämmelsen regleras en tystnadsplikt för den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst som

inte är en Noik har fått del av eller tillgång till vissa närmare angivna uppgifter. Tystnadsplikten gäller för

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

Denna tystnadsplikt infördes redan i telelagen (1993:597) i samband med bolagiseringen av Televerket. I den ursprungliga lydelsen var formuleringen *annan uppgift som angår ett telemeddelande*. Med det avsågs bl.a. uppgift om mellan vilka abonnemang som ett telefonsamtal har förmedlats.[12] I samband med anpassningar till gemenskapsrätten ersattes begreppet *telemeddelande* med begreppet *elektroniskt meddelande* i 6 kap. 20 § gamla LEK, men någon förändring i sak avsågs inte.[13] Regeringen uttalade i samma lagstiftningsärende att begreppet trafikuppgift i princip torde avse ha samma innebörd som uppgifter som angår ett särskilt telemeddelande.[14]

Med utgångspunkt från den breda definitionen av begreppet trafikuppgift, särskilt med beaktande av vad som framgår av skälen i e-dataskyddsdirektivet och vad vi har redovisat ovan, gör vi bedömningen att begreppet trafikuppgift har samma innebörd som begreppet annan uppgift som angår ett särskilt elektroniskt meddelande. Begreppet trafikuppgift innefattar även lokaliseringsuppgifter som är trafikuppgifter. Visserligen finns det nu fler typer av trafikuppgifter än vid telelagens tillkomst, men det beror på utvecklingen av den teknik som används för elektronisk kommunikation.

Det framstår som otillfredsställande att det i nya LEK finns två begrepp med samma innebörd. Begreppet trafikuppgift används exempelvis i 9 kap. 1 och 4 §§ nya LEK angående behandlingen av sådana uppgifter. I den nuvarande regleringen om vilka uppgifter som tjänsteleverantörerna ska lagra används emellertid begreppet annan uppgift som angår ett särskilt elektroniskt meddelande, genom hänvisning till 9 kap. 31 § första stycket 3 nya LEK.

Sammantaget kan förekomsten av de båda begreppen i nya LEK ge upphov till tolkningssvårigheter i fråga om omfattningen av tystnadsplikten och därmed om vad som omfattas av lagringsskyldigheten.

[12] Se prop. 1992/93:200 s. 162 f. och 310.
[13] Se prop. 2002/03:110 s. 269 och 397.
[14] Se prop. 2021/22:136 s. 411 och prop. 2002/03:110 s. 389 och 390.

Mot denna bakgrund föreslår vi att begreppet *trafikuppgift* ska ersätta begreppet *annan uppgift som angår ett särskilt elektroniskt meddelande.* Begreppet trafikuppgift i den bestämmelsen blir också mer konsekvent i förhållande till våra kommande överväganden i avsnitt 7.3.9. om tystnadsplikt för lokaliseringsuppgifter som inte är trafikuppgifter. I sak avses inte någon ändring i fråga tystnadsplikten. Den tystnadsplikt som hittills gällt för annan uppgift som angår ett särskilt elektroniskt meddelande ska således alltjämt gälla.

Det bör avslutningsvis nämnas att begreppet annan uppgift som angår ett särskilt elektroniskt meddelande också förekommer i offentlighets- och sekretesslagen bl. a. i anledning av den verksamhet som bedrevs av Televerket. När begreppet telemeddelande utmönstrades i lagstiftningen ändrades även bestämmelsen i 29 kap. 2 § OSL.[15] Televerket finns inte längre kvar men på grund av bl.a. bestämmelserna om överföring av sekretess i 11 kap. 6 § kan exempelvis Riksarkivet ha att tillämpa 29 kap. 2 § OSL på äldre uppgifter.[16] Som en konsekvens av våra förslag bör begreppet annan uppgift som angår ett särskilt elektroniskt meddelande ersättas av begreppet trafikuppgift även i offentlighets- och sekretesslagen.

6.6.3 Behov av anpassningar till EU-rätten och teknikutvecklingen

Utredningens bedömning: EU-domstolens praxis innebär att förslag bör lämnas om lagring av trafikuppgifter och lokaliseringsuppgifter för att skydda den nationella säkerheten. Det finns även anledning att lämna förslag om riktad lagring för att bekämpa grov brottslighet.

Något undantag från lagring avseende personer med tystnadsplikt bör inte införas.

Nationell säkerhet

Som framgår av avsnitt 6.3.2 tillåter EU-rätten en mer omfattande lagringsskyldighet med koppling till nationell säkerhet. När det gäller nationell säkerhet kan behöriga myndigheter alltså ges rätt att ålägga

[15] Se prop. 2011/12:55 s. 58 och 59.
[16] Lenberg Eva, Tansjö Anna och Geijer Ulrika, kommentaren till 29 kap. 2 § offentlighets- och sekretesslagen (2 december 2022, version 26, JUNO).

tjänsteleverantörer en generell och odifferentierad lagringsskyldighet under en begränsad tid avseende trafik- och lokaliseringsuppgifter, om målet är att skydda nationell säkerhet. Enligt nu gällande bestämmelser sker ingen datalagring för det uttalade syftet att skydda den nationella säkerheten. Vi bedömer att det finns ett behov av att införa en särskild möjlighet till lagring av trafik- och lokaliseringsuppgifter i syfte att skydda Sveriges säkerhet. Det ingår också i vårt uppdrag att se över regleringen och återkomma med förslag hur en sådan reglering kan utformas. Vi återkommer i avsnitt 7 till frågor om lagring och tillgång till trafik- och lokaliseringsuppgifter i syfte att skydda den nationella säkerheten.

Det blir allt vanligare att kommunikation sker genom tjänster som inte omfattas av någon rättslig skyldighet att lagra och tillhandahålla uppgifter, nämligen via tjänster som tillhandahålls av andra än de traditionella teleoperatörerna. Sådana tjänster kallas OTT-tjänster (over the top) eller nummeroberoende interpersonella kommunikationstjänster. Exempel på OTT-tjänster är Apple Imessage och Facetime, Messenger from Meta (tidigare Facebook Messenger) och Whatsapp. Det ingår i vårt uppdrag att analysera om OTT-tjänster ska omfattas av samma skyldigheter som gäller för de traditionella teleoperatörerna. Vi återkommer till denna och nära anslutande frågor i avsnitt 9.

Riktad lagring

Den nu gällande lagringsskyldigheten är, som vi beskrivit i avsnitt 6.2, ett resultat av de anpassningar till EU-rätten som gjordes efter Tele2-domen. EU-domstolen har dock i flera avgöranden efter Tele2-domen entydigt underkänt nationella bestämmelser som ålägger tjänsteleverantörer att lagra trafik- och lokaliseringsuppgifter i en omfattning som berör alla eller nästan alla personer som ingår i befolkningen, om syftet med lagringen är att bekämpa grov brottslighet. EU-domstolen förordar i stället riktad lagring som modell för att bekämpa grov brottslighet.

Som framgår av avsnitt 6.2.2 har regeringen tidigare haft starka betänkligheter mot att införa riktad lagring i Sverige. En riktad lagringen ansågs varken vara en ändamålsenlig, proportionerlig eller lämplig lösning. Vi delar i allt väsentligt denna syn på riktad lagring. Detta

talar mot riktad lagring som en modell för datalagring i Sverige. Frågan blir då om vi över huvud taget bör lämna förslag om riktad lagring.

Även om den svenska regleringen inte har prövats av EU-domstolen kan vi konstatera att den har likheter med de tyska reglerna om datalagring som prövades av EU-domstolen i SpaceNet-målet och som underkändes av domstolen. Det finns en risk för att EU-domstolen skulle kunna göra motsvarande bedömning beträffande den svenska regleringen, om den blev föremål för EU-domstolens prövning. Om datalagringen för att bekämpa grov brottslighet upphör, skulle förutsättningarna för det brottsbekämpande arbetet försämras avsevärt. Under sådana förhållanden anser vi att det finns skäl att lämna ett förslag om riktad lagring, som är förenligt med EU-domstolens krav. Vi gör sammanfattningsvis bedömningen att det finns ett behov av överväganden kring riktad lagring som vi redovisar i avsnitt 8. I avsnitt 9 överväger vi om OTT-tjänster ska omfattas av regler om riktad lagring.

Inget undantag från lagring för personer med tystnadsplikt

I Utredningen om datalagring och EU-rätten diskuterades om det borde införas något undantag från lagringen för personer med tystnadsplikt. Utredningen lämnade dock inget förslag på ett sådant undantag.[17] Frågan har aktualiserats även i vår utredning. Vi delar den bedömning som gjordes av Utredningen om datalagring och EU-rätten. Inte heller vi lämnar därför något förslag på ett sådant undantag.

6.6.4 Sanktionsavgifter

I avsnitt 10.5 tar vi upp frågan om sanktionsavgifter för den som inte lagrar uppgifter i enlighet med vårt förslag ovan angående abonnemangsuppgifter och våra förslag i avsnitt 7, 8 och 9.

[17] Se SOU 2017:75, s. 248–250.

7 Särskilt om lagring och tillgång till uppgifter i syfte att skydda nationell säkerhet

7.1 Inledning

Vi har i avsnitt 6 konstaterat att de svenska reglerna om lagring av uppgifter om elektronisk kommunikation för att bekämpa den grova brottsligheten kan behöva reformeras och att det finns behov av att införa en särskild möjlighet till lagring av trafik- och lokaliseringsuppgifter i syfte att skydda Sveriges säkerhet.

EU-rätten tillåter, en lagstiftning som ger behöriga myndigheter rätt att, med iakttagande kravet på proportionalitet, ålägga tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster, härefter tillhandahållare, generell och odifferentierad lagringsskyldighet under en begränsad tid avseende trafik- och lokaliseringsuppgifter, om målet är att skydda nationell säkerhet.

För en sådan lagringsskyldighet krävs

- att det föreligger 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 den kan bli föremål för en effektiv kontroll av en domstol eller en oberoende myndighet, och
- att den är tidsmässigt begränsad till vad som är strängt nödvändigt (men kan förlängas om hotet består).

I detta avsnitt överväger vi hur en sådan lagringsskyldighet skulle kunna utformas och hur tillgången till de lagrade uppgifterna bör regleras.

7.2 Vad menas med nationell säkerhet?

I våra överväganden om en lagringsskyldighet och tillgång till uppgifter i syfte att skydda nationell säkerhet finns det anledning att belysa vad som avses med uttrycket nationell säkerhet. Det kan redan här konstateras att det inte finns någon tydlig definition av uttrycket nationell säkerhet i vare sig svensk eller internationell rätt.

7.2.1 Uttrycket nationell säkerhet i EU-rätten och Europarätten

Utgångpunkten i fördraget om Europeiska unionen är att varje befogenhet som inte har tilldelats unionen i fördragen tillhör medlemsstaterna, se artikel 5. Av artikel. 4.2 samma fördrag framgår att unionen ska respektera medlemsstaternas likhet inför fördragen samt deras nationella identitet, som kommer till uttryck i deras politiska och konstitutionella grundstrukturer, inbegripet det lokala och regionala självstyret. Unionen ska respektera medlemsstaternas väsentliga statliga funktioner, särskilt funktioner vars syfte är att hävda staternas territoriella integritet, upprätthålla lag och ordning och skydda den nationella säkerheten. I synnerhet ska den nationella säkerheten också i fortsättningen vara varje medlemsstats eget ansvar.

I artikel 72 i fördraget om Europeiska unionens funktionssätt anges att fördragets avdelning om ett område med frihet, säkerhet och rättvisa inte ska påverka medlemsstaternas ansvar för att upprätthålla lag och ordning och skydda den inre säkerheten.

Någon definition av begreppet nationell säkerhet finns dock inte i något av dessa fördrag. EU-domstolen har inte heller fastställt någon tydlig definition av begreppet nationell säkerhet.

I artikel 1.3 i e-dataskyddsdirektivet anges att direktivet inte i något fall ska tillämpas på verksamheter som avser allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välstånd när verksamheten rör statens säkerhet) och statens verksamhet på straffrättens område. EU-domstolen har uttalat att de verksamheter som nämns som exempel i denna artikel i samtliga fall är verksamheter som endast kan bedrivas av staten eller statliga myndigheter och som inte kan bedrivas av enskilda.[1]

[1] Se La Quadrature du Net-domen p. 92 med hänvisningar till rättspraxis.

EU-domstolen har vidare slagit fast att målet att skydda den nationella säkerheten motsvarar det grundläggande intresset av att skydda statens väsentliga funktioner och samhällets grundläggande intressen och inbegriper förebyggande och beivrande av verksamhet som allvarligt kan störa de grundläggande konstitutionella, politiska, ekonomiska eller sociala strukturerna i ett land och i synnerhet direkt hota samhället, befolkningen eller staten som sådan, såsom bland annat terrorverksamhet.[2]

Uttrycket nationell säkerhet används också i artiklarna 8, 10 och 11 i Europakonventionen som ett av de legitima mål som kan motivera en begränsning av rättigheter. Någon definition av begreppet nationell säkerhet finns dock inte heller i denna konvention. Europadomstolen har inte heller utvecklat vad begreppet innebär men har dock klargjort under vilka omständigheter som ingrepp i de grundläggande rättigheterna kan ske med hänsyn till nationell säkerhet. Europadomstolen har bl.a. uttalat att de hot som finns mot nationell säkerhet kan variera och vara svåra att i förväg definiera.

Rådet för de europeiska advokatsamfunden (Council of Bars and Law Societies of Europe, CCBE)[3] har 2019 tagit fram rekommendationer när det gäller skyddet av grundläggande rättigheter inom ramen för nationell säkerhet. I rekommendationerna konstaterar CCBE att det saknas en definition av begreppet nationell säkerhet och att medlemsstaterna ger begreppet olika innebörd. CCBE rekommenderar följande definition av nationell säkerhet.[4]

Nationell säkerhet förstås som statens inre och yttre säkerhet, som består av ett eller flera av följande element:

- statens suveränitet,
- integriteten hos dess territorium, dess institutioner och dess kritiska infrastruktur,
- skyddet av statens demokratiska ordning,

[2] Se Garda Síochána-domen p. 61.
[3] CCBE är en internationell, icke-vinstdrivande organisation bestående av medlemmar från mer än 40 länder. Organisationen företräder advokater andra jurister inför europeiska och internationella institutioner i frågor om regleringen av professionen samt försvaret av legalitetsprincipen, mänskliga rättigheter och demokratiska värden m.m.
[4] https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf. Hämtat den 20 april 2023.

- skydd av dess medborgare och invånare mot allvarliga hot mot liv, hälsa och mänskliga rättigheter och
- uppförande och främjande av dess utrikesförbindelser och engagemang för fredlig samexistens mellan nationer.

7.2.2 Uttrycket nationell säkerhet i Sverige

I svensk författning används uttrycken rikets säkerhet, Sveriges säkerhet och nationell säkerhet synonymt. Uttrycken förekommer bl.a. i offentlighets- och sekretesslagen (2009:400), säkerhetsskyddslagen (2018:585), lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter och lagen (2022:700) om särskild kontroll av vissa utlänningar. I förarbetena till den sistnämnda lagen uttalade regeringen att det inte är lämpligt att inom ramen för det lagstiftningsärendet införa en legaldefinition av uttrycket Sveriges säkerhet, bl.a. eftersom det också förekommer i annan lagstiftning.[5]

I januari 2017 antog regeringen en svensk nationell säkerhetsstrategi.[6] I strategin anges bl.a. följande. Målen för vår säkerhet är att värna befolkningens liv och hälsa, liksom samhällets funktionalitet, samt förmågan att upprätthålla grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter. En förutsättning för att kunna uppnå dessa mål är att vårt lands politiska oberoende och självständighet säkras samt att vår territoriella integritet kan upprätthållas. Utmaningarna mot vår säkerhet är komplexa och kan snabbt växla. Samtidigt har förutsättningarna för att skydda befolkningen och upprätthålla de viktigaste samhällsfunktionerna förändrats i grunden. De aktörer som har betydelse för samhällets säkerhet är inte bara fler än tidigare, utan dessutom mer diversifierade. Inflytande över centrala områden och samhällsfunktioner, som tidigare i högre grad låg hos staten, kan i dag delas av många. Som en följd av globaliseringen är sambandet mellan inre och yttre säkerhet mer direkt än tidigare.

[5] Se prop. 2021/22:131 s. 79.
[6] Nationell säkerhetsstrategi, publicerad januari 2017, Regeringskansliet, Statsrådsberedningen.

7.3 Överväganden och förslag

I fortsättningen överväger vi hur en lagringsskyldighet i syfte att skydda Sveriges säkerhet kan utformas som ger en behörig myndighet rätt att ålägga tillhandahållare en generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter och hur tillgången till dessa uppgifter bör ordnas.

7.3.1 Den behöriga myndigheten och bedömningen av hotet mot Sveriges säkerhet

Utredningens förslag: Säkerhetspolisen ska bedöma hotet mot den nationella säkerheten och får besluta om generell och odifferentierad lagringsskyldighet. En sådan lagringsskyldighet är tillåten om den bedöms vara strängt nödvändig för att bekämpa brottslighet som kan utgöra ett allvarligt hot mot nationell säkerhet som är verkligt och aktuellt eller förutsebart. Säkerhetspolisen ska i fråga om hotbilden samråda med Försvarsmakten.

Utredningens bedömning: Säkerhetspolisen får inhämta relevant information från andra myndigheter och organ. Myndigheter som har information om hot mot den nationella säkerheten kan på eget initiativ uppmärksamma Säkerhetspolisen på dessa förhållanden.

EU-rätten tillåter, som redovisats ovan, under vissa förutsättningar en lagstiftning som ger behöriga myndigheter rätt att ålägga tillhandahållare en generell och odifferentierad lagringsskyldighet under en begränsad tid i syfte att skydda nationell säkerhet.

Den behöriga myndighetens beslut om att ålägga tillhandahållare en sådan lagringsskyldighet ska vidare kunna bli föremål för en effektiv kontroll av en domstol eller en oberoende myndighet, vars avgörande har bindande verkan, i syfte att kontrollera om förutsättningarna för en sådan lagringsskyldighet är uppfyllda. Hur denna kontroll bör utformas beror bl.a. på vilket eller vilka organ som ska vara behörig myndighet att besluta om lagringsskyldigheten och om den behöriga myndigheten även ska pröva huruvida det föreligger ett allvarligt hot mot den nationella säkerheten. Vi återkommer till frågan om hur den effektiva kontrollen bör utformas i avsnitt 7.3.4.

Den behöriga myndigheten ska bedöma hotet mot Sveriges säkerhet

Den behöriga myndighetens beslut att ålägga tillhandahållare en generell och odifferentierad lagringsskyldighet ska grunda sig på bedömningen att det föreligger ett allvarligt hot mot den nationella säkerheten. I någon mening handlar det alltså om två olika beslut, som i och för sig nog kan fattas av olika organ.

Ett alternativ är alltså att den behöriga myndigheten beslutar både i frågan om det föreligger ett allvarligt hot mot den nationella säkerheten och om lagringsskyldigheten. Det andra alternativet är att ett organ beslutar i frågan om det föreligger ett allvarligt hot mot den nationella säkerheten och att ett annat organ beslutar om lagringsskyldigheten.

Det nära sambandet mellan dessa båda frågor talar för att samma myndighet bör pröva båda frågorna. Om det är en myndighet som bedömer säkerhetsläget och en annan som beslutar om datalagring, förutsätter det att den sistnämnda myndigheten har full insyn i den förstnämnda myndighetens bedömning av säkerhetsläget för att kunna besluta om lämplig lagringsskyldighet. Det är inte givet att förutsättningar för detta alltid kommer att finnas. Vidare ska den domstol eller det oberoende organ som ska utgöra en effektiv kontroll när det gäller den beslutade lagringsskyldigheten kunna pröva om förutsättningarna för lagringsskyldigheten är uppfyllda, vilket innefattar frågan om hotet mot den nationella säkerheten är sådant att lagringsskyldigheten är påkallad. En sådan prövning kan bli svårare att göra om det är olika organ som har beslutat om säkerhetsläget och lagringsskyldigheten. Vi menar därför att det är mest lämpligt att samma myndighet prövar båda frågorna.

Det bör inte föreskrivas kriterier för bedömningen av säkerhetsläget

EU-domstolen har påpekat att det, för att kravet på proportionalitet ska vara uppfyllt, i 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. Det måste 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. Lagstiftningen ska vara rättsligt bindande enligt nationell rätt och i synner-

het 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.[7]

När det gäller tvångsmedelsanvändning och andra övervakningsåtgärder framgår det, bl.a. av Europadomstolens praxis, att det måste finnas klara och detaljerade regler som beskriver i vilka situationer och under vilka förutsättningar som sådana får användas. Det krävs enligt Europadomstolen inte en lista med namngivna brott som kan föranleda tvångsmedelsåtgärden men det är normalt inte tillräckligt att hänvisa till så generella begrepp som nationell säkerhet eller allmän ordning. Domstolen har samtidigt tydliggjort att de hot som finns mot nationell säkerhet kan variera och vara svåra att i förväg definiera.[8]

De krav på förutsebarhet och tydlighet som ställs på en reglering som gäller under vilka omständigheter som hemliga tvångsmedel får användas gör sig inte på samma sätt gällande vid en reglering av när en generell och odifferentierad lagringsskyldighet är tillåten. Det går nämligen inte med någon större säkerhet att förutse vilka företeelser som kan komma att innebära ett hot mot den nationella säkerheten. Vi anser att det skulle vara för onyanserat att föreskriva att en generell och odifferentierad lagringsskyldighet kan beslutas exempelvis när terrorhotsnivån i Sverige är på en viss nivå. En sådan reglering skulle kunna innebära att en generell och odifferentierad lagring blir huvudregeln. Vi bedömer det inte lämpligt att i författning precisera vilka omständigheter som ska föreligga för att hotet mot den nationella säkerheten är sådant att en generell och odifferentierad lagringsskyldighet är påkallad. Det måste rimligen vara den behöriga myndigheten som, på ett så komplett underlag som möjligt, avgör om det finns tillräckligt konkreta omständigheter för att anse att det finns ett allvarligt och verkligt hot mot Sveriges som är aktuellt eller förutsebart. Omständigheter som kan vara av betydelse vid bedömningen av hotet mot den nationella säkerheten är t.ex. om terrorhotsnivån 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. Vid bedömningen av sådana hot kan exempelvis underrättelseinformation som rör brottslig verksamhet som innefattar terroristbrott och andra systemhotande brott beaktas.

[7] Se SpaceNet-domen p. 69.
[8] Se SOU 2018:61 s. 78 och 79.

Förutsättningarna för *när* en generell och odifferentierad lagringsskyldighet ska vara tillåten bör alltså inte vara mer konkretiserade i författning än att lagringen bedöms vara strängt nödvändig när det föreligger ett allvarligt hot mot nationell säkerhet som är verkligt och aktuellt eller förutsebart.

I det här sammanhanget vill vi uppmärksamma att vi i betänkandet genomgående använder uttrycket strängt nödvändigt eftersom uttrycket används av EU-domstolen. Uttrycket är emellertid inte etablerat i svensk lagstiftning. Vi kommer därför i våra författningsförslag att använda uttrycket absolut nödvändigt. Vår avsikt är att uttrycken ska ha samma innebörd. Med strängt eller absolut nödvändigt avser vi att bedömningen ska föregås av noggranna överväganden kring behov och att tillämpning ska ske restriktivt.

Valet av behörig myndighet

Det kan konstateras att uppgiften att bedöma om Sverige står inför ett allvarligt hot mot den nationella säkerheten kräver tillgång till den mest skyddsvärda information som finns i landet och att uppgifterna ofta lär vara kvalificerat hemliga. För bedömningen måste den behöriga myndigheten och kontrollorganet få tillgång till omfattande mängder uppgifter så att frågan får en allsidig belysning. Detta ställer krav på att såväl den behöriga myndigheten som kontrollorganet på ett säkert sätt kan hantera den synnerligen skyddsvärda informationen. En annan viktig aspekt är att den synnerligen känsliga informationen bör hållas inom en så snäv krets som möjligt inom den behöriga myndigheten och kontrollorganet.

Det finns, enligt vår uppfattning, en del som talar för att det bör vara regeringen som bedömer hotet mot den nationella säkerheten. Det är regeringen som styr riket (1 kap. 6 § RF). Frågor om landets säkerhetsläge får anses ligga inom den styrande uppgiften. Regeringen har möjlighet att få relevant information från alla myndigheter och torde alltså kunna få den mest kompletta bilden av hotet mot Sveriges säkerhet.

Det finns emellertid skäl som talar mot att regeringen ska besluta om hotet mot den nationella säkerheten. En omständighet som talar mot regeringen som beslutsfattare är att vi ovan gjort bedömningen att det bör vara samma myndighet som beslutar om säkerhetshotet

och om lagringsskyldigheten. Om regeringen prövar den nationella säkerheten, skulle regeringen i så fall även besluta om datalagringen. Det är emellertid inte en typisk uppgift för regeringen att förelägga tillhandahållare en lagringsskyldighet. Vidare är det förenat med svårigheter att välja ett lämpligt och oberoende organ som skulle kunna utgöra ett effektivt kontrollorgan i förhållande till regeringens beslut. Mot denna bakgrund gör vi bedömningen att något annat organ än regeringen bör vara behörig myndighet.

Den behöriga myndigheten bör vara sådan att den har god kompetens när det gäller att bedöma frågor om hotet mot rikets säkerhet. Myndigheten bör också ha en gedigen erfarenhet av behandling av personuppgifter i sin kärnverksamhet, särskilt när det gäller behandling av personuppgifter i brottsbekämpande verksamhet. En fördel är förstås om myndigheten också har erfarenhet av behandling av personuppgifter som rör nationell säkerhet.

De två myndigheter som mot denna bakgrund har störst möjlighet att bedöma hotet mot Sveriges säkerhet är Säkerhetspolisen och Försvarsmakten. Säkerhetspolisens uppdrag är just att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot Sveriges säkerhet och terrorbrott, dvs. inre hot mot Sverige. Försvarsmaktens uppdrag omfattar bl.a. att upptäcka och identifiera yttre hot mot Sverige och svenska intressen.

Det finns emellertid andra myndigheter som inom sitt verksamhetsområde har kunskap om omständigheter som har betydelse för bedömningen av hotet mot Sveriges säkerhet, t.ex. Polismyndigheten, Försvarets radioanstalt (FRA), Försvarets materielverk (FMV), Totalförsvarets forskningsinstitut (FOI), Myndigheten för psykologiskt försvar, Myndigheten för samhällsskydd och beredskap (MSB) och Post- och telestyrelsen (PTS). Vidare finns det myndighetsgemensamma samverkansgrupper inom olika områden med god kännedom om den nationella säkerheten som Nationellt centrum för terrorhotsbedömning och Nationellt cybersäkerhetscenter.

Man kan överväga om exempelvis PTS, som är reglerings- och tillsynsmyndighet enligt nya LEK, skulle kunna vara behörig myndighet i nu aktuellt avseende. PTS har stor kompetens när det gäller frågor om elektronisk kommunikation och lagring av uppgifter från sådan. Myndigheten har även viss kompetens när det gäller bedömningar av hotet mot Sveriges säkerhet. PTS är exempelvis besluts-

myndighet när det gäller tillstånd att använda radiosändare.[9] Bland de frågor som PTS då ska bedöma är om radioanvändningen kommer att orsaka skada för Sveriges säkerhet.[10] I ärenden om tillstånd att använda radiosändare ska PTS samråda med Försvarsmakten och Säkerhetspolisen i syfte att klarlägga om radioanvändningen kan antas orsaka skada för Sveriges säkerhet och om behovet av att förena ett tillstånd med villkor om krav som är av betydelse för Sveriges säkerhet.[11] Säkerhetspolisen och Försvarsmakten kan överklaga beslut av PTS i tillståndsfrågor som berör Sveriges säkerhet.[12] I förarbetena till reglerna om skydd av Sveriges säkerhet vid radioanvändning anförde regeringen att det bara är Säkerhetspolisen och Försvarsmakten som tillsammans har en helhetsbild när det gäller säkerhetsläget och hotbilden mot Sverige samt tillgång till de uppgifter som behövs för att bedöma om radioanvändning kan antas orsaka skada för Sveriges säkerhet.[13]

Frågan är om det är lämpligt att utse PTS till beslutsorgan i detta sammanhang. Bedömningen av om det föreligger ett allvarligt hot mot Sveriges säkerhet är betydligt vidare än frågan om tillstånd till radiosändare och rör frågor som ligger utanför PTS kompetensområde. Såväl Säkerhetspolisen som Försvarsmakten och eventuellt andra myndigheter eller organ skulle behöva till PTS lämna ett utförligt underlag i fråga om hotbilden mot Sverige. Vår bedömning är därför att ingen annan myndighet än Säkerhetspolisen eller Försvarsmakten bör komma i fråga som behörig myndighet.

I valet mellan Säkerhetspolisen och Försvarsmakten som behörig myndighet gör vi följande bedömning. Såväl Säkerhetspolisen som Försvarsmakten torde ha kompetensen att bedöma hotet mot den nationella säkerheten. För att underlaget till bedömningen av detta hot ska bli så komplett och allsidigt som möjligt bör bedömningen grundas på båda myndigheternas men vid behov även andra organs kunskap i frågan. Oavsett vilken av myndigheterna som ska vara behörig myndighet bör de alltså samråda med varandra och ha möjlighet att inhämta information från alla organ som kan antas ha relevant information i frågan.

[9] Se 3 kap. nya LEK.
[10] Se 3 kap. 6 § första stycket 7 nya LEK.
[11] Se 3 kap. 13 § nya FEK.
[12] Se 15 kap. 2 § andra stycket nya LEK.
[13] Se prop. 2019/20:15 s. 35.

Frågan är dock om det är lämpligt att Försvarsmakten ska kunna ålägga tillhandahållare att lagra uppgifter från kommunikation inom landet. De uppgifter som kan omfattas av lagringsskyldigheten torde i första hand inte avse utländska förhållanden. Med hänsyn till att de uppgifter som kan komma att lagras i syfte att skydda den nationella säkerheten sannolikt i första hand kommer kunna inhämtas av Säkerhetspolisen (se avsnitt 7.3.7 nedan) framstår det som ändamålsenligt att det är Säkerhetspolisen som gör bedömningen av vad som ska omfattas av lagringsskyldigheten. Vi bedömer att Säkerhetspolisen har störst kompetens i dessa frågor.

Vi föreslår därför att Säkerhetspolisen ska vara den myndighet som ska kunna besluta om en generell och odifferentierad lagringsskyldighet (nationell säkerhetslagring) när läget är sådant att Sverige står inför ett allvarligt hot mot den nationella säkerheten. För att Säkerhetspolisen ska ha ett så fullgott underlag som möjligt inför sitt beslutsfattande bör det föreskrivas att Säkerhetspolisen ska samråda med Försvarsmakten inför sin bedömning vad gäller hotet mot den nationella säkerheten.

Säkerhetspolisen kan också inhämta information från andra myndigheter och organ som kan antas ha relevant kunskap om omständigheter som har betydelse för bedömningen av hotet mot Sveriges säkerhet. Det bör också påtalas att det inte föreligger något hinder mot att myndigheter som har information om hot mot den nationella säkerheten, exempelvis Försvarsmakten, Polismyndigheten, Tullverket eller Ekobrottsmyndigheten, på eget initiativ uppmärksammar Säkerhetspolisen på dessa förhållanden så länge detta sker med iakttagande av tillämpliga sekretessregler. En sådan inhämtning av information eller kontakt kan ske utan särskilda formkrav och inom ramen för det befintliga samarbete som myndigheterna har.

7.3.2 Förvaltningslagens tillämplighet

Utredningens bedömning: De åtgärder som Säkerhetspolisen vidtar inom ramen för ärenden om nationell säkerhetslagring utgör brottsbekämpande verksamhet. Förvaltningslagen är därför tillämplig endast i vissa delar.

Säkerhetspolisen ska enligt vårt förslag bedöma hotet mot den nationella säkerheten och får besluta om nationell säkerhetslagring. Frågan är om arbetsuppgifterna motsvarar de åtgärder som vidtas inom ramen för myndighetens brottsbekämpande verksamhet.

I förvaltningslagen (2017:900) görs undantag från flertalet av lagens bestämmelser i den brottsbekämpande verksamheten. Enligt 3 § förvaltningslagen tillämpas inte 9 § andra stycket och 10–49 §§ i brottsbekämpande verksamhet hos bl.a. Säkerhetspolisen. Det innebär att de särskilda förfarandereglerna om partsinsyn, underrättelseskyldighet före beslut, omröstning, motivering av beslut och rättelse m.m. inte gäller i denna verksamhet. Vidare är inte heller de allmänna bestämmelserna om tolk, ombud och biträde, bestämmelserna om jäv eller bestämmelsen om när en handling ska anses inkommen tillämpliga i den brottsbekämpande verksamheten. Paragrafen innebär att det enbart är bestämmelserna i förvaltningslagens 5–8 §§ om legalitet, objektivitet, proportionalitet, service, tillgänglighet i förhållande till allmänheten och samverkan med andra myndigheter samt bestämmelsen i 9 § första stycket om krav på enkel, snabb och kostnadseffektiv handläggning som ska tillämpas vid ärendehandläggning i den brottsbekämpande verksamheten hos Säkerhetspolisen.[14]

Det innebär naturligtvis inte att Säkerhetspolisens verksamhet är undantagen från grundläggande rättssäkerhetskrav. Regleringen finns i stället i andra författningar som är anpassade efter den brottsbekämpande verksamheten, exempelvis rättegångsbalken och polislagen (1984:387).

Skälet till att undantag gjordes för brottsbekämpande verksamhet vid genomförandet av förvaltningsrättsreformen 1971 var att lagstiftaren från lagens tillämpningsområde ville undanta handläggningen av ärenden som nära anknöt till rättegången i allmän domstol. För att uppnå detta ansågs det nödvändigt att undanta inte bara domstolarnas rättskipande verksamhet utan också handläggningen av ärenden i förfaranden som kunde mynna ut i, vara en följd av eller på annat sätt anknyta till rättegången.[15] Denna begränsning behölls i 1986 års och 2017 års förvaltningslagar. Regeringen angav i de senaste lagmotiven att den nära koppling som finns mellan förfarandet hos myndigheter i den brottsbekämpande verksamheten och rättegången i all-

[14] Se prop. 2016/17:180 s. 288.
[15] Se prop. 1971:30 del 2 s. 306 och 323.

män domstol medför att skälen för begränsningen av förvaltningslagens tillämpningsområde i detta avseende alltjämt är relevanta.[16]

Vi kan konstatera att nationell säkerhetslagring syftar till att skapa förutsättningar för användning av hemliga tvångsmedel. De åtgärder som ska vidtas inom ramen för ärenden om nationell säkerhetslagring innefattas enligt vår bedömning i sin helhet i den brottsbekämpande verksamheten, som beskrivits i avsnitt 5.2. Åtgärderna mynnar ytterst ut i att förhindra eller lagföra brott som innebär ett hot mot den nationella säkerheten. Förfarandet utgör med andra ord brottsbekämpande verksamhet och är undantaget från förvaltningslagens tillämpningsområde i de delar som vi beskrivit ovan.

Nationell säkerhetslagring tillhör sådan verksamhet som måste tillgodose högt ställda krav på rättssäkerhet. Delar av förfarandet regleras som nämnts i de författningar som gäller för de brottsbekämpande myndigheternas verksamhet. Exempelvis blir bestämmelsen om jäv enligt 7 § polislagen (1984:387) även tillämplig vid arbete med frågor om nationell säkerhetslagring. I andra delar, särskilt vad gäller frågor om beslutsformer och möjligheterna till överklagande behövs särskilda överväganden för våra förslag. Vi återkommer till dessa frågor i kommande avsnitt.

7.3.3 Säkerhetspolisens beslut om lagring

Utredningens förslag: Säkerhetspolisen ska, inom ramen för vad som anges i författning, besluta vilka tillhandahållare som ska omfattas av ett föreläggande om nationell säkerhetslagring och om lagringsskyldighetens närmare omfattning.

Ett sådant beslut ska begränsas till vad som är absolut nödvändigt för syftet med lagringen.

Ett föreläggande om lagring ska gälla så länge behovet kan förväntas föreligga och längst under ett års tid. Lagringsskyldigheten ska därefter kunna förlängas om Säkerhetspolisen gör bedömningen att hotet mot den nationella säkerheten kvarstår. Säkerhetspolisen ska löpande ompröva om hotet består och upphäva lagringsskyldigheten om förhållandena ändras.

[16] Se prop. 2016/17:180 s. 33.

Säkerhetspolisens uppgifter som behörig myndighet ska regleras i en ny lag benämnd lagen om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

När Säkerhetspolisen gör bedömningen att den nationella säkerheten påkallar ett beslut om datalagring ska Säkerhetspolisen alltså kunna fatta ett sådant beslut. Frågan är vilken ordning som då bör gälla. Det finns närmast två alternativ att välja mellan. Det ena är att Säkerhetspolisen beslutar att en redan på förhand fastslagen författningsreglering om datalagring ska träda i kraft. Det andra alternativet är att Säkerhetspolisen får besluta om lagringsskyldighetens närmare omfattning. Det första alternativet har fördelen att det är transparent och förutsebart. En annan väsentlig fördel med det alternativet är att det är enklare för tillhandahållarna att förhålla sig till. Att lagringsskyldighetens omfattning bestäms med kort varsel och kanske också varierar från tid till annan ställer stora krav på tillhandahållarna, vilket undviks om lagringsskyldighetens omfattning är fastställd i författning. En nackdel med det första alternativet är emellertid att det i det särskilda fallet inte medger någon proportionalitetsbedömning av lagringsskyldigheten. Risken är exempelvis att fler uppgiftstyper än vad som är strängt nödvändigt kan omfattas av lagringen och att regleringen inte lever upp till EU-rättens krav. Som vi beskrivit i avsnitt 7.3.1 innebär proportionalitetsprincipen bl.a. att det genom författning ska säkerställas att ett ingrepp i enskildas grundläggande rättigheter begränsas till vad som är absolut nödvändigt.

Vi föreslår därför att Säkerhetspolisen ska kunna fatta ett efter omständigheterna differentierat beslut inom ramen för vad som föreskrivs i författning. Säkerhetspolisen bör alltid kunna besluta om vilka tillhandahållare som ska lagra uppgifter. Omständigheterna kan vara sådana att det inte är strängt nödvändigt att alla tillhandahållare omfattas av lagringsskyldigheten. Säkerhetspolisen bör också kunna besluta om den närmare omfattningen av lagringsskyldigheten, när det gäller vilka typer av uppgifter som ska lagras. När det gäller frågan hur länge uppgifterna ska lagras gör vi dock bedömningen att detta ska regleras direkt i författning.

Vi har i avsnitt 7.3.1 beskrivit att Säkerhetspolisen ska samråda med Försvarsmakten, och i förekommande, även med andra myndigheter i fråga om hotet mot den nationella säkerheten. Motsvarande samråd bör äga rum även i fråga om lagringsskyldighetens omfattning. Inför

ett beslut om lagring bör Säkerhetspolisen kunna samråda med andra myndigheter i frågan om lagringsskyldighetens omfattning, i första hand med Polismyndigheten, PTS och Tullverket. Det kan inte heller uteslutas att Säkerhetspolisen behöver ta kontakt med berörda tillhandahållare inför ett beslut om lagring. Vi ser inget behov av att författningsreglera dessa samråd och kontakter. Normalt bör det inte bli aktuellt för Säkerhetspolisen att i dessa situationer röja sekretessbelagda uppgifter. Om så ändå skulle bli fallet, bör uppgifterna kunna lämnas ut med stöd av 10 kap. 2 § OSL (nödvändigt utlämnande). En sekretessbelagd uppgift får också lämnas till en myndighet, om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda (10 kap. 27 § OSL). Vi återkommer nedan till frågan om tillhandahållarnas tystnadsplikt i avsnitt 7.3.9.

Ett föreläggande om nationell säkerhetslagring ska gälla under en viss tid. Som framgår av EU-domstolens praxis får denna tid inte vara längre än vad som är strängt nödvändigt. Det bör därför föreskrivas en längsta tid som ett föreläggande får gälla. Med hänsyn till att en generell lagringsskyldighet bara kan beslutas när det föreligger ett allvarligt hot mot den nationella säkerheten bör denna tid inte vara alltför kort. Det är sannolikt ofta så att de förhållanden som lagts till grund för bedömningen att Sverige står inför ett allvarligt hot mot den nationella säkerheten inte ändras särskilt snabbt. Vi föreslår därför att den generella lagringsskyldigheten ska få gälla i högst ett år. Om Säkerhetspolisen gör bedömningen att det allvarliga hotet mot den nationella säkerheten därefter kvarstår, ska den genom ett nytt föreläggande kunna förlänga lagringsskyldigheten. Säkerhetspolisen bör emellertid ha en skyldighet dels att löpande ompröva om hotet består, dels att upphäva lagringsskyldigheten om förhållandena ändras. Vi återkommer i avsnitt 7.3.6. till frågor om vilka uppgifter som ska kunna lagras och själva lagringstiden för uppgifterna.

Vi föreslår att Säkerhetspolisens uppgifter som behörig myndighet regleras i en ny lag som lämpligen kan benämnas lagen om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet. Som redovisas nedan kommer i lagen även förfarandet, lagringen och åtkomsten till uppgifterna att regleras.

7.3.4 En effektiv kontroll av lagringsskyldigheten

Utredningens förslag: 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.

I huvudsak motsvarande regler som gäller för offentliga ombud enligt rättegångsbalken ska tillämpas när det gäller kraven på samt nomineringen och förordnanden av ombuden, liksom beträffande ersättning till och tystnadsplikt för ombuden.

Säkerhetspolisen ska besluta om ersättning till det offentliga ombudet. För det fall Säkerhetspolisens beslut överklagas, ska kontrollorganet besluta om ersättning till det offentliga ombudet.

Kontrollorganet ska pröva om förutsättningarna för lagringsskyldigheten är uppfyllda och om lagringsskyldigheten är proportionell. Kontrollorganet ska bara kunna fastställa eller upphäva Säkerhetspolisens beslut om lagring. Kontrollorganet ska även kunna pröva Säkerhetspolisens beslut om ersättning. Ett offentligt ombud bör få överklaga Säkerhetspolisens beslut om ersättning även i situationer när beslutet om nationell säkerhetslagring inte överklagas. Ett sådant beslut får överklagas utan inskränkning i tid.

En av förutsättningarna för en lagstiftning som ger behöriga myndigheter rätt att ålägga tillhandahållare en generell och odifferentierad lagringsskyldighet i syfte att skydda den nationella säkerheten är, som nämnts ovan, att lagringsskyldigheten kan bli föremål för en effektiv kontroll. Kontrollen ska utföras av en domstol eller ett oberoende organ, vars avgörande har bindande verkan, i syfte att kontrollera om förutsättningarna för en sådan lagringsskyldighet är uppfyllda.

Vi har ovan föreslagit att Säkerhetspolisen ska vara den behöriga myndigheten som både ska bedöma om det föreligger ett allvarligt hot mot den nationella säkerheten och kunna förelägga tillhandahållarna en generell lagringsskyldighet. Frågan är hur denna kontroll ska utövas.

Vad menas med effektiv kontroll?

Enligt EU-domstolen ska den effektiva kontrollen syfta till en granskning av att förutsättningarna för lagringsskyldigheten är uppfyllda. Eftersom den grundläggande förutsättningen för lagringsskyldigheten är att det föreligger ett allvarligt hot mot den nationella säkerheten måste kontrollorganet ha möjlighet att göra en egen bedömning av denna fråga. Vidare ska kontrollorganets avgöranden ha bindande verkan. Kontrollorganet måste således ha möjlighet att upphäva en lagringsskyldighet i de fall förutsättningarna inte är uppfyllda. Frågan är om kravet på en effektiv kontroll innefattar något annat än en möjlighet till sådan överprövning av lagringsskyldigheten, exempelvis ett krav på någon form av fortlöpande tillsyn. Enligt EU-domstolen ska en generell och odifferentierad lagringsskyldighet vara föremål för begränsningar och åtföljas av strikta garantier för att på ett effektivt sätt skydda de berördas personuppgifter från riskerna för missbruk.[17] Den effektiva kontrollen ska, förutom att säkerställa att lagringen de facto är begränsad till situationer där det föreligger ett allvarligt hot mot nationell säkerhet, omfatta att de villkor och garantier som krävs är uppfyllda.[18] Detta skulle visserligen kunna tala för att den effektiva kontrollen även ska innefatta någon form av fortlöpande tillsyn av själva lagringsskyldigheten. Å andra sidan är det enligt EU-domstolen själva beslutet om lagring som ska bli föremål för en effektiv kontroll och inte den efterföljande lagringen. Detta innebär, enligt vår uppfattning, att den effektiva kontrollen måste avse att de förutsättningar för lagringsskyldigheten som föreskrivs i nationell rätt är uppfyllda.

EU-domstolen har också i andra sammanhang ställt krav på kontroll av domstol eller annan oberoende myndighet. Exempelvis uttalade sig EU-domstolen om detta i den s.k. Prokuratuur-domen, där frågan gällde tillgången till lagrade trafik- och lokaliseringsuppgifter för att bekämpa grov brottslighet.[19] EU-domstolen konstaterade att den nationella lagstiftningen måste vara grundad på objektiva kriterier som avgör under vilka omständigheter och på vilka villkor behöriga nationella myndigheter ska ges tillgång till de aktuella uppgifterna. För att säkerställa att dessa villkor uppfylls i praktiken, är det väsentligt att tillgången till de lagrade uppgifterna är underkastad

[17] Se La Quadrature du Net-domen p. 138.
[18] Se a. dom p. 139.
[19] EU-domstolens dom den 2 mars 2021 i mål C-746/18.

förhandskontroll av en domstol eller en oberoende myndighet. En sådan förhandskontroll ska innebära att den domstol eller det organ som ska utföra kontrollen har alla befogenheter och lämnar alla nödvändiga garantier för att kunna göra en vederbörlig avvägning mellan de olika intressen och rättigheter som är i fråga (se p. 50–52 i domen). Inte heller i detta sammanhang synes en kontroll av en domstol eller ett annat oberoende organ ställa krav på någon form av fortlöpande tillsyn. Vår slutsats är därför att EU-rätten inte kräver att kontrollorganet ska bedriva någon form av fortlöpande tillsyn såvitt gäller själva lagringsskyldigheten.

Hur ska beslutet underställas kontrollorganet?

En central fråga i sammanhanget är på vilket sätt Säkerhetspolisens beslut om lagring ska kunna underställas kontrollorganet. Ett alternativ är att Säkerhetspolisens beslut alltid ska överprövas av kontrollorganet. Vad som talar för denna lösning är främst arten och vikten av de frågor som ska prövas. Det kan därför anses lämpligt att kontrollorganet alltid kontrollerar om förutsättningarna för lagringsskyldigheten är uppfyllda. Ett annat alternativ är att ett offentligt ombud ska kunna överklaga Säkerhetspolisens beslut när ombudet finner det påkallat. Det offentliga ombudet skulle kunna ges i uppdrag att bevaka enskildas intressen i allmänhet, dvs. utan att företräda någon särskild fysisk eller juridisk person. Ett offentligt ombud skulle också kunna bevaka att lagringsskyldigheten inte blir alltför betungande för tillhandahållarna, liksom eventuella andra motstående intressen.

En liknande ordning finns när det gäller beslut om vissa hemliga tvångsmedel, då ett offentligt ombud ska bevaka enskildas integritetsintressen i de aktuella ärendena.[20] Vidare ska, vid Försvarsunderrättelsedomstolens prövning av tillstånd till signalspaning, ett integritetsskyddsombud bevaka enskildas integritetsintressen.[21]

Det kan konstateras att EU-rätten kräver att den behöriga myndighetens beslut *kan* bli föremål för en effektiv kontroll. Det kan därför framstå som överflödigt att besluten alltid ska bli föremål för kontroll. Om besluten per automatik blir föremål för kontrollorganets prövning, kan det dessutom ifrågasättas om det är kontroll-

[20] Se 27 kap. 26–30 §§ RB.
[21] Se 5–8 §§ lagen (2009:966) om Försvarsunderrättelsedomstol.

organet som blir den faktiska beslutsfattaren och att Säkerhetspolisen snarast är att betrakta som ansökande i förfarandet. Denna farhåga blir särskilt tydlig om Säkerhetspolisens beslut om lagring inte skulle få verkställas innan kontrollorganet gjort sin prövning. En fördel med att ett offentligt ombud ges möjlighet att överklaga Säkerhetspolisens beslut är att förfarandet blir mer kontradiktoriskt, vilket främjar frågornas allsidiga belysning.

En nackdel med att involvera offentliga ombud i förfarandet är att kretsen som får tillgång till den synnerligen skyddsvärda informationen utökas. Denna nackdel ska dock inte överdrivas. Det torde nämligen inte krävas att något stort antal personer förordnas till offentliga ombud i dessa sammanhang. Vi återkommer till denna fråga nedan.

Av de skäl som nu anförts förordar vi en ordning med ett offentligt ombud som bevakar enskildas intressen och som har möjlighet att begära överprövning av Säkerhetspolisens beslut om nationell säkerhetslagring. Med enskilda åsyftas här inte bara enskilda fysiska personer utan även tillhandahållarnas intressen och andra motstående intressen.

Man kan naturligtvis överväga om de ombud som är aktuella i detta sammanhang ska kallas just offentliga ombud. Det kan finnas en risk för sammanblandning med sådana offentliga ombud som ska bevaka enskildas intressen i ärenden om vissa hemliga tvångsmedel. Vi anser att ombuden inte bör kallas för integritetsskyddsombud, eftersom vårt förslag innebär att ombuden ska bevaka annat än bara integritetsskyddsintressen. Ombuden skulle i stället kunna kallas exempelvis allmänna ombud eller dataskyddsombud, men även dessa begrepp används i andra sammanhang. Vi anser att risken för förväxling när det gäller olika uppdrag som offentligt ombud är så liten att detta begrepp kan användas även i detta sammanhang.

Motsvarande regler som gäller för offentliga ombud enligt rättegångsbalken bör i huvudsak finnas när det gäller kraven på samt nomineringen och förordnanden av ombuden, liksom beträffande ersättning till och tystnadsplikt för ombuden. Säkerhetspolisen bör besluta om ersättning till det offentliga ombudet. För det fall Säkerhetspolisens beslut överklagas, ska kontrollorganet besluta om ersättning till det offentliga ombudet.

När det gäller kraven på de offentliga ombuden kan det övervägas om inte bara den som har varit ordinarie domare utan också den som

är ordinarie domare skulle kunna vara offentligt ombud i ärenden om nationell säkerhetslagring. Risken för att ordinarie domare hamnar i någon intressekonflikt torde vara mindre i denna typ av ärenden än i ärenden om hemliga tvångsmedel. Vi anser dock att det inte finns något behov av ordinarie domare som offentliga ombud, om även advokater och andra med motsvarande juridisk erfarenhet kan komma i fråga som offentligt ombud.

Till skillnad mot vad som gäller för offentliga ombud enligt rättegångsbalken föreslår vi dock att regeringen förordnar endast ett ordinarie offentligt ombud för denna typ av ärenden. Det offentliga ombudet ska alltså inte förordnas i ett specifikt ärende om nationell säkerhetslagring. Av sårbarhetsskäl måste det dock finnas ersättare för det offentliga ombudet. Vi föreslår därför att regeringen även förordnar ett första och ett andra ställföreträdande offentligt ombud. Om det ordinarie offentliga ombudet har förhinder, träder det första ställföreträdande ombudet in i dennes ställe. Om även den förste ställföreträdaren har förhinder, träder den andre ställföreträdaren in. Avsikten med en sådan ordning är dels att minimera kretsen av de personer som får tillgång till den känsliga informationen, dels att det inte ska gå att välja vilket ombud som förordnas i ett ärende om nationell säkerhetslagring.

Med hänsyn till den synnerligen känsliga information som ska ligga till grund för Säkerhetspolisens bedömning av hotet mot den nationella säkerheten anser vi att de offentliga ombuden alltid ska vara säkerhetsprövade och placerade i säkerhetsklass. Detta följer dock redan av 3 kap. 1 § säkerhetsskyddslagen. Vi återkommer till frågorna om tystnadsplikt och meddelarfrihet för offentliga ombud i avsnitt 7.3.9.

Vi bedömer att följande kan vara en lämplig ordning för förfarandet. Om Säkerhetspolisen efter beredning av ett ärende om nationell säkerhetslagring gör bedömningen att ett beslut om nationell säkerhetslagring ska fattas, ska den kalla det offentliga ombudet till ett särskilt sammanträde. Företrädare för Säkerhetspolisen ska vid sammanträdet redogöra för myndighetens överväganden och för det tilltänkta beslutet. Det offentliga ombudet ska ha möjlighet att yttra sig och ställa frågor. Ombudet ska vid sammanträdet också få ta del av de omständigheter som ligger till grund för ställningstagandet och det tilltänkta beslutet. Med hänsyn till den känsliga informationen om hotet mot den nationella säkerheten bör ett sammanträde inte

kunna ersättas av ett enbart skriftligt förfarande. Efter att det offentliga ombudet fått möjlighet att framföra sina synpunkter kan Säkerhetspolisen besluta om nationell säkerhetslagring. Säkerhetspolisen har således möjlighet att beakta de synpunkter som framförts av det offentliga ombudet och att göra justeringar i förhållande till det tilltänkta beslutet som presenterats för ombudet, exempelvis när det gäller under vilken tid beslutet ska gälla eller vilka uppgifter som ska omfattas av lagringsskyldigheten.

Inom viss tid efter att beslutet har meddelats ska det offentliga ombudet ha möjlighet att överklaga Säkerhetspolisens beslut. Vi anser att överklagandetiden inte bör vara längre än en vecka. Anledningen till att vi föreslår en så kort överklagandetid är att det ofta torde vara angeläget att den nationella säkerhetslagringen kan påbörjas så snart som möjligt efter det att hotet mot den nationella säkerheten har konstaterats. Vidare bör ett överklagande inte ta någon längre tid i anspråk för det offentliga ombudet, eftersom vi menar att det är olämpligt att ombudet i skrift utvecklar skälen för överklagandet. Om beslutet inte överklagas inom denna tid, får Säkerhetspolisen förelägga aktuella tillhandahållare att verkställa lagringsbeslutet. Säkerhetspolisens beslut bör alltså inte få verkställas dessförinnan. Det offentliga ombudets överklagande ska lämnas till Säkerhetspolisen som i sin tur ska underrätta kontrollorganet att ett beslut om nationell säkerhetslagring har överklagats. Det offentliga ombudet kan också meddela att han eller hon inte kommer att överklaga beslutet. Efter ett sådant meddelande får beslutet verkställas omedelbart. Eftersom ett sådant meddelande är bindande, bör det avges skriftligen.

Ett offentligt ombud bör få överklaga Säkerhetspolisens beslut om ersättning även i situationer när beslutet om nationell säkerhetslagring inte överklagas. Det finns i sådana situationer inget skyndsamhetskrav. Det bör därför inte föreskrivas någon överklagandefrist när enbart ett ersättningsbeslut överprövas.

Kontrollorganets beslut

För att kontrollorganet ska kunna utgöra en effektiv kontroll bör det som nämnts ovan kunna pröva om förutsättningarna för lagringsskyldigheten är uppfyllda, dvs. om hotet mot den nationella säkerheten är sådant att det kan motivera nationell säkerhetslagring och att andra villkor för lagringsskyldigheten är uppfyllda. Om kontrollorganet inte anser att ett sådant hot föreligger, ska det upphäva Säkerhetspolisens beslut. Om kontrollorganet finner att det finns förutsättningar för nationell säkerhetslagring, bör det kunna pröva om lagringsskyldigheten är författningsenlig, exempelvis att den endast omfattar sådana uppgifter som får omfattas av lagringsskyldigheten. Prövningen bör också omfatta lagringsskyldighetens proportionalitet i förhållande till det bedömda hotet. Kontrollorganet bör då kunna antingen fastställa eller upphäva lagringsbeslutet. Om kontrollorganet bedömer att lagringsskyldigheten visserligen är författningsenlig men inte proportionell, ska Säkerhetspolisens beslut alltså upphävas. Vi anser att en sådan ordning, där kontrollorganet kan antingen fastställa eller upphäva Säkerhetspolisens beslut om nationell säkerhetslagring, är att föredra framför att kontrollorganet ska kunna göra ändringar i beslutet. Kontrollorganet blir på detta sätt en mer renodlad kontrollinstans, vilket torde utesluta risken för att kontrollorganet anses vara den egentliga beslutsfattaren, vars beslut måste kunna bli föremål för en effektiv kontroll. Säkerhetspolisen bör alltid ha möjlighet att fatta ett nytt beslut om lagring, som därefter kan bli föremål för kontrollorganets prövning.

Kontrollorganets prövning bör ske vid ett sammanträde vid vilket såväl företrädare för Säkerhetspolisen som det offentliga ombudet närvarar. Inte heller vid kontrollorganets prövning bör ett sammanträde kunna ersättas av en enbart skriftlig handläggning med hänsyn till den synnerligen känsliga information som ska behandlas. Det bör inte ställas krav på sammanträde när endast ombudets ersättning prövas.

Kontrollorganet bör vid sammanträdet få del av Säkerhetspolisens beslut liksom ett underlag som redovisar de omständigheter som ligger till grund för beslutet. Företrädare för Säkerhetspolisen bör även vid detta sammanträde redogöra för myndighetens överväganden. Både kontrollorganet och det offentliga ombudet bör få ställa frågor vid sammanträdet.

Kontrollorganets beslut bör inte få överklagas. Överklagandeförbudet bör även omfatta ersättning till det offentliga ombudet.[22] Om kontrollorganet fastställer beslutet, får Säkerhetspolisen förelägga aktuella tillhandahållare att verkställa lagringsbeslutet.

Bestämmelser om offentliga ombud och förfarandet vid ärenden om nationell säkerhetslagring bör finnas i den av oss föreslagna lagen om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

7.3.5 Kontrollorganet

Utredningens förslag: Ett nytt särskilt beslutsorgan inom Säkerhets- och integritetsskyddsnämnden, Datalagringsdelegationen, ska vara kontrollorgan.

Som konstaterats ovan måste kontrollorganet kunna göra en egen bedömning av hotet mot den nationella säkerheten. Kontrollorganet bör därför ha kompetens att bedöma sådana frågor. För att utgöra en effektiv kontroll bör kontrollorganet vidare ha kompetens bl.a. när det gäller frågor om elektronisk kommunikation och om integritetsskyddsfrågor.

Nedan överväger vi för- och nackdelar med domstolar och vissa andra myndigheter och organ i rollen som kontrollorgan.

Domstolar

Ett alternativ är att den effektiva kontrollen ska utföras av domstol. En fördel med detta alternativ är att oberoendet vid en domstolsprövning är svårt att ifrågasätta. Domstolar är också vana att bedöma frågor av mycket varierande slag. Man kan överväga om kontrollen i så fall ska ske vid allmän domstol, förvaltningsdomstol eller en specialdomstol, t.ex. Försvarsunderrättelsedomstolen. Ett alternativ är också att skapa en för ändamålet särskild specialdomstol.

När det gäller allmänna domstolar och förvaltningsdomstolar kan det dock ifrågasättas om det är lämpligt att dessa domstolar ska hantera så omfattande och synnerligen känslig information. Frågor om

[22] Jfr 16 § lagen (2009:966) om försvarsunderrättelsedomstol och prop. 2008/09:201 s. 121.

nationell säkerhet hanteras inte av dessa domstolar även om det finns något enstaka undantag. Om dessa domstolar skulle få uppdraget att utgöra kontrollorgan, måste det övervägas hur kompetensbehovet hos dem bäst ska tillgodoses. Dessutom har vi ovan föreslagit en särskild ordning för prövningen som passar mindre bra hos allmänna domstolar och förvaltningsdomstolar.

Försvarsunderrättelsedomstolen eller en för ändamålet tillskapad specialdomstol framstår mot den bakgrunden som bättre alternativ än en allmän domstol eller en förvaltningsdomstol.

Att skapa en ny specialdomstol har naturligtvis den stora fördelen att den skulle kunna helt anpassas för det aktuella ändamålet. Här kan erinras om Polismetodutredningens förslag om att inrätta en särskild nämnd för beslut om tillstånd till särskilt ingripande åtgärder i underrättelseverksamhet.[23] Det finns dock starka skäl mot att skapa en ny domstol eller nämnd, särskilt de höga kostnader som är förknippade med att bilda en sådan. En domstol med en så begränsad uppgift som att vara kontrollorgan i förhållande till Säkerhetspolisens beslut om nationell säkerhetslagring är svår att administrera på ett effektivt och ändamålsenligt sätt. Det är knappast möjligt att på förhand med någon säkerhet bedöma hur stor arbetsbördan kan bli. Vidare kan det ifrågasättas om en sådan domstol, med enda uppgift att överpröva Säkerhetspolisens beslut, verkligen kan betraktas som en domstol i formell mening. Domstolar ska ägna sig åt rättskipning. Det är tveksamt om kontroll av här aktuellt slag kan anses utgöra rättskipning.

Av befintliga domstolar framstår Försvarsunderrättelsedomstolen som mest lämpad.

Försvarsunderrättelsedomstolen är en specialdomstol som prövar ansökningar om tillstånd till signalspaning i försvarsunderrättelseverksamheten. Signalspaningen ska bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för att kartlägga yttre hot mot landet. De organ som har rätt att inrikta signalspaning är regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten. Verksamheten får bara avse utländska förhållanden. Domstolen består av en ordförande, en eller högst två vice ordförande, samt minst två och

[23] Se SOU 2010:103 s. 311–313. Se även Utredningen om datalagring och EU-rättens överväganden i detta avseende i delbetänkandet *Datalagring – brottsbekämpning och integritet*, SOU 2017:75 s. 272.

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. Vid tillståndsprövningen deltar ett integritetsskyddsombud som bevakar enskildas intressen i allmänhet. Vid domstolen finns ett kansli. Domstolens verksamhet bedrivs i lokaler som hyrs av FOI.[24]

Det kan således konstateras att Försvarsunderrättelsedomstolen har kompetens när det gäller frågor om hot mot Sveriges säkerhet, även om domstolens prövningar endast avser utländska förhållanden. Vidare är Försvarsunderrättelsedomstolen van vid att hantera uppgifter som omgärdas av sträng sekretess och antalet personer knutna till domstolen är begränsat. Försvarsunderrättelsedomstolens verksamhet skulle kunna utvidgas till att vara kontrollorgan i förhållande till den beslutade lagringsskyldigheten. En variant på detta skulle kunna vara att skapa ett nytt beslutsorgan som administrativt samordnas med Försvarsunderrättelsedomstolen.

Mot Försvarsunderrättelsedomstolen som kontrollorgan talar dock att det i Sverige finns en relativt skarp gräns mellan organ på den militära respektive civila sidan och att lämpligheten av att domstolen prövar frågor som inte enbart avser utländska förhållanden kan ifrågasättas.

Ett nytt beslutsorgan inom Försvarsunderrättelsedomstolen skulle enligt vår bedömning kunna vara ett lämpligt kontrollorgan. Frågan är dock om det finns något bättre alternativ. Vi återkommer till detta nedan.

Post- och telestyrelsen

Ett annat alternativ är att kontrollfunktionen skulle utföras av PTS. Som konstaterats ovan har PTS stor kompetens vad gäller frågor om elektronisk kommunikation och i viss mån när det gäller frågor om hot mot Sveriges säkerhet. Som konstaterats ovan när det gällde PTS som behörig myndighet har PTS troligen inte den särskilda kompetens som krävs för att bedöma hotet mot Sveriges säkerhet. Det kan också ifrågasättas om PTS kan jämställas med en domstol eller

[24] Beträffande Försvarsunderrättelsedomstolen, se lagen (2009:966) om Försvarsunderrättelsedomstol. Mer information om domstolen finns på https://www.undom.se. Hämtat den 20 april 2023.

annat oberoende organ, vilket krävs enligt EU-domstolens praxis. Vi anser därför inte att PTS bör vara kontrollorgan.

Säkerhets- och integritetsskyddsnämnden

Ytterligare ett alternativ är att Säkerhets- och integritetsskyddsnämnden (SIN) skulle vara kontrollorgan i förhållande till Säkerhetspolisens beslut.

SIN leds av en nämnd. Nämnden inom SIN har tillsyn över viss brottsbekämpande verksamhet, bl.a. brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter samt Säkerhetspolisens användning av tvångsmedel vid särskild kontroll av vissa utlänningar. Nämnden utövar också tillsyn över viss personuppgiftsbehandling som utförs av Polismyndigheten, Säkerhetspolisen och Ekobrottsmyndigheten samt över Polismyndighetens och Säkerhetspolisens tillämpning av lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott. Tillsynen ska särskilt syfta till att säkerställa att verksamheten bedrivs i enlighet med lag eller annan författning. Nämnden får uttala sig om konstaterade förhållanden och sin uppfattning om behov av förändringar i verksamheten och ska verka för att brister i lag eller annan författning avhjälps. Nämnden ska ha högst tio ledamöter. Ledamöterna ska med hänsyn till omdömesförmåga, självständighet, laglydnad och övriga omständigheter vara lämpliga för uppdraget. Ordföranden och vice ordföranden ska vara eller ha varit ordinarie domare eller ha annan motsvarande juridisk erfarenhet. Övriga ledamöter ska utses bland sådana personer som har föreslagits av partigrupperna i riksdagen.

Vid SIN finns ytterligare två beslutsorgan, Registerkontrolldelegationen och Skyddsregistreringsdelegationen, samt ett kansli. Registerkontrolldelegationen har till uppgift att besluta om huruvida uppgifter som kommit fram vid registerkontroll och särskild personutredning enligt 3 kap. 19 § säkerhetsskyddslagen ska lämnas ut till en presumtiv eller befintlig arbetsgivare för dennes säkerhetsprövning. Delegationen ska även pröva frågor om utlämnande av vissa andra uppgifter. Skyddsregistreringsdelegationen har till uppgift att besluta om kvalificerade skyddsidentiteter inom den brottsbekämpande verksamheten och prövar andra frågor som hör till ärenden

om kvalificerade skyddsidentiteter. Ordföranden och vice ordföranden i de båda delegationerna ska vara eller ha varit ordinarie domare eller ha annan motsvarande juridisk erfarenhet.[25]

Det kan konstateras att nämnden inom SIN visserligen utövar tillsyn över delar av Säkerhetspolisens och Polismyndighetens verksamhet men att nämnden inte torde ha den särskilda kompetens som kommer att krävas av kontrollorganet. Vad som ytterligare kan tala mot nämnden som kontrollorgan är att flertalet ledamöter i nämnden är tillsatta för att representera allmänheten och garantera en medborglig insyn i verksamheten och att det inte ställs något krav på att ledamöterna ska ha sakkunskap i de frågor som prövas. Det är naturligtvis i och för sig möjligt att i framtiden ställa andra kompetenskrav, om man vill göra SIN till kontrollorgan, särskilt om man som nedan sägs knyter kontrollverksamheten till en ny delegation.

En fördel med SIN som kontrollorgan är att myndigheten är van att hantera uppgifter som omgärdas av sträng sekretess och att antalet personer knutna till SIN är begränsat.

Man kan visserligen överväga om det är lämpligt att SIN – som bl.a. utövar tillsyn över viss verksamhet vid Säkerhetspolisen – ska överpröva Säkerhetspolisens lagringsbeslut. En tänkbar lösning, för att undvika att överprövningen görs av själva tillsynsorganet inom SIN men också för att stärka kompetensen, skulle kunna vara att det till SIN knyts ytterligare ett beslutsorgan som har till uppgift att just utgöra kontrollorgan i förhållande till Säkerhetspolisens beslut om nationell säkerhetslagring. Det skulle kunna föreskrivas att ordföranden och vice ordföranden i ett sådant beslutsorgan ska vara eller ha varit ordinarie domare eller ha annan motsvarande juridisk erfarenhet och att övriga ledamöter ska ha den särskilda kompetens som kommer att krävas för att utöva erforderlig kontroll. Det kan i detta sammanhang noteras att nämnden och de två delegationerna inom SIN inte består av samma ledamöter. Regeringen har inte heller ansett det oförenligt att Skyddsregistreringsdelegationen beslutar i frågor om kvalificerade skyddsidentiteter samtidigt som nämnden utövar tillsyn över användningen av kvalificerade skyddsidentiteter. Vi anser sammanfattningsvis att ett nytt beslutsorgan inom SIN, med en sådan sammansättning som vi ovan nämnt, är att betrakta som ett

[25] Beträffande SIN, se lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet och förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden.

oberoende organ i den bemärkelse som EU-rätten kräver och att det framstår som ett lämpligt kontrollorgan i detta sammanhang.

Riksdagens ombudsmän

Det finns också anledning att överväga om någon myndighet under riksdagen skulle kunna vara kontrollorgan i nu aktuellt avseende. Den myndighet som ligger närmast till hands är Riksdagens ombudsmän (JO). JO granskar om myndigheter och enskilda tjänstemän följer lagar och förordningar. Ombudsmännen torde dock inte ha den särskilda kompetens som kan krävas av kontrollorganet. Vidare ter sig uppgiften att överpröva och kunna upphäva den behöriga myndighetens beslut som främmande och kanske även förtroendeskadligt för ett extraordinärt tillsynsorgan som JO. JO framstår därför inte som ett lämpligt kontrollorgan i detta sammanhang.

Regeringen

Slutligen finns alternativet att regeringen ska utgöra kontrollorgan i förhållande till Säkerhetspolisens beslut. Som vi tidigare anfört gällande valet av behörig myndighet (se avsnitt 7.3.1) förefaller uppgiften att bedöma hotet mot den nationella säkerheten som en naturlig uppgift för det organ som styr riket, dvs. regeringen. Regeringen har som nämnts ovan möjlighet att få relevant information från alla myndigheter och torde alltså kunna få den mest kompletta bilden av hotet mot Sveriges säkerhet. Exempelvis anges i 8 § förordningen (2014:1103) med instruktion för Säkerhetspolisen att underrättelser som kan ha betydelse för Sveriges säkerhet eller som av annan anledning bör komma till regeringens kännedom utan dröjsmål ska rapporteras till Regeringskansliet (Justitiedepartementet) på det sätt som regeringen närmare bestämmer.

Den allmänna trenden har under lång tid varit att flytta hanteringen av enskilda ärenden från regeringen till i första hand någon förvaltningsmyndighet. Det har ansetts att regeringen inte bör ägna sig åt beslutsfattande i enskilda fall utan att detta lämpar sig bättre för en förvaltningsmyndighet. Syftet är att regeringen ska avlastas prövningen av förvaltningsärenden.[26] Med hänsyn till arten och vik-

[26] Se betänkandet En ny rymdlag SOU 2021:91 s. 172.

ten av det beslut som ska överprövas kan man dock knappast påstå att en sådan prövning kan jämställas med ett sedvanligt förvaltningsärende. Det kan också konstateras att regeringen är beslutsfattare i vissa näraliggande frågor, exempelvis i vissa frågor enligt lagen om särskild kontroll av vissa utlänningar.

Vi menar dock att regeringen inte kan jämställas med en domstol eller annat oberoende organ, vilket krävs enligt EU-domstolens praxis. Vi anser därför sammanfattningsvis att regeringen inte bör vara kontrollorgan i nu aktuellt avseende.

Vår bedömning avseende lämpligt kontrollorgan

Av de alternativ som vi ovan övervägt anser vi att Försvarsunderrättelsedomstolen och ett nytt beslutsorgan inom SIN framstår som de mest lämpliga myndigheterna att utgöra kontrollorgan. Fördelen med Försvarsunderrättelsedomstolen är att den redan har kompetens att bedöma hot mot den nationella säkerheten och att pröva integritetskyddsaspekter. Det finns dessutom en ordning med integritetsskyddsombud som skulle kunna fylla den av oss föreslagna funktionen med offentliga ombud. Däremot skulle domstolen behöva tillföras kompetens när det gäller t.ex. behovet av uppgifter om elektronisk kommunikation i brottsbekämpande verksamhet och om hur tillhandahållarnas verksamhet påverkas av lagringsbesluten.

Ett nytt beslutsorgan inom SIN kan utformas så att det säkerställs att rätt kompetens finns hos ledamöterna. Vi anser att ett nytt beslutsorgan inom SIN framstår som ett bättre alternativ än Försvarsunderrättelsedomstolen, eftersom såväl nämnden som beslutsorganen inom SIN hanterar frågor som rör brottsbekämpning och att SIN redan har ett etablerat samarbete med Säkerhetspolisen vad gäller praktiska frågor kring hantering av känslig information. Ett nytt beslutsorgan inom SIN riskerar inte heller en sammanblandning av uppgifter och myndigheter på den militära respektive den civila sidan.

Det kan i detta sammanhang nämnas att SIN är en tämligen liten myndighet som successivt har fått ett alltmer omfattande uppdrag. SIN har påtalat att det finns ett behov av en översyn av myndighetens organisation innan fler beslutsorgan knyts till myndigheten, bl.a. när det gäller frågan om myndighetens ledning i förhållande till

de särskilda beslutsorganen. Vi anser dock inte att denna omständighet i sig påverkar lämpligheten av att ytterligare ett beslutsorgan knyts till SIN i avvaktan på en sådan översyn.

Det särskilda beslutsorganet kan lämpligen kallas Datalagringsdelegationen.

Regleringen avseende Säkerhets- och integritetsskyddsnämnden

Det bör i den av oss föreslagna lagen om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet anges att Säkerhetspolisens beslut om nationell säkerhetslagring kan överklagas till SIN och, för tydlighetens skull, att SIN:s beslut inte får överklagas.

Det bör också i förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden göras ändringar. Det bör införas en ny paragraf, 3 a §, som anger att myndigheten har till uppgift att överpröva beslut om nationell säkerhetslagring. Det innebär att en följdändring behövs i 1 §, som anger vilka uppgifter myndigheten har. Vidare bör det i 8 § anges att det inom myndigheten ska finnas tre, i stället för två särskilda beslutsorgan, och att Datalagringsdelegationen ska pröva frågor som avser i 3 a §. I 8 § andra stycket anges att varje delegation består av en ordförande, en vice ordförande samt högst tre andra ledamöter. Detta bör kunna gälla även för Datalagringsdelegationen. Någon ändring av denna bestämmelse behövs därför inte. SIN:s kansli bör ansvara för kallelser till och protokollföring vid Datalagringsdelegationens sammanträden, expediering av delegationens beslut samt för utbetalning av arvoden och reseersättning till delegationens ledamöter och det offentliga ombudet. Kansliet bör också ansvara för Datalagringsdelegationens diarium och arkiv. Säkerhetspolisens beslut och det underlag för beslutet som ska finnas tillgängligt vid delegationens sammanträde ska dock inte diarieföras och arkiveras hos SIN. Sådana handlingar ska återlämnas till Säkerhetspolisen efter delegationens beslut. För att understryka delegationens självständighet i förhållande till Säkerhetspolisen, bör delegationens sammanträden hållas i SIN:s lokaler. En annan ordning kan dock vara nödvändig till dess SIN har ordnat för ändamålet adekvata sammanträdeslokaler.

I 13 § bör det anges att även ledamöterna i Datalagringsdelegationen ska utses av regeringen för en bestämd tid, att ordföranden och vice ordföranden ska vara eller ha varit ordinarie domare eller ha annan motsvarande juridisk erfarenhet och att det bland de övriga ledamöterna ska finnas särskild erfarenhet av integritetsskyddsfrågor, av frågor som avser elektronisk kommunikation och av verksamhet som avser nationell säkerhet. Slutligen bör det i förordningen införas en ny rubrik om handläggningen av ärenden i Datalagringsdelegationen. Under denna rubrik bör det införas två bestämmelser, 26 a och 26 b §§. I dessa paragrafer bör det anges att Datalagringsdelegationen ska sammanträda så snart som möjligt efter det att ett beslut om nationell säkerhetslagring har överklagats samt att delegationen är beslutsför när ordföranden och minst två andra ledamöter är närvarande samt att, för det fall både ordföranden och vice ordföranden i delegationen har förhinder, nämndens ordförande får träda in som delegationens ordförande. Någon möjlighet för delegationens ordförande eller vice ordförande att ensam överpröva beslut om nationell säkerhetslagring bör inte finnas, inte ens i brådskande fall.

7.3.6 Lagringsskyldighetens omfattning

Utredningens bedömning: Det finns förutsättningar för att nationell säkerhetslagring kan innebära en mer omfattade lagringsskyldighet än den som gäller i dag.

Utredningens förslag: Ramarna för vad lagringsskyldigheten får omfatta ska framgå av lag och de mer detaljerade föreskrifterna av förordning.

Lagringstiden ska vara två år från den dag kommunikationen avslutades. Om tillhandahållarna saknar uppgift om när kommunikationen avslutades, ska lagringstiden räknas från den dag då uppgiften genererades.

Lagringsskyldigheten får även omfatta uppgifter som genereras eller behandlas vid misslyckad uppringning.

Under vissa förutsättningar finns det, som nämnts ovan, en möjlighet att besluta om en generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter. Vi har ovan föreslagit att Säkerhetspolisen

som behörig myndighet ska kunna förelägga tillhandahållarna en sådan lagringsskyldighet under en begränsad tid. Både gränserna för och det närmare innehållet i ett sådant lagringsbeslut bör, som nämnts ovan, regleras i författning.

Som även nämnts tidigare bör den behöriga myndigheten kunna besluta vilka tillhandahållare som ska omfattas av lagringsskyldigheten. Den som ska anmäla sin verksamhet enligt 2 kap. 1 § nya LEK bör kunna omfattas av ett sådant föreläggande. Vi återkommer i avsnitt 9 till frågan om tillhandahållare av nummeroberoende interpersonella kommunikationstjänster ska kunna omfattas av lagringsskyldigheten.

Arbetet med att bekämpa brott mot Sveriges säkerhet

För att bedöma lagringsskyldighetens omfattning i stort bör något sägas om arbetet med att bekämpa brott mot Sveriges säkerhet. Det är framför allt Säkerhetspolisens uppgift att bekämpa brottslighet som rör Sveriges säkerhet. Men även Polismyndighetens uppdrag omfattar bekämpning av sådan brottslighet. En del av den brottslighet som Polismyndigheten har i uppdrag att bekämpa kan vara systemhotande på sådant sätt att den utgör ett hot mot den nationella säkerheten. Polismyndigheten kan också överta en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen (se vidare avsnitt 7.3.7). Även andra myndigheter har brottsbekämpande uppgifter som rör hotet mot den nationella säkerheten. Det kan exempelvis nämnas att Tullverket har befogenhet att förhindra och utreda terroristbrott enligt 4 § terroristbrottslagen (2022:666) som begås genom vissa smugglingsbrott.[27]

Säkerhetspolisen får sällan in anmälningar från allmänheten om begångna brott. I stället måste myndigheten själv i underrättelsearbetet dels leta efter intressanta personer och grupperingar samt företeelser, skeenden och modus som är eller som senare kan komma att utvecklas till brottslighet kopplad till nationell säkerhet, dels ta ställning till bl.a. tips och information om hot som myndigheten får del av. Underrättelseverksamheten är därför tyngdpunkten i Säkerhetspolisens bekämpning av t.ex. spionerи och terrorism.

[27] Se 1 § lagen (2000:1225) om straff för smuggling.

En mycket stor del av de utredningar eller annat arbete som Säkerhetspolisen genomför, såväl i underrättelsearbetet som i förundersökningar, har en koppling till kvalificerade aktörer som är tränade och styrda av främmande makt eller av större organisationer, 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 faktiskt görs, samt att analysera vilka slutsatser som kan dras av dessa.

Brott mot nationell säkerhet, som spioneri och terrorism, är speciella till sin karaktär i den meningen att brottsligheten ofta pågår under mycket lång tid. För främmande makt kan det ta flera år att värva en agent med tillgång till skyddsvärd information. Brottsligheten är utdragen i tiden och sker i flera steg med faser som karaktäriseras av analys, målsökning, kartläggning, närmande, vänskap, värvning och inhämtning av information. Även terrorism präglas av att brottsligheten många gånger är utdragen i tiden och att den sker i samverkan mellan flera. En process där en person utvecklas till en ideologiskt motiverad aktör med terroravsikt kan ta lång tid. Dessutom måste personen skaffa sig förmåga att planera och fullborda brott. Det är ofta inte möjligt att redan i ett inledningsskede av kartläggningsarbetet förutse vilka trafik- och lokaliseringsuppgifter som bör inhämtas.

En mer omfattande lagringsskyldighet än i dag behövs för att skydda Sveriges säkerhet

EU-rätten reglerar lagringen av trafik- och lokaliseringsuppgifter på en övergripande nivå. Det ankommer på medlemsstaterna att reglera lagringens omfattning till vad som är strängt nödvändigt. Bedömningen när det gäller lagringen av, och i senare led även tillgången till, uppgifterna behöver göras med utgångspunkt från sedvanliga principer som gäller enligt svensk rätt.

De författningsändringar som gjordes i Sverige år 2019, om en begränsning i lagringsskyldigheten för teleoperatörer, syftade till att tillgodose det EU-rättsliga kravet på att lagringsskyldigheten inte får vara generell och odifferentierad. Några särskilda överväganden kring vilka uppgifter som får lagras för nationell säkerhet gjordes inte då.

Det ansågs vid tidpunkten vara oklart om EU-rätten var tillämplig på området nationell säkerhet i fråga om datalagring.[28]

När det föreligger ett allvarligt hot mot den nationella säkerheten får lagringsskyldigheten däremot vara generell och odifferentierad och följaktligen bör ramarna för en sådan lagringsskyldighet vara vidare än vad som gäller enligt dagens reglering, både när det gäller vilka uppgifter som kan lagras och själva lagringstiden.

Den lagstiftning som infördes 2019 innebär att vissa typer av uppgifter inte längre omfattas av lagringsskyldigheten och att lagringstiden har differentierats (se jämförelsetabell i bilaga 3 för en översiktlig beskrivning av lagringsskyldigheten).

När det gäller *telefonitjänster och meddelandehantering* gäller lagringsskyldigheten i dag enbart kommunikation via mobil nätanslutningspunkt. Före reformen 2019 omfattades uppgifter från såväl fast telefoni som fast ip-telefoni av lagringsskyldigheten. Lagringsskyldigheten omfattade tidigare också flera slags uppgifter vid kommunikation via mobil nätanslutningspunkt än vad som i dag är fallet.[29]

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 den enskilde får internetåtkomst t.ex. fast fiberanslutning. Den nu gällande lagringsskyldigheten avseende internetåtkomst är också mer teknikneutral än tidigare. Anledningen till denna förändring var att möjligheten att kunna koppla en användare till en viss uppgift inte skulle vara beroende av vilken teknik en tjänsteleverantör använder sig av. Till exempel har det blivit vanligare att leverantörerna använder sig av s.k. NAT-teknik (se avsnitt 9.3). Till skillnad från tidigare omfattas därför t.ex. uppgifter om portnummer och tidsangivelser av den nu gällande lagringsskyldigheten.

För att tillgodose myndigheternas behov av uppgifter för att bekämpa brott mot Sveriges säkerhet behöver, för det första, samtliga uppgiftskategorier som togs bort genom 2019 års lagstiftning kunna omfattas av ett föreläggande om lagring i syfte att skydda den nationella säkerheten. För det andra har den tekniska utvecklingen i vårt samhälle medfört att uppgiftskategorierna behöver uppdateras. I många situationer leder användning av en viss teknik eller tjänst till att det

[28] Se prop. 2018/19:86 s. 19.
[29] Uppgifter om lokalisering vid meddelandehantering omfattas dock av den nu gällande lagringsskyldigheten, vilket inte tidigare var fallet.

i efterhand kan vara svårt att få tillgång till uppgifter som är av betydelse för brottsbekämpningen, inte minst när det gäller brott som rör nationell säkerhet.

Vi föreslår dock inte någon lagring av trafikuppgifter för ip-adresser. Vi hänvisar till avsnitt 6.6.1 för en närmare redogörelse av skillnaden mellan en abonnemangsuppgift kopplad till en ip-adress och trafikuppgifter kopplade till en ip-adress.

Trafikuppgifter koppade till en ip-adress kan användas för att kartlägga en internetanvändares online-aktivitet. Sådan aktivitet kan även indirekt avslöja innehållet i aktiviteten, exempelvis då en viss webbsida har besökts. Inte ens för syftet nationell säkerhet framstår det emellertid som försvarligt att lagra sådana uppgifter. Härutöver skulle den mängd trafikdata som behöver lagras bli stor.

Vårt ställningstagande innebär alltså att skyldigheten att lagra trafik- och lokaliseringsuppgifter i syfte att skydda den nationella säkerheten ska kunna omfatta fler uppgiftskategorier än i dag och även uppgifter som tidigare inte omfattades av den svenska lagringsskyldigheten. Nedan redogör vi i detalj för uppgifterna. I sammanhanget är det viktigt att påpeka att den uppgiftslagring som ägde rum före 2019 års ändringar i huvudsak byggde på dataskyddsdirektivet som kom till år 2006. Såväl teknikutveckling och enskildas kommunikationsmönster som ändamålet med lagringen, dvs. Sveriges nationella säkerhet, motiverar att fler uppgifter än tidigare ska kunna lagras.

Principer för lagringsskyldighetens omfattning

Enligt vår bedömning bör fyra huvudprinciper styra hur lagringsskyldigheten ska utformas.

För det *första* ska lagringens omfattning inte vara mer långtgående än vad som är absolut nödvändigt för det angivna syftet. Vi har i avsnitt 7.3.1 beskrivit EU-rättens krav på proportionalitet. Enligt EU-domstolen innebär kravet bl.a. 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. Under senare år har EU-domstolen återkommande tagit upp kravet på proportionalitet i sina avgöranden om datalagring.[30]

Tolkningen av EU-rätten måste utgå från EU-domstolens samlade budskap om vilka förutsättningar som ska vara uppfyllda för att lagring ska få ske. Enligt vår mening kan inte EU-domstolens domar tolkas på annat sätt än att kravet på proportionalitet också gäller frågor om den nationella säkerheten. Vår utgångspunkt är vidare att kravet på proportionalitet gäller alla aspekter av lagring som syftar till att skydda den nationella säkerheten.

För det *andra* bör regleringen utarbetas på en övergripande nivå. Vi vill därigenom frångå detaljregleringen i förhållande till hur enskilda kommunicerar med varandra och vilken specifik teknik eller tjänst de använder. I det här perspektivet saknar det nämligen betydelse om kommunikation sker genom fast telefoni, mobiltelefoni, ip-telefoni, eller en nummeroberoende interpersonell kommunikationstjänst. Det centrala är att det sker någon form av *kommunikation* och att någon har tillhandahållit *medel för kommunikationen*. Härutöver föreslår vi nedan att även lokaliseringsuppgifter som inte är trafikuppgifter ska kunna omfattas av ett föreläggande om nationell säkerhetslagring. I dessa fall är lagringsskyldigheten inte beroende av att någon kommunikation äger rum. Lagringsskyldighetens utformning ska således ske utifrån kommunikation och tillgång till infrastruktur för kommunikation.

För att ta ställning till vilka uppgifter som ska kunna omfattas av ett föreläggande om nationell säkerhetslagring menar vi att urvalet bör göras på så sätt att följande frågor alltid kan besvaras i efterhand, oavsett vilken typ av kommunikation det är fråga om.

1. Vem kommunicerade med vem?
2. När ägde kommunikationen rum?
3. Var fanns användarnas utrustning?
4. Vilken typ av kommunikation var det fråga om?

Ovanstående bör enligt vår mening utgöra ramen för vad lagringsskyldigheten kan omfatta och bör regleras i lag.

[30] Se SpaceNet-domen p. 69, Garda Síochána-domen p. 54 och La Quadrature du Net-domen p. 132.

För det *tredje* bör regleringen vara sådan att lagringsskyldighetens omfattning inte påverkas av användarens utrustning. På samma sätt som tidigare menar vi att det väsentliga är att någon har kommunicerat med en annan. Om kommunikationen har skett genom t.ex. en mobiltelefon, en dator eller en surfplatta är av underordnad betydelse. I praktiken kommer emellertid den utrustning som används att generera olika typer av uppgifter. De uppgifter som genereras när en mobiltelefon används kommer att skilja sig från de uppgifter som genereras vid användning av en dator. Utformningen bör dock vara teknikneutral och omfatta de uppgifter som genereras och behandlas i tillhandahållarnas verksamhet.

För det *fjärde* ska regleringen av lagringsskyldighetens omfattning utgå från tillhandahållarnas verksamhet. Dagens lagringsskyldighet omfattar uppgifter som genereras eller behandlas i tillhandahållarens verksamhet. Det betyder att leverantören inte har någon skyldighet att införskaffa uppgifter som denne annars inte genererar eller behandlar. Med behandling avses här alla typer av åtgärder, inklusive radering eller förstöring.[31] Däremot ska en uppgift lagras så fort den har funnits hos leverantören, även om det bara rör sig om en ytterst kort tid.[32] Vår utgångspunkt är att även ett föreläggande om nationell säkerhetslagring ska omfatta endast sådana uppgifter som behandlas i tillhandahållarnas verksamhet. Vi bedömer att det vore oproportionerligt om tillhandahållarna skulle behöva inhämta och behandla sådana uppgifter som kan behövas för att bekämpa hot mot den nationella säkerheten men som de själva inte får del av i sin verksamhet.

Detta ställningstagande kan dock i framtiden behöva omprövas, om det visar sig att tillhandahållare exempelvis bygger om sina tjänster i syfte att undgå lagringsskyldigheten.

En fråga som bör uppmärksammas är att tillhandahållare i enlighet med artikel 25 i EU:s dataskyddsförordning har en skyldighet att implementera funktioner för dataskydd i sina tjänster, dvs. inbyggt dataskydd (Privacy by design). Bestämmelserna om dataskydd gäller i tillhandahållarnas verksamhet enligt 1 kap. 5 § nya LEK när de behandlar personuppgifter. För nummeroberoende kommunikationstjänster har det tidigare inte funnits någon lagringsskyldighet. En sådan kommunikationstjänst kan därför vara utformad så att trafik- och

[31] Jfr artikel 2 i e-dataskyddsdirektivet, 1 kap. 5 § nya LEK och artikel 4 i EU:s dataskyddsförordning.
[32] Se prop. 2010/11:46 s. 77.

lokaliseringsuppgifter raderas när uppgifterna har behandlats för att leverera tjänsten. Våra förslag innebär en förändring för tillhandahållare av Noik, i den mån de behandlar personuppgifter som också är trafik- och lokaliseringsuppgifter, och omfattas av våra förslag om lagringsskyldighet. Se mer om lagringsskyldighet för tillhandahållare av Noik i avsnitt 9.

Regleringen i EU:s dataskyddsförordning fråntar inte leverantörerna deras ansvar för lagring av trafik- och lokaliseringsuppgifter enligt nya LEK. Funktionalitet för dataskydd ska utformas på ett sådant sätt att lagringsskyldigheten kan uppfyllas. Tillhandahållarna får därför inte radera uppgifter som vid något tillfälle har behandlats av dem, om det finns en lagringsskyldighet för uppgifterna. Det undantar samtidigt inte deras skyldigheter i övrigt att minimera förekomsten av personuppgifter i tjänster och it-stöd, i delar som inte rör lagring av trafik- och lokaliseringsuppgifter.

Vi föreslår att detsamma ska gälla i de fall uppgifterna omfattas av ett föreläggande om nationell säkerhetslagring. Det blir således inte tillåtet för en tjänsteleverantör att utforma sina tjänster på ett sådant sätt att trafik- och lokaliseringsuppgifter som träffas av en lagringsskyldighet omedelbart förstörs, raderas, eller avidentifieras. Det spelar ingen roll om åtgärden sker på teknisk nivå, i ett inledande skede, eller utan mänsklig inblandning.

Det bör avslutningsvis påtalas att vad vi beskrivit ovan inte förändrar möjligheten för tillhandahållarna att uppdra åt någon annan att utföra lagringen enligt 9 kap. 19 § fjärde stycket nya LEK.

Uppgifter som omfattas av lagringsskyldigheten

Med utgångspunkt i de principer som vi redogjort för ovan bör följande uppgifter kunna omfattas av ett föreläggande om nationell säkerhetslagring. Vilka uppgifter som kan omfattas av lagringsskyldigheten bör regleras i nya LEK och preciseras i förordning.

1. Vem kommunicerade med vem?
   - Telefonnummer, ip-adress eller annan meddelandeadress.
   - Abonnemangs-, konto- eller utrustningsidentitet och kopplingen mellan permanenta och tillfälliga identifierare.
   - Uppgifter om abonnent och registrerad användare.

- Uppgifter som krävs för att identifiera slutmålet för kommunikationen i de situationer där den som avskiljer kommunikationen inte omfattas av lagringsskyldighet, exempelvis när kommunikationen övergår från tjänsteleverantörens nät till ett företagsnätverk.

2. När ägde kommunikationen rum?
   - Datum och spårbar tid för då samtalet påbörjades och avslutades, då ett meddelande skickades och togs emot, eller då viss internettrafik ägde rum.
3. Var fanns användarnas utrustning?
   - Lokaliseringsuppgifter vid kommunikation eller internetåtkomst, alltså inte endast vid kommunikationens början och slut.
   - Övriga lokaliseringsuppgifter som inte är trafikuppgifter (t.ex. satellitpositioneringsuppgifter som genererats i utrustningen).
4. Vilken typ av kommunikation var det fråga om?
   - Uppgifter om den eller de tjänster som använts.
   - Uppgift om kapacitet för överföring (t.ex. fast bredband via fiber).

Lagringsskyldigheten får även omfatta uppgifter som genereras eller behandlas vid misslyckad uppringning, dvs. uppringning som kopplas fram utan att nå en mottagare.

Våra förslag innebär att brottsbekämpande myndigheter genom straffprocessuella tvångsmedel i vissa fall kan få tillgång till lokaliseringsuppgifter som inte är trafikuppgifter. Sådana uppgifter genereras i användarens utrustning och överförs till tillhandahållaren oavsett om utrustningen används för samtal och meddelandehantering. Satellitpositioneringsuppgifter som genererats i utrustningen kan vara en sådan. Med satellitpositioneringsuppgifter avses exempelvis gpspositioner från det amerikanska systemet eller det europeiska systemet Galileo (GNSS).

Lokaliseringsuppgifter som inte är trafikuppgifter kan också avse olika typer av signaleringsuppgifter som genereras i en mobiltelefon eller i ett mobiltelefoninät. Det kan exempelvis vara fråga om periodiska uppdateringar, registrering- och bortkoppling från mobilnätet

och andra uppgifter som genererats i syfte att initiera, upprätthålla och avsluta sessioner och tjänster under pågående internetåtkomst.

Lagring av sådana uppgifter kommer att underlätta kartläggning av var enskilda har befunnit sig eftersom det i vissa fall räcker att utrustningen är påslagen och uppkopplad mot ett nätverk. Våra förslag innebär dock inte att samtliga sattelitpositioneringsuppgifter och signaleringsuppgifter ska lagras. En sådan lagring skulle bli alltför omfattande med hänsyn till antalet enheter och antalet uppgifter som genereras. Många lokaliseringsuppgifter skulle dessutom vara identiska när kommunikationsutrustningen är stillastående, exempelvis under nattetid då många användare sover.

Det bör därför göras ett urval bland de lokaliseringsuppgifter som ska lagras. Ett sådant urval kan dock behöva utvärderas och omvärderas med hänsyn till den snabba tekniska utvecklingen och den utrustning som för tiden används. Enligt vår bedömning är det därför inte lämpligt att i författning närmare precisera mängden uppgifter som ska lagras när det gäller lokaliseringsuppgifter som inte är trafikuppgifter. Det bör i stället ankomma på PTS att utforma en närmare reglering på området. Lämpligen bör en sådan reglering föregås av samråd med de brottsbekämpande myndigheterna och vid behov tillhandahållarna.

Lokaliseringsuppgifter som inte är trafikuppgifter omfattas inte av den lagringsskyldighet som gäller i dag och omfattades inte heller av den tidigare gällande lagringsskyldigheten. I praktiken innebär dock våra förslag inte någon större skillnad än dagens reglering för lagring som sker av traditionella teleoperatörer. Det har sin grund i den teknikutveckling som har ägt rum. En modern mobiltelefon lämnar vid samtal eller datatrafik kontinuerlig uppgift om plats när den används i ett traditionellt telenät. Det är framför allt tillhandahållare av Noik som påverkas. Vårt förslag utjämnar skillnaden mellan användning av Noik och traditionella kommunikationstjänster.

Lokaliseringsuppgifter kan vara av stor, i vissa fall rent av avgörande, betydelse för att bekämpa hot mot den nationella säkerheten. Vi bedömer att det är strängt nödvändigt att lagringsskyldigheten ska kunna omfatta var användarnas utrustning fanns. En lagring av lokaliseringsuppgifter som inte är trafikuppgifter innebär ett ytterligare intrång i enskildas personliga integritet. Vi återkommer till denna fråga i vår konsekvensanalys, se avsnitt 13.

Vi bedömer i övrigt att en lagringsskyldighet i enlighet med våra förslag är proportionerlig, eftersom lagringen påbörjas först när Sverige står inför ett allvarligt hot mot den nationella säkerheten som är verkligt och aktuellt eller förutsebart. Som tidigare reglering bör ramarna för vad lagringsskyldigheten kan omfatta framgå av lag och de mer detaljerade föreskrifterna av förordning. I beslutet om nationell säkerhetslagring framgår slutligen vad som, inom de ramarna, ska lagras.

Det bör påpekas att de typer av uppgifter om elektronisk kommunikation som omfattas av lagringsskyldigheten i 9 kap. 19 § nya LEK regleras genom en hänvisning till tystnadsplikten i 9 kap. 31 § första stycket 1 och 3, dvs. uppgift om abonnemang och annan uppgift som angår ett särskilt elektroniskt meddelande. Vi har dock i avsnitt 6.6.2 föreslagit att uttrycket *annan uppgift som angår ett särskilt elektroniskt meddelande* ersätts av uttrycket *trafikuppgift*.

Tystnadsplikten i 9 kap. 31 § nya LEK gäller inte för lokaliseringsuppgifter som inte är trafikuppgifter. Det har sin grund i att sådana uppgifter, om de rör användare som är fysiska personer eller abonnenter, får behandlas endast sedan de har avidentifierats eller användaren eller abonnenten har gett sitt samtycke till behandlingen (se 9 kap. 7 § nya LEK). I avsnitt 7.3.9 föreslår vi bl.a. att lokaliseringsuppgifter som inte är trafikuppgifter och som rör användare som är fysiska personer eller abonnenter ska omfattas av tillhandahållarnas tystnadsplikt. Vi återkommer till frågan om tillhandahållarnas behandling av lokaliseringsuppgifter som inte är trafikuppgifter i avsnitt 7.3.8.

Upplysning om verkställighetsföreskrifter

I 9 kap. 23 § nya LEK finns en upplysning om att regeringen eller den myndighet som regeringen bestämmer får meddela närmare föreskrifter om vilka uppgifter som ska lagras enligt 19 § och om lagringstiden enligt 22 § första stycket.

Upplysningsbestämmelser om verkställighetsföreskrifter är enligt Lagrådet inte nödvändiga. Regeringen har dock gjort bedömningen att upplysningsbestämmelsen i 9 kap. 23 § nya LEK kan bidra till att

regleringen blir transparent och tydlig.[33] Vi saknar skäl att nu göra en annan bedömning.

Vi föreslår att tillhandahållarnas lagringsskyldighet ska regleras i andra paragrafer än 9 kap. 19 § nya LEK. Bestämmelsen i 9 kap. 23 § bör därför anpassas till våra förslag.

Lagringstiden

Enligt den tidigare gällande lagringsskyldigheten, alltså före 2019 års lagstiftning, skulle alla slags uppgifter lagras i sex månader räknat från den dag kommunikationen avslutades. Enligt den nu gällande lagringsskyldigheten gäller olika lagringstider för olika slags uppgifter, allt räknat från den dag kommunikationen avslutades. Uppgifter 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 endast 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 dock lagras i endast sex månader.

Vi har ovan föreslagit att ett föreläggande om nationell säkerhetslagring ska kunna gälla i högst ett år. Frågan är då hur länge de uppgifter som omfattas av ett sådant föreläggande ska lagras hos den lagringsskyldige. Ett alternativ är att alla uppgifter som omfattas av ett föreläggande om nationell säkerhetslagring ska lagras så länge som föreläggandet gäller och därefter omedelbart raderas. Uppgifter lagrade kort tid efter beslutet skulle i sådant fall lagras under nästan ett år medan de uppgifter som lagras under föreläggandets sista dag skulle raderas redan dagen därpå. Om ett beslut om nationell säkerhetslagring skulle förlängas, blir följden att alla uppgifter fortsatt ska lagras under den tid den nationella säkerhetslagringen gäller. En reglering som den här beskrivna framstår inte som helt logisk.

[33] Se prop. 2021/22:136 s. 326.

Vi anser att ett bättre alternativ är att lagringstiden regleras separat och att den liksom i dag räknas från den dag kommunikationen avslutades. Om tillhandahållaren saknar uppgift om när kommunikationen avslutades, ska lagringstiden i stället utgå från när uppgifterna genererades. I fråga om lokaliseringsuppgifter som inte är trafikuppgifter bör lagringstiden i stället räknas från då uppgifterna genererades. Med en sådan ordning raderas uppgifterna löpande när lagringstiden går ut. Det innebär visserligen att uppgifter kommer att lagras även efter det att ett föreläggande om nationell säkerhetslagring har upphört att gälla, men vi ser inga principiella hinder mot detta.

När det gäller frågan om hur lång lagringstiden ska vara har EU-domstolen slagit fast att lagringstiden ska fastställas på objektiva grunder och begränsas till vad som är strängt nödvändigt. De brottsbekämpande myndigheterna har påtalat vikten av att uppgifter lagras under en längre tid än i dag. Vi bedömer att lagringstiden vid ett föreläggande om nationell säkerhetslagring bör, med hänsyn till arten av den brottslighet som ska bekämpas, vara betydligt längre än vad som i dag är fallet. När det gäller brottslighet som t.ex. spionerі, som typiskt sett pågår under lång tid, kan mycket gamla uppgifter vara avgörande för att exempelvis kunna analysera mönster i kommunikationen. Men för att lagringstiden inte ska riskera att bli längre än vad som är strängt nödvändigt, måste den emellertid begränsas. En sådan begränsning kan innebära att äldre uppgifter, som visserligen är avgörande för bekämpningen av brott mot Sveriges säkerhet, inte blir tillgängliga för de brottsbekämpande myndigheterna när behovet av uppgifterna uppstår. Vid en proportionalitetsbedömning anser vi att lagringstiden bör vara två år. Det bör förtydligas att uppgifter kan vara lagrade även efter det att ett föreläggande om nationell säkerhetslagring har upphört. Det har sin grund i att uppgifterna genereras löpande under hela den tid föreläggandet gäller.

För att syftet med lagringen ska kunna uppnås på bästa sätt behövs en helhetsbild. Olika typer av uppgifter bör därför inte ha olika lång lagringstid även om uppgifternas känslighetsgrad kan variera. Under sådana förhållanden bör samma lagringstid gälla för alla typer av uppgifter.

Vi anser att lagringstiden vid nationell säkerhetslagring bör föreskrivas i författning. Det är nämligen knappast möjligt att i ett enskilt beslut om nationell säkerhetslagring också besluta om lagringstid, eftersom det normalt inte går att veta hur länge uppgifterna kan

behövas. Det skulle också vara besvärligt för tillhandahållarna att behöva anpassa sina system när det gäller gallring av uppgifter efter varje enskilt beslut om lagring.

7.3.7 Tillgången till lagrade uppgifter

Några utgångspunkter

Som nämnts tillåter EU-rätten under vissa förutsättningar en lagstiftning som ger behöriga myndigheter rätt att ålägga tillhandahållare en generell och odifferentierad lagringsskyldighet under en begränsad tid avseende trafik- och lokaliseringsuppgifter, om det sker i syfte att skydda nationell säkerhet. Samtidigt har EU-domstolen klargjort att uppgifter som har lagrats för att skydda den nationella säkerheten inte kan användas inom ramen för straffrättsliga förfaranden i syfte att bekämpa allvarlig brottslighet. I SpaceNet-domen gör EU-domstolen följande uttalande.

> (130) Dessutom och framför allt kan trafik- och lokaliseringsuppgifter, i enlighet med den rättspraxis som det erinrats om i punkt 74 i förevarande dom, inte lagras på ett generellt och odifferentierat sätt i syfte att bekämpa grov brottslighet, och tillgång till dessa uppgifter kan således inte motiveras av dessa syften. När dessa uppgifter undantagsvis har lagrats på ett generellt och odifferentierat sätt, i syfte att skydda den nationella säkerheten mot ett verkligt och aktuellt eller förutsebart hot, under de förutsättningar som anges i punkt 71 ovan, kan de nationella brottsbekämpande myndigheterna inte ha rätt att få tillgång till dessa uppgifter inom ramen för straffrättsliga förfaranden, eftersom det skulle betyda att förbudet mot en sådan lagring i syfte att bekämpa allvarlig brottslighet, som det erinras om i punkt 74 ovan, förlorade sin ändamålsenliga verkan (dom av den 5 april 2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, punkt 100).

Mot bakgrund av den terminologi som i övrigt används i domen uppkommer frågan vad som avses med *straffrättsliga förfaranden* i detta sammanhang. Uttrycket förekommer inte i e-dataskyddsdirektivet men används i många rättsakter inom det straffrättsliga samarbetet inom EU. Det finns i dessa rättsakter inte någon definition av straffrättsliga förfaranden och uttrycket har heller inte harmoniserats i

EU:s lagstiftning.[34] Innebörden får därför tolkas med ledning av den rättsakt där uttrycket förekommer. Tolkningen av uttrycket straffrättsligt förfarande har övervägts i lagstiftningsärenden gällande genomförande av nämnda rättsakter. Vid genomförandet av Europaparlamentets och rådets direktiv 2010/64/EU av den 20 oktober 2010 om rätt till tolkning och översättning vid straffrättsliga förfaranden gjordes bedömningen att direktivets krav omfattar de förfaranden som kan mynna ut i en brottspåföljd och att det ska finnas bestämmelser i svensk rätt som uppfyller direktivets krav vid handläggningen av brottmål, såväl vid rättegången i domstol som under förundersökningen.[35]

Termen straffrättsligt förfarande förekommer också i Europaparlamentets och rådets direktiv 2014/41/EU av den 3 april 2014 om en europeisk utredningsorder på det straffrättsliga området. Direktivet har i Sverige genomförts genom lagen (2017:1000) om en europeisk utredningsorder. I förarbetena till denna lag gör regeringen skillnad på underrättelsestadiet och det straffrättsliga förfarandet.[36]

Att de brottsbekämpande myndigheterna inte kan få tillgång till uppgifter inom ramen för straffrättsliga förfaranden, skulle kunna uppfattas som att EU-domstolen inte har några invändningar mot att uppgifter som har lagrats för nationell säkerhet får användas i underrättelseverksamhet för att bekämpa brottslig verksamhet. EU-domstolen har dock i sin tidigare praxis på detta område inte gjort någon åtskillnad mellan uppgifter som får användas för straffrättsliga förfaranden och som får användas för att förebygga, upptäcka eller förhindra brottslig verksamhet. Som redan nämnts har EU-domstolen slagit fast att uppgifter som har lagrats för nationell säkerhet inte får lämnas ut till de brottsbekämpande myndigheterna för att bekämpa allvarlig brottslighet. Vår bedömning är därför att EU-rätten inte tillåter att uppgifter som har lagrats för att skydda den nationella säkerheten lämnas ut för annan brottsbekämpande underrättelseverksamhet än sådan som sker i syfte att skydda den nationella säkerheten.

Det kan i detta sammanhang noteras att det enligt bestämmelserna om s.k. bevarandeföreläggande finns en möjlighet för brottsutredande myndigheter att skyndsamt säkra och bevara lagrade elek-

[34] Uttrycket förekommer däremot i ett upphävt rambeslut av rådet den 15 mars 2001 om brottsoffrets ställning i straffrättsliga förfaranden (2001/220/RIF). I rambeslutet definieras termen på följande sätt i artikel 1 c: ”straffrättsligt förfarande: straffrättsligt förfarande i överensstämmelse med tillämplig nationell rätt”.
[35] Ds 2017:53 s. 41. Se även prop. 2012/13:132, s. 14 f. och prop. 2018/19:71 s. 14.
[36] Prop. 2016/17:218 s. 82.

troniska uppgifter som kan antas ha betydelse för utredning om ett brott (se 27 kap. 16 och 16 a §§ RB). Bestämmelserna har tillkommit för att Sverige ska uppfylla sina förpliktelser enligt artikel 16.1 i Budapestkonventionen om skyndsamt säkrande av datorbehandlingsbara uppgifter, innefattande trafikuppgifter (se avsnitt 11.5.1). Ett bevarandeföreläggande skulle kunna komma att riktas mot uppgifter som lagras i syfte att skydda den nationella säkerheten. Den som beslutar om ett bevarandeföreläggande torde nämligen inte ha någon kännedom om i vilket syfte de aktuella uppgifterna lagras hos tjänsteleverantören. Inte heller torde den som i ett senare skede beslutar om utlämnande av uppgifter som omfattas av ett sådant föreläggande ha någon kännedom om för vilka ursprungliga syften uppgifterna finns lagrade hos tjänsteleverantören.

EU-domstolen har också uttalat att det i nationell lagstiftning måste finnas vissa krav när det gäller skyndsamt säkrande av trafikuppgifter, bl.a. att endast bekämpning av grov brottslighet och skyddet av den nationella säkerheten kan motivera ett sådant ingrepp.[37] Några motsvarande begränsningar finns inte i Budapestkonventionen.

Tillgång till uppgifter i syfte att skydda nationell säkerhet

Utredningens förslag: Tillgången genom straffprocessuella tvångsmedel till uppgifter som har lagrats för att skydda den nationella säkerheten ska begränsas till bekämpning av brott och brottslighet som kan innebära ett hot mot Sveriges säkerhet. Sådana uppgifter ska också kunna inhämtas genom HAK eller HÖK som meddelats enligt lagen om särskild kontroll av vissa utlänningar.

Det ska i tillståndsbeslutet framgå att tillgång ges till uppgifter som lagrats för att skydda den nationella säkerheten.

Som framgår av avsnitt 7.2. har lagstiftaren valt att inte införa någon legaldefinition av uttrycket nationell säkerhet, eftersom frågor om nationell säkerhet spänner över många områden. Det innebär att hot mot den nationella säkerheten kan anta olika former. I den ovan nämnda nationella säkerhetsstrategin anges bl.a. följande.[38]

[37] Se Garda Síochána-domen, p. 87.
[38] Se Nationell säkerhetsstrategi 2017 s. 21 och 22.

> Organiserad brottslighet är ett hot mot det demokratiska samhället. I Sverige har denna brottslighet utvecklats till att omfatta grövre och mer organiserade inslag, ibland med kopplingar till internationell kriminalitet av stor omfattning. Den kan omfatta handel med människor, vapen eller droger. Hos vissa nätverk finns både avsikt och förmåga att skada och störa grundläggande demokratiska processer. Det kan gälla att hindra verkställandet av politiska beslut eller att söka strypa den fria debatten. Kriminella nätverks förmåga till våld och otillåten påverkan, liksom de stora penningsummor som kriminella personer tillskansar sig, kan i förlängningen leda till maktförskjutningar som påverkar samhället och dess demokratiska strukturer. Att vapen i ökande omfattning används på offentliga platser och i kriminella konflikter leder till ökad rädsla och otrygghet bland personer som vistas eller bor på platser där sådana våldsbrott äger rum. Upprepade våldsbrott där skjutvapen eller explosiva varor används riskerar att minska förtroendet för rättsväsendet och även tilltron till samhället som helhet.

Hot mot Sveriges säkerhet behöver inte heller alltid bestå av kriminella gärningar. Tillgång till lagrade uppgifter för andra syften än brottsbekämpning faller emellertid utanför våra direktiv och behandlas därför inte i detta sammanhang. Våra överväganden i denna del avser således tillgången till uppgifter i syfte att förebygga, förhindra, upptäcka, utreda och beivra brott mot nationell säkerhet. Enligt nuvarande regelverk finns inga särskilda författningar som samlat reglerar eller begränsar de brottsbekämpande myndigheternas tillgång till uppgifter som rör frågor om brott mot Sveriges säkerhet eller brottslighet som är systemhotande. Tillgången regleras i stället, med undantag av abonnemangsuppgifter, i regleringen av de tvångsmedel som används för att få tillgång till uppgifterna.

När det införs regler om lagring i syfte att skydda den nationella säkerheten mot ett verkligt och aktuellt eller förutsebart hot behövs, med utgångspunkt från EU-domstolens resonemang, bestämmelser som skiljer på en tillgång till uppgifter som har lagrats för att skydda den nationella säkerheten från uppgifter som har lagrats för bekämpning av annan allvarlig brottslighet eller som lagrats för tillhandahållarnas egna syften. Uppgifter som lagrats för bekämpning av annan allvarlig brottslighet eller för leverantörernas egna syften bör få lämnas ut för syftet att bekämpa brott mot den nationella säkerheten medan uppgifter som lagrats för att skydda den nationella säkerheten inte får lämnas ut i syfte att bekämpa annan allvarlig brottslighet.[39] Det behövs således en brottskatalog eller motsvarande för att

[39] Se om detta resonemang La Quadrature du Net-domen p. 166.

definiera vilka brott eller vilka typer av brottslighet som sett till fara eller effekt får påverkan på Sveriges säkerhet och för vilka de lagrade uppgifterna får lämnas ut. Som tidigare anförts behöver en sådan reglering vara förutsägbar och föreskriva tydliga rekvisit för tillgången till uppgifterna. Det ligger i sakens natur att brottslighet i största allmänhet, om än allvarlig sådan, inte per automatik utgör ett hot mot Sveriges säkerhet. Utgångspunkten bör i stället vara brottslighet som till sin karaktär eller omfattning är sådan att den hotar den nationella säkerheten. Gränsdragningen mellan allvarlig brottslighet och sådan brottslighet som hotar den nationella säkerheten låter sig inte göras endast utifrån brottslighetens straffvärde. Det finns synnerligen allvarlig brottslighet som isolerat inte kan skada eller hota den nationella säkerheten, liksom brottslighet som inte är synnerligen allvarlig men i visst sammanhang eller viss omfattning kan innebära ett hot mot Sveriges säkerhet. Vi anser att det är lämpligare att utgå från brotten eller brottslighetens karaktär för att ringa in sådan brottslighet som har påverkan på den nationella säkerheten.

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. Enligt 3 § förordningen (2014:1103) med instruktion för Säkerhetspolisen ansvarar Säkerhetspolisen för att förebygga, förhindra och upptäcka brottslig verksamhet samt utreda och beivra följande brott:

1. brott mot 18 eller 19 kap. BrB eller annat brott mot Sveriges säkerhet, i fråga om brott mot medborgerlig frihet dock endast om det finns särskilda skäl för det,
2. brott mot terroristbrottslagen (2022:666),
3. sådana brott mot 13 kap. BrB som har syftat till att framkalla fara för Sveriges säkerhet eller att allvarligt hota eller skada centrala samhällsfunktioner,
4. företagsspioneri eller olovlig befattning med en företagshemlighet, 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,
5. brott där våld, hot eller tvång har använts för politiska syften, om brottet har riktat sig mot någon vars personskydd Säkerhetspolisen

ansvarar för eller om gärningen har riktats mot ett särskilt viktigt samhällsintresse,

6. brott som rör sanktionslagstiftning, krigsmateriel eller produkter med dubbla användningsområden, dock endast brott som har anknytning till verksamhet som Säkerhetspolisen har till uppgift att förebygga och förhindra, och
7. brott mot lagen (2022:700) om särskild kontroll av vissa utlänningar.

Det kan konstateras att samtliga brott och brottslig verksamhet som Säkerhetspolisen har att bekämpa har en koppling till nationell säkerhet. Vi menar därför att tillgång till uppgifter som lagrats i syfte att skydda den nationella säkerheten bör kunna ges avseende alla brott som Säkerhetspolisen har att bekämpa och för vilka inhämtning av uppgifter kan ske efter beslut enligt inhämtningslagen, eller efter tillstånd till HAK eller HÖK enligt rättegångsbalken och preventivlagen. Tillgång bör också kunna ges vid försök, förberedelse eller stämpling till ovan nämnda brott, om en sådan gärning är belagd med straff. Därtill bör tillgång till uppgifter som lagrats genom beslut om nationell säkerhetslagring kunna ges vid beslut om HAK eller HÖK som meddelats med stöd av 5 kap. 5 § lagen om särskild kontroll av vissa utlänningar, dvs. exempelvis om en utlänning tillhör eller verkar för en organisation eller grupp som planlägger eller förbereder brott enligt terroristbrottslagen.

Att enbart utgå från ovan nämnda brott, som Säkerhetspolisen har att bekämpa, för att reglera tillgången till uppgifter som har lagrats för den nationella säkerheten är dock, enligt vår mening, inte tillräckligt. Även andra brott än dessa kan på grund av sin omfattning eller karaktär utgöra ett allvarligt hot mot Sveriges säkerhet. Som exempel på sådan brottslighet kan nämnas grov brottslig verksamhet som till slut blivit så allvarlig att den riskerar att slå ut eller försvaga viktiga funktioner i samhället. Det kan bl.a. röra sig om s.k. systemhotande brottslighet som syftar till att otillbörligt påverka rättskedjan eller andra myndigheter som bär upp den offentliga förvaltningen. Det kan handla om brottslighet som en eller flera gärningsmän utövar för egen vinning men där effekten av brottsligheten blivit så allvarlig att den riskerar att slå ut eller försvaga viktiga funktioner i samhället. Sådan brottslighet kan ge upphov till omfattande vålds-

brottslighet, som kan innebära risker för allmänheten, och framväxten av parallella samhällsstrukturer.

Vi förordar alltså att tillgång till uppgifter som lagrats för nationell säkerhet ges även för andra brott än de som Säkerhetspolisen har att bekämpa. Detta under förutsättning att brottet eller brottsligheten på grund av sin omfattning eller karaktär kan anses utgöra ett allvarligt hot mot Sveriges säkerhet. Vi vill understryka att detta innebär att tillgång till uppgifterna bara kan ges då det är fråga om brottslighet som hotar den nationella säkerheten. Enligt vår bedömning bör det aktuella brottet i vart fall ha ett straffminimum om fängelse i två år. Vi anser inte att någon straffvärdeventil bör införas i detta sammanhang. Vi menar att möjligheten till inhämtning bör vara begränsad enbart till sådana brott som har ett högt straffminimum. När det gäller inhämtning av uppgifter i underrättelseverksamheten är det dessutom svårt att göra ens en någorlunda rimlig bedömning av straffvärdet. Regler om tillgång till uppgifter som har lagrats för nationell säkerhet bör införas i den av oss föreslagna lagen om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

En särskild fråga är hur prövningen av tillgång till uppgifter som lagrats för nationell säkerhet i praktiken ska gå till. Inom Säkerhetspolisen finns kunskapen om huruvida uppgifter lagras för syftet att skydda den nationella säkerheten. Vid andra brottsbekämpande myndigheter finns inte alltid den kunskapen. Även om sådan kunskap finns känner myndigheterna sannolikt inte till den närmare omfattningen av lagringsskyldigheten. Som nämnts ovan är det sannolikt så att inte heller den domstol eller åklagare som ska pröva tillståndet till det hemliga tvångsmedlet känner till om det föreligger någon nationell säkerhetslagring och än mindre omfattningen av en sådan. Det är alltså befattningshavare inom Säkerhetspolisen och hos de tillhandahållare som omfattas av lagringsskyldigheten som med säkerhet känner till den närmare omfattningen av lagringen.

Vid en ansökan om hemliga tvångsmedel för att få tillgång till historiska trafik- och lokaliseringsuppgifter (genom HAK eller HÖK enligt RB, preventivlagen eller LSU samt vid inhämtning enligt inhämtningslagen) måste sökanden uttryckligen ange att tvångsmedlet avser även uppgifter som är lagrade för nationell säkerhet. När domstolen eller åklagaren ger tillstånd till tvångsmedlet måste den alltså ange om inhämtningen får avse uppgifter som är lagrade för detta

syfte oavsett huruvida man känner till att sådana uppgifter finns lagrade eller inte. Ges tillstånd till sådan inhämtning, får inhämtningen avse alla uppgifter som finns hos leverantören. Om några uppgifter inte är lagrade för nationell säkerhet ska de eventuella andra uppgifter som leverantören har lämnas ut. Om domstolen visserligen beviljar det hemliga tvångsmedlet, men inte anser att aktuellt brott eller brottslighet innefattar ett hot mot den nationella säkerheten, får eventuella uppgifter lagrade för nationell säkerhet inte lämnas ut, bara andra uppgifter som leverantören behandlar.

De tillhandahållare som lagrar uppgifter enligt ett föreläggande om nationell säkerhetslagring måste således särskilja de uppgifter som lagras för detta ändamål från sådana uppgifter som lagras för andra syften. Tillhandahållarnas skyldighet att lämna ut uppgifter lagrade för nationell säkerhet bör endast gälla om det i tillståndsbeslutet särskilt angetts att inhämtningen får avse uppgifter som lagrats med stöd av lagen om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet. En bestämmelse som reglerar detta bör tas in i lagen.

7.3.8 Personuppgiftsbehandling vid lagring för nationell säkerhet

I detta avsnitt diskuterar vi frågan om behovet av att reglera den personuppgiftsbehandling som tillhandahållarna och de brottsbekämpande myndigheterna måste utföra när det gäller lagring för den nationella säkerheten.

Tillhandahållarnas behandling av uppgifter som lagras för nationell säkerhet

Utredningens förslag: Det ska finnas författningsstöd för tillhandahållarnas behandling av personuppgifter när det gäller lagring och utlämnande av uppgifter i syfte att skydda den nationella säkerheten.

Tillhandahållarnas behandling av fysiska personers trafik- och lokaliseringsuppgifter är reglerade i nya LEK med bl.a. begränsningar kring hur uppgifterna får hanteras (se 9 kap. 1–3 och 9 kap. 7–9 §§ nya LEK). Utgångspunkten är att uppgifterna ska utplånas eller avidentifieras när de inte längre behövs för överföring av ett elektroniskt meddelande. Det finns vissa undantag från detta krav i 9 kap. 1 § andra stycket, 2, 4 och 10 §§ nya LEK.

Trafikuppgifter får enligt 9 kap. 1 § andra stycket nya LEK behandlas för brottsbekämpande ändamål enligt 9 kap. 19 § nya LEK. Vi föreslår att tillhandahållarnas lagringsskyldighet vid nationell säkerhetslagring ska regleras i 9 kap. 19 b § nya LEK. Det krävs därför en motsvarande ändring i 9 kap. 1 § andra stycket nya LEK.

Vi har ovan föreslagit att lokaliseringsuppgifter som inte är trafikuppgifter ska kunna omfattas av ett föreläggande om nationell säkerhetslagring. Vi föreslår därför att det i 9 kap. 10 § nya LEK föreskrivs att lokaliseringsuppgifter som ska lagras enligt ett föreläggande om nationell säkerhetslagring får behandlas trots vad som föreskrivs i 9 kap. 7–9 §§.

I 9 kap. 19 § nya LEK regleras lagringsskyldigheten för brottsbekämpande ändamål. Uppgifter som har lagrats med stöd av denna bestämmelse får behandlas endast för att lämnas ut enligt 9 kap. 33 § första stycket 2 eller 5 i nya LEK, 27 kap. 19 § rättegångsbalken, eller inhämtningslagen (se 9 kap. 21 § nya LEK). För att tillhandahållarna ska kunna lämna ut uppgifter som lagrats i syfte att skydda den nationella säkerheten behövs författningsstöd för sådan behandling. Ett sådant författningsstöd kan regleras genom att ett nytt stycke läggs till i 9 kap. 21 § nya LEK, som anger att uppgifter som lagrats för nationell säkerhet får behandlas för att lämnas ut enligt den av oss föreslagna lagen om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

De brottsbekämpande myndigheternas behandling av uppgifter som lagras för nationell säkerhet

Utredningens bedömning: Våra förslag om lagring och tillgång till trafik- och lokaliseringsuppgifter i syfte att skydda den nationella säkerheten föranleder inga ändringar i de brottsbekämpande myndigheternas registerförfattningar.

Behöriga myndigheters behandling av personuppgifter i syfte att bekämpa brott regleras i brottsdatalagen (2018:1177) i förening med de särskilda registerförfattningar som gäller för verksamheten, exempelvis polisens brottsdatalag (2018:1693).

Det gäller inte Säkerhetspolisens och Polismyndighetens behandling av uppgifter som rör brottsbekämpning och lagföring i frågor om nationell säkerhet. Personuppgiftsbehandling rörande nationell säkerhet sker i stället med stöd av lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter (SDL). Enligt 2 kap. 1 § SDL får Säkerhetspolisen behandla personuppgifter om det är nödvändigt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar bl.a. brott mot Sveriges säkerhet och terrorbrott samt för att utreda eller lagföra sådana brott. Bestämmelsen gäller även Polismyndigheten om Säkerhetspolisen lämnar över en arbetsuppgift som rör nationell säkerhet.

Personuppgifter får behandlas bara för särskilda, uttryckligt angivna och berättigade ändamål (2 kap. 3 § SDL). Att ändamålet ska vara särskilt innebär att det måste vara tillräckligt preciserat för att det ska kunna avgöras om de personuppgifter som behandlas är adekvata och relevanta för ändamålet med behandlingen eller om för många personuppgifter behandlas.[40] Om Säkerhetspolisen avser att behandla personuppgifter för ett nytt ändamål, måste myndigheten pröva om det nya ändamålet är förenligt med det ändamål som låg till grund för den ursprungliga behandlingen.

Av 2 kap. 4 § första stycket 1 SDL framgår att Säkerhetspolisen får utföra den behandling som behövs för att till andra brottsbekämpande myndigheter vidarebefordra uppgifter om brott eller brottslig verksamhet. I samma paragraf finns också beskrivet för vilka andra ändamål uppgifter rörande bl.a. nationell säkerhet får vidarebefordras till andra aktörer.

Med hänsyn till Säkerhetspolisens, och i tillämpliga fall även Polismyndighetens, redan befintliga uppdrag i frågor om nationell säkerhet samt de regelverk som gäller i verksamheterna, kräver våra förslag inga författningsändringar när det gäller myndigheternas personuppgiftsbehandling. Säkerhetspolisen kan i dag behandla personuppgifter beträffande frågor som rör nationell säkerhet och vid behov kan Säkerhetspolisen vidarebefordra sådana uppgifter till Polismyndigheten. Våra förslag förändrar inte de rättsliga grunderna eller ändamålen för

[40] Prop. 2018/19:163 s. 68 och 220.

Säkerhetspolisens eller Polismyndighetens behandling av uppgifter i fråga om brottsbekämpning som rör nationell säkerhet. Om Polismyndigheten genom hemliga tvångsmedel får tillgång till uppgifter som lagrats i syfte att skydda den nationella säkerheten för sådana arbetsuppgifter som inte överlämnats från Säkerhetspolisen, ska polisens brottsdatalag tillämpas vid behandlingen av uppgifterna. Om uppgifterna i stället inhämtas för en arbetsuppgift som överlämnats från Säkerhetspolisen blir lagen om Säkerhetspolisens behandling av personuppgifter tillämplig.

Våra förslag förändrar inte heller de rättsliga grunderna eller ändamålen för exempelvis Tullverket eller andra brottsbekämpande myndigheter som eventuellt kan få del av uppgifter som lagrats för nationell säkerhet i brottsbekämpning som rör nationell säkerhet. I likhet med vad som gäller för Säkerhetspolisen och Polismyndigheten måste personuppgiftsbehandlingen ha stöd i det regelverk som gäller för verksamheten. Våra förslag innebär ingen förändring i detta hänseende.

7.3.9 Sekretess och tystnadsplikt m.m.

Sekretess i angelägenheter om nationell säkerhetslagring

Utredningens bedömning: Nuvarande sekretessregler till skydd för intresset av att förebygga eller beivra brott ger ett tillräckligt sekretesskydd för uppgifter i angelägenheter om nationell säkerhetslagring. Däremot finns i befintliga regler inte motsvarande skydd för enskilda intressen och det bör därför införas en kompletterande bestämmelse.

Utredningens förslag: Sekretess ska gälla för uppgifter om en enskilds personliga och ekonomiska förhållanden i angelägenheter 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.

När det gäller lagring av uppgifter i syfte att skydda nationell säkerhet kommer, enligt våra förslag, flera aktörer vara involverade. Säkerhetspolisen ska, som behörig myndighet, bedöma om det föreligger ett allvarligt hot mot den nationella säkerheten och får, om så be-

döms vara fallet, förelägga tillhandahållare att lagra trafik- och lokaliseringsuppgifter. Under beredningen ska Säkerhetspolisen samråda med Försvarsmakten och får vid behov även samråda med och inhämta information från andra myndigheter. Ett offentligt ombud ska ta del av Säkerhetspolisens beslut och underlaget för detta. Ett beslut om lagring för den nationella säkerheten kan överklagas av det offentliga ombudet till Datalagringsdelegationen inom Säkerhets- och integritetsskyddnämnden. Vid verkställighet av beslut om lagring involveras tillhandahållare och vid tillsyn även PTS. Om PTS beslut överklagas, involveras också de allmänna förvaltningsdomstolarna.

Säkerhetspolisens handläggning, dvs. både beredning och beslut, av ett ärende om nationell säkerhetslagring sker, som vi har konstaterat i avsnitt 7.3.2, som ett led i Säkerhetspolisens brottsbekämpande verksamhet. Beslut om nationell säkerhetslagring möjliggör i senare led användning av hemliga tvångsmedel såväl inom som utom förundersökningar. Enligt vår bedömning sker åtgärderna vid beredning och beslut i ett ärende om nationell säkerhetslagring uteslutande inom ramen för Säkerhetspolisens underrättelseverksamhet. Handläggningen medför hantering av en mängd uppgifter som behöver få ett adekvat sekretesskydd. Skyddsintressena i Säkerhetspolisens verksamhet gör det angeläget att allmänhetens insyn begränsas. Vår utgångspunkt är att det ska finnas ett fullgott sekretesskydd för såväl det allmänna som för enskilda i ärenden om nationell säkerhetslagring. Vi återkommer till frågor om meddelarfrihet i kommande avsnitt.

I 18 kap. 1–3 och 17–17 a §§ och 35 kap. 1 § OSL finns bestämmelser om sekretess i underrättelseverksamheten. Utredningssekretessen och underrättelsesekretessen enligt 18 kap. 1 och 2 §§ OSL är i viss mån överlappande.

Av 18 kap. 1 § första stycket OSL följer att sekretess gäller för uppgift som hänför sig till förundersökning i brottmål eller till angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs. Sekretess gäller, under motsvarande förutsättningar som anges i första stycket, för uppgift som hänför sig till annan verksamhet än sådan som avses i bl.a. första stycket och som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs av de brottsbekämpande myndigheterna (18 kap. 1 § andra stycket 2 OSL). Med *annan verksamhet* åsyftas

både brottsförebyggande och brottsbeivrande verksamhet i allmänhet utan anknytning till något konkret fall. Uppgifter hänförliga till sådan verksamhet kan gälla resurs- och organisationsfrågor av vital betydelse, arbetsrutiner, spaningsmetoder, personskydd, personuppgifter rörande personal och tjänstgöringslistor. Även uppgifter om namn på personer som biträder polisen vid spaningsarbete, med tolkning eller genom att lämna förtrolig information (dvs. källor) kan falla under bestämmelsen.[41] Uppgifter av nu nämnt slag kan ibland också omfattas av sekretess till skydd för rikets säkerhet enligt 15 kap. 2 § OSL, vilket vi återkommer till nedan.

Enligt 18 kap. 2 § OSL gäller sekretess för underrättelseuppgifter om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas.

Sekretess enligt 18 kap. 1 och 2 §§ gäller även hos myndigheter som biträder de brottsbekämpande myndigheterna i bl.a. underrättelseverksamheten (18 kap. 3 § OSL). Vidare finns särskilda bestämmelser om sekretess i verksamhet som avser rättsligt eller polisiärt samarbete i internationella förhållanden (se 18 kap. 17 och 17 a §§ OSL).

I underrättelseverksamheten finns också sekretessregler till skydd för enskilda. Enligt 35 kap. 1 § första stycket 4 OSL gäller sekretess 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 verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott eller verkställa uppbörd om verksamheten bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen.

Sekretessregleringen i 18 kap. 1 och 2 §§ OSL är utformad så att sekretess gäller uppgift som *hänför sig till* brottsförebyggande eller brottsbeivrande verksamhet. Det betyder att sekretessen följer med uppgiften när den lämnas till en annan myndighet. Regleringen innebär också att uppgifterna inte måste komma direkt från den brottsbekämpande myndigheten för att omfattas av sekretessen.[42] Det betyder att en uppgift som exempelvis PTS lämnar till Säkerhetspolisen

[41] A.a.
[42] Se Lenberg, Tansjö och Geijer (5 juli. 2022, Version 25, JUNO), kommentaren till 18 kap. 1 § OSL.

i ett ärende om nationell säkerhetslagring kommer att omfattas av sekretessregleringen i 18 kap. 2 §.

Ärenden om nationell säkerhetslagring aktualiserar även hantering av uppgifter som regleras av annan sekretess. Några exempel är 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 § OSL. Bestämmelserna är tillämpliga i all offentlig verksamhet, dvs. utgör en primär sekretessregel för den myndighet som får tillgång till uppgifterna.

De sekretessregler som vi beskrivit hittills ger enligt vår bedömning ett tillräckligt sekretesskydd för allmänna intressen i ärenden om nationell säkerhetslagring, men även enskilda, vars uppgifter förekommer i ett ärende om nationell säkerhetslagring, behöver ett fullgott sekretesskydd. Det kan röra sig om personer som både direkt och indirekt har koppling till det nationella säkerhetshotet. Det kan även omfatta tillhandahållarnas ekonomiska förhållanden. I motsats till vad som föreskrivs i 18 kap. 1 och 2 §§ OSL gäller inte sekretess enligt 35 kap. 1 § första stycket 4 OSL, utanför de brottsbekämpande myndigheternas verksamhet. Det innebär att uppgifter som rör enskildas personliga och ekonomiska förhållanden, med nuvarande 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 sekretessskydd när de överförs mellan Polismyndigheten och Säkerhetspolisen men inte när en uppgift överförs från Säkerhetspolisen till Försvarsmakten eller SIN eftersom de senare inte omfattas av 35 kap. 1 § första stycket 4 OSL.

Vi föreslår därför att en ny punkt förs in i 35 kap. 1 § OSL enligt vilken sekretess ska gälla för uppgift om en enskilds personliga och ekonomiska förhållanden i angelägenhet om nationell säkerhetslagring. 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 OSL.

Sekretessen ska alltså gälla oavsett vilken myndighet eller domstol som involveras i handläggningen. När det gäller sekretessens styrka föreslår vi ett omvänt skaderekvisit motsvarande det som finns enligt 35 kap. 1 § första stycket OSL, dvs. att ett utlämnande förutsätter att det ska stå klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men.

Det bör uppmärksammas att den föreslagna bestämmelsen medför att sekretessen i vissa situationer blir överlappande med sekretess enligt andra bestämmelser. Under sådana förhållanden tillämpas 7 kap. 3 § OSL. Som huvudregel följer av 7 kap. 3 § OSL att det vid konkurrens mellan flera sekretessbestämmelser är den eller de bestämmelser som ger sekretesskydd i det enskilda fallet som ska tillämpas, oavsett vilka sekretessbestämmelser som konkurrerar. Från huvudregeln finns vissa undantag som inte är relevanta i detta sammanhang.

Ett beslut om nationell säkerhetslagring ska omfattas av sekretess

Utredningens bedömning: Sekretessen ska även omfatta ett beslut om nationell säkerhetslagring.

En fråga som bör uppmärksammas särskilt är om själva beslutet om nationell säkerhetslagring ska omfattas av sekretess. Ett beslut om att tillhandahållarna ska påbörja en generell och odifferentierad lagring av uppgifter är i och för sig ett beslut som innebär en rättighetsinskränkning. Sådana beslut bör som huvudregel vara tillgängliga för allmänhetens insyn. Det finns skäl att överväga möjligheten att föreskriva att ett beslut om lagring delvis ska vara offentligt. Det skulle i sådana fall handla om uppgiften att Sverige står inför ett nationellt säkerhetshot. Övriga delar av beslutet, dvs. vilka uppgifter som ligger till grund för Säkerhetspolisens bedömning, vilka tillhandahållare som ska omfattas, hur lång tid lagringen ska ske m.m. bör kunna hemlighållas.

Vår bedömning är emellertid att offentlighet även för uppgiften att Sverige står inför ett nationellt säkerhetshot kan begränsa handlingsutrymmet för Säkerhetspolisen. Exempelvis skulle det kunna röja Säkerhetspolisens metoder om ett beslut om nationell säkerhetslagring meddelas i anslutning till åtgärder som Säkerhetspolisen har vidtagit. Vår bedömning är att det är lämpligare att beslut om lagring för nationell säkerhet, i likhet med beslut om vissa straffprocessuella tvångsmedel, i sin helhet omfattas av sekretess. Genom att beslutet kan överklagas av ett offentligt ombud till Säkerhets- och integritetsskyddsnämnden, och genom att tillgången till uppgifterna i senare led förutsätter tillstånd till användning av hemliga tvångsmedel, till-

försäkras enskilda enligt vår bedömning tillräckliga rättssäkerhetsgarantier.

Vi påminner i sammanhanget om att sekretessen enligt de av oss redovisade bestämmelserna inte är 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. En sådan uppgift avslöjar ensamt inte någonting om lagringsskyldighetens omfattning eller Säkerhetspolisens metoder. Det bör dock ankomma på Säkerhetspolisen att i det enskilda fallet göra en sådan prövning.

Vi bedömer sammanfattningsvis att det inte ska föreskrivas något undantag för sekretessen beträffande beslut om nationell säkerhetslagring. Det innebär att sekretessen även omfattar beslut av SIN i samband med överprövning av Säkerhetspolisens beslut.

Tystnadsplikt för tillhandahållare i ett ärende om nationell säkerhetslagring

Utredningens förslag: Tillhandahållarnas tystnadsplikt ska gälla i angelägenheter om nationell säkerhetslagring. Tillhandahållarnas tystnadsplikt ska även omfatta lokaliseringsuppgifter som inte är trafikuppgifter och som rör användare som är fysiska personer eller abonnenter.

Säkerhetspolisen kan, såväl under handläggning som vid verkställighet av beslut om nationell säkerhetslagring, behöva komma i kontakt med tillhandahållarna. En förutsättning för en sådan kontakt är att skyddet för eventuella uppgifter som lämnas kan bibehållas hos tillhandahållarna. Tillhandahållarna träffas inte av regleringen i offentlighets- och sekretesslagen. Tystnadsplikt för tillhandahållarna regleras i stället i 9 kap. 31 och 32 §§ nya LEK. I 9 kap. 32 § nya LEK finns en straffsanktionerad tystnadsplikt för uppgifter som hänför sig till vissa angelägenheter bl.a. avseende användning av hemliga tvångsmedel.

Vi bedömer att en motsvarande reglering bör införas för handläggning och beslut om nationell säkerhetslagring genom ett tillägg i 9 kap. 32 § nya LEK. Tystnadsplikten ska omfatta ärendet i dess

helhet. Det innefattar exempelvis informationen om att Säkerhetspolisen har varit i kontakt med tjänsteleverantören, vad som har kommunicerats, föreläggande om lagring och att lagring har påbörjats eller avslutats. Vi återkommer i avsnitt 9.6.2 till frågan om tystnadsplikt för tillhandahållare av nummeroberoende interpersonella kommunikationstjänster (Noik).

En bestämmelse om tystnadsplikt innebär en begränsning av yttrandefriheten enligt 2 kap. 1 § RF och artikel 10.1 Europakonventionen. Enligt 2 kap. 20–21 och 23 §§ RF och artikel 10.2 Europakonventionen får begränsningar i yttrandefriheten endast göras i lag under vissa förutsättningar och för vissa särskilt angivna ändamål. En begränsning får bl.a. 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. Yttrandefriheten får begränsas med bl.a. hänsyn till allmän ordning och säkerhet, förebyggandet och beivrandet av brott eller om särskilt viktiga skäl föranleder det.

Som redan nämnts vid ett flertal tillfällen i föregående avsnitt är det av stor betydelse att uppgifter som rör angelägenheter om nationell säkerhetslagring får ett ändamålsenligt skydd. Att som tjänsteleverantör inte få yttra sig fritt i angelägenheter om nationell säkerhetslagring innebär i realiteten ingen påtaglig inskränkning i yttrandefriheten. Vi bedömer därför att behovet av tystnadsplikt för tillhandahållare i angelägenheter som rör nationell säkerhetslagring väger tyngre än intresset av yttrandefrihet. Vidare anser vi att tystnadsplikt i detta sammanhang är proportionerligt och att en sådan tystnadsplikt även i övrigt uppfyller de krav som gäller för begränsningar i yttrandefriheten enligt regeringsformen och Europakonventionen. Vi återkommer till frågor om meddelarfrihet i kommande avsnitt.

En annan fråga som aktualiseras med anledning av att vi ovan föreslår att lagringsskyldigheten i detta avseende ska kunna omfatta lokaliseringsuppgifter som inte är trafikuppgifter är huruvida dessa uppgifter ska omfattas av tystnadsplikt hos tillhandahållarna.

Det kan konstateras att uppgift om var en elektronisk utrustning finns när det inte sker någon kommunikationen kan vara en för den enskilde användaren lika känslig uppgift som var utrustningen finns under kommunikation. Vi anser därför att lokaliseringsuppgifter som inte är trafikuppgifter bör omfattas av tystnadsplikten. Tystnadsplikten bör gälla endast för sådana lokaliseringsuppgifter som rör

användare som är fysiska personer eller abonnenter, eftersom det är i dessa fall som integritetsskyddsintresset gör sig särskilt gällande (jfr 9 kap. 7 § nya LEK). Vi föreslår att denna tystnadsplikt regleras i en ny fjärde punkt i 9 kap. 31 § första stycket nya LEK. På samma sätt som för uppgift om abonnemang och annan uppgift som angår ett särskilt elektroniskt meddelande (trafikuppgift) bör tystnadsplikten för lokaliseringsuppgifter som inte är trafikuppgifter dock inte gälla i förhållande till innehavaren av abonnemanget. Vi föreslår att ett sådant tillägg görs i 9 kap. 31 § tredje stycket nya LEK. Detta stycke bör också ändras på det sättet att formuleringen *som har använts för ett elektroniskt meddelande* tas bort. Lokaliseringsuppgifter som inte är trafikuppgifter är nämligen inte kopplande till ett elektroniskt meddelande. Vi bedömer att innebörden av detta stycke i förhållande till abonnemangsuppgifter och trafikuppgifter inte förändras genom den förändring som vi föreslår.

Tystnadsplikt och sekretessbrytande bestämmelse för offentligt ombud i ett ärende om nationell säkerhetslagring

Utredningens förslag: Den som förordnats som offentligt ombud i ett ärende om nationell säkerhetslagring får inte obehörigen röja vad han eller hon i ärendet fått kännedom om.

I offentlighets- och sekretesslagen (2009:400) införs en bestämmelse som innebär att ett offentligt ombud utan hinder av sekretess får ta del av uppgifter i ärenden om nationell säkerhetslagring hos Säkerhetspolisen och Datalagringsdelegationen.

Det offentliga ombudets uppdrag innebär att han eller hon får del av en mängd uppgifter som omfattas av sekretess. Med hänsyn till graden av känslighet hos de uppgifter som kan förväntas förekomma i ett ärende om nationell säkerhetslagring är det av yttersta vikt att det offentliga ombudet inte lämnar ut uppgifter som han eller hon har fått del av genom sitt uppdrag. Det bör även ligga i det enskilda ombudets intresse att det finns ett förbud att hänvisa till, om han eller hon från utomstående får förfrågningar om uppdraget. Det offentliga ombudet företräder endast 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 § OSL.[43]

För att även det offentliga ombudet ska vara skyldigt att inte obehörigen röja vad han eller hon erfar under sitt uppdrag bör det införas en särskild regel om tystnadsplikt i likhet med vad som gäller för offentliga ombud enligt rättegångsbalken. Uttrycket *obehörigen röja* hindrar inte att ombudet lämnar uppgifter till Datalagringsdelegationen.[44] Vad gäller begränsningar i yttrandefriheten gör vi samma bedömning som i föregående avsnitt om tillhandahållarna.

Enligt 10 kap. 10 § andra stycket OSL hindrar inte sekretess 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. Att denna bestämmelse finns beror på regleringen i 8 kap. 1 § OSL, enligt vilken en sekretessbelagd uppgift inte får röjas för en enskild eller för andra myndigheter i annat fall än när det särskilt anges i offentlighets- och sekretesslagen, eller i en annan lag eller förordning till vilken offentlighets- och sekretesslagen hänvisar.

I likhet med vad som gäller för ett offentligt ombud eller integritetsskyddsombud enligt 10 kap. 10 § andra stycket OSL kommer ett offentligt ombud i ärenden om nationell säkerhetslagring inte anses vara part.[45] Som vi tidigare har konstaterat är det offentliga ombudet inte knuten till det allmännas verksamhet. Utan en sekretessbrytande regel saknas det således lagliga möjligheter att lämna ut uppgifter som omfattas av sekretess till ett offentligt ombud. Vi föreslår därför ett nytt tredje stycke i 10 kap. 10 § OSL av vilket det ska framgå att sekretess inte hindrar att uppgift i ett ärende om nationell säkerhetslagring lämnas till ett offentligt ombud.

Meddelarfrihet

Utredningens förslag: I ett ärende om nationell säkerhetslagring ska tystnadsplikten inskränka rätten att meddela och offentliggöra uppgifter enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen.

[43] Jfr prop 1979/80:2 Del A s. 127.
[44] Jfr prop. 2002/03:74 s. 29 och 30.
[45] Jfr prop. 2008/09:201 s. 71 och prop. 2002/03:74 s. 29 och 30.

Gällande rätt innebär i huvudsak att den tystnadsplikt som följer av 18 kap. 1–3 §§ OSL inskränker rätten att meddela och offentliggöra uppgifter i viss utsträckning medan så inte är fallet med den tystnadsplikt som följer av 35 kap. 1 § OSL. Frågan är då om rätten att meddela och offentliggöra uppgifter bör inskränkas av den tystnadsplikt som följer av 18 kap. 1–3 §§ OSL, som kommer att vara tillämplig på angelägenheter om nationell säkerhetslagring, och den tystnadsplikt som följer av den av oss ovan föreslagna nya punkten i 35 kap. 1 § OSL om sekretess för uppgift om en enskilds personliga och ekonomiska förhållanden i angelägenhet om nationell säkerhetslagring.

Med meddelarfrihet avses rätten att meddela och offentliggöra uppgifter i vilket ämne som helst för publicering i de medier som grundlagarna omfattar.[46] Meddelarfriheten har sin grund i att sekretessbestämmelserna ger uttryck för ganska allmänna avvägningar mellan insyns- och sekretessintressena på de berörda områdena. Detta innebär att önskemålet om insyn i ett särskilt fall kan vara starkare än det sekretessintresse som har föranlett den aktuella sekretessregeln. Det kan vidare förhålla sig så att en regel om skydd t.ex. för ett enskilt intresse ibland på ett olämpligt sätt hindrar insyn i en myndighets sätt att fullgöra sina uppgifter. Offentlighetsprincipen skulle inte förverkligas till fullo om de offentliga funktionärerna i sådana situationer skulle vara förhindrade att bidra med uppgifter till den allmänna debatten. Reglerna om meddelarfrihet är avsedda att motverka sådana icke önskade resultat av sekretessregleringen.[47] Meddelarfriheten är emellertid inte oinskränkt. I vissa fall ges tystnadsplikten företräde framför meddelarfriheten. En sådan tystnadsplikt brukar kallas kvalificerad tystnadsplikt.

Nationell säkerhetslagring syftar till att skapa förutsättningar för att Säkerhetspolisen och andra brottsbekämpande myndigheter som ska bekämpa brottslighet som kan utgöra ett hot mot den nationella säkerheten i framtiden ska kunna använda sig av hemliga tvångsmedel. De uppgifter som dessa myndigheter kommer att ha tillgång till kommer ofta att vara av mycket känslig natur. Frågan är alltså hur avvägningen mellan meddelarfrihet och sekretess ska göras i dessa fall.

[46] Se 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen.
[47] Se prop. 1979/80:2 del A s. 104–105.

Någon helt entydig praxis om när en tystnadsplikt ska inskränka rätten att meddela och offentliggöra uppgifter finns knappast. I förarbetena till sekretesslagen (1980:100) redovisas dock några grundläggande utgångspunkter för när meddelarfriheten bör begränsas. Som exempel nämns att meddelarfrihet bör vara utesluten när det gäller uppgifter som har lämnats av enskilda i en förtroendesituation. Rör det sig däremot om uppgifter som hänför sig till ett ärende om myndighetsutövning bör meddelarfrihet oftast föreligga.[48]

I betänkandet en *Ny sekretesslag* (2003:99) illustreras omständigheter som talar för respektive mot meddelarfrihet genom följande tabell.[49]

Tabell 7.1 Omständigheter som talar för respektive mot meddelarfrihet

För meddelarfrihet	Mot meddelarfrihet
Myndighetsutövning mot enskild	Frivillig kontakt
Meddelarfrihet har gällt tidigare	Inget skaderekvisit
Efterforskningsförbudet och anonymitetsskyddet bör vara så omfattande som möjligt	Omvänt skaderekvisit (i viss mån)
	Förtroendesituation
	Spärr för uppgiftslämnande mellan myndigheter
	Rikets säkerhet eller annan allvarlig skada för landet
	Viktiga samhällsfunktioners effektivitet (t.ex. tvångsåtgärder i brottmål)
	Insynen kan tillgodoses på annat sätt (t.ex. offentlighet i domstol)

Det betonas att tabellen inte ska uppfattas som en checklista utan det avgörande är utfallet av en avvägning mellan behovet av insyn och behovet av skydd för uppgifterna. En uppgift skulle alltså kunna träffas av de flesta omständigheter mot meddelarfrihet men ändå inte vara lämplig att undanta från meddelarfriheten, t.ex. för att insynsintresset är mycket starkt.[50] Om syftet med åtgärden skulle kunna gå förlorat får meddelarfriheten dock ge vika.[51] Det gäller bl.a. när

[48] Se a. a. s. 110–112.
[49] Se SOU 2003:99 s. 397.
[50] Se a.a.s. 397.
[51] Se t.ex. prop. 2005/06:178 s. 81.

det är fråga om uppgifter som gäller användning av hemliga tvångsmedel (18 kap. 19 § OSL).

Något meddelarförbud gäller emellertid inte för uppgifter om enskildas personliga och ekonomiska förhållanden enligt 35 kap. 1 § första stycket 2 OSL. För dessa uppgifter har alltså rätten att meddela och offentliggöra uppgifter företräde framför tystnadsplikten trots att det rör sig om användning av hemliga tvångsmedel. Användning av sådana tvångsmedel kan typiskt sett röja förtroliga samtal eller andra känsliga uppgifter om privatlivet. Det kan tyckas oklart varför behovet av skydd för de enskildas integritet i sammanhanget inte skulle väga lika tungt och på samma sätt motivera ett avsteg från huvudregeln om meddelarfrihet. I sammanhanget bör det erinras om att enskilda som är föremål för tvångsmedelsanvändningen endast är misstänkta för brott och att ärendena många gånger innehåller för utredningen ovidkommande information om närstående eller andra personer. Det är med andra ord sådana uppgifter som typiskt sätt motiverar en inskränkning i meddelarfriheten.

I ovan nämnda betänkande förs allmänna resonemang om vikten av insyn i den polisära verksamheten under förundersökningar. Något motsvarande resonemang finns inte beträffande tvångsmedel och underrättelseverksamhet.[52] Frågan berördes heller inte i samband med införandet av lagen (2020:62) om hemlig dataavläsning.

En möjlig förklaring till detta kan vara att det är svårt att i praktiken utnyttja meddelarfrihet för uppgifter som omfattas av sekretess enligt 35 kap. 1 § OSL utan att samtidigt bryta mot meddelarförbudet i 18 kap. 19 § OSL.

Uppgifter som rör Säkerhetspolisens handläggning av ärenden om nationell säkerhet kommer, som har sagts, att vara bland de känsligare delarna av underrättelseverksamheten, bl.a. med hänsyn till att de rör hot mot Sveriges säkerhet. Ett röjande av sådana uppgifter skulle kunna leda till allvarlig skada för Sveriges nationella säkerhet. Vi anser därför att den tystnadsplikt som följer av 18 kap. 1–3 §§ OSL i angelägenheter om nationell säkerhetslagring ska ha företräde framför meddelarfriheten. Enligt vår bedömning får sekretessintresset i dessa fall anses vara starkare än det allmänna intresset av insyn i den verksamhet som bedrivs av de berörda myndigheterna. Vi gör samma bedömning när det gäller insynen i enskildas personliga och ekonomiska förhållanden i angelägenheter om nationell säkerhetslagring.

[52] Se SOU 2003:99 s. 404–405.

Vi föreslår därför att den tystnadsplikt som följer av sekretess för nationell säkerhetslagring ska inskränka rätten att meddela och offentliggöra uppgifter enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen oberoende av vilket intresse sekretessen avser att skydda.

I och för sig finns det argument för inskränkningar i meddelarfriheten för uppgifter som omfattas av sekretess enligt 35 kap. 1 § OSL även beträffande tvångsmedelsanvändning. Lagstiftaren har dock inte inskränkt meddelarfriheten i sådana situationer. Med hänsyn till vårt uppdrag och direktiven för detta avstår vi dock från att föreslå en generell inskränkning i meddelarfriheten för uppgifter som rör användning av tvångsmedel.

Enligt 18 kap. 19 § andra stycket OSL inskränker den tystnadsplikt som följer av 18 kap. 1–3 §§ rätten att meddela och offentliggöra uppgifter hänförliga till hemliga tvångsmedel. Vi föreslår att det i paragrafen ska göras ett tillägg så att meddelarförbudet omfattar även ärenden om nationell säkerhetslagring.

Meddelarförbud för uppgifter i 35 kap. OSL regleras i 35 kap. 24 § OSL. För att införa motsvarande inskränkning avseende ärenden om nationell säkerhetslagring föreslår vi att ett tillägg om detta görs i 35 kap. 24 § OSL.

Våra överväganden hittills har berört inskränkningar i meddelarfriheten för medarbetare i de berörda myndigheterna. Vi övergår nu till behovet av motsvarande inskränkningar vad gäller tillhandahållare och det offentliga ombudet.

I 44 kap. OSL 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 OSL inskränks meddelarfriheten för tillhandahållare i fråga om straffprocessuella tvångsmedel. En motsvarande inskränkning bör i samma paragraf finnas även i angelägenheter om nationell säkerhetslagring.

Här bör uppmärksammas att meddelarförbud behöver regleras även för ett offentligt ombud i ett ärende om nationell säkerhetslagring. 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 § RB. Bestämmelsen ger domstol möjlighet att ålägga de närvarande personerna tystnadsplikt. Den som omfattas av ett sådant förordnande har inte meddelarfrihet i fråga om de uppgifter som förordnandet avser. Det

följer av 44 kap. 2 § OSL. Bryter ett offentligt ombud mot ett sådant förordnande kan han eller hon dömas till ansvar enligt en särskild bestämmelse i 9 kap. 6 § RB.[53]

Eftersom ett offentligt ombud i ärenden om nationell säkerhetslagring inte omfattas av rättegångsbalkens regler behövs en särskild reglering för denna situation. Mot den bakgrunden föreslår vi att meddelarförbud för offentliga ombud i ärenden om nationell säkerhetslagring regleras genom att en ny punkt förs in i 44 kap. 5 § OSL.

[53] Se prop. 2002/03:74 s. 30.

8 Särskilt om lagring och tillgång till uppgifter i syfte att bekämpa grov brottslighet

8.1 Inledning

Vi har i avsnitt 6.6.3 konstaterat att det finns skäl för oss att lämna förslag om riktad lagring för att bekämpa grov brottslighet. I detta avsnitt överväger vi hur en sådan lagring av trafik- och lokaliseringsuppgifter skulle kunna utformas.

EU-domstolen har, som redovisats ovan, i flera domar pekat på just möjligheten till riktad lagring. Med begreppet riktad lagring avses normalt 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.

EU-domstolen överlåter åt medlemsländerna att utforma den modell för datalagring som bäst passar landets egna förhållanden, så länge lagringen till sin omfattning inte berör alla, eller nästan alla personer, som ingår i befolkningen. Detta gäller också under förutsättning att lagringen sker för att bekämpa grov brottslighet samt att den är proportionerlig och baserad på objektiva och icke-diskriminerande faktorer.

Vi lämnar därför i fortsättningen förslag på hur riktad lagring skulle kunna se ut. Utgångspunkten för dessa förslag är att de ska främja en effektiv brottsbekämpning samtidigt som de ska vara proportionerliga och rimliga. Ytterligare en utgångspunkt är att lagringen måste vara praktiskt hanterbar. I detta ligger bl.a. att reglerna för lagringen helst inte bör bli föremål för täta ändringar över tid. Lagringen och omfattningen av denna får alltså inte kränka enskildas personliga integritet på ett sätt som inte är acceptabelt i en rättsstat. Detta gäller också tillgången till lagrade uppgifter. Vid den närmare utformningen

av regleringen måste man alltså ha denna helhetssyn för ögonen och i alla enskildheter göra proportionerliga och rimliga avvägningar.

8.2 Vad menas med grova brott och grov brottslighet?

Utredningens bedömning: Brott och brottslighet som i dag ger rätt att använda hemliga tvångsmedel är att betrakta som grova brott och grov brottslighet.

Tillgång till lagrade uppgifter kan enligt EU-domstolen bara beviljas för uppgifter om personer som misstänks planera, begå eller ha begått ett grovt brott, eller som har en annan inblandning i ett sådant brott. I våra överväganden om en lagringsskyldighet och tillgång till uppgifter i syfte att bekämpa grova brott och brottslig verksamhet som innefattar grova brott finns det därför anledning att närmare belysa vad som avses med begreppen. EU-domstolen har inte uttalat sig om vad som avses med begreppet grov eller allvarlig brottslighet när det rör sig om datalagring. Det finns inte heller någon generell definition av grov eller allvarlig brottslighet i EU-rätten eller enligt svensk rätt. Regeringen har i förarbetena till den nu gällande datalagringsregleringen gjort bedömningen att de brott som ger rätt att använda hemliga tvångsmedel enligt rättegångsbalken, inhämtningslagen, preventivlagen och lagen om särskild utlänningskontroll[1] är att betrakta som sådan grov brottslighet som enligt EU-domstolen kan motivera att brottsbekämpande myndigheter ges tillgång till lagrade uppgifter.[2] Vi gör ingen annan bedömning när det gäller begreppets innebörd i detta sammanhang.

Efter regeringens uttalanden har lagen om hemlig dataavläsning tillkommit men den lagen omfattar endast sådan brottslighet som andra hemliga tvångsmedel kan användas för och påverkar inte bedömningen.

Det bör även nämnas att vi inte gör någon skillnad mellan begreppen allvarlig brottslighet, som är ett begrepp som ibland också förekommer i dessa sammanhang, och grov brottslighet i datalagringshänseende.

[1] Lagen (1991:572) om särskild utlänningskontroll upphävdes genom lagen (2022:700) om särskild kontroll av vissa utlänningar.
[2] Se prop. 2018/19:86 s. 64–65.

8.3 Överväganden och förslag

8.3.1 Geografiskt riktad lagring

Som vi skrivit ovan bör vi lämna ett förslag om hur riktad lagring skulle kunna utformas i Sverige. Riktad lagring på grundval av geografiska kriterier förekommer i Belgien och Danmark. Vi resonerar nedan kring hur riktad lagring skulle kunna genomföras i Sverige.

Vilken inriktning bör en geografiskt riktad lagring ha?

Utredningens bedömning: Geografiskt riktad lagring bör 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.

Vi har i avsnitt 6.5.1 och 6.5.3 beskrivit hur riktad geografisk lagring är reglerad i Danmark och Belgien. Mot bakgrund av EU-domstolens krav gör vi bedömningen att geografisk riktad lagring är ett alternativ som bör övervägas för att kunna lagra trafik- och lokaliseringsuppgifter för brottsbekämpning. Som vi redogjort för ovan finns det dock principiell kritik mot geografiskt riktad lagring. Ett argument mot sådan lagring är att den inte alltid är effektiv, eftersom det på förhand inte går att avgöra var brott kommer att begås. Ytterligare ett argument mot geografiskt riktad lagring är att en sådan skulle innebära olika möjligheter att bekämpa brottslighet i olika delar av landet. En viss möjlighet till anpassning genom vad vi kallar *utökad riktad lagring* skulle emellertid delvis kunna läka denna brist. Vi återkommer till frågan om utökad riktad lagring i avsnitt 8.3.2. Vi vill här sammanfattningsvis beskriva hur en reglering med geografiskt riktad lagring som syftar till att bekämpa grov brottslighet kan utformas.

En riktad lagringsåtgärd avseende trafik- och lokaliseringsuppgifter kan med strikt iakttagande av proportionalitetsprincipen grundas på ett geografiskt kriterium. Det får ske när behöriga myndigheter på grundval av objektiva och icke-diskriminerande faktorer bedömer att det i ett eller flera geografiska områden finns en förhöjd risk för förberedelse eller genomförande av grov brottslighet.[3] EU-domstolen

[3] Se SpaceNet-domen p. 108.

understryker att behöriga nationella myndigheter kan vidta en riktad lagringsåtgärd som grundar sig på bl.a. den genomsnittliga graden av brottslighet inom ett geografiskt område, utan att de nödvändigtvis har några konkreta indikationer på att allvarliga brott håller på att förberedas eller begås i de berörda områdena. En riktad lagring som grundar sig på ett sådant kriterium, kan avse både platser som kännetecknas av ett stort antal allvarliga brott och platser som är särskilt utsatta från brottssynpunkt, beroende på den grova brottslighet som avses och situationen i respektive medlemsstat. Det innebär, enligt EU-domstolen, att den i princip inte heller är av sådan art att den kan ge upphov till diskriminering, eftersom kriteriet avseende den genomsnittliga graden av allvarlig brottslighet i sig inte har något samband med potentiellt diskriminerande omständigheter.[4] Sammantaget tillåter EU-rätten att geografiskt riktad lagring får ske i områden där det går att konstatera att det finns större sannolikhet för att det begås allvarliga brott.

Hur ska risken för grov brottslighet på en viss geografisk plats bedömas?

Utredningens förslag: Geografiskt riktad lagring ska grunda sig på den officiella statistiken över anmälda brott som redovisas av Brå och med kommunerna som geografiska enheter. Sannolikheten för att en viss kommun är mer brottsutsatt än en annan ska bedömas utifrån ett genomsnitt av anmälda brott delat med befolkningsmängden under en treårsperiod som föregår lagringsskyldigheten.

Enligt EU-domstolens praxis kan, som nämnts, den genomsnittliga graden av brottslighet inom ett geografiskt område utgöra ett kriterium för riktad lagring. EU-domstolen anser under sådana förhållanden att det kriterium lagringen utgår ifrån är objektivt och icke-diskriminerande. Vi är medvetna om att det kan anläggas ett annat perspektiv på denna fråga. Som regeringen redogjorde för i förarbetena till den nu gällande datalagringsregleringen finns en tämligen stor risk för diskriminering eller i övrigt stötande effekter när lagringen

[4] Se SpaceNet-domen p. 109.

riktas mot bl.a. ett visst utpekat område.[5] Det finns således olika syn på frågan om geografiskt riktad lagring som modell för datalagring. Eftersom våra förslag i denna del utgår från EU-domstolens praxis lägger vi, trots regeringens tidigare uttalanden, fram förslag om geografiskt riktad lagring. Vi strävar dock efter att utforma förslagen på ett sådant sätt att de negativa effekterna av lagringen blir så små som möjligt.

Beslutsunderlaget för den geografiskt riktade lagringen

Vi har i avsnitt 6.5 redogjort för olika modeller för geografiskt riktad lagring i andra länder. Enligt den danska lagstiftningen får riktad geografisk lagring ske baserat på kriminalstatistik avseende anmälda brott som sätts i relation till landet som helhet. Den danska modellen har fördelen att kriterierna för den geografiskt riktade lagringen utgår från sannolikheten att en plats är mer brottsutsatt än en annan plats. Jämfört med den belgiska modellen, där den genomsnittliga brottsligheten inom en region först måste uppgå till i genomsnitt minst tre allvarliga brott per 1 000 invånare, framstår den danska modellen enligt vår mening av flera skäl som mer välgrundad än den belgiska.

Vi ser, när det gäller den belgiska modellen, problem med en reglering som bygger på att man ska utgå från att det förekommer ett visst antal grova brott i ett område innan datalagring får ske. En sådan modell kräver att man tar ställning till antalet grova brott som skulle utlösa en datalagring. Ett sådant ställningstagande riskerar att bli godtyckligt. Vidare är det också problematiskt ur det perspektivet att om den nedre gränsen sätts för lågt blir följden att den geografiskt riktade lagringen kan komma att omfatta hela landet. Om den å andra sidan sätts för högt, går själva syftet med datalagringen att bekämpa grov brottslighet, förlorat.

Den riktade lagringen i Belgien omfattar för närvarande hela landet och det pågår även en rättsprocess om giltigheten av den belgiska datalagringsregleringen vid landets konstitutionsdomstol. En modell av riktad lagring som i praktiken resulterar i generell lagring kan ge upphov till nya tolkningsfrågor som kan komma att prövas av EU-domstolen. Mot den bakgrunden ställer vi oss tveksamma till utformningen av en sådan modell.

[5] Se prop. 2018/19:86. s. 34.

Den danska modellen för lagring baserad på kriminalstatistik avseende anmälda brott i relation till landet som helhet är dock inte utan nackdelar. En nackdel med den danska modellen är att den tillåter lagring även om brottsligheten skulle upphöra i hela eller stora delar av landet. En sådan utveckling verkar dock tyvärr inte särskilt sannolik i dag. Motsatsvis skulle lagringen inte öka om brottsligheten tilltog kraftigt men jämnt fördelat över hela landet. Om den utvecklingen har sin grund i ett akut hot mot den nationella säkerheten, finns i och för sig möjligheten att besluta om nationell säkerhetslagring. I annat fall behöver lagringen kompletteras med ytterligare möjligheter till datalagring.

En variant för geografiskt riktad lagring som vi övervägt är en modell som bygger på att lagringen ska ske med utgångspunkt från ett beräknat nationellt medelvärde av brottsanmälningar för de senaste tio åren. Medelvärdet skulle sedan sättas i relation till förekomsten av brottsanmälningar i geografiskt avgränsade områden. Lagringen ska sedan ske i de områden där antalet brottsanmälningar är högre än medelvärdet. Nackdelen med en sådan modell är dock att det kommer att ta väldigt lång tid för aktuell brottslighet att få genomslag i statistiken. Det finns en alltför stor tröghet inbyggd i modellen. Ett nationellt medelvärde kommer också att leda till att få områden kommer att omfattas av lagring, se mer om beräkning av medelvärdet nedan. Det blir således inte fråga om någon bred lagring. Det är alltså sammantaget ingen riktigt bra modell för brottsbekämpningen.

Vi kan konstatera att de ovan berörda modellerna inte är utan nackdelar. Den danska modellen framstår dock enligt vår bedömning som ett bättre alternativ jämförd med de andra förslagen.

Vi menar att utgångspunkten för riktad geografisk lagring bör vara att sannolikheten för allvarlig brottslighet i ett visst område sätts i relation till sannolikheten för allvarlig brottslighet i andra områden i likhet med vad som gäller i Danmark.

En sådan modell för lagring behöver dock anpassas till svenska förhållanden. Ett sätt att skapa en motsvarande reglering i Sverige är att utgå från den officiella statistiken som regleras i lagen (2001:99) om den officiella statistiken och den kompletterande förordningen (2001:100) om den officiella statistiken. Brå ansvarar enligt bilagan till förordningen för statistik över brott, personer lagförda för brott, kriminalvård och återfall i brott. Myndighetens rapporter som utgör officiell statistik är för närvarande:

- Anmälda brott.
- Konstaterade fall av dödligt våld.
- Handlagda brott.
- Misstänka personer.
- Handlagda brottsmisstankar.
- Personer lagförda för brott.
- Återfall i brott.
- Kriminalvård.
- Nationella trygghetsundersökningen (NTU).
- Skolundersökningen om brott (SUB).
- Politikernas trygghetsundersökning (PTU).

De två sistnämnda rapporterna (SUB och PTU) omfattar begränsade delar av brottsligheten. Den tredje sista rapporten i listan (NTU) avser en urvalsbaserad frågeundersökning till befolkningen om deras utsatthet för brott, som dels inte fångar många av de grova brotten i samhället dels normalt sett inte redovisas ned till kommunnivå varje år. Därför bedöms den vara mindre lämplig för den användning det nu handlar om. När det gäller flera av de åtta först listade rapporterna, som alla bygger på registerbaserade uppgifter, knyter de an till senare skeden i rättsprocessen och omfattar därför bara den mindre andel av de registrerade brotten som går igenom hela rättskedjan och utmynnar i lagföringar och domar och så vidare. Den av de registerbaserade rapporterna som så att säga ligger närmast själva brottsligheten och som därför också innehåller högst antal är statistiken över anmälda brott. Den statistiken har också en annan viktig egenskap och det är att den årligen redovisas ned till kommunnivå, vilket inte de övriga av de åtta registerbaserade rapporterna gör.

Brå redovisar de anmälda brotten sammanlagt och indelat efter typ av brott. Uppgifterna ges per kalenderår, kvartal och månad. Statistiken redovisas för hela landet, efter det område där det anmälda brottet har handlagts och efter kommun respektive den stadsdel i storstadskommunerna där brottet har begåtts. Sedan 2015 indelas sta-

tistiken efter Polismyndighetens sju regioner, som har ersatt den tidigare indelningen efter län.

För vissa brott saknas uppgift om kommun eller stadsdel där brottet begåtts och då redovisas brotten endast på regionnivå (efter var brottet har handlagts). Statistiken över anmälda brott omfattar samtliga händelser som har anmälts och registrerats som ett brott i Sverige under ett kalenderår. I statistiken ingår även anmälda händelser som efter utredning inte visar sig vara brott eller där brott inte kan styrkas. Av samtliga anmälda brott i statistiken utgör endast några procent varje år sådana ”icke brottsliga” händelser. För vissa enstaka brottstyper, t.ex. mord och dråp, kan denna andel dock vara betydligt större. Det kan även i viss mån gälla anmälda brott på mer detaljerad geografisk nivå. I statistiken redovisas antalet anmälda brott totalt och per 100 000 invånare. Även antalet anmälda fall av en viss brottstyp redovisas.

Statistiken över anmälda brott grundar sig på de uppgifter som polis och åklagare med flera registrerar i sina ärendehanteringssystem. När ett brott exempelvis kommer till Polismyndighetens kännedom upprättas en brottsanmälan som läggs in i ärendehanteringssystemet DurTvå. Uppgifterna i anmälningarna levereras sedan i förbestämda utbyten digitalt till Brå. Även uppgifter från andra myndigheters ärendesystem levereras på likande sätt digitalt till Brå. Hos Brå granskas och bearbetas uppgifterna innan de sammanställs till statistik.

Brottsredovisningen omfattar brott mot brottsbalken, lagen (1951:649) om straff för vissa trafikbrott, narkotikastrafflagen (1968:64) och brott mot andra specialstraffrättsliga författningar för vilka fängelse ingår i straffskalan. Försök, förberedelse och stämpling till brott redovisas i statistiken som regel tillsammans med fullbordade brott. Försöksbrotten redovisas separat enbart för mord och dråp, våldtäkt, tillgrepp av motorfordon och bostadsinbrott. I samband med att ett brott registreras hos Polismyndigheten klassificeras brottet med hjälp av en brottskod i enlighet med anvisningar som utfärdas av Brå i samråd med Polismyndigheten, Åklagarmyndigheten, Ekobrottsmyndigheten och Tullverket.[6]

Med ledning av den brottsstatistik som förs av Brå finns ett användbart underlag för att bedöma om det finns en förhöjd risk för grov brottslighet i ett avgränsat geografiskt område. En fördel med

[6] https://bra.se/statistik/kriminalstatistik/anmalda-brott/om-statistiken.html. Hämtat den 20 april 2023.

att inhämta underlag från Brå:s officiella statistik är att den just är officiell och därmed kvalitetssäkrad på hög nivå. En annan fördel är att myndigheten har en oberoende ställning i förhållande till de brottsbekämpande myndigheterna. Den brottsstatistik som Brå presenterar lever enligt vår bedömning upp till EU-domstolens krav på bedömningsunderlag som är objektivt och icke-diskriminerande. Vi anser därför att den officiella statistiken som redovisas av Brå ska utgöra grunden för den geografiskt riktade lagringen. Frågan blir närmast hur den geografiska avgränsningen ska ske.

Den geografiska avgränsningen vid riktad lagring

Nästa fråga är hur den geografiska avgränsningen bör göras. Det går i och för sig att i likhet med den belgiska lagstiftningen utgå från polisområdesregioner. Nackdelen med det är emellertid, för svenska förhållanden, att det endast finns sju polisregioner varav polisregion Norr täcker en stor del av Sveriges yta. Så få och stora regioner riskerar att leda till att den riktade lagringen i praktiken kan jämställas med en generell lagring, vilket står i strid med EU-rätten enligt den praxis som vi har redogjort för i avsnitt 6.3. Den danska modellen med områden på 3 gånger 3 kilometer stämmer inte med hur brottsstatistiken redovisas i Sverige och bör av det skälet inte heller vara en förebild för våra förslag.

En modell skulle kunna vara att utgå från en administrativ indelning av Sverige som styr annan statlig och regional verksamhet, nämligen länen. En fördel med länen är att de är 21 till antalet, alltså tre gånger fler än polisregionerna, och att Polismyndighetens regioner också är baserad på länsindelning. Sedan den nya regionindelningen inom Polismyndigheten tillkom redovisar Brå emellertid inte statistiken över anmälda brott uppdelat på län, eftersom det saknas data för det. Det finns i och för sig inget som hindrar att uppgifter om anmälda brott skulle kunna hämtas direkt från Polismyndigheten, men vi bedömer att även länen är för få till antalet om områden ska kunna sättas i relation till varandra.

Ytterligare en geografisk avgränsning som bör övervägas är kommunerna. I Sverige finns det i dag 290 kommuner med stor variation i storlek och antalet invånare. Kommunerna är tydligt avgränsade och har som geografisk enhet fördelen att Brå:s statisk redovisas per

kommun, respektive stadsdel i storstadskommunerna Stockholm, Göteborg och Malmö. En annan fördel är att antalet kommuner med varierande storlek och antal invånare skapar en relativ tillförlitlig bild av om det finns större sannolikhet för att en viss kommun utgör en plats för grova brott jämfört med en annan kommun. En möjlig invändning mot kommunerna som geografiska enheter är att även dessa utgör relativt stora områden och att mindre geografiska enheter bör övervägas. Vi gör dock bedömningen att för små geografiska enheter innebär en alltför inskränkt lagring för en effektiv brottsbekämpning. Dessutom innebär normalt den omständigheten att ett visst område är brottsutsatt att även närområdet blir förhållandevis brottsutsatt. Den som begår grova brott eller ägnar sig åt grov brottslig verksamhet stannar sällan kvar på ett och samma ställe. Även av det skälet är den kommunikation som sker i anslutning till ett brottsutsatt område av betydelse för de brottsbekämpande myndigheterna.

Vi anser mot den bakgrunden att kommunerna är den mest lämpliga geografiska avgränsningen. Vi har kommit till denna slutsats trots att brott som saknar uppgift om plats redovisas på regionnivå eller beroende av var brottet har handlagts.

Urval av brott

Nästa fråga är om samtliga brottsanmälningar eller endast ett urval av dessa ska ingå i det statistiska underlaget. Enbart sett till innehållet i statistiken över anmälda brott innehåller den till övervägande del lindriga brott, eftersom det hör till brottslighetens karaktär att den lindriga delen av brottsligheten är mer omfattande än den allvarliga. Om beräkningen ska avgränsas till att enbart utgå från grova brott, behöver det göras bearbetningar av statistiken så att beslut om lagring i större utsträckning bygger på uppgifter om förhållandevis grov brottslighet och i mindre utsträckning på lindriga brott.

Ur tydlighetshänseende finns det fördelar med en avgränsning som knyter an till straffskalorna, exempelvis brott för vilket det inte är föreskrivet lindrigare straff än fängelse exempelvis sex månader. Brottsindelningen i statistiken över anmälda brott följer visserligen kapitelindelningen i brottsbalken och vissa specialstraffrättsligt reglerade brott. Men den tar inte fasta på straffskalornas utformning. I stället rör det sig om uppdelningar genom lista med ett 30-tal övergripande

kategorier (motsvarande 22 kapitel i brottsbalken och ett drygt tiotal specialstraffrättsliga förordningar), samt över 800 rader med olika brottstyper som baseras på brottskoder som registreras hos myndigheterna. Brottskoderna baseras i grunden alltid på enskilda brott eller grupper av brott med egna bestämmelser i lagstiftningen, men de är inte så detaljerade att det går att utläsa de anmälda brottens exakta straffvärde. Som nämndes inledningsvis redovisas till exempel fullbordade brott sammantaget med försöksbrott. Statistikens grundläggande uppbyggnad såsom den ser ut i dag leder således till att det inte kan bli fråga om statistik som endast omfattar grov brottslighet.

Syftet med geografiskt riktad lagring är att identifiera områden där det finns behov av lagring, eftersom det i dessa områden finns en jämförelsevis större sannolikhet att det kommer att begås grova brott. Det är inte självklart hur urvalet bör se ut för att bäst få fram vilka kommuner där lagring bör förekomma. Det kan ligga nära till hands att anta att urvalet bör grunda sig endast på mer allvarlig brottslighet. Men det är svårt att dra några säkra slutsatser om detta.

Vi har övervägt om Brå ska ges i uppdrag att ta fram statistik som tydligare ringar in den grova brottsligheten, men vi bedömer inte att fördelarna med ett sådant underlag är tillräckliga för att väga upp det merarbete som uppdraget skulle innebära. Någon exakthet går det heller aldrig att uppnå med utgångspunkt i ett statistiskt underlag som utgår från anmälningar om brott. Ett högt antal brottsanmälningar över lag torde i sig ofta vara en indikator på även grov brottslighet. Vi bedömer därför att denna uppgift utgör en tillräckligt god indikator på behovet av lagring.

Vår slutsats är att det är tillräckligt att beräkningen sker utifrån samtliga brottsanmälningar.

Beräkning av sannolikheten

Utgångspunkten är att de kommuner som har genomsnittligt högre sannolikhet för grova brott än andra kommuner ska lagra uppgifter. För det krävs en beräkning av sannolikheten.

Vårt förslag är att beräkningarna ska grunda sig på årsvisa statistiska uppgifter. Vidare är det viktigt att inte tillfälliga avvikelser i underlaget får för stor inverkan på utfallet. Därför föreslår vi att genomsnittet beräknas genom att det tas fram aritmetiska medel-

värden av antalet anmälda brott över tre på varandra följande år i kommunerna.

För att undvika en allt för stor eftersläpning mellan anmälningar om brott och beslut om geografiskt riktad lagring, bör beslut fattas så snart som Brå redovisat den officiella statistiken. Med dagens periodisering av statistiken skulle det även behövas ett mellankommande år före det år som beslutet avser, dvs. att 2023 års beslut skulle utgå från 2019–2021 års statistik. Det beror på att statistiken för år 2022 inte är färdigställd vid inledningen av år 2023.

Ett alternativ, som vi bedömer är mer lämpligt, är att använda sig av s.k. brutna år, eftersom föregående års statistik kan användas tidigare. Medelvärdet bör således beräknas genom att summan av de tre årens anmälda brott divideras med tre (jfr den danska modellen i avsnitt 6.5). Brå publicerar i regel sin slutliga statistik under tidig vår.[7] Ett beslut om geografiskt riktad lagring bör därför kunna fattas den 1 juni.

Därutöver råder det mycket stora variationer i kommunernas invånarantal, och därmed hur omfattande den anmälda brottsligheten av den anledningen är. Om inte hänsyn tas till antalet invånare kommer några få kommuner, med högt antal invånare och därmed hög andel brottsanmälningar, att driva upp medelvärdet på totalen. Följden skulle bli att den geografiskt riktade lagringen endast skulle omfatta cirka 20 procent av landets samtliga 290 kommuner.

För att komma fram till jämförbara sannolikheter föreslår vi därför att det framräknade antalet anmälda brott i kommunerna, dvs. medelvärdet över tre år, relateras till befolkningsstorleken, genom en beräkning av antalet anmälda brott per 1 000 invånare.

Någon exakthet är dock svår att uppnå även i det här avseendet. Exempelvis förekommer fler brottsanmälningar i stora städer på grund av att fler människor vistas där än de som är folkbokförda.

Vi har övervägt om det årligen sammantagna geografiska området för riktad lagring som vår föreslagna modell kommer att generera kan anses bli för stort, inte minst med tanke på våra kompletterande förslag om utökad riktad lagring, se avsnitt 8.3.3. Som framgår av ögonblicksbilden i nästa avsnitt omfattar det geografiska området för riktad lagring mindre än halva landets yta. Vi bedömer därför att så inte är fallet.

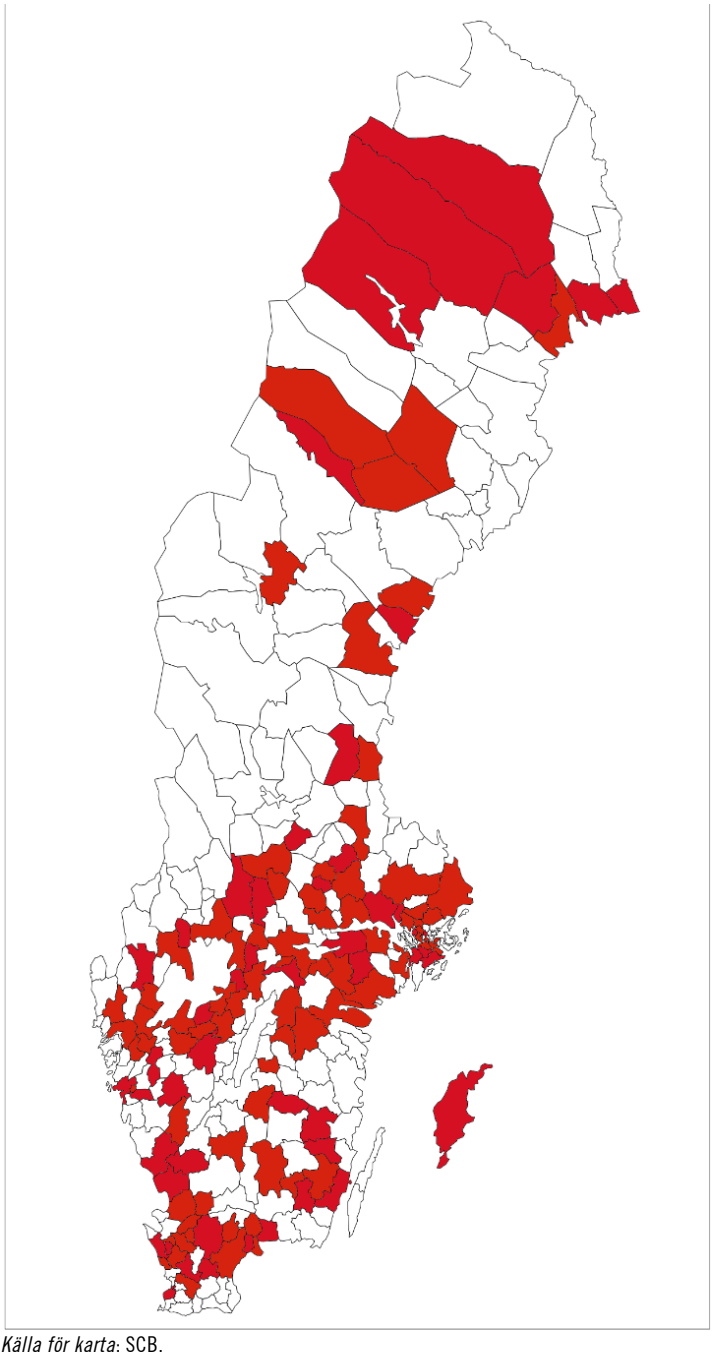
[7] Se Brås Publiceringsplan 2023, https://bra.se/statistik/publiceringsplan.html. Hämtat den 20 april 2023.

Vi är medvetna om att gränsvärdet kan utformas på annat sätt och då få en annan träffyta. Vi gör dock bedömningen att den beskrivna modellen i förening med möjligheten att fatta beslut om utökad riktad lagring, se avsnitt 8.3.2 ger ett proportionerligt och rimligt resultat i avvägningen mellan brottsbekämpningen och skyddet för den personliga integriteten. Den föreslagna modellen kan förstås modifieras, exempelvis genom att bara kommuner med ännu högre eller lägre nivå av brottsanmälningar ska ha riktad lagring, exempelvis bara kommuner vars antal anmälningar ligger inom den översta kvartilen respektive den nedersta kvartilen.

Ögonblicksbild

Enligt våra beräkningar motsvarar gränsvärdet för geografiskt riktad lagring 92,1 anmälda brott per 1 000 invånare, räknat utifrån brottsanmälningar per kommun för åren 2020–2022. Ett sådant resultat motsvarar geografiskt riktad lagring i 132 av landets alla 290 kommuner. Invånarna i de kommuner som omfattas av lagringen enligt våra beräkningar motsvarar cirka 7,3 miljoner av Sveriges 10,4 miljoner invånare. För att tydligt illustrera utfallet av geografiskt riktad lagring redovisar vi i det följande såväl karta som tabeller.

Figur 8.1 Kommuner som baserat på statistik för år 2020–2022 skulle omfattats av lagring enligt utredningens beräkningar



Källa för karta: SCB.

De tre kolumnerna med årtal motsvarar antalet brottsanmälningar i respektive kommun vid varje angivet år. Kolumnen med medelvärde motsvarar det genomsnittliga värdet av brottsanmälningar för åren 2020–2022 delat med antalet invånare och multiplicerat med 1 000.

Tabell 8.1 Kommuner vars medelvärden understiger gränsen för geografiskt riktad lagring

Kommuner	År 2020	År 2021	År 2022	Invånare	Medelvärde
Ale kommun	2 591	2 731	2 450	32 148	80,6
Alvesta kommun	1 598	1 487	1 625	20 287	77,4
Aneby kommun	431	399	405	6 892	59,7
Arboga kommun	1 522	1 147	1 206	14 100	91,6
Arvidsjaur kommun	532	396	396	6 143	71,8
Arvika kommun	2 184	2 206	2 245	25 854	85,5
Askersund kommun	912	862	939	11 534	78,4
Berg kommun	509	480	549	7 135	71,9
Bjurholm kommun	167	191	159	2 395	72,0
Bollebygd kommun	532	667	653	9 634	64,1
Borgholm kommun	842	864	963	10 895	81,7
Boxholm kommun	434	266	329	5 512	62,2
Bräcke kommun	543	453	429	6 175	76,9
Båstad kommun	1 315	1 145	1 169	15 636	77,4
Dals-Ed kommun	328	356	324	4 756	70,6
Eda kommun	723	806	793	8 490	91,2
Ekerö kommun	2 004	2 050	2 020	29 096	69,6
Essunga kommun	622	491	354	5 698	85,8
Falun kommun	4 985	4 648	4 542	59 837	79,0
Finspång kommun	1 586	1 495	1 912	21 889	76,0
Forshaga kommun	645	798	593	11 606	58,5
Färgelanda kommun	589	586	486	6 576	84,2
Gagnef kommun	399	470	456	10 502	42,1
Gislaved kommun	3 028	2 181	2 286	29 556	84,5
Gnesta kommun	1 094	947	1 098	11 513	90,9
Gnosjö kommun	715	695	687	9 570	73,0
Grästorp kommun	406	433	382	5 730	71,0
Habo kommun	489	461	481	12 810	37,2
Hagfors kommun	1 037	982	998	11 553	87,0
Hallstahammar kommun	1 522	1 600	1 415	16 608	91,1
Hammarö kommun	726	732	669	16 765	42,3
Heby kommun	1 111	1 037	999	14 303	73,3
Hedemora kommun	1 506	1 254	1 427	15 458	90,3
Herrljunga kommun	808	751	795	9 501	82,6

Kommuner	År 2020	År 2021	År 2022	Invånare	Medelvärde
Hjo kommun	557	534	684	9 233	64,1
Hofors kommun	780	737	842	9 578	82,1
Hudiksvall kommun	3 570	3 259	3 183	37 744	88,4
Härjedalen kommun	885	845	822	10 114	84,1
Höganäs kommun	1 954	1 903	1 897	27 589	69,5
Höör kommun	1 423	1 523	1 576	16 954	88,9
Jönköping kommun	13 564	12 345	13 177	143 579	90,7
Karlsborg kommun	412	348	483	6 965	59,5
Karlskrona kommun	5 484	5 128	5 810	66 708	82,1
Kil kommun	700	782	795	12 134	62,6
Kinda kommun	625	635	522	10 048	59,1
Kiruna kommun	2 170	1 801	1 727	22 555	84,2
Knivsta kommun	1 262	1 403	1 337	19 818	67,3
Krokom kommun	985	1 033	822	15 352	61,7
Kungsbacka kommun	5 717	5 771	5 934	85 301	68,1
Kungsör kommun	625	558	518	8 787	64,5
Kungälv kommun	4 460	4 240	4 036	48 271	87,9
Kävlinge kommun	2 425	2 488	2 626	32 341	77,7
Lekeberg kommun	420	493	597	8 603	58,5
Leksand kommun	768	758	885	16 012	50,2
Lerum kommun	3 331	3 339	3 117	43 399	75,2
Lidingö kommun	3 399	4 122	3 518	48 162	76,4
Lindesberg kommun	1 869	1 892	2 155	23 601	83,6
Ljungby kommun	2 669	2 418	2 769	28 433	92,1
Ljusdal kommun	1 521	1 442	1 414	18 804	77,6
Lomma kommun	1 466	1 404	1 753	24 638	62,5
Lysekil kommun	1 436	1 332	1 109	14 266	90,6
Malung-Sälen kommun	704	766	1 027	10 218	81,5
Malå kommun	205	206	181	3 034	65,0
Mark kommun	2 980	2 993	2 752	35 201	82,6
Mora kommun	1 521	1 961	1 455	20 670	79,6
Mullsjö kommun	570	601	601	7 430	79,5
Munkfors kommun	323	205	231	3 680	68,8
Mölndal kommun	6 531	6 329	6 392	69 943	91,8
Mönsterås kommun	1 068	1 233	1 158	13 258	87,0
Mörbylånga kommun	775	818	974	15 722	54,4
Nora kommun	739	723	621	10 721	64,8
Nordanstig kommun	846	864	731	9 480	85,8
Nordmaling kommun	612	599	352	7 100	73,4
Norsjö kommun	291	264	214	3 971	64,6
Nykvarn kommun	1 039	838	826	11 500	78,3

Kommuner	År 2020	År 2021	År 2022	Invånare	Medelvärde
Ockelbo kommun	535	571	386	5 865	84,8
Orsa kommun	611	496	551	6 918	79,9
Orust kommun	1 135	1 047	1 068	15 345	70,6
Osby kommun	1 129	1 138	1 309	13 269	89,8
Oskarshamn kommun	2 383	2 320	2 110	27 220	83,4
Ovanåker kommun	767	755	595	11 711	60,3
Oxelösund kommun	993	1 143	1 188	12 132	91,3
Pajala kommun	428	466	358	5 973	69,9
Piteå kommun	3 449	2 952	3 244	42 323	76,0
Ragunda kommun	366	329	345	5 210	66,5
Robertsfors kommun	546	388	546	6 786	72,7
Ronneby kommun	2 402	2 475	2 789	29 200	87,5
Rättvik kommun	622	766	716	11 103	63,2
Salem kommun	1 595	1 607	1 457	17 252	90,0
Simrishamn kommun	1 480	1 478	1 416	19 267	75,7
Sjöbo kommun	1 658	1 601	1 837	19 497	87,1
Skellefteå kommun	6 902	6 333	6 599	73 393	90,1
Skurup kommun	1 338	1 497	1 346	16 419	84,9
Smedjebacken kommun	687	685	705	10 933	63,3
Sorsele kommun	181	154	144	2 460	64,9
Sotenäs kommun	808	841	715	9 125	86,4
Staffanstorp kommun	1 840	1 855	1 906	26 242	71,1
Stenungsunds kommun	2 474	2 334	2 604	27 556	89,7
Storfors kommun	264	197	282	3 948	62,7
Storuman kommun	472	392	460	5 808	76,0
Strömstad kommun	1 251	1 205	1 179	13 277	91,3
Strömsund kommun	1 000	973	799	11 473	80,5
Sunne kommun	807	915	866	13 355	64,6
Surahammar kommun	1 005	785	803	10 099	85,6
Svedala kommun	1 383	1 629	1 666	23 222	67,1
Säter kommun	696	615	682	11 242	59,1
Sävsjö kommun	795	776	848	11 709	68,9
Söderköping kommun	784	835	906	14 673	57,4
Tanum kommun	926	1 010	971	12 965	74,7
Tibro kommun	837	776	947	11 281	75,6
Tidaholm kommun	1 332	917	1 009	12 825	84,7
Tierp kommun	2 080	1 943	1 765	21 485	89,8
Timrå kommun	1 761	1 630	1 334	17 923	87,9
Tingsryd kommun	1 043	1 003	1 170	12 319	87,0
Tjörn kommun	1 096	980	1 005	16 312	63,0
Tomelilla kommun	1 372	1 059	1 231	13 712	89,0
Torsby kommun	787	794	928	11 472	72,9
Torsås kommun	749	454	482	7 113	79,0

Kommuner	År 2020	År 2021	År 2022	Invånare	Medelvärde
Tranemo kommun	876	1 092	828	11 937	78,1
Trelleborg kommun	4 060	3 391	4 006	46 231	82,6
Trosa kommun	1 173	1 101	1 507	14 658	86,0
Täby kommun	6 378	6 462	5 075	73 955	80,7
Ulricehamn kommun	1 978	1 947	1 942	24 898	78,5
Umeå kommun	12 114	10 879	11 098	130 997	86,7
Uppvidinge kommun	731	681	664	9 449	73,2
Vadstena kommun	454	489	574	7 528	67,2
Vaggeryd kommun	1 104	1 098	1 209	14 746	77,1
Valdemarsvik kommun	501	450	440	7 660	60,5
Vansbro kommun	424	363	427	6 776	59,7
Varberg kommun	4 809	5 143	5 132	66 658	75,4
Vaxholm kommun	721	553	483	11 996	48,8
Vellinge kommun	2 248	2 010	2 105	37 452	56,6
Vetlanda kommun	1 925	1 672	2 124	27 621	69,0
Vimmerby kommun	1 174	1 079	1 274	15 578	75,5
Vindeln kommun	387	384	427	5 550	72,0
Vårgårda kommun	943	952	876	12 180	75,8
Vännäs kommun	623	469	377	9 054	54,1
Värmdö kommun	4 323	4 015	3 846	46 232	87,8
Västervik kommun	3 158	2 813	3 281	36 747	83,9
Ydre kommun	174	144	131	3 695	40,5
Ystad kommun	2 536	2 414	2 818	31 560	82,0
Åmål kommun	1 310	1 024	1 026	12 318	90,9
Ånge kommun	856	704	697	9 233	81,5
Åre kommun	1 102	925	1 133	12 271	85,8
Årjäng kommun	620	562	514	9 942	56,9
Åtvidaberg kommun	641	597	684	11 462	55,9
Älmhult kommun	1 203	1 382	1 607	17 963	77,8
Älvdalen kommun	470	511	724	7 042	80,7
Älvkarleby kommun	832	903	853	9 627	89,6
Älvsbyn kommun	797	565	544	8 009	79,3
Ängelholm kommun	4 349	3 539	3 641	43 633	88,1
Öckerö kommun	620	742	672	12 902	52,5
Ödeshög kommun	357	389	434	5 309	74,1
Örnsköldsvik kommun	5 271	5 285	4 472	55 823	89,7
Österåker kommun	3 948	3 744	3 414	48 234	76,8
Östhammar kommun	1 703	1 529	1 586	22 364	71,8
Överkalix kommun	241	298	212	3 252	77,0
Övertorneå kommun	272	313	361	4 211	74,9

Tabell 8.2 Kommuner vars medelvärden överstiger gränsen för geografiskt riktad lagring

Kommuner	År 2020	År 2021	År 2022	Invånare	Medelvärde
Alingsås kommun	3 819	4 138	3 769	41 853	93,4
Arjeplog kommun	334	192	284	2 707	99,7
Avesta kommun	2 366	2 429	2 079	22 925	99,9
Bengtsfors kommun	1 016	1 042	703	9 409	97,8
Bjuv kommun	2 063	1 808	1 894	15 842	121,3
Boden kommun	3 341	2 727	2 572	28 160	102,3
Bollnäs kommun	2 935	2 742	2 606	26 753	103,2
Borlänge kommun	5 821	6 162	6 239	52 254	116,2
Borås kommun	13 014	13 593	12 354	114 091	113,8
Botkyrka kommun	13 660	12 773	12 881	95 318	137,5
Bromölla kommun	1 384	1 304	1 084	12 650	99,4
Burlöv kommun	2 517	2 421	2 599	19 753	127,2
Danderyd kommun	3 565	4 078	4 122	32 803	119,6
Degerfors kommun	954	1 001	1 042	9 534	104,8
Dorotea kommun	307	217	210	2 459	99,5
Eksjö kommun	1 928	1 886	1 971	17 834	108,1
Emmaboda kommun	1 077	946	1 001	9 329	108,1
Enköping kommun	5 171	5 271	5 210	47 489	109,9
Eskilstuna kommun	15 900	15 516	16 381	107 593	148,1
Eslöv kommun	3 165	3 276	3 971	34 593	100,3
Fagersta kommun	1 588	1 446	1 195	13 319	105,8
Falkenberg kommun	4 332	4 465	4 838	46 773	97,2
Falköping kommun	3 750	3 505	3 309	33 270	105,8
Filipstad kommun	1 104	1 077	1 154	10 403	106,9
Flen kommun	1 944	1 650	1 826	16 316	110,7
Gotland kommun	5 543	5 425	5 899	61 001	92,2
Grums kommun	1 086	727	758	9 091	94,3
Gullspång kommun	475	680	443	5 206	102,3
Gällivare kommun	1 929	1 460	1 448	17 449	92,4
Gävle kommun	13 780	12 832	11 916	103 136	124,5
Göteborgs kommun	94 036	89 446	94 125	587 549	157,5
Götene kommun	1 187	1 145	1 367	13 263	93,0
Hallsberg kommun	1 618	1 703	1 688	16 196	103,1
Halmstad kommun	12 386	12 817	13 529	104 573	123,5
Haninge kommun	13 304	11 797	11 856	95 658	128,8
Haparanda kommun	1 136	1 048	1 141	9 496	116,7
Helsingborg kommun	21 831	21 710	22 180	150 109	145,9
Huddinge kommun	14 954	14 519	13 228	113 951	124,9
Hultsfred kommun	1 468	1 462	1 551	14 056	106,3

Kommuner	År 2020	År 2021	År 2022	Invånare	Medelvärde
Hylte kommun	1 484	1 250	1 177	10 619	122,8
Håbo kommun	2 289	2 043	2 130	22 344	96,4
Hällefors kommun	785	691	616	6 849	101,8
Härnösand kommun	3 285	3 459	3 099	25 012	131,2
Härryda kommun	3 412	3 585	3 849	39 006	92,7
Hässleholm kommun	6 001	5 319	5 933	52 309	109,9
Högsby kommun	656	700	642	5 645	118,0
Hörby kommun	1 345	1 459	1 567	15 745	92,5
Jokkmokk kommun	523	450	384	4 780	94,6
Järfälla kommun	10 573	9 647	9 807	83 170	120,3
Kalix kommun	1 895	1 607	1 472	15 768	105,1
Kalmar kommun	9 158	8 849	9 296	71 328	127,6
Karlshamn kommun	3 269	3 169	2 923	32 226	96,8
Karlskoga kommun	3 373	3 756	3 187	30 437	113,0
Karlstad kommun	9 798	9 373	9 007	95 408	98,4
Katrineholm kommun	4 173	3 688	4 302	34 764	116,6
Klippan kommun	2 286	2 025	2 237	17 783	122,7
Kramfors kommun	2 503	2 181	1 938	18 005	122,6
Kristianstad kommun	10 307	10 065	9 782	86 641	116,0
Kristinehamn kommun	2 715	2 528	2 677	24 099	109,5
Kumla kommun	2 548	2 569	2 735	22 144	118,2
Köping kommun	3 069	3 027	2 781	26 133	113,2
Laholm kommun	2 660	2 385	2 437	26 319	94,8
Landskrona kommun	6 075	5 453	6 000	46 488	125,7
Laxå kommun	531	549	641	5 582	102,8
Lessebo kommun	881	899	842	8 574	101,9
Lidköping kommun	4 114	3 775	3 676	40 460	95,3
Lilla Edet kommun	1 357	1 345	1 337	14 509	92,8
Linköping kommun	18 344	15 998	16 196	165 527	101,8
Ljusnarsberg kommun	871	788	482	4 604	155,0
Ludvika kommun	2 706	2 505	2 175	26 497	92,9
Luleå kommun	10 692	9 229	8 876	78 867	121,7
Lund kommun	12 851	11 457	12 599	127 376	96,6
Lycksele kommun	1 195	1 363	1 362	12 264	106,5
Malmö kommun	58 420	51 666	54 370	351 749	155,8
Mariestad kommun	2 755	2 736	2 938	24 723	113,6
Markaryd kommun	1 288	1 355	1 245	10 320	125,6
Mellerud kommun	962	1 034	872	9 268	103,2
Mjölby kommun	2 970	2 620	2 662	28 269	97,3
Motala kommun	4 460	4 494	4 996	43 674	106,5
Munkedal kommun	979	1 068	1 150	10 588	100,6

Kommuner	År 2020	År 2021	År 2022	Invånare	Medelvärde
Nacka kommun	10 954	10 241	9 111	108 234	93,3
Norberg kommun	592	629	620	5 714	107,4
Norrköping kommun	16 834	16 305	19 126	144 458	120,6
Norrtälje kommun	7 732	7 013	7 623	64 762	115,1
Nybro kommun	2 457	2 035	2 181	20 284	109,7
Nyköping kommun	7 072	7 338	7 339	57 633	125,8
Nynäshamn kommun	4 537	4 186	3 962	29 495	143,4
Nässjö kommun	3 435	3 425	3 076	31 782	104,2
Olofström kommun	1 280	1 241	1 374	13 263	97,9
Partille kommun	3 840	3 874	4 029	39 529	99,0
Perstorp kommun	1 019	890	965	7 565	126,6
Sala kommun	2 537	2 739	2 848	22 998	117,7
Sandviken kommun	3 669	4 006	3 638	39 250	96,1
Sigtuna kommun	6 991	6 920	7 456	50 273	141,7
Skara kommun	2 179	2 133	2 096	18 732	114,0
Skinnskatteberg kommun	648	473	492	4 371	123,0
Skövde kommun	5 899	5 720	6 119	57 016	103,7
Sollefteå kommun	2 284	1 961	2 032	18 814	111,2
Sollentuna kommun	8 829	8 582	7 981	75 108	112,7
Solna kommun	12 778	11 999	11 518	84 187	143,7
Stockholms kommun	210 192	208 210	191 896	978 770	207,8
Strängnäs kommun	3 829	3 639	3 965	38 129	100,0
Sundbyberg kommun	8 037	7 216	6 280	53 564	134,0
Sundsvall kommun	12 388	10 989	10 857	99 383	114,8
Svalöv kommun	1 328	1 254	1 491	14 412	94,2
Svenljunga kommun	929	1 051	1 129	10 864	95,4
Säffle kommun	1 509	1 281	1 563	15 396	94,2
Söderhamn kommun	2 957	2 959	2 537	25 446	110,7
Södertälje kommun	16 879	15 571	14 845	101 209	155,8
Sölvesborg kommun	1 686	1 652	1 871	17 540	99,0
Tranås kommun	1 790	1 754	1 848	18 874	95,2
Trollhättan kommun	7 489	7 384	6 941	59 154	122,9
Tyresö kommun	5 477	4 962	4 586	49 062	102,1
Töreboda kommun	858	931	883	9 207	96,7
Uddevalla kommun	6 759	6 074	6 198	57 122	111,1
Upplands Väsby kommun	7 338	6 662	5 483	47 820	135,8
Upplands-Bro kommun	4 526	3 819	3 836	31 082	130,6
Uppsala kommun	24 786	24 560	23 992	237 596	102,9
Vallentuna kommun	3 472	2 757	3 416	34 246	93,9
Vara kommun	1 962	1 869	1 785	16 162	115,8
Vilhelmina kommun	611	582	625	6 485	93,4

Kommuner	År 2020	År 2021	År 2022	Invånare	Medelvärde
Vingåker kommun	972	685	903	9 063	94,2
Vänersborg kommun	3 847	4 041	3 951	39 636	99,6
Värnamo kommun	3 401	3 138	3 448	34 661	96,0
Västerås kommun	21 944	23 492	20 148	156 838	139,4
Växjö kommun	9 049	8 907	8 825	95 995	93,0
Åsele kommun	293	357	336	2 807	117,1
Åstorp kommun	2 347	1 929	1 868	16 308	125,6
Örebro kommun	22 746	23 060	22 232	156 987	144,5
Örkelljunga kommun	1 339	1 170	1 172	10 499	116,9
Östersund kommun	9 225	8 342	7 760	64 324	131,2
Östra Göinge kommun	1 490	1 508	1 476	14 941	99,8

Den behöriga myndighetens beslut

Utredningens förslag: PTS ska varje år, senast den 1 juni genom normbeslut föreskriva vilka kommuner som ska omfattas av den geografiskt riktade lagringen. Samtliga tillhandahållare som omfattas av dagens lagringsskyldighet ska vara lagringsskyldiga, om de tillhandahåller sina tjänster i en kommun där lagringsskyldighet föreligger.

I detta avsnitt överväger vi lagringsskyldighet för sådana tillhandahållare som omfattas av dagens lagringsskyldighet. Vi återkommer i avsnitt 9 till frågan om lagringsskyldighet för den som tillhandahåller vissa OTT-tjänster för kommunikation, nämligen tillhandahållare av nummeroberoende interpersonella kommunikationstjänster (Noik).

För att tillhandahållarna ska kunna påbörja lagring av trafik- och lokaliseringsuppgifter i en viss kommun krävs att de får kännedom om att den kommunen är mer brottsutsatt än riksgenomsnittet för kommunerna. De uppgifter som ska ligga till grund för den geografiskt riktade lagringen utgår från den officiella statistiken och är tillgängliga för envar. Det skulle därför vara möjligt att reglera lagringsskyldigheten genom att i författning ålägga tillhandahållarna att direkt utföra beräkningen, med användande av uppgifterna i den officiella statistiken, och därefter genomföra den riktade geografiska lagringen. Vi gör dock bedömningen att en sådan lösning är olämplig, inte minst av det skälet att det vid en beräkning kan uppstå tolkningsfrågor som leder till olika uppfattningar om skyldigheten att lagra uppgifter i en

viss kommun. En bättre lösning är att en behörig myndighet utifrån den officiella statistiken, beräknar och fastställer lagringsskyldigheten som tillhandahållarna sedan ska verkställa.

En behörig myndighet bör således fastställa lagringsskyldigheten vid geografiskt riktad lagring. Ett alternativ vore, eftersom underlaget utgår från den statistik som Brå för, att låta Brå utföra dessa uppgifter. Brå har emellertid till uppgift att bidra till kunskapsutvecklingen inom rättsväsendet och det kriminalpolitiska området samt att främja brottsförebyggande arbete (1 § förordning [2016:1201] med instruktion för Brottsförebyggande rådet). Även om myndighetens uppdrag handlar om att ta fram fakta och sprida kunskap om brottslighet, brottsbekämpning och brottsförebyggande arbete, framstår det som svårt att förena med Brå:s uppdrag att låta Brå fatta beslut om lagring av trafik- och lokaliseringsuppgifter för att bekämpa grov brottslighet. Vi gör bedömningen att en sådan uppgift kan riskera att rubba förtroende för Brå som en kunskapsmyndighet.

Ett annat alternativ vore att låta Polismyndigheten beräkna och fastställa vilka kommuner som ska bli föremål för riktad lagring. Det finns i sak inga starka invändningar mot Polismyndigheten i detta avseende. Vi anser emellertid, främst av följande skäl, att PTS är ett lämpligare alternativ. Dels krävs ingen särskild polisiär kompetens vid beräkningen och fastställandet av vilka kommuner som är mer brottsutsatta än riksgenomsnittet eftersom detta kommer att göras på grundval av den officiella statistiken, dels är det PTS som i huvudsak för dialog om lagring med tillhandahållarna. PTS är också bl.a. tillsynsmyndighet enligt nya LEK.

PTS framstår enligt vår mening som en mer naturlig samtalspart för tillhandahållarna när det gäller regelefterlevnad och kan genom att fastställa var lagringsskyldigheten ska äga rum underlätta för dessa aktörer att göra rätt. Vi anser därför att PTS bör vara den myndighet som beräknar och fastställer var geografiskt riktad lagring ska gälla. Vi föreslår att PTS genom normbeslut ska föreskriva vilka kommuner som omfattas av den geografiskt riktade lagringen.

Vi har i föregående avsnitt föreslagit att geografiskt riktad lagring bör beslutas för det resterande året efter det att Brå har redovisat den slutliga statistiken. PTS bör därför föreskriva vilka kommuner som omfattas av den geografiskt riktade lagringen årligen, senast den 1 juni. Vi ser inga formella hinder mot att föreskrifterna meddelas tidigare om statistiken blivit fastställd. Lämpligen bör föreskrifterna med-

delas i tillräcklig god tid för att tillhandahållarna ska hinna anpassa sina it-stöd. Eftersom Brå i regel publicerar statistiken under tidig vår, bör en publicering senast den 1 juni inte föranleda några praktiska problem.

Vårt förslag innebär sammanfattningsvis att PTS årligen, senast den 1 juni, ska meddela föreskrifter med utgångspunkt från den slutliga statistiken efter att Brå har tillgängliggjort den. I föreskrifterna ska anges vilka kommuner som omfattas av beslutet. Föreskrifterna äger sedan giltighet tills de har ersatts av ett nytt beslut.

Besluten kommer inte att vara överklagbara, se 41 § förvaltningslagen (2017:900) och 30 § myndighetsförordningen (2007:515).

Föreskrifter om vilka kommuner som omfattas av geografiskt riktad lagring ska kungöras i PTS:s författningssamling, PTFS (se bilaga 1 till författningssamlingsförordningen [1976:725]). Med anledning av våra förslag bör också myndighetens uppdrag förtydligas genom en ändring i förordningen (2007:951) med instruktion för Post- och telestyrelsen. I avsnitt 8.3.3 redovisar vi våra överväganden när det gäller omfattningen av lagringen m.m.

Hur ofta ska behov av geografiskt riktad lagring omprövas?

En fråga att överväga i sammanhanget är hur ofta PTS ska fastställa lagringsskyldigheten. Enligt EU-domstolen ska de geografiska områden som berörs av en geografiskt riktad lagring ändras beroende på hur den situation som motiverade att de valdes utvecklas. Det har sin grund i att riktade lagringsåtgärder inte får pågå längre än vad som är strängt nödvändigt med hänsyn till det eftersträvade målet och de omständigheter som motiverar dem. Detta utgör dock inget hinder mot att förnya åtgärderna om lagringen fortsätter att vara strängt nödvändig.[8] Brå redovisar kriminalstatistik med avseende på anmälda brott per kalenderår, kvartal och månad. Den beräkning av sannolikhet för förekomsten av grova brott som ska ligga till grund för geografiskt riktad lagring ställer vissa krav på kvantitet och stabilitet i de uppgifter som utgör underlag. Med hänsyn till detta och även till den administrativa och ekonomiska börda det skulle innebära för tillhandahållarna att anpassa sin lagring framstår det som ändamålsenligt att beräkningar och fastställelse av vilka kommuner

[8] Jfr SpaceNet-domen p. 111.

som ska omfattas av den geografiskt riktade lagringen görs en gång per år.

Vilka tillhandahållare ska omfattas av ett beslut om geografiskt riktad lagring?

När lagring av trafik- och lokaliseringsuppgifter ska ske med utgångspunkt från den genomsnittliga graden av brottsanmälningar uppstår frågan om lagringsskyldigheten också ska omfatta samtliga tillhandahållare som omfattas av skyldigheten att anmäla sin verksamhet enligt 2 kap. 1 § nya LEK inom de relevanta områdena. Det avgörande kriteriet för geografiskt riktad lagring är om den genomsnittliga graden av grov brottslighet inom en viss kommun är högre än genomsnittet för kommunerna i hela landet. Det framstår som angeläget för de brottsbekämpande myndigheterna att kunna få tillgång till trafik- och lokaliseringsuppgifter inom ett sådant geografiskt område, oberoende av vilka tjänster som enskilda använder sig av. Det är därför svårt att motivera att en geografiskt riktad lagring också ska avgränsas till vissa särskilt utvalda tillhandahållare. Om det ska göras någon form av urval kring tillhandahållare, behöver den urvalsprocessen också föregås av en kartläggning av vilka som har förmåga att genomföra lagringen. Vi gör bedömningen att det är mer ändamålsenligt att låta samtliga tillhandahållare som omfattas av dagens lagringsskyldighet bli lagringsskyldiga om de är verksamma inom en kommun där geografiskt riktad lagring ska ske. Vi återkommer i avsnitt 9.6.1 till frågan om även tillhandahållare av Noik ska omfattas av lagringsskydigheten.

8.3.2 Utökad riktad lagring

Den geografiskt riktade lagringen ska kunna kompletteras i vissa situationer med utökad riktad lagring

Utredningens förslag: En möjlighet till s.k. utökad riktad lagring ska komplettera den geografiskt riktade lagringen. Utökad riktad lagring ska få användas avseende

1. ett begränsat geografiskt område där grov brottslighet har förekommit eller där det är sannolikt att grov brottslighet kommer att äga rum,
2. en skyddsvärd plats,
3. en person som är eller har varit föremål för hemliga tvångsmedel,
4. en person som dömts för grova brott, eller
5. utrustnings- eller abonnemangsidentitet som använts vid eller skäligen kan antas komma till användning vid ett grovt brott eller vid grov brottslig verksamhet.

Som framgår av vår redovisning ovan är det generellt sett ganska svårt att med hjälp av olika statistiska beräkningar slå fast i vilka områden det finns en jämförelsevis större sannolikhet för grov brottslighet än i andra områden. Särskilt svårt blir detta om man i förväg ska bestämma ett statistiskt underlag som sedan ska vara styrande för lagringen. En stor fördel med den av oss föreslagna modellen är att den är tillförlitlig när det gäller att skapa en förutsebar nivå för lagringen. Lagringen blir vidare förhållandevis bred. Många personer blir föremål för lagring utan att lagringen kan sägas bli för långtgående enligt EU-rätten. Den breda lagringen minskar i vart fall något de olägenheter som brukar förknippas med riktad lagring.[9] Tilläggas kan också att modellen är ganska enkel att tillämpa för berörda aktörer.

Men förslaget bör kompletteras för att säkra en effektiv brottsbekämpning. En brist med geografiskt riktad lagring som vi föreslår är att den kommer att ge de brottsbekämpande myndigheterna sämre möjligheter att bekämpa grov brottslighet i de delar av landet där den brottsligheten inte har fått genomslag i kriminalstatistiken. I prak-

[9] Se prop. 2018/19:86 s. 33.

tiken kan det bli svårare att bekämpa grov brottslighet i vissa delar av landet trots att de brottsbekämpande myndigheterna har kunskap om att en viss plats är särskilt utsatt för grov brottslighet. Det kan exempelvis handla om att en viss kriminell gruppering har etablerat sig i ett avgränsat område inom en kommun där antalet brottsanmälningar avseende grov brottslighet historiskt varit låg eller att ett stort antal grova brott har begåtts i ett område där sådana tidigare inte förekommit eller varit ovanliga. Det kan också handla om plötsliga händelser där ett särskilt allvarligt brott motiverar lagring avseende området. Det krävs i sådana fall ett komplement till geografiskt riktad lagring avseende områden där grov brottslighet har förekommit eller där det är sannolikt att grov brottslighet kommer att äga rum.

Ett annat problem är när det finns en specifik plats som är särskilt skyddsvärd. Enligt EU-domstolen kan strategiskt viktiga platser som flygplatser, järnvägsstationer, kusthamnar eller vägtullstationer, motivera ett särskilt behov av lagring av trafik- och lokaliseringsuppgifter.[10]

Enligt EU-domstolen finns också möjligheten för medlemsstaterna att vidta lagringsåtgärder avseende vissa personer, om dessa personer direkt eller indirekt, kan sättas i samband med grova brott eller grov brottslig verksamhet, under förutsättning att bedömningen sker på objektiva och icke-diskriminerande grunder.[11] Det framstår i sådana situationer som en mindre ingripande åtgärd att låta lagringen vara personbestämd än att låta ett helt område bli föremål för datalagring på grund av att vissa personer uppehåller sig i området. För att säkerställa att lagringen sker på objektiva och icke-diskriminerande grunder och med ett så litet integritetsintrång som möjligt bör lagring ske endast i förhållande till personer som är eller har varit föremål för hemliga tvångsmedel eller personer som har dömts för grova brott.

EU-domstolen har avslutningsvis lämnat ett utrymme för medlemsländerna att föreskriva andra särskiljande kriterier för lagring än ett personligt eller geografiskt kriterium. Det får ske under samma förutsättningar som vi beskrivit tidigare, dvs. i situationer när det är absolut nödvändigt och när det finns ett direkt eller indirekt samband mellan lagringskriteriet och grov brottslighet. Så kan vara fallet när de brottsbekämpande myndigheterna kan sätta användningen av viss utrustning eller ett visst abonnemang i direkt eller indirekt för-

[10] Se SpaceNet-domen p. 110.
[11] Se SpaceNet-domen p. 107.

bindelse med grov brottslighet. Det är här inte fråga om situationer när en innehavare av viss utrustning eller abonnemang misstänks för att ha begått ett grovt brott eller deltar i sådan brottslig verksamhet som omfattar grova brott. Det är i stället fråga om situationer när själva utrustningen eller abonnemanget går att knyta till grova brott eller grov brottslighet. För tydlighetens skull använder vi oss därför framöver av uttrycket utrustnings- eller abonnemangsidentitet.

Sammanfattningsvis menar vi att vårt förslag om riktad lagring bör kompletteras på olika sätt med en reglering som vi kallar för utökad riktad lagring för att främja brottsbekämpningen. Syftet med sådan utökad riktad lagring är att den ska läka brister som kan följa av den geografiskt riktade lagringen. Utökad riktad lagring gör det också möjligt anpassa lagringen till de behov som gäller för stunden. De möjligheter till lagring som EU-domstolen ger för att främja brottsbekämpningen bör också utnyttjas. Vi menar därför att den geografiskt riktade lagringen i vissa fall bör kunna utökas. Vi föreslår att sådan utökad lagring bör kunna avse:

1. ett begränsat geografiskt område där grov brottslighet har förekommit eller där det är sannolikt att grov brottslighet kommer att äga rum,
2. en skyddsvärd plats,
3. en person som är eller har varit föremål för hemliga tvångsmedel,
4. en person som dömts för grova brott, eller
5. utrustnings- eller abonnemangsidentitet som använts vid eller skäligen kan antas komma till användning vid ett grovt brott eller vid grov brottslig verksamhet.

Våra förslag innebär att lagringsskyldigheten kan bli överlappande i vissa situationer. Det betyder inte att samma uppgifter måste lagras flera gånger. Det väsentliga är i stället att det finns en rättslig grund för datalagringen och att tillhandahållarna uppfyller sin lagringsskyldighet för den tid ett beslut om utökad riktad lagring gäller.

I fråga om begreppet strategiskt viktiga platser kommer vi framöver att använda uttrycket skyddsvärda platser. Vi avser ingen skillnad i fråga om innebörden mellan dessa begrepp.

Vi utvecklar nedan närmare vår syn på den utökade lagring som vi föreslår.

Vilka myndigheter ska besluta om utökad riktad lagring?

Utredningens förslag: Polismyndigheten, Säkerhetspolisen och Tullverket ska besluta om utökad riktad lagring. Ett sådant beslut ska innehålla de skäl som beslutet grundas på. Myndigheterna ska samråda med varandra och vid behov även med andra myndigheter före beslut om utökad riktad lagring. I brådskande fall, eller om samråd är olämpligt av sekretesskäl, får beslut fattas utan samråd. Ett beslut om utökad riktad lagring ska verkställas utan dröjsmål.

Utredningens bedömning: Det saknas skäl att föreskriva närmare om vilka personer inom de behöriga myndigheterna som ska få fatta beslut om utökad riktad lagring.

Den eller de myndigheter som ska besluta om utökad riktad lagring bör ha en bred kompetens vad gäller förmågan att bedöma risk för grov brottslighet avseende områden, platser och personer. En sådan myndighet bör även ha viss teknisk förmåga. Det är angeläget att en sådan myndighet inte bara har en god bild av hur den grova brottsligheten utvecklar sig i samhället utan också har förutsättningar att inhämta nödvändig information för att göra kvalificerade bedömningar. Detta utesluter i princip andra aktörer än de brottsbekämpande myndigheterna.

Av de brottsbekämpande myndigheterna är det Polismyndigheten som har bredast uppdrag vad gäller att bekämpa grova brott och grov brottslighet. Polismyndigheten bör därför få besluta om utökad riktad lagring. Vi har övervägt en modell som innebär att Polismyndigheten skulle vara den enda myndigheten när det gäller beslut om utökad riktad lagring. Det finns dock ett flertal invändningar mot en sådan ordning. En väsentlig sådan invändning är att modellen skulle innebära att sekretessbelagda uppgifter måste cirkulera mellan olika aktörer i en större omfattning än vad som är önskvärt och nödvändigt. Om exempelvis Säkerhetspolisen inom ramen för sin underrättelseverksamhet har behov av att besluta om utökad riktad lagring avseende en viss person, skulle det bli nödvändigt för Säkerhetspolisen att vidarebefordra information, som under normala förhållanden inte hade lämnat Säkerhetspolisens verksamhet, till Polismyndigheten inför ett sådant beslut.

Vi ser samtidigt ett problem med att ge alla brottsbekämpande myndigheter rätt att besluta om utökad riktad lagring. Till de brottsbekämpande myndigheterna hör förutom Polismyndigheten, Säkerhetspolisen, och Tullverket även Ekobrottsmyndigheten, Kustbevakningen, Skatteverket, Försvarsmakten (genom militärpolisen) och Åklagarmyndigheten. Det skulle dels belasta tillhandahållarna i en omfattning som vi inte anser rimlig, dels innebära ett ineffektivt förfarande där myndigheterna ständigt måste samordna sina beslut. Vi ser därför ett behov av att begränsa möjligheten att ansöka om utökad riktad lagring till de myndigheter som oundgängligen har ett sådant behov.

Vi gör bedömningen att det bör vara Polismyndigheten, Säkerhetspolisen och Tullverket som ska ha möjlighet att besluta om utökad riktad lagring eftersom dessa myndigheter också har en väl utvecklad förmåga till att bedriva underrättelseverksamhet. När det gäller de övriga brottsbekämpande myndigheterna får dessa genom etablerade kanaler för samarbete, hos de behöriga myndigheterna, informera om uppkomna behov av utökad riktad lagring. Det bör därefter vara den beslutande myndighetens ansvar att självständigt bedöma behovet av utökad riktad lagring.

För att undvika onödiga parallella beslut om utökad riktad lagring ska de behöriga myndigheterna samråda med varandra inför beslut om utökad riktad lagring. De behöriga myndigheterna bör också vid behov samråda med andra myndigheter som kan antas ha relevant information. Vi avstår från att föreslå formkrav för samrådet, eftersom det bör anpassas från situation till situation. I brådskande fall bör samråd kunna underlåtas med hänsyn till behovet av ett skyndsamt beslut. Någon skyldighet att samråda bör inte heller föreligga när ett sådant bedöms olämpligt av sekretesskäl. Särskilt i Säkerhetspolisens arbete kan det förekomma behov av att minimera kretsen av de som är involverade i angelägenheter om utökad riktad lagring till ett absolut minimum. Det bör förtydligas att vi inte föreslår att de behöriga myndigheterna ska underlåta att samråda med varandra av det skälet att uppgifter som ligger till grund för beslutet omfattas av sekretess. Typiskt sett är sådana uppgifter alltid omgärdade av sekretess. Vårt förslag syftar i stället till att skapa förutsättningar för att underlåta samråd i särskilt känsliga ärenden.

I föregående stycke har vi diskuterat behovet av skyndsam handläggning av ett beslut om utökad riktad lagring. Ett beslut om utökad

riktad lagring måste i sådana situationer också kunna verkställas utan dröjsmål. I annat fall skulle för brottsbekämpningen viktiga uppgifter kunna gå förlorade. Mot den bakgrunden bör det föreskrivas ett skyndsamhetskrav för tillhandahållarna att verkställa lagringen, i likhet med vad som gäller vid utlämnande av uppgifter om elektronisk kommunikation. Vi föreslår därför att det i 9 kap. 19 § nya LEK anges att de lagringsskyldiga ska påbörja lagringen av uppgifter utan dröjsmål. Med uttrycket utan dröjsmål avser vi alltså samma skyndsamhetskrav som föreskrivs i 9 kap. 29 b § nya LEK.

I nästa avsnitt redovisar vi våra överväganden kring hur tillsyn över de behöriga myndigheternas beslut kan utformas. En sådan granskning förutsätter att besluten innehåller specifika beslutsskäl. Skälen ska vara av sådan art och omfattning att den som i efterhand ska granska beslutet kan avgöra om beslutet är fattat i enlighet med de föreskrifter som gäller för lagringen.

Sammanfattningsvis gör vi bedömningen att beslut om utökad riktad lagring ska få fattas av Polismyndigheten, Säkerhetspolisen och Tullverket och att dessa myndigheter, med undantag för vissa situationer, inför beslut ska samråda med varandra och vid behov med andra myndigheter. Ett sådant beslut ska verkställas utan dröjsmål.

Vi har avslutningsvis övervägt om det bör meddelas föreskrifter om vilka befattningshavare inom de behöriga myndigheterna som ska få besluta om utökad riktad lagring. För en sådan ordning talar att beslut om utökad riktad lagring utgör en rättighetsinskränkning som bör föregås av noggranna överväganden. De behöriga myndigheterna har för utredningen föreslagit att en lämpligare lösning vore att låta respektive myndighet få delegera behörigheten genom interna styrdokument, eftersom beslut av motsvarande vikt redan i dag delegeras på detta sätt och är förbehållna medarbetare med högre befattningar. Vi instämmer i det. Det saknas därmed skäl att lämna förslag om föreskrifter om vilka inom respektive myndighet som ska få fatta beslut om utökad riktad lagring.

Beslut om utökad riktad lagring ska vara föremål för Säkerhets- och integritetskyddsnämndens tillsyn

Utredningens förslag: SIN ska utöva tillsyn över tillämpningen av reglerna om utökad riktad lagring. Den beslutande myndigheten ska underrätta SIN om beslutet och skälen för detta senast en vecka efter det att beslutet fattades.

Vi har i föregående avsnitt gjort bedömningen att PTS i föreskrift ska fastställa den geografiskt riktade lagringen på grundval av kriminalstatistiken. När det gäller utökad riktad lagring måste beslutet föregås av en noggrann bedömning av uppställda kriterier. Ett beslut om utökad riktad lagring kommer alltså inte att vara resultatet av en på förhand given beräkning, utan kräva en nyanserad bedömning av om ett visst område eller en viss plats ska omfattas av lagring eller inte. Ett sådant beslut kräver en mängd olika överväganden. Vid sidan av de faktiska omständigheter som utgör kriterierna för lagringsskyldigheten behövs även överväganden kring:

- hur stort området för den utökade lagringen ska vara, vilka platser som är skyddsvärda, vilka personer som ska bli föremål för beslut om datalagring, och om utrustnings- eller abonnemangsidentitet direkt eller indirekt har ett samband med grova brott eller grov brottslig verksamhet,
- hur länge beslutet ska gälla,
- vilka uppgifter som ska lagras, och
- vilka tillhandahållare som ska omfattas av lagringsskyldigheten.

Vi bedömer därför att det inte bara måste vara förutsebart när utökad riktad lagring får äga rum utan också att ett beslut om utökad riktad lagring ska vara föremål för någon form av kontroll. En form av kontroll vore att låta ett oberoende organ kontrollera förutsättningarna för den utökade riktade lagringen innan den får verkställas. En ordning av detta slag innebär i praktiken att en eller flera behöriga myndigheter måste ansöka om utökad riktad lagring hos ett kontrollorgan. Vi anser dock att en sådan kontroll inte är nödvändig, eftersom tillgången till de lagrade uppgifterna kommer att föregås av en förhands-

kontroll. En lämpligare ordning vore att låta de behöriga myndigheternas beslut bli föremål för tillsyn av SIN.

I dag utövar nämnden tillsyn över bl.a. de brottsbekämpande myndigheternas användning av hemliga tvångsmedel. Nämnden utövar också tillsyn över Säkerhetspolisens användning av hemliga tvångsmedel vid särskild kontroll av vissa utlänningar. Vi hänvisar till avsnitt 7.3.5 där vi mer utförligt beskrivit SIN:s verksamhet.

Det finns ett direkt samband mellan datalagring och användning av hemliga tvångsmedel. Enligt våra förslag blir såväl beslut om utökad riktad lagring som beslut om tillgång till trafik- och lokaliseringsuppgifter genom hemliga tvångsmedel föremål för SIN:s granskning och på så sätt får SIN ett bättre granskningsunderlag. Vi gör sammantaget bedömningen att SIN:s tillsyn utgör en tillräcklig rättssäkerhetsgaranti vid Polismyndighetens, Säkerhetspolisens och Tullverkets beslut om utökad riktad lagring.

Vi föreslår därför att SIN:s tillsynsuppdrag utökas så att det även avser de brottsbekämpande myndigheternas tillämpning av bestämmelserna om utökad riktad lagring. För att nämnden ska kunna utöva sin tillsyn på ett effektivt sätt bör den myndighet som beslutar om utökad riktad lagring underrätta SIN om beslutet och skälen för detta senast en vecka efter det att beslutet fattades. Det krävs därför ändringar i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet så att nämndens tillsyn även omfattar Polismyndighetens, Säkerhetspolisens och Tullverkets tillämpning av reglerna om utökad riktad lagring. Vi anser dock inte att nämnden bör ha en skyldighet att på begäran av en enskild kontrollera om han eller hon har varit föremål för utökad riktad lagring och om lagringen har varit författningsenlig.

Ett beslut om utökad riktad lagring får inte överklagas

Utredningens förslag: Polismyndighetens, Säkerhetspolisens och Tullverkets beslut om utökad riktad lagring ska inte kunna överklagas.

Datalagring för att bekämpa grov brottslighet syftar till att ge förutsättningar för de brottsbekämpande myndigheterna att inhämta relevanta uppgifter efter beslut om hemliga tvångsmedel. Som vi kon-

staterat i föregående avsnitt är själva datalagringen en mindre ingripande åtgärd än faktisk användning av hemliga tvångsmedel. Reglerna om tillgång till uppgifterna innefattar i sig ett flertal rättssäkerhetsgarantier. Det kan också konstateras att den utökade riktade lagringen, i motsats till nationell säkerhetslagring, inte kommer vara generell och odifferentierad. Mot den bakgrunden gör vi bedömningen att den tillsyn som SIN kommer att utöva när det gäller utökad riktad lagring är tillräcklig och att någon möjlighet till överprövning alltså inte behövs. Härutöver bör påtalas att EU-domstolen inte har ställt några krav på att datalagring i syfte att bekämpa grov brottslighet måste kunna bli föremål för effektiv kontroll i form av en överprövningsmöjlighet. Vi föreslår därför att Polismyndighetens, Säkerhetspolisens och Tullverkets beslut om utökad riktad lagring inte ska kunna överprövas.

Utökad riktad lagring avseende geografiska områden

Utredningens förslag:

- Datalagring får ske inom ett begränsat geografiskt område där grov brottslighet har förekommit eller där det är sannolikt att grov brottslighet kommer att äga rum.
- Brott och brottslig verksamhet som innefattar sådana brott som ger rätt att använda HÖK enligt rättegångsbalken får ligga till grund för beslut om utökad riktad lagring.
- Ett beslut om lagring ska gälla så länge behovet kan förväntas föreligga och längst under ett års tid.
- Lagringsskyldigheten ska därefter kunna förlängas genom ett nytt beslut om behovet kvarstår.
- De behöriga myndigheterna ska vid ändrade förhållanden ompröva om grunden för den utökade riktade lagringen består och annars upphäva lagringsbeslutet.

Som vi redan har beskrivit syftar förfarandet med utökad riktad lagring till att motverka de negativa konsekvenserna av att vissa brottsutsatta platser inte täcks av den geografiskt riktade lagringen avse-

ende brottsutsatta kommuner. Här handlar det om att myndigheterna måste vara proaktiva i arbetet med att försöka förutsäga om det finns skäl att utöka den riktade lagringen till områden som inte omfattas av geografiskt riktad lagring. Den geografiskt riktade lagringen bör alltså enligt vår bedömning kompletteras med utökad riktad lagring i syfte att bekämpa grova brott och sådan brottslig verksamhet som innefattar grova brott. En fråga som behöver besvaras är vilka brott och vilken brottslig verksamhet som kan ligga till grund för ett beslut om utökad riktad lagring. Vi har i avsnitt 8.2 beskrivit att tillgången till lagrade uppgifter enligt befintliga bestämmelser om hemliga tvångsmedel är förenlig med EU-rätten. Vi gör bedömningen att motsvarande princip bör gälla vid utökad riktad lagring avseende områden. Enligt 27 kap. 19 § tredje stycket RB får HÖK användas vid en förundersökning om

1. brott för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader,
2. dataintrång enligt 4 kap. 9 c § brottsbalken, barnpornografibrott enligt 16 kap. 10 a § brottsbalken som inte är att anse som ringa, narkotikabrott enligt 1 § narkotikastrafflagen (1968:64), narkotikasmuggling enligt 6 § första stycket lagen (2000:1225) om straff för smuggling,
3. brott som avses i 27 kap. 18 § andra stycket 2–7 RB, eller
4. försök, förberedelse eller stämpling till brott som avses i 1–3, om en sådan gärning är belagd med straff.

Vi bedömer att utökad riktad lagring avseende områden ska få ske när de brott som anges i bestämmelsen har begåtts, eller det är sannolikt att brott eller brottslig verksamhet som innefattar ovanstående brott, kan komma att förekomma. Det saknas skäl att i författning hänvisa till andra bestämmelser om hemliga tvångsmedel som reglerar tillgång till uppgifter om elektronisk kommunikation, eftersom övriga bestämmelser om hemliga tvångsmedel förutsätter grövre brott än HÖK. Annorlunda uttryckt utgör de s.k. HÖK-brotten den lägsta nivån för brott som anses grova.

Nästa fråga är hur de behöriga myndigheterna ska kunna göra en bedömning av om det är sannolikt att grova brott kan komma att begås. När det gäller planerade händelser som exempelvis ett stats-

besök eller ett värdskap för ett internationellt sammanträde, bör det inte vara några större svårigheter att identifiera områden i vilka det finns skäl för en utökad riktad lagring. Inte heller om det på en viss plats har begåtts ett allvarligt brott. Var grova brott kan komma att begås eller grov brottslighet i övrigt kan förekomma är däremot svårt att förutse och det får accepteras att de brottsbekämpande myndigheterna måste ha en bred ansats så länge bedömningen baseras på objektiva faktorer. Det bör finnas konkreta omständigheter som utgör grunden för bedömningen att det är sannolikt att grova brott kan komma ett begås inom ett område eller att den brottsliga verksamheten planeras och diskuteras i ett visst område.

Informationen som utgör underlag för bedömningen av om ett område är särskilt brottsutsatt bör kunna inhämtas från olika håll. Det bör enligt vår bedömning inte ställas något formkrav på underlaget, så länge det på något sätt kan bidra till upplysning om det föreligger en risk för grov brottslighet i ett visst område. Bedömningen kan således bygga på såväl underrättelseinformation som på offentliga uppgifter, exempelvis en ansökan om tillstånd för en allmän sammankomst enligt ordningslagen (1993:1617). Det bör i det här sammanhanget nämnas att de exempel som vi tidigare har lämnat om exempelvis nyetablering av kriminella gäng eller statsbesök m.m. inte är uttömmande.

Vi ser inga skäl att i författning föreskriva några närmare kriterier för hur de behöriga myndigheterna ska göra sin bedömning. Däremot behöver det, på samma sätt som när det gäller frågor om nationell säkerhetslagring, föreskrivas i vilka situationer de behöriga myndigheterna ska få besluta om utökad riktad lagring avseende ett område. Ett sådant beslut får fattas när det finns ett behov av lagring som bedöms vara strängt nödvändig för att bekämpa grov brottslighet.

I bedömningen av vad som är strängt nödvändigt ligger, förutom de konkreta omständigheter som ger den beslutande myndigheten skäl att tro att risken för grov brottslighet är hög i ett visst område, också hur lång tid ett beslut om riktad lagring ska gälla. Inom ramen för bedömningen av vad som är strängt nödvändigt behöver myndigheten också ta ställning till den närmare omfattningen av lagringsskyldigheten, dvs. hur stort område den riktade lagringen ska gälla, vilka typer av uppgifter som ska lagras och hur länge uppgifter ska lagras, samt vilka tillhandahållare som ska omfattas av ett beslut om utökad lagring. I motsats till vad som föreslås gälla vid geografiskt

riktad lagring bedömer vi att angelägenheter om utökad riktad lagring inte bör vara offentliga. Vi återkommer till frågor om sekretess och tystnadsplikt i avsnitt 8.3.7.

Vad gäller frågan om hur länge ett beslut om utökad riktad lagring avseende områden ska gälla ligger det i sakens natur att det kan vara svårt för myndigheterna att i förväg göra en prognos kring när ett behov av lagring kan tänkas upphöra. Typiskt sett kan förekomsten av grov brottslighet i vissa områden vara av varaktig karaktär. EU-rätten kräver dock att beslut om riktad geografisk lagring ska upphöra när skälen för lagringen inte längre finns. En utökad riktad lagring kan, på samma sätt som vid geografiskt riktad lagring, behöva omprövas efter viss tid. Vi föreslår därför att ett beslut om utökad riktad lagring ska tidsbegränsas för att inte riskera att gälla längre än vad som är absolut nödvändigt. Vi föreslår att ett beslut om utökad riktad lagring avseende områden ska få gälla i högst ett år. Om behovet av datalagring i området kvarstår, får de behöriga myndigheterna förlänga sitt beslut i högst ett år åt gången.

De behöriga myndigheterna måste löpande bevaka brottslighetens utveckling i områden som är föremål för utökad riktad lagring och ska vid ändrade förhållanden ompröva om grunden för den utökade riktade lagringen består och annars upphäva lagringsbeslutet. Så kan exempelvis vara fallet om ett område som är föremål för utökad riktad lagring vid ett senare tillfälle omfattas av geografiskt riktad lagring.

Det bör avslutningsvis sägas någonting om avgränsningen mellan ett begränsat geografiskt område och en viss plats, som vi återkommer till i nästa avsnitt. Med det förstnämnda menar vi ett geografiskt område som inte behöver vara knutet till någon särskild byggnad, anläggning eller infrastruktur. Det kan således röra sig om stadsdelar, postområden eller ett område som innefattar flera av varandra oberoende byggnader. Vi bedömer att det inte är lämpligt att i författning ange hur ett stort ett område får vara. Ytterst är det de behöriga myndigheterna som, med exempelvis beaktande av basstationer för telefoni eller knytpunkter för markbunden internettrafik, får avgöra hur avgränsningen ska ske. Vi erinrar här dock om att lagringen inte får omfatta så stora områden som hela kommuner, regioner eller landsdelar, eftersom det annars kan uppstå en situation där hela eller nästan hela Sveriges yta blir föremål för riktad lagring. Om det föreligger en sådan allvarlig situation att hela landet bör bli före-

mål för datalagring, är det snarare fråga om behov av nationell säkerhetslagring som vi beskrivit i avsnitt 7.

Utökad riktad lagring avseende skyddsvärda platser

Utredningens förslag:

- Datalagring får avse en skyddsvärd plats. Vid bedömningen av vad som avses med en skyddsvärd plats ska särskilt beaktas om platsen är ett skyddsobjekt, det vid platsen bedrivs säkerhetskänslig verksamhet, eller platsen bedöms vara av särskild betydelse från brottsbekämpningssynpunkt.
- Ett beslut om lagring ska gälla så länge behovet kan förväntas föreligga och längst under tre års tid.
- Lagringsskyldigheten ska därefter kunna förlängas genom ett nytt beslut om behovet kvarstår.
- De behöriga myndigheterna ska vid ändrade förhållanden ompröva om grunden för den utökade lagringen består och annars upphäva lagringsbeslutet.

En riktad lagringsåtgärd som avser skyddsvärda platser, såsom flygplatser, tågstationer, kusthamnar eller vägtullstationer, gör det möjligt för de brottsbekämpande myndigheterna att inhämta trafikuppgifter och särskilt lokaliseringsuppgifter för alla personer som vid en viss tidpunkt använder elektroniska kommunikationstjänster på en sådan plats. En riktad lagringsåtgärd av denna typ kan således göra det möjligt för de brottsbekämpande myndigheterna att, genom att få tillgång till de lagrade uppgifterna, få information om personers närvaro på de platser eller inom de geografiska områden som omfattas av åtgärden, och om deras förflyttningar mellan eller inom dessa områden. I syfte att bekämpa grov brottslighet kan myndigheterna dra slutsatser om personers närvaro och förehavanden på dessa platser vid en viss tidpunkt under lagringsperioden.[12] Frågan är hur sådana platser ska väljas ut.

Ett sätt att avgränsa vilka platser som bör omfattas av riktad lagring avseende skyddsvärda platser kan vara att utgå från bestämmel-

[12] SpaceNet-domen p. 110.

ser om skyddsobjekt enligt skyddslagen (2010:305). Skyddslagen ger rättsliga förutsättningar för ett kvalificerat skydd för vissa byggnader och anläggningar m.m.[13] Enligt 1 § skyddslagen ska för samhället viktiga byggnader, andra anläggningar, områden och objekt kunna ges ett förstärkt skydd mot sabotage, terroristbrott, spionerі m.m. och grovt rån. Lagen innehåller också bestämmelser om skydd för allmänheten mot skada som kan uppkomma till följd av militär verksamhet, se 2 §. I 3 § skyddslagen anges att det kan beslutas att något ska vara ett skyddsobjekt för att tillgodose behovet av skydd enligt 1 eller 2 §§ skyddslagen. Enligt 7 § skyddslagen innebär ett beslut om skyddsobjekt att obehöriga inte har tillträde till skyddsobjektet. Tillträdesförbudet omfattar även tillträde med hjälp av en obemannad farkost. Genom ett särskilt beslut får tillträdesförbudet förenas med ett förbud mot att göra avbildningar, beskrivningar eller mätningar av eller inom skyddsobjektet. Enligt 20 § skyddslagen kan ett beslut om skyddsobjekt gälla tills vidare eller under viss tid.

Klart är att bedömningen att något är ett skyddsobjekt i sig skulle kunna utgöra tillräcklig grund också för behovet av utökad riktad lagring, eftersom skyddslagens syfte är att ge viss typ av kritisk infrastruktur ett kvalificerat skydd. Som framgår av 1 och 2 §§ skyddslagen har dock reglerna för skyddsobjekt inte utformats med hänsyn till förekomsten av grov brottslighet rent generellt. Vi ser därför framför oss fler platser som motiverar riktad lagring men som inte är eller skulle kunna vara skyddsobjekt. Även om syftet med skyddslagen delvis sammanfaller med syftet för den riktade lagringen gör vi alltså bedömningen att urvalet för riktad lagring skulle bli för snävt om enbart skyddsobjekt skulle omfattas av riktad geografisk lagring med avseende på skyddsvärda platser. Vi förordar i stället ett bredare anslag där fler platser ska kunna omfattas av utökad riktad lagring.

Ett annat sätt att avgränsa vilka platser som bör omfattas av riktad lagring avseende skyddsvärda platser är att utgå från bestämmelserna i säkerhetsskyddslagen (2018:585). I likhet med skyddslagen kan säkerhetsskyddslagen också tjäna som vägledning för att kunna identifiera behov av lagring avseende skyddsvärda platser. Enligt 1 § första stycket säkerhetsskyddslagen tillämpas lagen bl.a. för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet. Med säkerhetskänslig verksamhet avses antingen en verksamhet som är av betydelse för Sveriges säkerhet eller en verksamhet som

[13] Se prop. 2009/10:87 s. 1.

omfattas av ett för Sverige förpliktigande internationellt åtagande om säkerhetsskydd. Begreppet säkerhetskänslig verksamhet omfattar såväl militär som civil verksamhet och är oberoende av om verksamheten bedrivs av det offentliga eller av enskilda aktörer.

Vi anser att det inte vore ändamålsenligt och alltför resurskrävande att låta Polismyndigheten, Säkerhetspolisen eller Tullverket ta kontakt med alla som bedriver säkerhetskänslig verksamhet för att närmare utröna behovet av utökad riktad lagring på den plats där den säkerhetskänsliga verksamheten bedrivs. En bättre lösning vore att låta de behöriga myndigheterna vid behov samråda med den som bedriver tillsyn över säkerhetskänslig verksamhet. Alla som på något sätt bedriver säkerhetskänslig verksamhet står under tillsyn av den myndighet som regeringen bestämt enligt 6 kap. 1 § säkerhetsskyddslagen. Tillsynsansvaret är fördelat mellan Försvarsmakten, Försvarets materielverk, Säkerhetspolisen, Affärsverket svenska kraftnät, Transportsstyrelsen, PTS, Finansinspektionen, Statens energimyndighet, Strålsäkerhetsmyndigheten och länsstyrelserna enligt 8 kap. 1 § säkerhetsskyddsförordningen.

Säkerhetspolisen och Försvarsmakten är samordningsmyndigheter enligt 8 kap. 2 § säkerhetsskyddsförordningen (2021:955).

I sammanhanget bör nämnas att det finns ett nära samband mellan säkerhetsskyddslagen och bestämmelserna i skyddslagen vad gäller frågor om fysisk säkerhet. Om den behöriga myndigheten redan konstaterat att det finns behov av riktad lagring avseende visst skyddsobjekt, behöver den inte utreda om det bedrivs säkerhetskänslig verksamhet där. Polismyndigheten, Säkerhetspolisen och Tullverket kan således med ledning av skyddslagen och säkerhetsskyddslagens bestämmelser bedöma vad som avses med en skyddsvärd plats inför ett beslut om utökad riktad lagring.

Vi kan dock inte utesluta att det kan finnas platser som bedöms vara särskilt utsatta från brottsbekämpningssynpunkt och som varken är skyddsobjekt eller en sådan plats som omfattas av säkerhetsskyddslagens bestämmelser. Det kan röra sig om gränsövergångar, trafikleder, knutpunkter för trafik eller annan plats som är av särskild betydelse från brottssynpunkt. Mot denna bakgrund bör det vid utökad riktad lagring avseende skyddsvärd plats också finnas möjlighet att beakta om en plats är särskilt utsatt för grov brottslighet. Som redan nämnts i föregående avsnitt ska bedömningen ske med iakttagande av proportionalitetsprincipen och på grundval av objektiva och icke-

diskriminerande faktorer, exempelvis genomströmning av ett stort antal människor på en viss plats eller att platsen som sådan möjliggör viss brottslighet, exempelvis smuggling.

Sammanfattningsvis bör utökad riktad lagring avseende skyddsvärd plats kunna avse en plats för ett skyddsobjekt, en plats där det bedrivs säkerhetskänslig verksamhet enligt säkerhetsskyddslagen eller en annan plats som bedöms vara av särskild betydelse från brottsbekämpningssynpunkt. I den danska lagstiftningen ges vissa exempel som kan vara vägledande, bl.a.

- statschefens och statsministerns bostäder,
- ambassader,
- polishus,
- kriminalvårdsanstalter,
- bro-, tunnel- och färjeförbindelser,
- knutpunkter för trafik och större tillfartsvägar,
- gränsövergångar,
- bussterminaler,
- stationer för stads- och fjärrtrafik,
- verksamhet som bl.a. hanterar farliga kemikalier och andra hälsovådliga ämnen,
- flygplatser, och
- militäranläggningar.[14]

Vi har i föregående avsnitt gjort bedömningen att tiden ska begränsas avseende ett beslut om utökad riktad lagring avseende geografiska områden. Samma huvudprincip bör även gälla för utökad riktad lagring avseende skyddsvärda platser. Det ligger i sakens natur att viss infrastruktur som exempelvis en hamn eller flygplats är av mer beständig natur och typiskt sett sker inga stora förändringar över tid i fråga om skyddsvärdet vid sådana platser. Att ständigt förnya dessa beslut framstår därför inte som ändamålsenligt. Mot den bakgrunden

[14] Lovforslag nr. L 93, § 786 c, Stk. 2.
https://www.ft.dk/ripdf/samling/20211/lovforslag/l93/20211_l93_som_fremsat.pdf.
Hämtat den 20 april 2023.

föreslår vi att ett beslut om utökad riktad lagring avseende skyddsvärda platser ska kunna gälla i tre år. Om behovet av datalagring på den skyddsvärda platsen kvarstår, bör beslutet kunna förlängas med högst tre år åt gången.

Det bör också sägas något om hur lagring avseende platser ska avgränsas i storlek. Med *plats* avses som huvudregel en yta som jämfört med ett *geografiskt område* är mindre till sin storlek, även om det kan hända att stora skyddsvärda anläggningar i vissa situationer leder till viss överlappning mellan dessa begrepp. I praktiken bör det inte föranleda några tillämpningssvårigheter, eftersom grunden för lagring skiljer sig åt beroende på om det är fråga om utökad riktad lagring avseende ett begränsat geografiskt område eller en plats.

När det gäller tillhandahållarna bör något sägas om hur lagringen ska verkställas. Det kommer i verkligheten sällan förhålla sig så att upptagningsområdet för en mobilmast, eller internetknutpunkt för fast bredband, kommer att vara avgränsad så att endast en viss angiven plats omfattas av lagringen. Det får accepteras att lagringen i vissa fall kommer att avse ett område som är större än själva platsen. Det är inte lämpligt att heller här ange hur stort ett sådant område får vara med angivelser av exakta mått. I likhet med vad vi har skrivit om utökad riktad lagring avseende områden måste bedömningen göras från fall till fall. Ytterst får lagringen utformas med beaktande av platsens belägenhet och karaktär samt tillhandahållarens infrastruktur. Beslutet bör dock vara tillräckligt preciserat för att tillhandahållarna ska kunna verkställa beslutet.

Som nämnts återkommer vi i avsnitt 9 om lagringsskyldighet för tillhandahållare av Noik.

Det torde höra till ovanligheterna, men vid förändrade förhållanden, såsom nedläggning av flygplatser eller omläggning av hamnar m.m., bör den beslutande myndigheten ha en skyldighet att ompröva behovet av lagring och upphäva lagringsbeslutet om lagringen inte längre bedöms strängt nödvändig.

I avsnitt 8.3.3 redovisar vi våra överväganden när det gäller omfattningen av lagringen.

Utökad riktad lagring avseende personer

Utredningens bedömning: Utökad riktad lagring avseende en viss person bör införas när det finns ett samband mellan personen och grova brott eller grov brottslig verksamhet under förutsättning att integritetsintrånget är proportionerligt och rimligt begränsat.

Enligt EU-domstolen har medlemsstaterna bl.a. möjlighet att vidta lagringsåtgärder avseende personer som är föremål för utredning, andra aktuella övervakningsåtgärder eller som förekommer i det nationella kriminalregistret på grund av en tidigare fällande dom för allvarliga brott som kan vara en indikation på att det föreligger en hög återfallsrisk.

En riktad lagring avseende en person kan riktas mot personer som förekommer i utredningar om grova brott och i underrättelseverksamhet avseende grov brottslighet, personer som är eller tidigare varit föremål för hemliga tvångsmedel, personer som förekommer i belastningsregistret och misstankeregistret samt personer som står under övervakning eller är villkorligt frigivna. Även personer som indirekt främjar brottslighet, såsom s.k. målvakter, kan bli föremål för riktad lagring. Det väsentliga är möjligheten att på objektiva och icke-diskriminerande grunder kunna sätta ett direkt eller indirekt samband mellan personen och grova brott eller grov brottslig verksamhet.

En reglering med personbestämd riktad lagring förutsätter att uppgifter om personen lämnas till den eller de tillhandahållare som därefter ska verkställa lagringen. Att till tillhandahållarna överlämna sådana uppgifter innebär risker för stort intrång i enskildas personliga integritet. Integritetsintrånget framstår som särskilt allvarligt om lagring kan ske beträffande personer utan att det föreligger någon konkret brottsmisstanke mot personen. Det finns en risk att uppgifter sprids om vilka personer som är föremål för riktad lagring. En sådan risk föreligger även om tillhandahållarnas tystnadsplikt skulle utvidgas till att avse uppgifter om vilka personer lagringen riktas mot. De enskilda personerna riskerar därmed att bli utpekade såsom misstänkta för brott.

Visserligen lämnar de brottsbekämpande myndigheterna redan i dag personuppgifter till tillhandahållarna i samband med verkställighet av vissa hemliga tvångsmedel. Det handlar dock om ett mycket begränsat antal uppgifter, som dessutom normalt lämnas till utvalda tillhandahållare efter noggranna överväganden av de brottsbekämpande

myndigheterna. Överföringen av uppgifter kräver också beslut av domstol eller åklagare.

Ett sätt att utforma utökad riktad lagring avseende person vore att överlåta till de behöriga myndigheterna att på eget ansvar fatta beslut om vilka personer som ska kunna bli föremål för lagring, exempelvis personer som förekommer i utredningar om grova brott eller i underrättelseverksamhet avseende grov brottslighet. För att lagringen inte ska bli godtycklig krävs att det ställs någon form av beviskrav i fråga om den enskildes anknytning till grova brott eller grov brottslig verksamhet. Det är emellertid svårt att föreskriva ett sådant beviskrav. Om det sätts lågt, finns det en risk att ett mycket stort antal personer blir föremål för riktad lagring. Sätts höga beviskrav, kan i stället ändamålet med lagringsåtgärden i stor utsträckning gå förlorat. Om beviskraven är lika höga som vid användning av hemliga tvångsmedel, skulle det i princip inte finnas anledning att först begära uppgifter lagrade när man på samma underlag skulle kunna begära uppgifterna utlämnade. I sådana situationer uppfyller användning av HÖK i realtid i princip samma funktion.

Vi gör bedömningen att det i praktiken är svårt att tillämpa ett beviskrav som inte medför att lagringen kan omfatta ett mycket stort antal personer. Förutom detta menar vi att det inte är lämpligt att låta de behöriga myndigheterna ensidigt och på eget ansvar fatta beslut om vilka personer som ska kunna bli föremål för lagring. Det har sin grund i, som vi beskrivit ovan, att det kan innebära ett stort integritetsintrång att bli föremål för tvångsåtgärder från de brottsbekämpande myndigheternas sida. Ett beslut om lagring av uppgifter knutna till en person utgör en rättighetsinskränkning, även om det är fråga om en mindre ingripande åtgärd jämfört med användning av hemliga tvångsmedel. Sådana beslut bör typiskt sett föregås av någon form av kontroll.

Vår utgångspunkt är därför att utökad riktad lagring avseende personer bör utformas på ett sådant sätt att risken för integritetsintrång är så liten som möjligt. Mot denna bakgrund föreslår vi två modeller för personbaserad lagring där integritetsintrånget, enligt vår mening, är proportionerligt och rimligt begränsat. En modell tar sikte på personer som är eller har varit föremål för hemliga tvångsmedel. Den andra modellen avser personer som genom lagakraftvunnen dom eller godkänt strafföreläggande ålagts påföljd för viss allvarlig brottslighet.

Utökad riktad lagring avseende personer som är eller har varit föremål för hemliga tvångsmedel

Utredningens förslag:

- Datalagring får avse en person som är eller har varit föremål för hemliga tvångsmedel som avses i rättegångsbalken, lagen om hemlig dataavläsning eller inhämtningslagen.
- Ett beslut om lagring får inte grunda sig på ett tvångsmedelsbeslut som är äldre än tre år.
- Ett beslut om lagring ska gälla så länge behovet kan förväntas föreligga och längst under ett års tid.
- Ett beslut om lagring får förlängas genom ett nytt beslut. Ett beslut om förlängning får dock inte beslutas senare än tre år efter det att tvångsmedelsbeslutet meddelats.
- De behöriga myndigheterna ska vid ändrade förhållanden ompröva om grunden för den utökade lagringen består och annars upphäva lagringsbeslutet.

Denna modell avser alltså personer som är eller har varit föremål för hemliga tvångsmedel. Sådana åtgärder föregås alltid av ett domstols- eller åklagarbeslut. Det finns därigenom tillräckliga rättssäkerhetsgarantier för de enskilda.

Med hemliga tvångsmedel avses i detta sammanhang de åtgärder som regleras i 27 kap. rättegångsbalken, lagen om hemlig dataavläsning och inhämtningslagen. Det omfattar även hemliga tvångsmedel enligt 27 kap. rättegångsbalken eller lagen om hemlig dataavläsning genom tillämpningen av preventivlagen, LIRB, EIO, och LSU.

En person som är eller har varit föremål för hemliga tvångsmedel kan sättas i direkt eller indirekt samband med grova brott eller grov brottslig verksamhet. Det bör dock nämnas att användning av hemliga tvångsmedel även kan omfatta andra personer än de som misstänks för grova brott eller deltagande i grov brottslig verksamhet, exempelvis en målsägande. I anslutning till detta bör nämnas att tillämpningsområdet för vissa av de hemliga tvångsmedel vi nämnt är bredare än att åtgärden riktas mot bara en person. Exempelvis kan inhämtning enligt inhämtningslagen ge tillgång till uppgifter om vilka

mobiltelefoner som haft kontakt med en viss basstation vid en viss tidpunkt, dvs. en s.k. basstationstömning. I en sådan situation riktar sig åtgärden snarare mot utrustningen. På motsvarande sätt kan en HÖK i vissa situationer användas för att ta reda på vem som innehar ett abonnemang. I dessa exempel avser åtgärderna alltså i första hand utrustning och abonnemang. Vi återkommer till dessa fall i avsnittet nedan om utökad riktad lagring avseende teknik.

Vi föreslår sammanfattningsvis en möjlighet till utökad riktad lagring avseende personer som är eller har varit föremål för hemliga tvångsmedel. De behöriga myndigheterna kan således fatta beslut om utökad riktad lagring avseende en sådan person när domstol eller åklagare har meddelat tillstånd till ett hemligt tvångsmedel. Inget hindrar att ett sådant beslut fattas vid en senare tidpunkt än då tillståndet meddelades. Det krävs dock att de behöriga myndigheterna gör bedömningen att det är strängt nödvändigt i det enskilda fallet. Vårt förslag utgår således inte från att alla som är, eller vid något tillfälle har varit, föremål för hemliga tvångsmedel per automatik också ska bli föremål för utökad riktad lagring. Även om det i många fall kan vara så att ett tvångsmedelsbeslut i sig kan utgöra skäl för ett beslut om utökad riktad lagring finns situationer när så inte är fallet. Det kan exempelvis vara så att det visar sig att en person, som varit föremål för hemliga tvångsmedel, saknar koppling till den aktuella brottsmisstanken.

För att inte riskera att ett beslut om utökad riktad lagring avseende en person i aktuella situationer går utöver vad som är absolut nödvändigt, bör det finnas tidsmässiga begränsningar. Det bör inledningsvis finnas en bortre gräns för hur gammalt ett beslut om hemliga tvångsmedel ska få vara när det läggs till grund för ett lagringsbeslut. Enligt vår bedömning framstår det inte som proportionerligt att låta äldre tvångsmedelsbeslut ligga till grund för lagring. Vi föreslår därför att de behöriga myndigheterna ska kunna fatta beslut om utökad riktad lagring i upp till tre år efter det att ett tvångsmedelsbeslut har fattats, förutsatt att det fortfarande finns ett behov i det enskilda fallet.

Utöver detta bör även giltighetstiden för beslut om utökad riktad lagring begränsas. Ett sådant beslut bör få gälla så länge det finns ett behov men längst under ett års tid. Om det finns ett fortsatt behov av lagring, får beslutet förlängas, men inte bortom tidsgränsen om tre år.

Ett beslut om lagring avseende en person som varit föremål för ett hemligt tvångsmedel måste innehålla uppgifter som gör det möjligt för tillhandahållaren att verkställa lagringen. Om det är ett namn, nummer, kontouppgift, abonnemangsuppgift eller uppgift om utrustning har inte någon betydelse. Det väsentliga är att det går att knyta personen till uppgiften och att tillhandahållarna de facto har möjlighet att verkställa lagringen. Vi ser fördelar med att beslut om utökad riktad lagring kan avse en person och inte begränsas till visst nummer, adress eller utrustning. Många gånger har den myndighet som beslutar om lagring av trafik- och lokaliseringsuppgifter även tillgång till uppgifter som behövs för att verkställa beslutet. Med vårt förslag får tillhandahållaren, för det fall sådana uppgifter saknas, bistå den beslutande myndigheten. Exempelvis kan tillhandahållarna genom uppgifter som de behandlar för egna ändamål, exempelvis för fakturering, knyta en viss person till ett visst konto, abonnemang eller enhet.

Utökad riktad lagring avseende personer som dömts för grova brott

Utredningens förslag:

- Datalagring får avse en person som genom lagakraftvunnen dom eller godkänt strafföreläggande ålagts påföljd för brott som ger rätt att använda HÖK enligt rättegångsbalken.
- Ett beslut om lagring avseende person får inte grundas på en dom eller ett godkänt strafföreläggande senare än tre år efter det att den ålagda påföljden till fullo har verkställts.
- Ett beslut om lagring ska gälla så länge behovet kan förväntas föreligga och längst under ett års tid.
- Ett beslut om lagring får förlängas genom ett nytt beslut. Förlängning får dock inte beslutas senare än tre år efter det att den ålagda påföljden till fullo har verkställts.
- De behöriga myndigheterna ska vid ändrade förhållanden ompröva om grunden för den utökade lagringen består och annars upphäva lagringsbeslutet.

Lagringen enligt denna modell tar i första hand sikte på personer som är dömda för grova brott.

Uppgifter om den som har dömts för brott eller har godkänt ett strafföreläggande finns i belastningsregistret, som förs av Polismyndigheten. Bestämmelser om belastningsregistret finns i lagen (1998:620) om belastningsregister med tillhörande förordning (1999:1134). Sekretess gäller i verksamhet som avser förande av eller uttag ur registret. Det finns dock särskilda föreskrifter om utlämnande av uppgifter ur registret, se 35 kap. 3 § OSL.

Den omständigheten att någon har blivit dömd för grovt brott kan vara en indikation på att det föreligger en återfallsrisk. Med grova brott avser vi även här brott för vilka det finns möjligheter att tillämpa reglerna om hemliga tvångsmedel, i praktiken s.k. HÖK-brott som vi beskrivit tidigare beträffande utökad riktad lagring avseende områden. Det skulle därför kunna vara motiverat med en möjlighet till lagring gentemot personer som blivit dömda för grova brott.

Vi menar dock att inte alla som förekommer i belastningsregistret som dömts för grova brott bör kunna bli föremål för utökad riktad lagring. En sådan ordning skulle i praktiken kräva att uppgifter kontinuerligt behöver överföras till tillhandahållarna på grund av de ständiga förändringar som sker i registret, eftersom tillhandahållaren behöver underrättas om nya eller gallrade avsnitt i belastningsregistret. I praktiken skulle i så fall krävas någon form av systemintegration mellan Polismyndighetens och tillhandahållarens uppgiftssamlingar, om innehållet i belastningsregistret ska styra den utökade riktade lagringen avseende personer. Att överföra stora delar av belastningsregistret eller att låta privaträttsliga subjekt ha någon form av direktåtkomst till dessa starkt integritetskänsliga samlingar av personuppgifter vore dock en främmande ordning. Skyddet för enskildas integritet skulle på detta sätt urholkas.

En lämpligare ordning är att låta de behöriga myndigheterna göra ett urval efter bedömning i det enskilda fallet. En sådan ordning bär större likhet med vad vi har beskrivit ovan vid utökad riktad lagring avseende personer som är eller har varit föremål för hemliga tvångsmedel. I sådana fall föregås bedömningen av överväganden i det enskilda fallet och är begränsade till antalet. Mot denna bakgrund gör vi bedömningen att det bör finnas en möjlighet för de behöriga myndigheterna att besluta om utökad riktad lagring avseende en person

som genom en lagakraftvunnen dom eller godkänt strafföreläggande ålagts påföljd för ett sådant brott som ger rätt att använda HÖK.

En sådan lagring skulle kunna utformas på ett sådant sätt att den har ett samband med den rättsverkan som den ålagda påföljden har. Med det menar vi att ett beslut om utökad riktad lagring inte ska få fattas när påföljden till fullo har verkställts, vilket som huvudregel betyder vid prövotidens utgång. En sådan modell har nackdelen att räckvidden av åtgärden begränsas. Typiskt sett kvarstår risken för återfall i brottslighet även efter en verkställd påföljd.

Å andra sidan kan det anföras principiella invändningar mot att grunda ett beslut om utökad riktad lagring på en dom eller godkänt strafföreläggande när påföljden till fullo har verkställts. Datalagringen skulle då kunna uppfattas som ytterligare en påföljd eller annan rättsverkan av brott. Vi ser dock inte saken på det sättet. Ett beslut om utökad riktad lagring avseende en person bör ses som en brottsbekämpande åtgärd som har sin grund i att den som blivit lagförd för ett grovt brott ofta har en förhöjd risk för att återfalla i ny brottslighet. EU-domstolens resonemang om sådan riktad lagring måste också förstås på detta sätt.

Vi gör sammantaget bedömningen att övervägande skäl talar för att det bör finnas en möjlighet att besluta om datalagring även en viss tid efter det att den ålagda påföljden till fullo har verkställts.

Frågan om hur lång tid det ska vara bör bedömas utifrån behovet av lagring. En längre tid än tre år torde generellt sett inte behövas. Vi föreslår därför att lagringen ska kunna ske upp till tre år efter det att påföljden till fullo har verkställts. Det betyder dock att den som döms till ett längre fängelsestraff kan komma att bli föremål för ett beslut om utökad riktad lagring under en relativ lång tid, eftersom ett beslut om lagring vid behov kan fattas under verkställigheten av fängelsestraffet och sedan komma att förlängas. Enligt vår bedömning är det inte oproportionerligt. Den omständigheten att myndigheterna har möjlighet att besluta om utökad riktad lagring betyder inte per automatik att så sker. Behovet ska alltid prövas genom en bedömning i det enskilda fallet. Det är de behöriga myndigheterna som i första hand ska avgöra om det finns ett sådant behov. Så kan exempelvis vara fallet när en person som är dömd för grova brott återkommer i underrättelseuppslag. Genom den tidigare domen föreligger en viss presumtion för risk för återfall i grov brottslighet. Den

risken bör vara tillräcklig om det i övrigt finns ett behov hos de behöriga myndigheterna att besluta om utökad riktad lagring.

När det sedan gäller frågan om hur lång tid ett beslut om lagring ska få gälla är vår utgångspunkt att en tidsbegränsning på ett år bör gälla. Vid behov får ett beslut förlängas. Ett beslut om lagring eller förlängning av ett sådant beslut bör dock, som vi utvecklat ovan, inte kunna fattas senare än tre år efter det att den ålagda påföljden till fullo har verkställts.

Som vi har beskrivit ovan ska tillhandahållarna vid behov bistå den beslutande myndigheten i fråga om verkställighet av beslutet. Tillhandahållarna förväntas dock inte ta ansvar för eller överpröva de behöriga myndigheternas beslut. Det är den myndighet som beslutar om utökad riktad lagring avseende person som bär ansvaret för att beslutet är korrekt. Bedömningen får ske med utgångspunkt från dels uppgifter som myndigheten själv förfogar över, dels uppgifter som myndigheten får av tillhandahållarna. Som huvudregel bör de behöriga myndigheterna kunna utgå från att den som tecknat ett visst abonnemang också är den som genererar trafik- och lokaliseringsuppgifterna som ska lagras. Om myndigheterna däremot får ett tvetydigt underlag från tillhandahållarna, exempelvis förekomsten av ett familjeabonnemang med flera användare eller motsvarande, bör det i normalfallet krävas ytterligare åtgärder för att säkerställa att beslutet inte avser fel person. Att en enhet tycks användas sporadiskt av någon annan än innehavaren bör dock inte utgöra hinder mot lagring.

I vissa situationer kan det förhålla sig så att utrustning och abonnemang byter ägare så att lagringen inte längre omfattar den person som ursprungligen avsågs. Om den myndighet som fattat beslutet får kännedom om sådana förhållanden, ska beslutet upphävas. Det bör förtydligas att beslutet om utökad riktad lagring avseende person inte i efterhand får kompletteras med nya uppgifter. Exempelvis kan inte ett beslut om utökad riktad lagring avseende person i efterhand kompletteras med nya abonnemangsuppgifter. Bortsett från uppenbara skrivfel eller motsvarande felaktigheter bör ett fattat beslut inte ändras. Vid ändrade förhållanden ska i stället ett nytt beslut fattas.

Som nämnts återkommer vi i avsnitt 9 om lagringsskyldighet för tillhandahållare av Noik.

Utökad riktad lagring avseende teknik

Utredningens förslag:

- Datalagring får ske avseende sådan utrustnings- eller abonnemangsidentitet som använts vid eller skäligen kan antas komma till användning vid ett grovt brott eller vid grov brottslig verksamhet.
- Brott och brottslig verksamhet som innefattar sådana brott som ger rätt att använda HÖK enligt rättegångsbalken får ligga till grund för beslut om utökad riktad lagring avseende utrustnings- eller abonnemangsidentitet.
- Ett beslut om lagring ska gälla så länge som behovet kan förväntas föreligga och längst under ett års tid.
- Lagringsskyldigheten ska därefter kunna förlängas genom ett nytt beslut om behovet kvarstår.
- De behöriga myndigheterna ska vid ändrade förhållanden ompröva om grunden för den utökade riktade lagringen består och annars upphäva lagringsbeslutet.

Förutom de modeller av lagring som vi föreslagit ovan tillåter EU-rätten att lagring grundas på andra objektiva och icke-diskriminerande kriterier, om dessa begränsas till vad som är strängt nödvändigt och det, åtminstone indirekt, finns ett samband mellan allvarlig brottslighet och de personer vilkas uppgifter lagras.[15] Ett sådant kriterium skulle kunna vara att använda riktad lagring beträffande viss utrustning, teknisk infrastruktur eller tjänst. Härefter använder vi oss av uttrycket utökad riktad lagring avseende teknik när vi beskriver sådan lagring.

En utmaning med utökad riktad lagring avseende teknik är att det krävs ett underlag som visar ett direkt eller indirekt samband mellan användningen av viss utrustning eller tjänst och grov brottslighet. I regel sker elektronisk kommunikation med hjälp av produkter och tjänster på den öppna marknaden och dessa har som huvudregel helt legitima användningsområden. Exempelvis kan krypterade kommunikationslösningar användas såväl för att skapa förutsättningar för

[15] SpaceNet-domen p. 112.

arbete på distans som för att dölja brottslig verksamhet. Det krävs därför ett särskiljande kriterium som lagringen kan utgå ifrån.

En annan utmaning är att en modell med utökad riktad lagring avseende teknik måste utformas på ett sådant sätt att det som särskiljer tekniken ska gå att identifiera av den som tillhandahåller tjänsten. Om trafiken är krypterad för tillhandahållaren, eller om utrustningen inte går att identifiera, finns ingen reell möjlighet att kunna rikta lagringen till tjänster och utrustning som identifierats av de brottsbekämpande myndigheterna. I vissa situationer behandlar tillhandahållarna exempelvis inte uppgifter om utrustningsidentitet.[16]

Det finns även utmaningar med utökad riktad lagring avseende teknik på grund av den snabba teknikutvecklingen och den ständiga förändringen i konsumtions- och kommunikationsvanor. Det medför praktiska svårigheter att på förhand föreskriva närmare kriterier för en sådan lagring när användarna ofta byter utrustning eller kommunikationssätt.

Vi har mot bakgrund av ovan beskrivna utmaningar ändå övervägt olika lösningar för utökad lagring avseende teknik. En teoretisk lösning skulle kunna vara att i lag slå fast de grundläggande principerna för hur utökad riktad lagring avseende teknik får ske och därefter överlåta till de brottsbekämpande myndigheterna, en domstol eller ett annat oberoende organ att i särskilda situationer uppdra åt tillhandahållarna att påbörja en viss typ av riktad lagring. Vi ställer oss emellertid klart tveksamma till en sådan lösning. En sådan oprecis reglering torde knappast vara förenlig med EU-rätten. Sett ur tillhandahållarnas perspektiv framstår det vidare som betungande och kostsamt att bli ålagda en lagringsskyldighet som inte präglas av tillräcklig grad av förutsebarhet. Det kan som vi gett exempel på ovan också uppstå situationer där det beslutas om en lagringsskyldighet som inte går att verkställa på grund av tekniska hinder. Sammantaget finns sådana utmaningar med utökad riktad lagring avseende teknik att de inger betänkligheter med att alls föreslå en sådan modell.

De brottsbekämpande myndigheterna har emellertid för oss påtalat att det finns ett angeläget behov i det brottsbekämpande arbetet att kunna fatta beslut om utökad riktad lagring som tar sikte på användning av viss utrustning, infrastruktur och tjänst. Som exempel har bl.a. nämnts hur myndigheterna har kunnat sätta krypterade kom-

[16] Exempelvis kan en Mac-adress (Media Access Control) identifiera enhetens nätverksanslutning men den uppgiften har tillhandahållare många gånger inte tillgång till.

munikationsenheter och tjänster som Encrochat, Sky ECC och Anom i förbindelse med grov brottslig verksamhet.[17] Som ytterligare exempel har nämnts hur s.k. målvakter kan försöka dölja förekomsten av grova brott eller grov brottslig verksamhet genom att registrera sig som innehavare av vissa sim-kort för mobiltelefoner.

För att uppfylla EU-rättens krav på proportionalitet måste det i nationell lagstiftning föreskrivas klara och precisa bestämmelser som reglerar räckvidden och tillämpningen av lagringen 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.[18] Vi anser mot bakgrund av vad vi beskrivit att det inte är förenligt med EU-rätten att rent generellt överlåta till de brottsbekämpande myndigheterna att fatta beslut om utökad riktad lagring avseende teknik. Proportionalitetskravet torde i regel hindra exempelvis beslut om utökad riktad lagring av en hel kommunikationsplattform eller tjänst.

Vi har däremot, med utgångspunkt från de konkreta behov som de brottsbekämpande myndigheterna har beskrivit, gjort bedömningen att utökad riktad lagring bör kunna föreskrivas i vissa konkreta situationer när det avser användning av viss utrustning eller ett specifikt abonnemang. Det är då till en början fråga om avgränsade och precisa fall. Det handlar om situationer när de brottsbekämpande myndigheterna kan konstatera att en viss utrustning eller ett visst abonnemang används för att begå grovt brott eller skäligen kan antas komma till användning vid ett grovt brott eller vid grov brottslig verksamhet. Lagringen tar sikte på själva utrustningsidentiteten eller abonnemangsidentiteten.

En viktig förutsättning är naturligtvis att de brottsbekämpande myndigheterna har tillgång till uppgifter som tillhandahållarna kan använda för att identifiera viss utrustning eller visst abonnemang. Exempel på uppgifter som den utökade riktade lagringen kan avse kan vara IMEI-nummer för mobiltelefoner, ICCID-nummer för simkort[19] eller IMSI-nummer för mobiltelefonabonnemang, fasta eller dynamiska ip-adress eller ett konto hos en tillhandahållare av tjänster

[17] Dessa kommunikationstjänster ställdes avsiktligt till kriminella organisationers förfogande, se exempelvis Riksåklagarens yttrande den 29 april 2021 i Högsta domstolens mål B 2222-21 avseende Encrochat, AMR-3420-21.
[18] SpaceNet-domen p. 69.
[19] ICCID-nummer kan även avse s.k. eSim som då är en integrerad del av enheten och bör bedömas som utrustningsidentitet.

för kommunikation (se avsnitt 9.3). Det finns inget som hindrar att även nummerserier används för att identifiera viss utrustning, exempelvis en viss serie av IMEI-nummer eller motsvarande.

Det bör i sammanhanget förtydligas att ett beslut om utökad riktad lagring avseende en ip-adress inte är samma sak som att lagring ska ske av den trafik som sker till och från en viss enhet. Som vi har redogjort för i avsnitt 6.6.1 måste innehavaren av en ip-adress hållas isär från ip-adress som trafikuppgift. Vad vi nu talar om är användningen av ip-adress som utgångspunkt för att tillhandahållarna ska verkställa ett beslut om utökad riktad lagring avseende ett visst abonnemang. Det är inte samma sak som att internettrafik till och från abonnemanget ska lagras. Sådan aktivitet kan indirekt avslöja innehållet i aktiviteten, exempelvis då en viss webbsida har besökts. Vi har, som framgår av avsnitt 7.3.6, gjort bedömningen att det av integritetsskyddskäl inte ska förekomma någon lagring av internettrafik. Vi gör ingen annan bedömning i fråga om utökad riktad lagring.

Sammanfattningsvis kan ip-adress vara ett bland många sätt för de behöriga myndigheterna att identifiera och begära lagring av ett abonnemang som direkt eller indirekt har koppling till grova brott och grov brottslighet. Vi övergår nu till frågan om hur en sådan koppling ska se ut.

Att konstatera om en enhet eller ett abonnemang används eller har använts vid ett grovt brott bör i regel vara oproblematisk. Så kan exempelvis vara fallet när de brottsbekämpande myndigheterna kan konstatera att en mobiltelefon eller en dator har använts eller alltjämt används för dataintrång, barnpornografibrott eller grova bedrägerier och de behöriga myndigheterna behöver datalagring under utredningstiden för att kunna klarlägga vem som är innehavare av enheten eller abonnemanget.

När det gäller kopplingen till grov brottslighet i övrigt krävs i regel underrättelseuppgifter som påvisar ett direkt eller indirekt samband mellan en viss enhet eller abonnemang och grov brottslig verksamhet. Bedömningen får inte bygga på spekulationer eller antaganden utan ska vara grundad i faktiska omständigheter inom ramen för ett enskilt fall eller händelseförlopp. I 27 kap. 1 § rättegångsbalken finns bestämmelser om att ett föremål får tas i beslag om det skäligen kan antas att det har betydelse för bl.a. utredning om brott. Vi anser att motsvarande beviskrav bör gälla för utökad riktad lagring avseende teknik. I fråga om bevisningens styrka kan vägledning hämtas från

begreppet skälig misstanke. Det är svårt att i generella termer ange när en skälig misstanke mot någon kan föreligga. Rent allmänt tar dock skälig misstanke sikte på situationer där konkreta omständigheter av en viss styrka pekar på att just den misstänkte har begått brottet.[20]

Det finns vissa svårigheter med att ställa samma beviskrav för underrättelseverksamheten, där det många gånger kan vara svårt att precisera vilka brott det är fråga om. I vissa fall kan misstankar riktas mot en större krets personer, utan att det går att avgöra vem eller vilka som kan misstänkas. Det finns dock inget som hindrar att det ställs motsvarande krav på att det ska finnas konkreta omständigheter som talar för att utrustningen eller abonnemanget kan antas komma till brottslig användning.

Som vi har redovisat tidigare får riktad lagring användas för att bekämpa grov brottslighet. Det innebär att brott och brottslig verksamhet som innefattar sådana brott som ger rätt att använda HÖK enligt rättegångsbalken får ligga till grund för beslut om utökad riktad lagring avseende utrustnings- och abonnemangsidentitet.

Ett beslut om utökad riktad lagring avseende teknik bör på samma sätt som övriga former av utökad riktad lagring begränsas i tid för att lagringen inte ska pågå längre än vad som är absolut nödvändigt. Vi har för merparten av övriga former av riktad lagring gjort bedömningen att ett år är lämpligt. Vi gör ingen annan bedömning för utökad riktad lagring avseende teknik och föreslår att ett beslut om utökad riktad lagring ska få gälla i högst ett år. Om behovet av datalagring avseende viss utrustnings- eller abonnemangsidentitet kvarstår, får de behöriga myndigheterna förlänga sitt beslut i högst ett år åt gången.

Som för alla former av utökad riktad lagring ska beslutet upphöra vid ändrade förhållanden. Vi har i ovanstående avsnitt om utökad riktad lagring avseende person beskrivit att överlåtelser av utrustning och abonnemang kan ge upphov till att lagringen behöver upphöra. På samma sätt som ovan ska alltså den myndighet som fattat ett beslut om utökad riktad lagring upphäva sitt beslut om det kommer till myndighetens kännedom att kopplingen mellan utrustnings- eller abonnemangsidentitet och grova brott eller grov brottslig verksamhet har upphört.

[20] Jfr Lindberg, Gunnel, Straffprocessuella tvångsmedel – när och hur får de användas, Juno version 5, publicerat digitalt 2022, s. 80–90.

8.3.3 Lagringsskyldighetens omfattning vid geografiskt riktad lagring och utökad riktad lagring

Utredningens förslag: Geografiskt riktad lagring ska omfatta fler uppgiftstyper än den lagringsskyldighet som gäller i dag och lagringsskyldighetens omfattning ska framgå av lag med närmare föreskrifter i förordning.

Ett beslut om utökad riktad lagring kan omfatta samma uppgiftstyper som geografiskt riktad lagring. Ramarna för lagringsskyldighetens omfattning ska framgå av lag och närmare föreskrifter anges i förordning.

Lagringstiden för såväl geografiskt riktad lagring som utökad riktad lagring ska vara ett år från den dag kommunikationen avslutades.

Om tillhandahållarna saknar uppgift om när kommunikationen avslutades, ska lagringstiden räknas från den dag då uppgiften genererades. Geografiskt riktad lagring ska även omfatta lagring av uppgifter som genereras eller behandlas vid misslyckad uppringning. Sådana uppgifter får även lagras vid utökad riktad lagring.

Vi har föreslagit två former av riktad lagring, geografiskt riktad lagring och utökad riktad lagring. Dessa kan i vissa situationer överlappa varandra.

Geografiskt riktad lagring ålägger tillhandahållare att lagra trafik- och lokaliseringsuppgifter inom vissa kommuner. För geografiskt riktad lagring bör lagringsskyldighetens omfattning framgå direkt av lag och närmare föreskrifter anges i förordning.

Utökad riktad lagring förutsätter ett beslut från Polismyndigheten, Säkerhetspolisen eller Tullverket. Vid utökad riktad lagring bör ramarna för lagringsskyldighetens omfattning, i likhet med vad vi har föreslagit för nationell säkerhetslagring, framgå av lag och närmare föreskrifter i förordning.

I syfte att bekämpa grov brottslighet behövs en mer omfattande lagringsskyldighet än i dag

Som vi redovisat i avsnitt 7.3.6 reglerar EU-rätten lagring av trafik- och lokaliseringsuppgifter på övergripande nivå och det ankommer på medlemsstaterna att reglera lagringens omfattning till vad som är strängt nödvändigt. Även om våra överväganden nu handlar om riktad lagring gör vi i huvudsak samma bedömningar som beträffande lagring i syfte att skydda den nationella säkerheten. Eftersom de författningsändringar som gjordes i Sverige år 2019, om en begränsning i lagringsskyldigheten för teleoperatörer, syftade till att tillgodose det EU-rättsliga kravet på att lagringsskyldigheten inte får vara generell och odifferentierad finns det nu anledning att överväga vilka uppgifter som bör kunna lagras vid riktad lagring.

I våra överväganden beaktar vi i denna del följande uttalanden som regeringen gjort i fråga om vikten av tillgång till information för att bekämpa grov brottslighet i Sverige. Våldsbrott i form av skjutningar och sprängningar har ökat markant i Sverige de senaste åren. Antalet skjutningar med dödlig utgång har också ökat. Men den grova brottsligheten är inte begränsad till skjutvapenvåld. Narkotikabrott, rån och utpressning är exempel på andra brott som är vanligt förekommande i sådana sammanhang. Denna brottslighet har ofta stark koppling till kriminella nätverk. Brott som begås inom ramen för kriminella nätverk kan av olika skäl vara särskilt svåra att utreda. För att öka tryggheten i landet och stärka skyddet mot sådan brottslighet, som utgör ett hot mot såväl enskilda människors liv och hälsa som det svenska samhället i stort, måste insatserna mot de kriminella nätverken ytterligare intensifieras. Ett viktigt led i detta är att säkerställa att de brottsbekämpande myndigheterna har tillgång till ändamålsenliga och verkningsfulla verktyg för att effektivt kunna förhindra och bekämpa allvarlig brottslighet. En avgörande faktor för att kunna förhindra skjutningar och sprängningar och annan grov brottslighet är att myndigheterna får tillgång till relevant information i ett tidigt skede.[21]

En modell med riktad lagring, dvs. både geografiskt riktad lagring och utökad riktad lagring, innebär att de brottsbekämpande myndigheterna kommer få en sämre förmåga att förhindra och bekämpa grov brottslighet än med nuvarande ordning. För att tillgodose myndig-

[21] Jfr kommittédirektiven 2020:66, 2020:104, 2021:102.

heternas behov av uppgifter för att bekämpa den grova brottsligheten behöver därför de uppgiftskategorier som togs bort genom 2019 års lagstiftning kunna omfattas av riktad lagring. Härutöver behöver viss anpassning ske i anledning av teknikutvecklingen, såsom utifrån hur användningen av permanenta och tillfälliga identifierare sker i 5G (se avsnitt 10.4.2). Vi hänvisar till avsnitt 7.3.6 för en beskrivning av uppgifter som lagrades före 2019 års reform. Se även jämförelsetabell i bilaga 3.

Vårt ställningstagande innebär att skyldigheten att lagra trafik- och lokaliseringsuppgifter i syfte att bekämpa grov brottslighet ska omfatta fler uppgiftskategorier än i dag. I nästa avsnitt redovisar vi samtliga uppgiftskategorier som antingen ska lagras vid geografiskt riktad lagring eller som kan omfattas av lagringsskyldigheten vid utökad riktad lagring. Den utökade riktade lagringen kan alltså, beroende på beslutet i det enskilda fallet, omfatta samma typer av uppgifter som den geografiskt riktade lagringen.

Lagringen kommer, i förhållande till nu gällande regelverk, omfatta färre abonnenter och registrerade användare av elektroniska kommunikationstjänster. Även den tekniska utvecklingen och nya kommunikationsmönster har gjort att mycket av den information som tidigare varit tillgänglig för brottsbekämpande myndigheter inte längre går att komma åt. Det motiverar en mer omfattande lagring. Vi bedömer därför att en lagringsskyldighet i enlighet med våra förslag är proportionerlig sett till syftet att bekämpa grov brottslighet.

Vi påminner avslutningsvis även här, se avsnitt 7.3.6, att regleringen i EU:s dataskyddsförordning inte fråntar leverantörerna ansvar enligt nya LEK. Trafik- och lokaliseringsuppgifter som vid något tillfälle har behandlats för att förmedla en viss tjänst kan således omfattas av lagringsskyldighet enligt nya LEK. Sådana uppgifter får således inte raderas, inte ens om det sker i omedelbar anslutning till att trafiken förmedlas. Vi återkommer i avsnitt 9 till frågan om tillhandahållare av Noik ska kunna omfattas av lagringsskyldigheten.

Principer för lagringsskyldighetens omfattning och uppgifter som omfattas av lagringsskyldigheten

Vi hänvisar till avsnitt 7.3.6 vad gäller principerna för lagringsskyldighetens omfattning och uppgifter som omfattas av lagringsskyldigheten. Samma principer ska alltså gälla vid lagring av uppgifter som sker i

syfte att bekämpa grova brott. Det innebär bl.a. lagringsskyldigheten endast ska gälla för uppgifter som genereras eller behandlas i leverantörens verksamhet och att fler uppgifter ska lagras. Se närmare om detta under rubrikerna *Principer för lagringsskyldighetens omfattning* och *Uppgifter som omfattas av lagringsskyldigheten* i avsnitt 7.3.6.

En fråga som uppkommer i anledning av våra förslag är om det vid lagring som sker för att bekämpa grov brottslighet ska lagras färre uppgifter än vid nationell säkerhetslagring. Det går att motivera en sådan åtskillnad, eftersom frågor om nationell säkerhet motiverar mer ingripande åtgärder. De brottsbekämpande myndigheterna har emellertid samma behov av uppgifter och använder i allt väsentligt samma metoder i det brottsbekämpande arbetet. Det talar emot en differentierad lagring när det gäller att bekämpa grov brottslighet. Var någon befunnit sig inför planeringen av ett brott, eller efter ett fullbordat brott, är lika betydelsefullt för brottsutredningen, oavsett om den avser bekämpning av grov brottslighet eller brottslighet som hotar den nationella säkerheten. Det är exempelvis svårt att motivera att färre uppgifter ska lagras när lagringen syftar till att förhindra eller lagföra ett mordförsök, föranlett av uppgörelser mellan kriminella grupperingar, än när mordförsöket har föregåtts av politiska motiv. Vi kan därför inte se några bärande argument för att de brottsbekämpande myndigheterna ska få sämre utredningsunderlag i vissa fall. Vi bedömer att det i stället är lämpligare att minska riskerna för intrång i de enskildas personliga integritet genom att reglera förutsättningarna för lagringsskyldigheten på det sätt som vi beskriver nedan. Utfallet blir under sådana förhållanden att de brottsbekämpande myndigheterna senare kan få tillgång till samma typer av uppgifter. Lagringstiden blir dock kortare och lagringen är inte heller generell och odifferentierad när den sker i syfte att bekämpa grov brottslighet. Sammantaget bör syftet med lagringen inte påverka vilka uppgifter som bör lagras. Efter att lagring skett ska således följande frågor kunna besvaras i efterhand.

1. Vem kommunicerade med vem?
   - Telefonnummer, ip-adress eller annan meddelandeadress.
   - Abonnemangs-, konto- eller utrustningsidentitet och kopplingen mellan permanenta och tillfälliga identifierare.
   - Uppgifter om abonnent och registrerad användare.

- Uppgifter som krävs för att identifiera slutmålet för kommunikationen i de situationer där den som avskiljer kommunikationen inte omfattas av lagringsskyldighet, exempelvis när kommunikationen övergår från tillhandahållarens nät till ett företagsnätverk.

2. När ägde kommunikationen rum?
   - Datum och spårbar tid för då samtalet påbörjades och avslutades, då ett meddelande skickades och togs emot, eller då viss internettrafik ägde rum.
3. Var fanns användarnas utrustning?
   - Lokaliseringsuppgifter vid kommunikation eller internetåtkomst, alltså inte endast vid kommunikationens början och slut.
   - Övriga lokaliseringsuppgifter som inte är trafikuppgifter (t.ex. satellitpositioneringsuppgifter som genererats i utrustningen).
4. Vilken typ av kommunikation var det fråga om?
   - Uppgifter om den eller de tjänster som använts.
   - Uppgift om kapacitet för överföring (t.ex. fast bredband via fiber).

Geografiskt riktad lagring bör även omfatta lagring av uppgifter som genereras eller behandlas vid misslyckad uppringning. Sådana uppgifter bör få lagras vid utökad riktad lagring.

Eftersom geografiskt riktad lagring och utökad riktad lagring inte kommer att omfatta hela landet behöver tillhandahållarna kunna avgöra när lagring ska ske. I praktiken behöver tillhandahållarna kontrollera om kommunikationsutrustningen finns inom en viss kommun som omfattas av geografiskt riktad lagring respektive inom ett område som omfattas av utökad riktad lagring. Frågan är hur tillhandahållarna ska agera när den som kommunicerar förflyttar sig, dvs. anländer till eller lämnar ett område som omfattas av lagringsskyldighet under pågående kommunikation. Det framstår som oproportionerligt att ålägga tillhandahållarna att kontrollera sådan kommunikation som inte omfattas av lagringsskyldighet när kommunikationen påbörjas. Det är vidare förenat med svårigheter att låta lagringsskyldigheten omfatta sådan kommunikation som avslutas i ett område som inte

omfattas av lagringsskyldighet. Tillhandahållarna har i dessa fall inte uppgifter om exempelvis när kommunikationen avslutas, vilket enligt nu gällande regler utgör utgångspunkten för lagringstiden. Vi har tidigare konstaterat att lagringsskyldigheten endast ska gälla för uppgifter som genereras eller behandlas i den egna verksamheten. Om tillhandahållaren saknar vissa uppgifter i anledning av en person förflyttar sig under kommunikationen, ska de uppgifter som är tillgängliga lagras. Om tillhandahållaren saknar uppgift om när kommunikationen inleddes eller avslutades, ska lagringstiden i stället utgå från när uppgifterna genererades. Sammanfattningsvis ska lagringsskyldigheten omfatta alla uppgifter som genererats inom det område som omfattas av geografiskt riktad lagring eller utökad riktad lagring.

Avslutningsvis kan frågan ställas om den lagringsskyldighet som vi föreslår i syfte att bekämpa grov brottslighet är proportionerlig och förenlig med EU-rätten. Med våra förslag kommer fler uppgiftskategorier att lagras än i dag men våra förslag innebär också att färre personer omfattas av lagringen. I proportionalitetsbedömningen bör ingå att den tekniska utvecklingen, ökade möjligheter till elektronisk kommunikation och förändrade kommunikationsmönster har påverkat förutsättningarna för de brottsbekämpande myndigheterna att få tillgång till trafik- och lokaliseringsuppgifter i syfte att bekämpa grov brottslighet. För viss typ av brottslighet, exempelvis sådan brottslighet som äger rum i digitala kanaler, är trafik- och lokaliseringsuppgifter en avgörande förutsättning för en effektiv brottsbekämpning. Lagringsskyldighet enligt dagens modell medger exempelvis inte att lokaliseringsuppgifter lagras när kommunikationen sker med hjälp av sådana kommunikationstjänster som vi beskriver i avsnitt 9. Våra förslag syftar därför också till att utjämna skillnaden mellan olika kommunikationstjänster. I avsnitt 13 återkommer vi till hur våra förslag påverkar den personliga integriteten. Sammantaget gör vi bedömningen att denna mer avgränsade lever upp till EU-rättens krav på proportionalitet.

Lagringstiden

Vi hänvisar till avsnitt 7.3.6 i fråga om en beskrivning av de nu och tidigare gällande lagringstiderna.

Som gäller för all datalagring måste lagringstiden fastställas på objektiva grunder och begränsas till vad som är strängt nödvändigt. De brottsbekämpande myndigheterna har påtalat vikten av att uppgifter lagras under en längre tid än i dag, bl.a. med hänsyn till att de brott för vilka de lagrade uppgifterna kan inhämtas inte sällan är sådana som kräver lång utredningstid. I likhet med vad vi beskrivit i föregående avsnitt om lagringsskyldighetens omfattning finns det ett större utrymme att nu föreslå en längre lagringstid än i dag, eftersom lagringen inte längre omfattar samtliga abonnenter och registrerade användare av kommunikationstjänster. Vi ser inga bärande argument för att låta olika typer av uppgifter ha olika lagringstider. För syftet att bekämpa grova brott behövs en helhetsbild. Vi gör sammantaget bedömningen att samma lagringstid ska gälla för alla typer av uppgifter och att den ska vara längre än i dag. Vi bedömer också att lagringstiden, liksom vid nationell säkerhetslagring, bör regleras direkt i författning. Det går nämligen inte att i förväg veta hur länge uppgifterna kan behövas. Utan en fast lagringstid måste tillhandahållarna också anpassa sina system inför varje enskilt lagringsbeslut så att uppgifter gallras i rätt tid. Vi har i avsnitt 7.3.6 redovisat att det finns fördelar med att i författning föreskriva en viss lagringstid även om det kan innebära att uppgifter kan komma att lagras längre tid än den som beslut gäller. Vi har ingen annan uppfattning när det gäller utökad riktad lagring.

Frågan är dock hur lång lagringstid som kan anses vara proportionerlig vid riktad lagring. Enligt nu gällande ordning lagras uppgifter mellan två och tio månader beroende på vilken typ av uppgift det är fråga om. Regeringen anförde bl.a. följande i fråga om lagringstiden.[22]

> De uppgifter om elektronisk kommunikation som inhämtas av polisen i underrättelseverksamheten är i de flesta fall yngre än en månad, men det finns även ärenden där historik upp till sex månader varit av stor vikt vid analysarbetet. I polisens utredningsverksamhet är den största andelen historiska uppgifter yngre än tre månader. Omkring 20–25 procent är äldre än tre månader och ungefär en tiondel av den totala mängden är äldre än fem månader. De utredningar i vilka det finns ett behov av äldre

[22] Se prop. 2018/19:86 s. 50.

uppgifter avser främst grova våldsbrott av spaningskaraktär samt grova seriebrott såsom våldtäkter och mordförsök (SOU 2015:31 s. 129). Detta bör beaktas vid bestämmandet av lagringstiden. En annan faktor att beakta är att de brottsbekämpande myndigheterna har behov av längre lagringstid för ip-adresser vid ärenden som har internationell koppling, t.ex. barnpornografibrott. Exempelvis har Polismyndigheten uppgett att den med en lagringstid på sex månader måste lägga ner ungefär hälften av alla barnpornografiärenden som upparbetas utomlands. Skälet till att dessa ärenden tar lång tid att utreda är att det krävs många olika typer av åtgärder (såsom beslag, analys av beslagtagen materiel och identifiering av gärningsman och brottsoffer) där det krävs samarbeten med en eller flera polismyndigheter utomlands. Myndigheterna har sammanfattningsvis uppgett att de har behov av längst lagringstider för uppgifter hänförliga till mobil telefoni och ip-telefoni samt för abonnemangsuppgifter hänförliga till internetåtkomst.

De brottsbekämpande myndigheterna har för oss påtalat behovet av en längre lagringstid för att nödvändiga åtgärder ska kunna vidtas innan uppgifterna gallras. Detta har blivit mer påtagligt för myndigheterna då den grova brottsligheten har tilltagit och att kommunikation flyttats från traditionella kanaler till internet. Sådan brottslighet kan vara svårupptäckt, utredningarna kan vara komplexa och involvera många aktörer. Inte sällan har sådan brottslighet även internationella inslag varför det behövs ytterligare utredningstid. Även det faktum att avancerad utrustning används vid grov brottslighet påverkar utredningstiden. Det kan i vissa fall ta lång tid för de brottsbekämpande myndigheterna att få tillgång till innehållet i en modern mobiltelefon eller dator.

För kort lagringstid i fråga om kommunikation som sker över internet kan leda till att utredningar måste läggas ned, eftersom trafik- och lokaliseringsuppgifter i regel är avgörande för att kunna identifiera de misstänkta.

Vi gör bedömningen att det behov de brottsbekämpande myndigheterna har gett uttryck för talar en längre lagringstid. Vi har härutöver i avsnitt 6.6.1 föreslagit att uppgifter om abonnemang ska lagras i ett år efter att abonnemanget upphört. Vi har som nämnts tidigare gjort bedömningen att det är viktigt att de brottsbekämpande myndigheterna får ett helhetsperspektiv. När tillgång väl ges till de lagrade uppgifterna behövs en samlad bild för att de brottsbekämpande myndigheterna ska kunna använda materialet på ett tillräckligt effektivt sätt. Vi föreslår därför att lagringstiden för geografiskt riktad lagring och utökad riktad lagring ska vara ett år från den dag kom-

munikationen avslutades. Om uppgift om när kommunikationen avslutades saknas ska lagringstiden räknas från den dag då uppgifterna genererades, se föreslagen lydelse av 9 kap. 22 § nya LEK.

Vid nationell säkerhetslagring har vi föreslagit att lagringstiden ska vara två år. Även om grov brottslighet kan planeras och pågå under flera år, gör vi bedömningen att det inte kan anses vara försvarligt att låta tillhandahållarna lagra trafik- och lokaliseringsuppgifter i så lång tid som två år. En längre lagringstid än ett år för riktad lagring framstår inte som proportionerlig. Det får accepteras att vissa äldre uppgifter som kan vara avgörande för bekämpningen av grov brottslighet kan falla utanför den riktade lagringsskyldigheten.

Avslutningsvis vill vi förtydliga att tiden för ett beslut om utökad riktad lagring ska hållas isär från lagringstiden för trafik- och lokaliseringsuppgifter. Ett beslut om utökad riktad lagring avseende exempelvis ett område gäller normalt ett år medan tiden för själva lagringen av uppgifterna normalt är ett år efter det att uppgifterna genererades. Det innebär att uppgifter kan vara lagrade även efter det att skyldigheten att lagra uppgifter har upphört.

Sammanfattning av våra förslag avseende lagring av uppgifter i syfte att bekämpa grov brottslighet

Vi föreslår två modeller av riktad lagring i syfte att bekämpa grov brottslighet: geografiskt riktad lagring och utökad riktad lagring. Geografiskt riktad lagring ska äga rum i de kommuner som PTS föreskrivit. Utökad riktad lagring ska äga rum avseende de områden, de platser, de personer eller den utrustning och de abonnemang som omfattas av Polismyndighetens, Säkerhetspolisens och Tullverkets beslut. Myndigheternas tillämpning av reglerna om utökad riktad lagring ska vara föremål för SIN:s tillsyn.

Vid geografiskt riktad lagring ska samtliga tillhandahållare som är lagringsskyldiga enligt 9 kap. 19 § nya LEK lagra de uppgifter om abonnemang samt trafik- och lokaliseringsuppgifter som är nödvändiga för att spåra och identifiera

- kommunikationskällan och slutmålet för kommunikationen,
- datum, tidpunkt och varaktighet för kommunikationen,
- typ av kommunikation,

- kommunikationsutrustning, samt
- lokalisering av kommunikationsutrustning.

Vid utökad riktad lagring beslutar Polismyndigheten, Säkerhetspolisen och Tullverket vilka uppgifter, av de ovan beskrivna, och vilka tillhandahållare som ska omfattas av lagringsskyldigheten. Lagringstiden vid riktad lagring ska vara ett år efter att kommunikationen avslutades eller om uppgiften saknas då uppgifterna genererades.

Våra förslag syftar till att anpassa dagens regler om datalagring till EU-rätten. Utgångspunkten har varit att skapa så goda förutsättningar som möjligt för de brottsbekämpande myndigheterna med iakttagande av vad EU-rätten tillåter samtidigt som skyddet för enskildas personliga integritet respekteras. Vår utgångspunkt har varit att lagringen ska vara proportionerlig och strängt nödvändig. Vi har eftersträvat en lagring som inte ska vara generell och omfatta hela eller nästan hela befolkningen. I stället är lagringen inriktad på områden, platser, personer, utrustning och abonnemang som är av särskilt intresse för det brottsbekämpande arbetet. De personer vars uppgifter lagras ges ett effektivt skydd mot att deras personuppgifter missbrukas dels genom tillsyn, dels genom föreslagna begränsningar av lagringen.

Regleringen bör sammantaget enligt vår mening ge de brottsbekämpande myndigheterna goda möjligheter att bekämpa allvarliga brott samtidigt som respekten för den enskildes personliga integritet upprätthålls.

8.3.4 En ny lag om riktad lagring av uppgifter om elektronisk kommunikation

Utredningens förslag: Förutsättningarna för riktad lagring ska regleras i en ny lag benämnd lagen om lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet.

En reglering av riktad lagring aktualiserar dels bestämmelser som vänder sig till tillhandahållarna, dels bestämmelser som berör myndigheter. Vi ser många fördelar med att bibehålla systematiken i nya LEK, som redan i dag berör och tillämpas av många olika intressen-

ter. Av det skälet föreslår vi att frågor som berör tillhandahållarna, dvs. frågor om lagringsskyldighet, vilka uppgifter som ska lagras, lagringstid m.m. ska regleras i nya LEK. Frågor som berör myndigheter, såsom vilket förfarande som ska gälla vid beslut om riktad lagring, passar däremot mindre väl i nya LEK. De generella förutsättningarna för riktad lagring bör regleras i en särskild lag på samma sätt som vi föreslagit för nationell säkerhetslagring. Vi föreslår därför en ny lag som lämpligen kan benämnas lagen om lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet.

8.3.5 Tillgången till lagrade uppgifter vid riktad lagring och rättssäkerhetsgarantier

Utredningens bedömning: Tillgång till lagrade trafik- och lokaliseringsuppgifter får endast ges för bekämpning av grov brottslighet. Reglerna i rättegångsbalken, preventivlagen, inhämtningslagen, lagen om särskild kontroll av vissa utlänningar och lagen om hemlig dataavläsning uppfyller EU-rättens krav i detta avseende. Reglerna i nämnda lagar uppfyller även övriga EU-rättsliga krav när det gäller tillgång till uppgifter i syfte att bekämpa allvarlig brottslighet i den mån de omfattas av våra överväganden. Våra förslag medför inte något behov av författningsändringar avseende tillgången till lagrade uppgifter.

Enligt EU-rätten måste medlemsstaterna föreskriva klara och precisa bestämmelser som anger under vilka omständigheter och på vilka villkor tillhandahållare av elektroniska kommunikationstjänster ska ge behöriga nationella myndigheter tillgång till lagrade trafik- och lokaliseringsuppgifter. Tillgång till lagrade uppgifter kan i princip bara beviljas för uppgifter om personer som misstänks planera, begå eller ha begått ett grovt brott eller på något annat sätt vara inblandade i ett sådant brott. Det har sin grund i att uppgifterna lagrats för ändamålet att bekämpa grov brottslighet.

Regeringen bedömde, i förarbetena till den nu gällande datalagringsregleringen, att tillgång till lagrade trafik- och lokaliseringsuppgifter får ges endast för bekämpning av grov brottslighet och att reglerna i rättegångsbalken, preventivlagen, inhämtningslagen och lagen om särskild utlänningskontroll uppfyller EU-rättens krav i detta av-

seende.[23] Efter regeringens bedömning i denna fråga har hemlig dataavläsning införts som ett nytt hemligt tvångsmedel som kan ge åtkomst till bl.a. kommunikationsavlyssningsuppgifter, kommunikationsövervakningsuppgifter och platsuppgifter (om hemlig dataavläsning, se avsnitt 5.3.4). Dessutom har lagen om särskild utlänningskontroll ersatts av lagen (2022:700) om särskild kontroll av vissa utlänningar (om denna lag, se avsnitt 5.3.3). Det kan konstateras att tillgång till trafik- och lokaliseringsuppgifter genom hemlig dataavläsning eller med stöd av lagen om särskild kontroll av vissa utlänningar endast kan beviljas för bekämpning av grov brottslighet. Vår bedömning är därför att det inte krävs några författningsändringar när det gäller för vilken brottslighet tillgång till de lagrade uppgifterna kan beviljas.

Det kan i detta sammanhang noteras att det i delbetänkandena *Utökade möjligheter att använda hemliga tvångsmedel* (SOU 2022:19) och *Utökande möjligheter att använda preventiva tvångsmedel* (SOU 2022:52) föreslås större möjligheter att använda hemliga tvångsmedel såväl inom som utom förundersökningar, se avsnitt 5.3.

I förarbetena till den nu gällande datalagringsregleringen bedömde regeringen att reglerna som ger tillgång till lagrade trafik- och lokaliseringsuppgifter uppfyller EU-rättens krav på att tillgången som huvudregel endast ska gälla personer som på något sätt kan vara inblandade i allvarlig brottslighet och att regleringen även i övrigt uppfyllde de EU-rättsliga kraven. Vi gör ingen annan bedömning i dessa avseenden.

När det gäller det EU-rättsliga kravet på att de brottsbekämpande myndigheternas tillgång till datalagrade uppgifter, utom i motiverade brådskande fall, ska föregås av en kontroll av domstol eller en oberoende myndighet gjorde regeringen en annan bedömning. Där föreslog regeringen, för att anpassa reglerna till EU-rätten, att åklagare vid Åklagarmyndigheten skulle besluta om tillstånd för inhämtning av uppgifter enligt inhämtningslagen, i stället för att Polismyndigheten, Säkerhetspolisen respektive Tullverket skulle fatta sådana beslut.[24] Det är denna reglering som gäller i dag. Det finns inte skäl för oss att nu igen överväga denna fråga, eftersom Utredningen om preventiva tvångsmedel (Ju 2021:15) enligt tilläggsdirektiv den 28 april 2022 (dir. 2022:32) har fått i uppdrag att ta ställning till om, och i så fall på vilket sätt, tillämpningsområdet för inhämtningslagen bör ut-

[23] Se prop. 2018/19:86 s. 64 f.
[24] Se a. prop. s. 72 f.

vidgas och till hur beslutsordningen bör se ut vid en eventuell utvidgning av inhämtningslagens tillämpningsområde. Vi lämnar därför inga förslag när det gäller beslutsordningen enligt inhämtningslagen.

Till skillnad från våra förslag gällande nationell säkerhetslagring, där tillgången till de lagrade uppgifterna behöver begränsas till bekämpning av brottslighet som innebär ett hot mot den nationella säkerheten, medför våra förslag om riktad lagring inte några motsvarande behov av begränsningar. Det bör för tydlighetens skull påpekas att uppgifter från riktad lagring även kan inhämtas för bekämpning av brottslighet som innefattar hot mot den nationella säkerheten eller för annan grov brottslighet än den som uppgifterna var avsedda att lagras för.

Vår bedömning är sammanfattningsvis att det inte krävs några författningsändringar när det gäller reglerna om tillgång till lagrade trafik- och lokaliseringsuppgifter i syfte att bekämpa allvarlig brottslighet. I denna bedömning ingår dock inte frågan om beslutsfattare enligt inhämtningslagen.

8.3.6 Personuppgiftsbehandling vid riktad lagring i syfte att bekämpa grov brottslighet

I detta avsnitt diskuterar vi eventuella behov av att reglera den personuppgiftsbehandling som måste utföras när det gäller lagring i syfte att bekämpa grov brottslighet. För en närmare beskrivning av nu gällande regler för personuppgiftsbehandling hänvisar vi till avsnitt 7.3.8.

Tillhandahållarnas behandling av lagrade uppgifter

Utredningens förslag: Det ska finnas författningsstöd för tillhandahållarnas behandling av personuppgifter när det gäller lagring och utlämnande av uppgifter i syfte att bekämpa grov brottslighet.

Tillhandahållarnas behandling av fysiska personers trafik- och lokaliseringsuppgifter är reglerade i nya LEK och nya FEK med bl.a. begränsningar kring hur uppgifterna får hanteras.

Vi har i avsnitt 7.3.8. föreslagit ändringar i nya LEK i anledning av våra förslag om nationell säkerhetslagring. Motsvarande ändring krävs även för geografiskt riktad lagring och utökad riktad lagring.

Eftersom vi föreslår att de olika formerna av lagringsskyldighet vid riktad lagring ska regleras i två nya paragrafer i nya LEK (9 kap. 19 c–d §§) bör motsvarande ändringar göras genom tillägg i 9 kap. 1, 10 och 21 §§ nya LEK.

Genom ändringarna finns författningsstöd för tillhandahållarnas behandling av trafik- och lokaliseringsuppgifter när det gäller lagring och utlämnande av uppgifter i syfte att bekämpa grov brottslighet.

Vi föreslår i övrigt inga förändringar i sak när det gäller rätten för tillhandahållare att behandla personuppgifter i syfte att bekämpa grov brottslighet.

De brottsbekämpande myndigheternas behandling av lagrade uppgifter

Utredningens bedömning: Vårt förslag om en modell för riktad lagring av trafik- och lokaliseringsuppgifter i syfte att bekämpa grov brottslighet föranleder inga ändringar i de brottsbekämpande myndigheternas registerförfattningar.

Behöriga myndigheters behandling av personuppgifter i syfte att bekämpa brott regleras i brottsdatalagen (2018:1177) i förening med de särskilda registerförfattningar som gäller för respektive verksamhet, exempelvis polisens brottsdatalag (2018:1693). Säkerhetspolisens behandling av personuppgifter regleras härutöver även i lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter.

Vårt förslag om att den nu gällande skyldigheten att lagra trafik- och lokaliseringsuppgifter ska inskränkas genom en modell med riktad lagring innebär inga förändringar när det gäller de rättsliga grunderna eller ändamålen för Polismyndighetens och Säkerhetspolisens och Tullverkets behandling av personuppgifter i syfte att bekämpa grova brott. Myndigheterna kan redan i dag behandla personuppgifter beträffande frågor som rör grov brottslighet. Det behövs därför inga författningsändringar avseende de brottsbekämpande myndigheternas behandling av personuppgifter.

PTS:s behandling av personuppgifter vid beslut om geografiskt riktad lagring

Utredningens bedömning: PTS behandlar inte personuppgifter i syfte att förebygga förhindra, utreda, avslöja och lagföra brott vid fastställandet av geografiskt riktad lagring. Våra förslag medför inte något behov av förändringar i nuvarande reglering.

PTS behandlar personuppgifter i sin verksamhet med stöd av EU:s dataskyddsförordning. Enligt nu gällande reglering har myndigheten inte något uppdrag eller någon lagreglerad skyldighet som aktualiserar personuppgiftsbehandling inom brottsdatalagens område. När PTS enligt våra förslag ska föreskriva i vilka kommuner geografiskt riktad lagring ska äga rum aktualiseras frågan om det krävs författningsändringar avseende myndighetens personuppgiftsbehandling. Vi har föreslagit att den officiella statistiken ska ligga till grund för PTS:s föreskrifter i detta avseende. Statistiken kan inte härledas till någon enskild person utan presenteras endast på aggregerad nivå och innehåller således inte personuppgifter. PTS behandlar alltså inte personuppgifter i syfte att förebygga förhindra, utreda, avslöja och lagföra brott i arbetet med att fastställa var geografiskt riktad lagring ska ske. En annan sak är att det vid detta arbete kan förekomma personuppgifter. En sådan uppgiftsbehandling skiljer sig dock inte från annan personuppgiftsbehandling i samband med utövandet av myndighetens tillsynsuppdrag. Exempelvis kan den jämställas med den personuppgiftsbehandling som sker när PTS utövar tillsyn över teleoperatörerna i deras lagring av trafik- och lokaliseringsuppgifter i syfte att bekämpa grov brottslighet. För sådan personuppgiftsbehandling finns stöd i befintlig reglering. Vi kan således inte identifiera något behov av författningsändringar för den personuppgiftsbehandling som sker inom PTS:s verksamhet i anledning av våra förslag.

8.3.7 Sekretess och tystnadsplikt

I detta avsnitt diskuterar vi frågan om behovet av att reglera sekretess vid beslut om riktad lagring.

Sekretess och meddelarfrihet vid utökad riktad lagring

Utredningens förslag: Sekretess ska gälla för uppgifter om en enskilds personliga och ekonomiska förhållanden i angelägenheter om utökad riktad lagring, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men. I en angelägenhet om utökad riktad lagring ska tystnadsplikten inskränka rätten att meddela och offentliggöra uppgifter enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen.

Utredningens bedömning: Nuvarande sekretessregler till skydd för intresset av att förebygga eller beivra brott ger ett tillräckligt sekretesskydd för uppgifter i angelägenheter om utökad riktad lagring. I befintliga regler om sekretess till skydd för enskilda i verksamhet som syftar till att förebygga eller beivra brott, m.m. finns däremot inte något motsvarande skydd för enskildas personliga och ekonomiska förhållanden. En kompletterande bestämmelse bör därför införas.

Vi har i avsnitt 7.3.9 bedömt att reglerna i 18 kap. OSL om sekretess till skydd främst för intresset av att förebygga eller beivra brott, ger ett tillräckligt skydd i angelägenheter om nationell säkerhetslagring. Vi har i samma avsnitt föreslagit en bestämmelse om att sekretess ska gälla för uppgifter om enskildas personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom lider skada eller men och uppgiften förekommer i angelägenhet om nationell säkerhetslagring, 35 kap. 1 § första stycket 10 OSL.

Vi bedömer att uppgifter som förekommer under handläggningen vid de beslutande myndigheterna i ärenden om utökad riktad lagring omfattas av sekretess enligt 18 kap. 1 och 2 §§ och 35 kap. 1 § OSL. Vi bedömer vidare att sekretess enligt 18 kap. 1 och 2 §§ OSL gäller

även vid SIN och vid andra myndigheter som kan involveras i angelägenheter om utökad riktad lagring. När det däremot gäller sekretess för uppgifter om enskildas personliga och ekonomiska förhållanden finns, på samma sätt som vid nationell säkerhetslagring, ett behov av sekretesskydd i angelägenheter om utökad riktad lagring.

Den nuvarande modellen för lagring ger enskilda ett skydd genom den sekretess som gäller i de brottsbekämpande myndigheternas verksamhet, 35 kap. 1 § första stycket 4 OSL och den tystnadsplikt som gäller i tillhandahållarnas verksamhet, 9 kap. 31 § nya LEK. När lagringsskyldigheten i stället följer av beslut om utökad riktad lagring kommer sekretess till skydd för enskildas personliga och ekonomiska förhållanden enligt 35 kap. 1 § OSL inte att gälla hos vissa andra myndigheter som kan involveras i angelägenheter om utökad riktad lagring. Sekretessen skulle exempelvis inte gälla hos SIN i samband med dess tillsyn. Sekretessen skulle inte heller gälla i PTS tillsynsverksamhet eller hos andra myndigheter än brottsbekämpande myndigheter som Polismyndigheten, Säkerhetspolisen eller Tullverket samråder med inför ett beslut om utökad riktad lagring. Det krävs således ett skydd för uppgifter om enskildas personliga och ekonomiska förhållanden utanför de brottsbekämpande myndigheternas verksamhet.

Vi har vidare föreslagit att rätten att meddela och offentliggöra uppgifter enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen bör inskränkas i ett ärende om nationell säkerhetslagring. Utifrån samma resonemang som vi har fört i avsnitt 7.3.9 bör tystnadsplikten få inskränka rätten att meddela och offentliggöra uppgifter enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen även när det gäller angelägenheter om utökad riktad lagring. Uppgifter i sådana angelägenheter kan innehålla såväl underrättelseuppgifter, uppgifter som omfattas av försvarssekretess och uppgifter om personer som eventuellt kan bli föremål för hemliga tvångsmedel. Som vi tidigare har redovisat i nämnda avsnitt är det typiskt sett sådana uppgifter där tystnadsplikten ska få inskränka rätten att meddela och offentliggöra uppgifter.

Vi föreslår mot denna bakgrund att sekretess ska gälla för uppgifter om en enskilds personliga och ekonomiska förhållanden i angelägenheter om utökad riktad lagring, 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 att tystnadsplikten ska inskränka rätten att meddela och offentliggöra uppgifter enligt tryckfrihetsför-

ordningen och yttrandefrihetsgrundlagen. Bestämmelserna bör, på samma sätt som beträffande nationell säkerhetslagring, föras in som en ny punkt i 35 kap. 1 § OSL (p. 11) respektive i 18 kap. 19 § och 35 kap. 24 § OSL.

Sekretess beträffande ett beslut om utökad riktad lagring

Utredningens bedömning: Sekretessen ska omfatta ett beslut om utökad riktad lagring.

I motsats till PTS:s föreskrifter om geografiskt riktad lagring fattas ett beslut om utökad riktad lagring av Polismyndigheten, Säkerhetspolisen eller Tullverket. Vi har i föregående avsnitt konstaterat att uppgifter som förekommer under handläggningen vid dessa myndigheter i en angelägenhet om utökad riktad lagring omfattas av sekretess enligt 18 kap. 1 och 2 §§ samt 35 kap. 1 § OSL. Frågan är om det bör göras något undantag från sekretessen avseende själva beslutet om utökad riktad lagring. Vi konstaterar att det finns flera skäl som talar emot detta, även om det i vissa fall kan finnas ett insynsintresse avseende omfattningen av ett beslut om utökad riktad lagring.

Den information som ligger till grund för bedömningen om utökad riktad lagring kan vara skyddsvärd och även innehålla integritetskänsliga personuppgifter. Om detta helt eller delvis återges i beslutet, försvårar det möjligheten att hemlighålla uppgifterna. Det går i och för sig att föreskriva att endast uppgifter om lagringsskyldigheten och dess omfattning ska vara offentliga, dvs. motsvarande domslutet i en dom. Vi gör dock bedömningen att detta inte skulle vara tillräckligt för att motverka de negativa effekter det skulle få för de brottsbekämpande myndigheternas verksamheter om det blev känt var den utökade riktade lagringen gäller. I många situationer skulle beslutet i sig indirekt kunna avslöja uppgifter om underrättelse- eller utredningsverksamheten. Till exempel kan ett beslut om riktad lagring som syftar till att bekämpa organiserad brottslighet på en viss plats avslöja för de personer som begår brott eller ägnar sig åt brottslig verksamhet att de är föremål för åtgärder. Det är inte heller önskvärt att uppgifter om skyddsvärda platser sprids till en alltför bred krets eftersom uppgifterna samlat skulle kunna användas för att åskådliggöra sårbarheter i fråga om Sveriges försvarsförmåga. Avslutnings-

vis kan den omständigheten att det inte är känt var utökad riktad lagring äger rum ha en avhållande effekt på den eller de individer som förbereder brott eller i övrigt ägnar sig åt brottslig verksamhet. Om det fanns en möjlighet att få ta del av beslut om utökad riktad lagring, skulle det de facto finnas utrymme för kriminella att kunna kartlägga var i landet det saknas datalagring. En följd skulle då kunna bli att viss kriminell verksamhet förläggs till sådana platser där datalagring inte äger rum. Vår bedömning är att det är lämpligare att beslut om utökad riktad lagring, i likhet med beslut nationell säkerhetslagring och vissa straffprocessuella tvångsmedel, i sin helhet omfattas av sekretess.

Tystnadsplikt och inskränkningar i meddelarfriheten för tillhandahållare i ett ärende om utökad riktad lagring

Utredningens förslag: Tillhandahållarnas tystnadsplikt ska gälla i angelägenheter om utökad riktad lagring. Tystnadsplikten ska ha företräde framför meddelarfriheten.

Enligt 9 kap. 31 § nya LEK får den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst som inte är en nummeroberoende interpersonell kommunikationstjänst (Noik), 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 (dvs. en trafikuppgift).

Vi återkommer i avsnitt 9.6.2. till frågan om även tillhandahållare av Noik bör omfattas av denna tystnadsplikt. I 9 kap. 32 § nya LEK finns en straffsanktionerad tystnadsplikt för de tillhandahållare som regleras i 9 kap. 31 § nya LEK när det gäller uppgifter som hänför sig till vissa angelägenheter, bl.a. användning av hemliga tvångsmedel. Enligt 44 kap. 4 § tredje stycket OSL inskränks meddelarfriheten för tillhandahållarna i fråga om straffprocessuella tvångsmedel.

Vi bedömer, på samma sätt som vi har föreslagit när det gäller nationell säkerhetslagring (se avsnitt 7.3.9), att det bör införas en tystnadsplikt för tillhandahållarna avseende angelägenheter om utökad riktad lagring och att detta bör regleras genom ett tillägg i 9 kap. 32 § nya LEK. Tystnadsplikten bör omfatta exempelvis information om att myndigheterna har varit i kontakt med tjänsteleverantören, vad som har kommunicerats, beslut om utökad riktad lagring och på vilka områden eller platser eller avseende vilka personer, utrustningar eller abonnemang lagringen gäller och att lagringen har påbörjats eller avslutats.

Vi föreslår också att meddelarfriheten för tillhandahållare inskränks när det gäller angelägenheter om utökad riktad lagring. Ett tillägg om detta bör därför föras in i 44 kap. 4 § OSL.

Finns det behov av en sekretessbrytande bestämmelse?

Utredningens bedömning: Det behövs inte en särskild sekretessbrytande bestämmelse för att myndigheter ska kunna lämna upplysningar till Polismyndigheten, Säkerhetspolisen och Tullverket i angelägenheter om utökad riktad lagring. Vid behov kan myndigheterna lämna sådana upplysningar till Polismyndigheten, Säkerhetspolisen och Tullverket med stöd av den s.k. generalklausulen.

Även om Polismyndigheten, Säkerhetspolisen och Tullverket bör ha en god kännedom i frågor relaterade till grov brottslighet kan dessa myndigheter ha behov av att samråda med andra myndigheter i frågor som gäller utökad riktad lagring, särskilt när det gäller skyddsvärda platser. Det förefaller naturligt att Polismyndigheten, Säkerhetspolisen och Tullverket inom ramen för pågående samverkan med andra brottsbekämpande myndigheter kan komma att inhämta synpunkter från bl.a. Åklagarmyndigheten, Ekobrottsmyndigheten, Skatteverket och Kustbevakningen.

Polismyndigheten, Säkerhetspolisen och Tullverket har dock inte en kontinuerlig samverkan med alla de myndigheter som kan komma att involveras inför ett beslut om utökad riktad lagring avseende skyddsvärda platser. I många fall bör det i och för sig vara tillräckligt för Polismyndighetens, Säkerhetspolisens och Tullverkets bedömning att de aktuella myndigheterna lämnar allmänna upplysningar

om platsen eller verksamheten. Som huvudregel bör det därför inte vara aktuellt att lämna ut känsligare detaljuppgifter. Bedömningen ska trots allt ske på en övergripande nivå. Det går dock inte att utesluta att det i undantagsfall kan uppkomma situationer där det finns behov att lämna ut uppgifter som omfattas av sekretess. För sådana situationer finns behov av en sekretessbrytande bestämmelse.

En möjlig lösning vore att föreskriva om en särskild uppgiftsskyldighet för att tillgodose detta behov. Nackdelen med en sådan lösning är att uppgiftsskyldigheten inte kan vara obegränsad, utan behöver villkoras, så att det intresse som sekretessen ska skydda inte går förlorat genom att uppgiften lämnas till Polismyndigheten, Säkerhetspolisen eller Tullverket. I allt väsentligt motsvarar en sådan bestämmelse den s.k. generalklausulen i 10 kap. 27 § OSL. Enligt generalklausulen får, med vissa undantag, en sekretessbelagd uppgift lämnas till en myndighet, om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda. Vi gör bedömningen att generalklausulen bör ge ett tillräckligt stöd för att Polismyndigheten, Säkerhetspolisen eller Tullverket ska kunna inhämta sekretessbelagda uppgifter från andra myndigheter i de fall detta behövs. Mot denna bakgrund ser vi inga fördelar med en särskild föreskrift om uppgiftsskyldighet i angelägenheter om utökad riktad lagring avseende skyddsvärda platser.

9 Särskilt om lagring och tillgång till uppgifter från s.k. OTT-tjänster

I detta avsnitt överväger vi om leverantörer av s.k. OTT-tjänster ska omfattas av skyldigheter att lagra och ge åtkomst till uppgifter om elektronisk kommunikation och lämnar förslag om detta.

9.1 Inledning

De brottsbekämpande myndigheterna behöver ha tillgång till ändamålsenliga och verkningsfulla verktyg för att kunna förebygga, förhindra, upptäcka, utreda och lagföra brott. Som framgår av tidigare avsnitt är tillgången till information från elektroniska kommunikationer ofta av stor betydelse för att myndigheterna ska kunna utföra sin brottsbekämpande verksamhet. Det blir samtidigt allt vanligare att kommunikation sker genom tjänster vars tillhandahållare inte omfattas av någon rättslig skyldighet att lagra eller tillhandahålla uppgifter, nämligen tjänster som tillhandahålls av andra än de traditionella teleoperatörerna. Exempel på sådana tjänster är OTT-tjänster i form av nummeroberoende interpersonella kommunikationstjänster. Det kan vara tjänster som Apple Imessage och Facetime, Discord, Google Messages, Kik Messenger, Line, Messenger from Meta, Skype, Slack, Telegram, Viber och Whatsapp för att nämna några bland många.[1]

Enligt våra direktiv ska vi analysera förutsättningarna, även ur ett tekniskt perspektiv, för att tillhandahållare av sådana OTT-tjänster som används för interpersonell kommunikation ska kunna omfattas av skyldigheterna att lagra och lämna ut uppgifter om elektroniska

[1] Vissa tjänster, såsom Apple Imessage och Google Messages, har också funktionalitet för att skicka ett meddelande genom teleoperatörerna om den egna tjänsten inte är tillgänglig.

kommunikationer. Vi ska lämna förslag på de författningsändringar och andra åtgärder som bedöms nödvändiga.

9.2 OTT-tjänster och nummeroberoende interpersonella kommunikationstjänster (Noik)

OTT är en förkortning för engelskans *over the top*. OTT-tjänster är operatörsoberoende tjänster i form av video, ljud eller meddelanden som sänds ut till användare via data- eller tele- eller kabelnätet av en fristående tjänst.[2] Benämningen *over the top* används på grund av att signalerna förekommer utöver – ovanpå – de vanliga sändningarna. Den fristående tjänsten tar normalt inte betalt för datakommunikationen; denna betalar användarna för genom sitt internetabonnemang. Internetleverantören ansvarar i sin tur inte för innehållet utan ser enbart till att materialet kommer fram.[3] Begreppet OTT-tjänster avsåg inledningsvis tjänster som erbjöd möjlighet att ta del av tv-sändningar och film direkt över internet, i stället för via exempelvis kabeltv-nätverk eller satellit. Med tiden har begreppet utvidgats till att även innefatta tjänster som avser interpersonell kommunikation. I våra direktiv används begreppet nummeroberoende interpersonella kommunikationstjänster (i fortsättningen kallade Noik).

9.3 Närmare om Noik

9.3.1 Definitioner

I nya LEK har vissa definitioner ändrats i förhållande till gamla LEK och vissa nya definitioner har tillkommit. Definitionerna finns i 1 kap. 7 § nya LEK och följer i många fall direkt av definitionerna i EU:s direktiv om inrättande av en europeisk kodex för elektronisk kommunikation (e-kodexen). Definitionen av *elektronisk kommunikationstjänst* i nya LEK motsvarar artikel 2.4 i e-kodexen. Definitionen innefattar inte något krav på att tjänsten helt eller huvudsakligen ska utgöras av överföring av signaler, vilket innebär en utvidgning i

[2] Se https://it-ord.idg.se/. Hämtat den 20 april 2023.
[3] Nationalencyklopedin, OTT. http://www.ne.se/uppslagsverk/encyklopedi/lång/ott. Hämtat den 20 april 2023.

förhållande till vad som tidigare ansågs vara en elektronisk kommunikationstjänst.[4]

För att tjänsten ska anses som en elektronisk kommunikationstjänst ska den vanligen tillhandahållas mot ersättning, alltså kommersiellt, via elektroniska kommunikationsnät. Sker tillhandahållandet på rent ideell basis, omfattas tjänsten inte av definitionen. I många fall tillhandahålls kommersiella tjänster dock gratis till slutkunden. Det kommersiella inslaget manifesteras då på något annat sätt. Det kan exempelvis vara så att tjänsten är reklamfinansierad eller kommer paketerad som en tjänst vid köp av en mobiltelefon från viss tillverkare.

Kravet på tillhandahållande mot ersättning bör anses vara uppfyllt även när tillhandahållaren får betalt av tredje part och inte av slutkunden, t.ex. om tillhandahållaren tjänar pengar på personuppgifter eller andra data som samlas in vid användningen av tjänsten.[5] Inom den digitala ekonomin anser marknadsaktörerna nämligen ofta att information om användare har ett ekonomiskt värde. Elektroniska kommunikationstjänster tillhandahålls allt oftare i utbyte mot att slutanvändarna tillhandahåller personuppgifter eller andra data. I skäl 16 i e-kodexen anges att begreppet ersättning i detta sammanhang bör omfatta sådana situationer där tillhandahållaren av en tjänst begär att slutanvändaren medvetet lämnar personuppgifter i den mening som avses i EU:s dataskyddsförordning eller andra data direkt eller indirekt till tillhandahållaren. Vidare anges i skäl 16 i e-kodexen att begreppet ersättning även bör omfatta situationer där slutanvändaren ger tillgång till information utan att aktivt tillhandahålla den, som till exempel personuppgifter, inklusive ip-adress, eller annan automatiskt genererad information. Det är information som samlas in och överförs via kakor.

En elektronisk kommunikationstjänst kan enligt definitionen i nya LEK vara av tre slag, som delvis kan överlappa varandra:

- internetanslutningstjänster,
- interpersonella kommunikationstjänster, och
- tjänster som helt eller huvudsakligen utgörs av överföring av signaler.

[4] Se prop. 2021/22 :136 s. 122 f.
[5] Se a. prop. s. 406.

Det som främst är av intresse i detta sammanhang är alltså *interpersonella kommunikationstjänster.* Definitionen av dessa motsvarar artikel 2.5 i e-kodexen. En interpersonell kommunikationstjänst definieras i nya LEK som en tjänst som vanligen tillhandahålls mot ersättning och som möjliggör ett direkt interpersonellt och interaktivt informationsutbyte via elektroniska kommunikationsnät mellan ett begränsat antal personer. En ytterligare förutsättning är att de personer som inleder eller deltar i kommunikationen bestämmer vem eller vilka som ska vara mottagare av denna. Definitionen omfattar dock inte en tjänst som möjliggör interpersonell och interaktiv kommunikation enbart som en extrafunktion av mindre betydelse som är direkt kopplad till en annan tjänst. En sådan extrafunktion av mindre betydelse är alltså inte en interpersonell kommunikationstjänst enligt definitionen i nya LEK.

Interpersonella kommunikationstjänster är således tjänster som möjliggör ett interaktivt utbyte av information mellan personer. Definitionen omfattar tjänster som traditionella röstsamtal mellan två eller flera fysiska personer, men även t.ex. e-posttjänster, meddelandetjänster och gruppchattar.

Definitionen täcker alltså bara tjänster där antalet deltagare i kommunikationen är begränsat och där deltagarna bestäms av kommunikationens avsändare eller deltagare. Interaktiv kommunikation innebär att tjänsten gör det möjligt för mottagaren av informationen att svara. Tjänster som inte uppfyller dessa krav omfattas inte av definitionen.

Sådana tjänster som faller utanför definitionen kan exempelvis vara linjära sändningstjänster för radio och tv, beställvideo, bloggar och informationsutbyte mellan maskiner. Sådana tjänster kan dock erbjudas på samma plattform som en tjänst som uppfyller kraven för en interpersonell kommunikationstjänst.[6]

Det finns inget krav på att interpersonella kommunikationstjänster helt eller huvudsakligen ska inkludera överföring av signaler. Därmed omfattas t.ex. mjukvarutjänster för direkt kommunikation mellan slutanvändares datorer där tjänstetillhandahållaren inte har inflytande eller rådighet över själva överföringen av kommunikationen.

[6] Se prop. 2021/22:136 s. 407 f.

I skäl 17 i e-kodexen anges bl.a. följande.

> I undantagsfall bör en tjänst inte anses som en interpersonell kommunikationstjänst om funktionen för interpersonell och interaktiv kommunikation enbart är en extrafunktion av mindre betydelse som är direkt kopplad till en annan tjänst och som av objektiva tekniska skäl inte kan användas utan den huvudtjänsten, och integreringen av den inte är ett sätt att kringgå tillämpningen av bestämmelserna för elektroniska kommunikationstjänster. Som delar i undantaget från definitionen bör mindre och extrafunktion tolkas restriktivt och ur ett objektivt slutanvändarperspektiv. En interpersonell kommunikationstjänstfunktion skulle kunna anses mindre om dess objektiva användbarhet för slutanvändaren är mycket begränsad och om den i själva verket knappt används av slutanvändarna.

Extrafunktioner av mindre betydelse kan t.ex. vara vissa kommunikationsfunktioner i online-spel, beroende på deras användning och funktion.[7] Mot bakgrund av vad som uttalas i skäl 17 i e-kodexen gör vi bedömningen att utrymmet är mycket begränsat för vad som kan anses vara en sådan extrafunktion av mindre betydelse.

De interpersonella kommunikationstjänsterna kan vara antingen nummerbaserade eller nummeroberoende. En *nummerbaserad interpersonell kommunikationstjänst* är enligt nya LEK en interpersonell kommunikationstjänst som etablerar en förbindelse till nummer i nationella eller internationella nummerplaner eller som möjliggör kommunikation med sådana nummer. En Noik etablerar inte en förbindelse till nummer i nationella eller internationella nummerplaner och möjliggör inte heller på något annat sätt kommunikation med sådana nummer. Tillhandahållare av Noik kan i och för sig ställa krav på att ett telefonnummer anges vid registreringen av ett konto i tjänsten, men telefonnumret har ingen betydelse för hur kommunikationen etableras eller förmedlas genom tjänsten. Däremot kan telefonnumret ibland användas för att slutanvändare ska kunna hitta varandra i tjänsten.[8]

I stället för telefonnummer använder tillhandahållare av Noik annat som identifierar de unika användarna. Det kan t.ex. vara en e-postadress eller en annan unik användaridentitet. Vilka tjänster som faktiskt kommer att bedömas vara Noik får utvisas av framtida praxis. Vi har i inledningen till detta avsnitt lämnat några exempel på Noik.

[7] Se a. prop. s. 408.
[8] Se a. prop. s. 408 f.

I rapporten svenskarna och internet 2021[9] finns ytterligare exempel på tjänster som omfattas av definitionen, exempelvis:

- Instagram (chatt och meddelande-delarna).
- Snapchat.
- Microsoft Teams.
- Zoom.
- Linkedin (chatt och meddelande-delarna).
- Tiktok (chatt och meddelande-delarna).
- Google Meet.

Härutöver finns ett flertal stora tillhandahållare av e-post som omfattas av begreppet Noik, exempelvis:

- Gmail.
- Apple Mail.
- Outlook (tidigare MSN, Hotmail).
- Yahoo! Mail.

Det går inte att uttömmande lista alla Noik eller att uppskatta hur många företag som tillhandahåller Noik. Det beror bl.a. på att sådana företag kan ha sin hemvist i olika länder samtidigt som deras tjänster tillhandahålls globalt och på att sådana tjänster kan uppstå och försvinna på relativt kort tid.[10]

9.3.2 Ip-adress i stället för telefonnummer

Som nämnts ovan förmedlas ett samtal eller ett meddelade genom en Noik över internet, såvida inte tjänsten har en reservlösning som skickar meddelandet på ett traditionellt sätt, exempelvis via den traditionella sms-tjänsten i ett mobiltelefoninät. Allt som kopplas upp mot internet måste ha en ip-adress (Internet Protocol Address) för att fungera. Vid internetåtkomsten tilldelas användaren en ip-adress

[9] Se https://svenskarnaochinternet.se/rapporter/svenskarna-och-internet-2021. Hämtat den 20 april 2023.
[10] Se a. prop. s. 384.

genom en tjänsteleverantör. Med ip-adress avses en unik adress som används för identifiering och kommunikation mellan datorer m.m. på internet med hjälp av Internet Protocol-standarden. Det finns två standarder i bruk, IPv4 och IPv6.[11] En IPv4-adress kan exempelvis se ut på följande sätt 193.11.1.15 medan en IPv6-adress kan se ut på följande sätt 2001:06b0:0048:0000:0000:0000:0000:0100 (2001:6b0:48::100 i komprimerad form[12]).

Ip-adresserna kan vara fasta, dvs. samma användare har alltid samma adress, eller dynamiska, dvs. de tilldelas användaren under en begränsad tid. När dynamiska ip-adresser används kan alltså samma användare ha olika adresser vid olika tillfällen och samma ip-adress kan användas av olika användare vid olika tillfällen.

Adresseringsstandarden IPv4, som introducerades i början av 1980-talet, är den standard som främst används för att kommunicera över internet i dag. Detta protokoll har en begränsad adressrymd, dvs. antalet enheter som kan tilldelas en ip-adress. Detta ledde till att standarden för IPv6 (med en mycket större adressrymd än IPv4) togs fram och började användas i slutet av 1990-talet parallellt med IPv4.[13]

IPv4-adresserna har i princip tagit slut, i den meningen att befintliga adresser redan har allokerats.[14] Det är delvis en förklaring till varför tillhandahållare använder adressöversättning. Adressöversättning är ett vedertaget sätt för aktörerna att hantera bristen på IPv4-adresser genom funktioner som t.ex. Network Address Translation (NAT) eller Carrier Grade NAT (CGN). Adressöversättning innebär att flera slutkunder delar på en publik IPv4-adress i stället för att få varsin unik, publik IPv4-adress. I teorin kan upp till cirka 60 000 slutkunder dela på en enda publik IPv4-adress men i praktiken är det betydligt färre slutkunder som delar på en sådan adress.[15] För att i dessa fall kunna veta vem som använt en ip-adress vid ett specifikt tillfälle måste man känna till den avsändande eller motta-

[11] Teknisk specifikation från för IPv4, IETF (RFC 791) publicerad 1981, https://www.rfc-editor.org/pdfrfc/rfc791.txt.pdf och IPv6 IETF (RFC 1883) publicerad 1995, https://www.rfc-editor.org/pdfrfc/rfc1883.txt.pdf. Hämtat den 20 april 2023.
[12] De inledande nollorna i varje grupp och grupper med nollor kan utelämnas.
[13] Rapport Koppla upp till internet med framtidssäkra IPv6-adresser, PTS-ER-2021:11.
[14] https://www.ripe.net/publications/news/about-ripe-ncc-and-ripe/the-ripe-ncc-has-run-out-of-ipv4-addresses. Hämtat den 20 april 2023.
[15] Rapport Tillhandahållande av IPv6 i fasta allmänna kommunikationsnät i Sverige, den 10 maj 2022, PTS-ER-2022:21.

gande användarens s.k. portnummer och ha en tämligen precis uppgift om tiden för kommunikationen.[16]

9.3.3 ”Svenska” ip-adresser

Ip-adresser är inte i sig kopplade till ett visst land. Något förenklat kan fördelningen av ip-adresser beskrivas på följande sätt. Organisationen IANA (Internet Assigned Numbers Authority), som drivs av ICANN (Internet Corporation for Assigned Names and Numbers), administrerar ip-adresser globalt. Ansvaret är sedan delegerat till fem regionala organisationer, RIR (Regional Internet Registries) som tilldelar ip-adresser till sina medlemmar, vanligen olika tillhandahållare. De regionala organisationerna är

- AFRINIC (African Network Information Centre).
- ARIN (American Registry for Internet Numbers).
- LACNIC (Latin America and Caribbean Network Information Centre).
- APNIC (Asia Pacific Network Information Centre).
- RIPE NCC (Réseaux IP Européens Network Coordination Centre, nedan RIPE).

Ip-adresserna tilldelas medlemmarna i stora block. Ett block med ip-adresser som tilldelas en specifik tjänsteleverantör, har samma tal i de inledande grupperna. Till exempel har Sunet (Swedish University Computer Network) bl.a. tilldelats blocken 193.10.0.0–193.11.255.255 för IPv4 vilket innebär att ip-adresserna i vissa delar av Sunets nät alltid börjar med 193.11. På motsvarande sätt har Sunet bl.a. tilldelats IPv6 block som börjar med 2001:06b0. På det sättet skulle man kunna säga att alla ip-adresser i ett block som tilldelats en svensk tjänsteleverantör är ”svenska ip-adresser”. Olika tillhandahållare kan dock dela på samma inledande tal och en leverantör kan ha verksamhet i flera olika länder.

[16] Av PTS föreskrifter (PTSFS 2019:2) framgår att den lagringsskyldige ska lagra uppgifter om publik ip-adress med tillhörande portnummer kopplat till användarens ip-adress och spårbar tid för kopplingen.

Enligt RIPE:s nuvarande policy ska ip-adresserna användas inom medlemmens egna resurser. Tjänsteleverantörens ip-adresser fördelas till olika autonoma system (AS). De stora svenska tillhandahållarna har ofta flera AS. Om leverantören t.ex. tar fram en ny internet-tjänst, så knyts ett antal ip-adresser till denna tjänst. Vilka publika ip-adresser som är knutna till vilket AS registreras och uppgifterna finns publikt tillgängliga. Det innebär att det utan svårigheter går att härleda ip-adressen 193.11.1.15 till Sunet med registrerad adress i Stockholm.

Ett AS behöver dock inte vara knutet till ett visst land och man kan inte med 100 procents säkerhet säga att en ip-adress används i ett visst land. Vid landsgränser är osäkerheten störst om internetåtkomsten sker via mobil nätanslutningspunkt.

Det kan i sammanhanget noteras att det finns kommersiella tjänster för lokalisering av ip-paket och ip-adresser. I en artikel i Journal of Information Technology and Control (ITC 3/46) från 2017, Location Accuracy of Commercial IP Address Geolocation Databases, anges att träffsäkerheten bland de undersökta lokaliseringstjänsterna uppgick till nästan 100 procent på landnivå.[17] När det däremot gällde region- och stadsnivå var träffsäkerheten lägre.

Det går också att, genom olika tekniska lösningar, spåra den nätutrustning som finns närmast innehavaren av ip-adressen och på det sättet få kännedom om ungefärligen var innehavaren befinner sig. Sammanfattningsvis går det med förhållandevis enkla medel och stor träffsäkerhet att fastställa var en viss enhet som använder en viss ip-adress finns.

Vi återkommer i avsnitt 9.6.1 kring frågor om Noik och anknytning till Sverige.

9.3.4 Hur sker kommunikation via Noik?

Tillhandahållare av Noik erbjuder tjänster som funktionsmässigt motsvarar de nummerbaserade interpersonella kommunikationstjänsterna. Området för elektronisk kommunikation är emellertid i ständig förändring och utvecklingen går mot allt fler hybridlösningar. Flertalet Noik kan dock sägas fungera enligt en kombination av följande alternativ:

[17] Se https://itc.ktu.lt/index.php/ITC/article/view/14451. Hämtat den 20 april 2023.

1. Kommunikationen sker antingen i realtid, eller enligt principen store-and-forward.
2. Kommunikationen passerar antingen tjänsteleverantörens infrastruktur, eller så gör den inte det.
3. Kommunikationen fortsätter antingen att vara lagrad hos tjänsteleverantören efter att den nått fram till mottagaren, eller så gör den inte det.

Ett exempel på realtidskommunikation är talkommunikation mellan två och flera personer. Principen store-and-forward innebär att kommunikationen mellanlagras på väg till mottagaren, vanligen i tjänsteleverantörens infrastruktur, och att mottagandet kan ske antingen direkt eller vid ett senare tillfälle. Exempel på tjänster av typen store-and-forward är e-post, chatt och röstbrevlådor.

Nästan alla tillämpningar av Noik förutsätter att kommunikationen på ett eller annat sätt passerar tjänsteleverantörens infrastruktur. Detta är särskilt tydligt för tjänster av typen store-and-forward, eftersom kommunikationen då kan anlända till mottagaren i ett senare skede (jfr när nya e-postmeddelanden hämtas efter att mobiltelefonen varit i flygplansläge).

Vissa typer av tjänster för realtidskommunikation kan dock vara utformade så att trafiken efter samtalsuppkoppling går direkt mellan de deltagande terminalerna, utan att passera tjänsteleverantörens infrastruktur. Det bör dock poängteras att själva etableringen av kommunikationen alltid förutsätter att tjänsteleverantörens infrastruktur nyttjas, bl.a. eftersom den initierande parten inte kan antas veta vilken ip-adress som den andra parten använder just då. En central egenskap hos Noik som stödjer realtidskommunikation är därför att aktiva användarkonton behöver meddela tjänsteleverantören att de är aktiva och hur de kan nås (exempelvis genom att de meddelar sin nuvarande ip-adress), för det fall ett talsamtal inkommer från en annan användare. Detta förfarande påminner om hur en mobiltelefons hemmanätverk får information om var i världen mobiltelefonen befinner sig (vid roaming), samt hur den nätinfrastruktur mobiltelefonen för tillfället är ansluten till får reda på ungefär var i nätet telefonen befinner sig (t.ex. någonstans i en specifik grupp av basstationer).

Denna typ av bakgrundsmeddelanden som sker mellan nätinfrastruktur och terminaler, eller internt inom nätinfrastrukturen, i syfte

att få kommunikationstjänsten att praktiskt fungera, benämns ofta *signalering*. Signaleringsmeddelanden innehåller ingen information om innehållet i kommunikationen, men kan innehålla information om när, hur, vad och med vem en viss användare kommunicerar, eller var användaren befinner sig vid en viss tidpunkt. Sådana lokaliseringsuppgifter kan avse fysisk position (t.ex. en gps-position eller uppgift om vilken basstation användaren är ansluten till), logisk position (t.ex. en ip-adress) eller båda.

Lagring hos tjänsteleverantören av trafik som redan levererats till mottagaren sker hos många Noik och innebär rent praktiskt bl.a. att användaren kan återfå sin kommunikationshistorik även om telefonen eller datorn t.ex. blir stulen. Vid inloggning i tjänsten med en ny telefon eller dator så finns hela kommunikationshistoriken tillgänglig för nedladdning. Beträffande tjänster som inte tillämpar sådan lagring kan användaren inte återfå gamla meddelanden om han eller hon loggar in med en ny telefon eller dator. Kommunikationstjänster som lagrar historisk trafik hos tjänsteleverantören är typiskt också enklare att förena med behovet hos användaren att kunna använda flera olika terminaler parallellt (t.ex. att kunna läsa sin e-post och sina chattmeddelanden från både sin dator och sin mobiltelefon). Det finns dock vissa tjänster som stödjer parallell användning av flera terminaler utan att lagring av överförda historiska data sker hos tjänsteleverantören – ett sådant exempel är tjänsten Signal.

En annan typ av lagring av trafik som redan levererats till mottagaren är när användaren nyttjar någon form av generell backuptagning av den information som finns på användarens telefon eller dator. Exempelvis erbjuder både Google och Apple sådana backuptjänster. Denna typ av backup-tagning medför ur användarens perspektiv att kommunikationshistorik kan återfås även om telefonen eller datorn går förlorad. Det är däremot tveksamt om denna slags generell backup-tagning kan betraktas som en del av aktuell Noik. Detta eftersom backup-tagningen inte är en del av själva kommunikationstjänsten och backup-tagningen även avser annan slags information, t.ex. digitala fotografier. Härutöver kan backuptagningen ske med hjälp av en helt annan tjänsteleverantör.

9.3.5 Totalsträckskryptering vid kommunikation

Totalsträckskryptering kan sägas innebära att innehållet i datatrafiken inte ska vara tillgängligt på något sätt för tjänsteleverantören, även om trafiken passerar dennes infrastruktur, och även om historisk trafik lagras i denna infrastruktur. Likaså är syftet att trafiken inte heller ska vara tydbar för de tillhandahållare som förmedlar trafiken mellan de kommunicerande parterna, eller för någon annan som har tillgång till trafiken längs vägen. För många tillhandahållare kan det dock vara kommersiellt fördelaktigt om innehållet är tillgängligt för analys, eftersom analysen kan ligga till grund för en profilering av användaren, vilket i sin tur kan användas för riktade reklamerbjudanden. Andra tillhandahållare vill differentiera sig just genom att försöka bevisa att de inte på något sätt ens kan skaffa sig tillgång till innehållet i trafiken, även om det skulle finnas domstolsbeslut på sådan inhämtning. Många traditionella e-posttjänster krypterar trafiken under överföring, men meddelandena ligger lagrade i icke-krypterad form på tjänsteleverantörens e-postserver, även om någon form av autentisering krävs för att läsa dem.

Det finns ingen reglering som styr hur Noik ska utformas, vilket gör att det kan finnas fler alternativ än de som nu beskrivits och att nya alternativ kan uppkomma. Vilka av dessa alternativ som används av en viss tillhandahållare av Noik, kombinerat med vilken information som angetts vid registrering av ett konto i denna Noik, påverkar i stor utsträckning förutsättningarna för de brottsbekämpande myndigheterna att få tillgång till information.

9.3.6 Vilka uppgifter har tillhandahållare av Noik tillgång till?

Vilka uppgifter om användaren (dvs. uppgifter om abonnemang) som tillhandahållaren av Noik har tillgång till kan skilja sig åt mellan de olika tjänsterna. Användningen av en Noik förutsätter någon form av registrering av kontouppgifter hos tillhandahållaren. Vid registrering av ett konto hos en tillhandahållare av Noik ska användaren ange ett unikt användarnamn, alternativt tilldelas användaren en unik användaridentitet av tillhandahållaren. Användaridentiteten eller användarnamnet kan sägas motsvara telefonnumret i traditionella telefonitjänster.

Vilka ytterligare uppgifter som krävs för registrering av ett konto varierar mellan olika Noik. För vissa Noik krävs exempelvis en giltig

e-postadress eller ett giltigt mobiltelefonnummer, medan andra Noik inte kräver några uppgifter om användaren över huvud taget. För att ingen obehörig ska kunna komma åt användarkontot tillämpas någon form av autentisering för åtkomst till kontot, t.ex. ett lösenord.

Få tillhandahållare av Noik ställer i dag krav på identifiering, dvs. att användaren ska kunna styrka sin faktiska och fysiska identitet. Användningen av Noik kan därför i många fall sägas vara jämförbar med användningen av oregistrerade kontantkort vid mobiltelefoni, dvs. vem som helst kan använda sådana tjänster utan att behöva styrka sin identitet, och tillhandahållaren har begränsad, eller ibland ingen, information om användaren.

Tillhandahållare av Noik kan även ha tillgång till användarens profilbild och uppgifter om t.ex. betalkort för betalning av tjänsten eller en tilläggstjänst. Vissa tjänster är knutna till andra tjänster eller produkter hos tillhandahållaren. Exempelvis förutsätter användning av Imessage och Facetime att användaren har registrerat ett Apple-ID.

Tillhandahållare av Noik har också, under i vart fall en kort period, information om den ip-adress och i förekommande fall det portnummer som användarens kommunikationsutrustning använder för att koppla upp sig mot tjänsten. Annars skulle kommunikationen inte kunna förmedlas. Användare kan dock använda sig av tjänster för att dölja sin ip-adress eller för att få det att se ut som att kommunikationen kommer från en annan plats än den verkligen gör. Vid användning av anonymiseringstjänster är det mycket svårt eller omöjligt att spåra ip-adressen. Exempel på sådana tjänster är VPN-tjänster (Virtual Private Network), proxyservrar och vissa webbhotell som tillhandahåller ip-adresser.

Även vilka trafikuppgifter och lokaliseringsuppgifter som genereras och behandlas hos en tillhandahållare av Noik skiljer sig åt beroende på hur tjänsten är uppbyggd. Tillhandahållarna har dock normalt ha tillgång till uppgifter om vilka användaridentiteter (eller användarnamn) som deltar vid ett samtal och under vilken tid samtalet äger rum, vilka användaridentiteter (eller användarnamn) som är avsändare respektive mottagare av ett meddelande och när meddelandet skickades. Meddelanden som skickas via vissa Noik kan mottas på olika enheter vid olika tillfällen. Det kan därför i dessa fall inte, på samma sätt som vid t.ex. ett sms, fastställas ett enskilt specifikt tillfälle när meddelandet mottogs. Tillhandahållarna torde även normalt ha tillgång till uppgifter om en s.k. misslyckad uppringning,

dvs. när mottagaren inte svarar, och uppgifter om vilken typ av kommunikation det är fråga om. I vissa fall kan tillhandahållarna ha tillgång till vilken typ av kommunikationsutrustning som används. Genom tillgången till ip-adresser kan tillhandahållarna normalt få information om ungefärliga lokaliseringsuppgifter för kommunikationsutrustningen. Tillhandahållarna kan också ha tillgång till andra uppgifter om kommunikationsutrustningens lokalisering, t.ex. gps-position. Till skillnad från teleoperatörerna har tillhandahållare av Noik däremot vanligtvis inte tillgång till lokaliseringsuppgifter via teleoperatörernas basstationer. Det beror på att tillhandahållare av Noik typiskt sett inte har någon direkt relation till den som äger infrastrukturen varigenom trafiken förmedlas. Den som använder en Noik-tjänst kan med andra ord fritt välja kanal för internetåtkomst och något utbyte av lokaliseringsuppgifter sker som huvudregel inte mellan den som tillhandahåller internettrafiken och den som tillhandahåller Noik.

Även om tillhandahållare av Noik inte omfattas av någon rättslig skyldighet att lagra eller ge brottsbekämpande myndigheter tillgång till uppgifter om elektronisk kommunikation lämnar tillhandahållarna i vissa fall ut information till brottsbekämpande myndigheter på frivillig basis. Större tillhandahållare av Noik har ofta egna policyer om i vilka fall uppgifter ska lämnas ut.

9.4 Pågående och genomfört arbete inom EU

Det finns inte någon gemensam reglering inom EU för lagring och tillgång till uppgifter om elektronisk kommunikation för den som tillhandahåller Noik. Inte heller finns det för närvarande något förslag till sådan reglering. Det pågår dock annat arbete med anknytning till frågan om skyldighet för tillhandahållare av Noik att lagra och ge brottsbekämpande myndigheter tillgång till uppgifter om elektronisk kommunikation. Nedan presenteras detta arbete i korthet.

9.4.1 Förslaget till förordning om tillgång till e-bevisning

Kommissionen presenterade i april 2018 ett förslag till förordning om europeiska utlämnandeorder och bevarandeorder för elektroniska bevis i straffrättsliga förfaranden, den s.k. e-bevisningsförordningen

(COM(2018) 225). Förslaget är fortfarande föremål för förhandlingar. Förslagets övergripande syfte är att skapa ett nytt ändamålsenligt regelverk som kompletterar befintlig lagstiftning och effektiviserar gränsöverskridande inhämtning av elektronisk bevisning. Samtidigt presenterade kommissionen ett förslag till direktiv om utseende av en rättslig företrädare för insamling av bevisning i straffrättsliga förfaranden.

Den föreslagna förordningen ska möjliggöra för en myndighet i en medlemsstat att begära ut eller begära bevarande av elektroniska uppgifter direkt hos en tjänsteleverantör som är etablerad i en annan jurisdiktion och oaktat var uppgifterna finns lagrade. En order ska i första hand översändas till den rättsliga företrädare som tjänsteleverantören enligt det föreslagna direktivet ska utse.

Grundläggande förutsättningar för att initiera ett förfarande enligt förslaget till förordning är att begäran görs inom ramen för ett straffrättsligt förfarande och att den tjänsteleverantör som begäran riktas mot erbjuder sina tjänster inom EU. De tillhandahållare som omfattas är sådana företag som erbjuder elektroniska kommunikations- och informationstjänster, däribland sociala medieföretag som Meta, samt företag som erbjuder rena it-infrastrukturtjänster som t.ex. ip-adresser och domännamn. Elektroniska uppgifter kan enligt förslaget till förordning vara t.ex. namn- och adressuppgifter, kontonummer och telefonnummer å ena sidan och det faktiska innehållet i dokumenterad skriftlig eller muntlig kommunikation å andra sidan. Förslaget omfattar enbart lagrade uppgifter.

Om tjänsteleverantören eller dess rättsliga företrädare inte efterlever ordern, kan den utfärdande myndigheten, enligt förslaget till förordning, vända sig till den behöriga myndigheten i den verkställande staten och be myndigheten att erkänna ordern och vidta åtgärder för att se till att den blir verkställd. Detta ska den verkställande myndigheten göra såvida det inte finns anledning att vägra verkställighet enligt de skäl som framgår av förslaget till förordning.

9.4.2 Särskild teknik för att bekämpa sexuella övergrepp mot barn på nätet

Vissa tillhandahållare av Noik använder inom sina tjänster en särskild teknik för att upptäcka sexuella övergrepp mot barn i tjänsterna, så att de kan avlägsna innehållet och rapportera övergreppen till brotts-

bekämpande myndigheter och organisationer som agerar i allmänhetens intresse för att bekämpa sexuella övergrepp mot barn.

Eftersom Noik omfattas av definitionen elektroniska kommunikationstjänster i e-kodexen, är bestämmelserna i direktiv 2002/58/EG om integritet och elektronisk kommunikation (e-dataskyddsdirektivet) tillämpliga för tillhandahållare av Noik. Till skillnad från EU:s dataskyddsförordning innehåller e-dataskyddsdirektivet ingen rättslig grund för frivillig behandling av innehåll eller trafikuppgifter i syfte att upptäcka sexuella övergrepp mot barn.

Europaparlamentet och rådet har därför antagit förordningen (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.

Kommissionen har därefter lämnat ett förslag till förordning för att bekämpa sexuella övergrepp mot barn.[18] Förslaget har diskuterats i Sverige och väckt omfattande debatt under våren 2023.[19] Kommissionens förslag beskrivs översiktligt i en faktapromemoria framtagen av Justitiedepartementet.[20] Som nämnts i avsnitt 4.2 har kommissionen lämnat ett förslag till en ny förordning om respekt för privatlivet och skydd för personuppgifter i samband med elektronisk kommunikation, som ska ersätta e-dataskyddsdirektivet.

9.4.3 Nya förordningar om digitala tjänster och marknader

Under hösten 2022 har ny EU-lagstiftning antagits gällande bl.a. digitala tjänster och sociala medier. Syftet med denna reform var att stärka skyddet för konsumenternas rättigheter och att bidra till en mer rättvis och öppen digital marknad för alla aktörer. Reformen består av två separata förordningar, EU:s förordning om en inre mark-

[18] Se Proposal for a Regulation of the European Parliament and the Council laying down rules to prevent and combat child sexual abuse (COM (2022) 209 final).
[19] Se bl.a.
https://www.dn.se/debatt/eus-nya-massovervakning-far-inte-forstora-kallskyddet/,
https://www.svd.se/a/oneeLR/eu-forslaget-innebar-en-orimlig-overvakning-skriver-paarup-petersen,
https://www.svd.se/a/zEkO4r/helene-fritzon-s-sexuella-overgrepp-mot-barn-maste-upptackas, och
https://www.svt.se/nyheter/utrikes/eu-forslaget-chat-control-kritiseras.
Hämtat den 20 april 2023.
[20] Se Faktapromemoria 2021/22:FPM99.

nad för digitala tjänster (Digital Services Act, i fortsättningen DSA[21]) och förordningen om öppna och rättvisa marknader inom den digitala sektorn (Digital Markets Act, i fortsättningen DMA[22]).

DSA innehåller bl.a. nya skyldigheter för tillhandahållare av digitala förmedlingstjänster, bl.a. online-plattformar. Sådana tjänster ska t.ex. tillhandahålla ett system för notifiering av påstått olagligt innehåll och inrätta interna klagomålsmekanismer. Det ska exempelvis vara möjligt att klaga på att visst innehåll tagits bort eller blockerats. Vidare föreskrivs det en skyldighet för tillhandahållarna att motivera beslut om borttagning eller blockering av innehåll. Det finns även regler för innehållet i och hanteringen av förelägganden att agera mot olagligt innehåll, regler för att säkra öppenhet kring bl.a. online-reklam och algoritmer som används för att rekommendera innehåll till användare, nya möjligheter att granska hur plattformarna fungerar och bestämmelser om spårbarhet av kommersiella användare av online-marknadsplatser för att möjliggöra spårning av användare som säljer olagliga varor och tjänster.

DMA syftar till att införa enhetliga regler för att förhindra otillbörligt agerande av så kallade ”gatekeepers”, dvs. plattformsleverantörer med en betydande inverkan på den gemensamma marknaden (såsom sökmotorer, sociala nätverk eller online-baserade förmedlingstjänster).

9.5 Lagringsskyldighet för tillhandahållare av Noik i vissa länder

Inom EU är det, enligt uppgifter som vi har fått, endast Belgien och Ungern som har en reglering som innebär en lagringsskyldighet för tillhandahållare av Noik.

I Belgien har en lagstiftning trätt i kraft om generell och odifferentierad lagring för att skydda nationell säkerhet och om geografiskt riktad lagring för bekämpning av allvarlig brottslighet (se avsnitt 6.5.3). Lagringsreglerna gäller även för tillhandahållare av Noik. För att vid geografiskt riktad lagring kunna avgöra om terminal-

[21] Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster).
[22] Europaparlamentets och rådets förordning (EU) 2022/1925 av den 14 september 2022 om öppna och rättvisa marknader inom den digitala sektorn och om ändring av direktiv (EU) 2019/1937 och (EU) 2020/1828 (Förordningen om digitala marknader).

utrustningen är lokaliserad i ett geografiskt område som omfattas av lagringsskyldigheten ska tillhandahållarna använda de mest pålitliga och exakta uppgifterna som möjligt. Tillhandahållarna ska använda uppgifter om utrustningens satellitpositioner om det är möjligt.

I Ungern finns en lagringsskyldighet för tillhandahållare av applikationstjänster för krypterad kommunikation. Lagringen avser metadata som genereras och behandlas i samband med meddelanden och kommunikation som överförs via sådana tjänster. Lagringstiden är ett år från och med den dag då uppgifterna genererades. Behöriga myndigheter har rätt att från dessa tillhandahållare inhämta uppgifter om typ av tjänst, abonnent eller användare av tjänsten, identifieringsuppgifter som är nödvändiga för användning av tjänsten, ip-adress och portnummer som används vid registrering, ip-adress och portnummer som används för att komma åt tjänsten samt användar-ID. I Ungern finns ingen reglering om riktad lagring.

9.6 Överväganden och förslag

9.6.1 En lagringsskyldighet för tillhandahållare av Noik

EU-rätten sätter upp ramarna för nationell lagstiftning om datalagring för brottsbekämpande ändamål. I avsnitten 6, 7 och 8 har vi föreslagit regler om lagring i syfte att skydda den nationella säkerheten samt lämnat ett förslag på hur riktad lagring i syfte att bekämpa grov brottslighet skulle kunna utformas. Denna reglering är enligt vår mening förenlig med de krav EU-rätten ställer. I detta avsnitt överväger vi om, och i så fall i vilken utsträckning, tillhandahållare av Noik ska omfattas av skyldigheten att lagra uppgifter om elektronisk kommunikation.

Nyttan och behovet i brottsbekämpande verksamhet av uppgifter om elektronisk kommunikation från tillhandahållare av Noik

Utredningens bedömning: De brottsbekämpande myndigheterna har stor nytta och ett påtagligt behov av uppgifter om elektronisk kommunikation även från tillhandahållare av Noik.

Vid bedömningen av hur långtgående inskränkningar i enskildas fri- och rättigheter som kan tolereras i ett demokratiskt samhälle är det av vikt att klargöra vilken betydelse en åtgärd som innebär intrång i en skyddad rättighet kan ha för att uppnå sitt ändamål, liksom ändamålets betydelse. En proportionalitetsavvägning måste därefter göras mellan åtgärdens betydelse för det eftersträvade ändamålet å ena sidan och den grad av intrång i enskildas skyddade rättigheter som åtgärden innebär å andra sidan. Vid en sådan proportionalitetsbedömning är det viktigt att bedöma vilken nytta åtgärderna innebär för den brottsbekämpande verksamheten och vilka behov av åtgärderna som finns. En allmän redogörelse för de brottsbekämpande myndigheternas nytta och behov av uppgifter om elektronisk information finns i avsnitt (5.5).

De brottsbekämpande myndigheternas nytta och behov av uppgifter om elektronisk kommunikation från tillhandahållare av Noik påverkas bl.a. av hur elektroniska kommunikationstjänster används i Sverige och hur brottsligheten utvecklas.

Dagens samhälle präglas av att informationsteknik genomsyrar i stort sett alla sektorer. En mycket stor andel av de svenska hushållen har tillgång till internet, datorer och smarttelefoner. Enligt Internetstiftelsen rapport, ”Svenskarna och internet 2022”, använder 94 procent av Sveriges befolkning internet, och nästan alla dessa använder internet dagligen. Enligt rapporten används digitala kommunikationstjänster i en hög utsträckning. Av internetanvändarna har 67 procent använt Facebook Messenger under det senaste året, 52 procent har använt tjänsten minst någon gång per vecka och 38 procent har använt tjänsten varje dag. Under det senaste året har 36 procent använt Whatsapp och 14 procent har använt Discord. 40 procent av internetanvändarna har videosamtal varje vecka.

Allt fler använder smarttelefoner, som ger möjlighet till kommunikation på flertalet sätt och genom tjänster tillhandahållna av andra aktörer än teleoperatörerna. I takt med att nya tjänster utvecklas ändras också våra kommunikationsmönster.

PTS har i uppdrag att följa tjänsteutvecklingen på marknaden för elektronisk kommunikation och som en del av detta uppdrag arbetar PTS med att årligen samla in och publicera marknadsdata. PTS för statistik över bl.a. trafiken i mobil-, tele- och fibernäten samt antalet och typen av abonnemang.[23] I takt med att användningen av Noik

[23] Se https://statistik.pts.se/svensk-telekommarknad/. Hämtat den 20 april 2023.

blir allt vanligare, har användningen av vissa tjänster som tillhandahålls av teleoperatörerna minskat. Enligt PTS statistik ökade användningen av sms till och med 2010, då det genomsnittliga antalet sms som skickades från mobiltelefon per samtalsabonnemang och månad var 139. Det genomsnittliga antalet sms har därefter sjunkit och 2021 uppgick det genomsnittliga antalet till 40. Det totala antalet mobilabonnemang har inte minskat på motsvarande sätt, men det blir allt vanligare att abonnemangen innehåller åtkomst till data (abonnemangen för enbart samtal har minskat varje år sedan 2004). Enligt en rapport från en arbetsgrupp vid Europaparlamentet förväntades Noik stå för närmare 90 procent av alla elektroniska kommunikationsmeddelanden 2020.[24]

Det kan antas att kriminella personer, i vart fall för sådan kommunikation som handlar om att planera och utföra brott, väljer att använda kommunikationstjänster som de vet eller antar att de brottsbekämpande myndigheterna inte med lätthet kan få tillgång till information från. Eftersom tillhandahållare av Noik inte omfattas av någon skyldighet att lagra uppgifter om elektronisk kommunikation, kan det rimligen antas att kriminella personer väljer att använda Noik i större utsträckning än sådana kommunikationstjänster som omfattas av en lagringsskyldighet.

Det kan också konstateras att antalet anmälda brott har ökat kontinuerligt sedan år 1975 enligt statistik från Brå för anmälda brott 2020. I Brås rapport It-inslag i brottsligheten och rättsväsendets förmåga att hantera dem framgår att en kraftig ökning skett av antalet anmälda brott som kan identifieras som it-relaterade.[25] Under perioden 2006–2015 var ökningen 949 procent.

It-relaterad brottslighet innebär att it-teknik används för att genomföra olika brott, medan brotten i sig kan vara av vilken typ som helst. De kan handla om allt från ekonomiska brott och dataintrång till bedrägerier, hot på internet och barnpornografibrott. I dag är en stor del av alla brottstyper it-relaterade. Även om it-teknik inte används för att genomföra själva brottet, kan internet och olika former av elektroniska kommunikationstjänster användas för planeringen av ett brott.

I den myndighetsgemensamma lägesbilden om organiserad brottslighet 2019 konstateras att omvärldsförändringarna med ökad globa-

[24] Directorate-General for Internal Policies, Over-the-Top players [OTTs], Study for the IMCO Committee, 2015, s. 43.
[25] Se Brå 2016:17.

lisering och digitalisering påverkar den organiserade brottsligheten i hög omfattning. Kriminella nätverk arbetar alltmer gränsöverskridande och utnyttjar teknik för att dölja brotten, distansera sig från brotten eller begå brotten på distans.[26] Den ökande användningen av informationsteknik innebär en förhöjd risk för att tekniken används som verktyg för att begå brott.

De brottsbekämpande myndigheterna behöver ha tillgång till ändamålsenliga och verkningsfulla verktyg för att kunna förebygga, förhindra, upptäcka, utreda och lagföra brott. Som framgår i avsnitt 5.5 är tillgången till uppgifter om elektronisk kommunikation ofta helt avgörande för att brottsutredningar ska kunna föras framåt. Trafik- och lokaliseringsuppgifter används i princip i varje utredning rörande grova brott och är ofta 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 förundersökning. Det finns alltså ingen tvekan om att uppgifter om elektronisk kommunikation ger de brottsbekämpande myndigheterna stor nytta och att det finns ett påtagligt behov av uppgifterna för att bekämpa brott. Den ökande användningen av sådana kommunikationstjänster som inte omfattas av en rättslig skyldighet att lagra och lämna ut uppgifter om elektronisk kommunikation har gjort att mycket av sådan information som tidigare var tillgänglig för brottsbekämpande myndigheter inte längre går att komma åt. De brottsbekämpande myndigheternas möjlighet att få tillgång till kommunikationsuppgifter minskar alltjämt i takt med att användningen av Noik ökar.

De brottsbekämpande myndigheterna har visserligen redan i dag vissa möjligheter att få tillgång till olika slags uppgifter från tillhandahållare av Noik. Tillhandahållarna lämnar ut uppgifter till de brottsbekämpande myndigheterna på frivillig basis. Flera sådana tillhandahållare har som nämnts egna policyer för i vilka fall uppgifter ska lämnas ut till brottsbekämpande myndigheter. En ordning som bygger på att tillhandahållarna själva bestämmer i vilka fall uppgifter ska lämnas ut är dock enligt vår mening inte tillräcklig för att säkerställa de brottsbekämpande myndigheternas berättigade tillgång till uppgifterna.

[26] Se Myndighetsgemensam lägesbild om organiserad brottslighet 2019, dnr A457.772/2019, https://polisen.se/siteassets/dokument/organiserad_brottslighet/rapport_org_brottslighet_2019_webb_200326.pdf. Hämtat den 20 april 2023.

De brottsbekämpande myndigheterna kan i vissa fall komma åt uppgifter om elektronisk kommunikation hos tillhandahållare av Noik genom användning av olika straffprocessuella tvångsmedel, såsom husrannsakan med efterföljande beslag. Möjligheten för myndigheterna att på egen hand hitta den eftersökta informationen vid en husrannsakan i exempelvis stora serverhallar är dock mycket begränsad. De brottsbekämpande myndigheterna kan också komma åt uppgifter om elektronisk kommunikation genom det nya tvångsmedlet genomsökning på distans (28 kap. 10 a § RB). Vid en sådan genomsökning får handlingar eftersökas i ett avläsningsbart informationssystem utanför den elektroniska kommunikationsutrustning som används för att utföra genomsökningen. Det kan röra sig om handlingar som finns lagrade på t.ex. externa servrar eller i molntjänster. Detta får dock bara ske genom autentisering eller inloggning i det system åtgärden avser. Det är vid genomsökning på distans nämligen inte tillåtet för myndigheterna att komma åt information genom att utnyttja sårbarheter i informationssystemet.

I teorin kan vidare de brottsbekämpande myndigheter redan i dag komma åt uppgifterna genom att få tillstånd till HÖK hos en tillhandahållare av Noik, eftersom regleringen i 27 kap. 19 § RB är teknikneutral. Tillhandahållarna omfattas dock inte av någon anpassningsskyldighet. Möjligheten för de brottsbekämpande myndigheterna att få del av uppgifterna beror alltså i dessa fall till stor del på om tillhandahållaren vill samarbeta med myndigheterna. I avsnitt 10.4.3 överväger vi frågan om en anpassningsskyldighet för tillhandahållare av Noik.

Myndigheterna kan också i vissa fall komma åt uppgifter om elektronisk kommunikation som avser kommunikation via Noik genom hemlig dataavläsning. Hemlig dataavläsning medför dock ett förhållandevis stort integritetsintrång. För att inhämta kommunikationsövervaknings- eller platsuppgifter får åtgärden vidare användas endast om den är av synnerlig vikt antingen för utredningen av allvarliga brott eller för att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som innefattar allvarliga brott. Tillhandahållarna av Noik har inte heller någon skyldighet att medverka i samband med verkställigheten av hemlig dataavläsning och har inte heller tystnadsplikt som teleoperatörerna har enligt lagen om hemlig dataavläsning.

En förutsättning för att de brottsbekämpande myndigheterna ska få tillgång till uppgifter hos tillhandahållare av Noik är vidare att upp-

gifterna finns bevarade hos dessa tillhandahållare. Tillhandahållare av allmänt tillgängliga Noik är, med vissa undantag och i likhet med andra tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster, skyldiga att enligt 9 kap. 1 § nya LEK utplåna eller avidentifiera trafikuppgifter och lokaliseringsuppgifter som avser användare som är fysiska personer eller som avser abonnenter, när uppgifterna inte längre behövs för att överföra meddelandet respektive för tillhandahållandet av tjänsten.

Det finns visserligen en möjlighet 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 (s.k. bevarandeföreläggande, 27 kap. 16 § RB). Ett sådant föreläggande kan riktas mot en tillhandahållare av Noik. Men skyldigheten i 9 kap. 33 § 5 nya LEK att på begäran lämna ut uppgifter till brottsbekämpande myndigheter om vilka övriga tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster som har deltagit vid överföringen av ett meddelande som omfattas av ett bevarandeföreläggande gäller inte för tillhandahållare av Noik.

Ett bevarandeföreläggande kan således vara av stor betydelse om myndigheterna känner till att viss elektronisk information finns lagrad hos en tillhandahållare av Noik, eftersom radering av informationen kan förhindras genom föreläggandet. Om myndigheterna däremot inte har sådan närmare kännedom om den elektroniska informationen, kan ett bevarandeföreläggande inte användas. Motsvarande begränsning torde föreligga beträffande de åtgärder som regleras i förslaget till förordning om tillgång till e-bevisning, dvs. bevarandeorder och utlämnandeorder.

Det kan också konstateras att ett bevarandeföreläggande endast kan användas i en brottsutredning och inte i underrättelseverksamheten. Även åtgärder enligt förslaget till förordning om tillgång till e-bevisning gäller enbart inom ramen för ett straffrättsligt förfarande.

De brottsbekämpande myndigheterna har uttryckt att nyttan och deras behov av uppgifter om elektronisk kommunikation är lika påtagligt oavsett vilken typ av leverantör som tillhandahåller kommunikationstjänsterna. I takt med att allt fler personer använder Noik för att kommunicera ökar dessutom nyttan och behovet av uppgifter om elektronisk kommunikation som genereras och behandlas hos tillhandahållare av sådana tjänster.

Avvägning i förhållande till motstående intressen

Utredningens bedömning: De brottsbekämpande myndigheternas nytta och behov av tillgång till uppgifter om elektronisk kommunikation från tillhandahållare av Noik väger tyngre än de motstående intressen som talar emot en sådan tillgång. Under vissa förutsättningar kan de inskränkningar i enskildas fri- och rättigheter som en lagringsskyldighet av sådana uppgifter innebär tolereras i ett demokratiskt samhälle.

De brottsbekämpande myndigheternas stora nytta och påtagliga behov av tillgång till uppgifter om elektronisk kommunikation måste vägas mot de fri- och rättigheter som tillförsäkras enskilda. Inskränkningar i dessa fri- och rättigheter får, som redogjorts för ovan, endast göras under vissa förutsättningar, däribland att de är proportionella och absolut nödvändiga.

Det kan konstateras att många tillhandahållares tjänster funktionsmässigt motsvarar de traditionella teleoperatörernas tjänster. Det är i båda fallen fråga om tjänster för meddelanden mellan fysiska personer via elektroniska kommunikationsnät. Vår utgångspunkt är att eventuell lagringsskyldighet för tillhandahållare av Noik inte ska omfatta andra typer av uppgifter än sådana som framgår av våra förslag i avsnitt 6, 7 och 8.

För den enskilde slutanvändaren är det i regel utan betydelse om en tillhandahållare (som teleoperatörerna) själv överför signaler eller om kommunikationen levereras via en internetanslutningstjänst (som tillhandahållarna av Noik).[27] Vissa populära tjänster, t.ex. Apples Imessage skickar ett textmeddelande antingen via Apples egen kommunikationstjänst Imessage, eller, vid leverans till mottagaren, som ett vanligt sms, beroende på om mottagaren också har ett Imessagekonto eller inte. Användaren kan också välja själv vilken teknik som ska användas.

Vi menar att de olika teknikerna att förmedla meddelanden inte i sig har någon betydelse från integritetssynpunkt. Den ena tekniken kan inte anses som mer integritetskänslig än den andra. Det är själva lagringen och tillgången till uppgifter som ger upphov till ökade risker för integritetsintrång.

[27] Se prop. 2021/22 :136 s. 122.

Vilket integritetsintrång en lagringsskyldighet för tillhandahållare av Noik skulle innebära för enskilda är naturligtvis beroende av bl.a. vilka tjänster och vilka uppgifter som omfattas av skyldigheten. Vi återkommer till dessa frågor nedan.

En annan fråga är om kommunikation som sker via Noik kan vara av mer integritetskänslig karaktär än sådan kommunikation som sker via teleoperatörernas tjänster. Det skulle exempelvis kunna handla om chattjänster som vänder sig till vissa specifika grupper av användare. Eftersom innehållet i chattarna inte ska lagras, föreligger det emellertid enligt vår mening inte någon särskild integritetsrisk i förhållande till sådana chattgrupper.

Det har inte framkommit några uppenbara omständigheter som gör att en lagringsskyldighet för en tillhandahållare av Noik, skulle innebära ett större ingrepp i den enskildes grundläggande fri- och rättigheter för de personer vars uppgifter berörs än vad motsvarande skyldighet hos en teleoperatör innebär. Det nu sagda gäller naturligtvis under förutsättning att skyldigheterna för tillhandahållare av Noik motsvarar de som gäller eller enligt våra förslag ska gälla för de aktörer som i dag omfattas av skyldigheterna att lagra uppgifter, t.ex. vad gäller vilka typer av uppgifter som ska lagras, lagringstiden, säkerhet, tystnadsplikt och villkor för behandling av uppgifter m.m. Under sådana förutsättningar är vår slutsats att de inskränkningar i fri- och rättigheterna, som en skyldighet för tillhandahållare av Noik att lagra uppgifter om elektronisk kommunikation skulle innebära, är proportionella och absolut nödvändiga i samma utsträckning som för teleoperatörerna.

En lagringsskyldighet som omfattar även tillhandahållare av Noik skulle i och för sig kunna sägas innebära att Sverige generellt inför en mer omfattande lagringsskyldighet än den som nu gäller. Mot detta ska dock framhållas att den ökande användningen av Noik under det senaste decenniet, i vart fall till stor del, har skett på bekostnad av en minskad användning av sådana kommunikationstjänster som teleoperatörerna tillhandahåller. Att allt fler använder Noik i stället för traditionella elektroniska kommunikationstjänster innebär i och för sig att fler aktörer än tidigare kan behöva lagra uppgifter. Sett till helheten torde dock inte lagringsskyldighetens omfattning öka, med hänsyn till den motsvarande minskade användning av traditionella tjänster som telefonsamtal, sms m.m. Genom våra förslag återgår snarare lagringsskyldighetens omfattning till vad som gällde innan

Noik blev det dominerande sättet för interpersonell elektronisk kommunikation. Det ska i detta sammanhang påpekas att vi i avsnitten 6, 7 och 8 har föreslagit ändringar av lagringsskyldigheten. Om våra förslag om riktad lagring i syfte att bekämpa grov brottslighet genomförs, kommer lagringsskyldigheten att inskränkas jämfört med i dag, eftersom den bara kommer att gälla i vissa geografiska områden, på vissa platser, avseende vissa personer eller viss teknik. Endast om Sverige står inför ett allvarligt hot mot den nationella säkerheten kan lagringsskyldigheten avseende trafik- och lokaliseringsuppgifter, enligt våra förslag i avsnitt 7, vara generell och odifferentierad.

Man kan vidare ifrågasätta om det är rimligt att det avgörande för om en lagringsskyldighet ska föreligga bör vara vilken teknik som används. Detta gäller särskilt eftersom tekniken inte längre har samma betydelse för hur samtal kopplas fram i moderna telefoninät. En lagringsskyldighet som omfattar även tillhandahållare av Noik skulle alltså vara mer teknikneutral.

Vår bedömning är att de brottsbekämpande myndigheternas nytta och deras behov av uppgifter om elektronisk kommunikation från tillhandahållare av Noik väger tyngre än de motstående intressen som talar emot en sådan tillgång. Under vissa förutsättningar kan de inskränkningar i enskildas fri- och rättigheter som en lagringsskyldighet för tillhandahållare av Noik innebär tolereras i ett demokratiskt samhälle. En viktig förutsättning för att i Sverige reglera en lagringsskyldighet som träffar även globala tillhandahållare av Noik är naturligtvis att lagringsskyldighetens omfattning och anknytning till Sverige är tydlig. I de följande avsnitten överväger vi dessa och andra förutsättningar för hur en skyldighet för tillhandahållare av Noik att lagra och ge tillgång till uppgifter bör utformas.

En harmonisering inom EU bör inte avvaktas

Utredningens bedömning: En EU-gemensam reglering av lagringsskyldighet för tillhandahållare av Noik är att föredra framför nationella regleringar. Med hänsyn till vikten av att uppgifter från tillhandahållare av Noik omfattas av lagringsskyldighet bör en EU-gemensam reglering emellertid inte avvaktas.

De stora tillhandahållarna av Noik i Sverige, såsom Apple, Google, Meta och Microsoft är globala aktörer. Dessa företag måste följa de regler som gäller i olika länder där de är etablerade, bedriver sin verksamhet eller lagrar sina uppgifter. Om reglerna är olika sätter det tillhandahållarna i en problematisk situation. En EU-gemensam reglering på detta område vore därför att föredra. Diskussioner om dessa frågor har förts på EU-nivå men såvitt vi har kunnat utreda sker inte något aktivt arbete med en EU-gemensam reglering av lagringsskyldighet. Om och när ett eventuellt sådant arbete inleds, kommer det att ta lång tid innan en reglering kan träda i kraft.

Med hänsyn till vikten av att uppgifter även från tillhandahållare av Noik ska omfattas av skyldigheten att lagra uppgifter om elektronisk kommunikation bör en EU-gemensam reglering inte avvaktas. Det kan också noteras att det i Belgien och Ungern finns en lagringsskyldighet för tillhandahållare av Noik, se ovan avsnitt 9.5.

Lagringsskyldighetens anknytning till Sverige

Utredningens förslag: Lagringsskyldigheten ska enbart omfatta uppgifter om sådan kommunikation som till någon del har skett i Sverige.

För att överväga en lagringsskyldighet i Sverige för tillhandahållare av Noik måste det klargöras vilken kommunikation som skulle träffas av skyldigheten. De globala tillhandahållarna av Noik erbjuder sina kommunikationstjänster över hela världen. En svensk lagringsskyldighet kan inte reglera sådan kommunikation som inte har någon svensk anknytning. Sverige måste med andra ord ha legislativ jurisdiktion för den lagringsskyldighet som regleras.

En utgångspunkt bör vara vilka uppgifter som det finns behov av att lagra. De brottsbekämpande myndigheterna arbetar primärt med brottsutredningar och underrättelseverksamhet beträffande sådana brott eller brottslig verksamhet som sker i Sverige eller som riktar sig mot svenska intressen. Det är alltså främst kommunikation där avsändare eller mottagare befinner sig i Sverige som är av relevans för den brottsbekämpande verksamheten. En lagringsskyldighet bör därför omfatta och begränsas till sådana uppgifter, om en sådan lösning är möjlig.

En avgränsning skulle kunna vara att lagringsskyldigheten omfattar sådana uppgifter om kommunikationen som faktiskt finns på servrar i Sverige. En sådan avgränsning har fördelen att den stämmer överens med den traditionella tolkningen av frågan om Sverige har legislativ jurisdiktion (se avsnitt 11.3). Det skulle vidare vara enkelt för tillhandahållarna att avgöra vilka uppgifter som ska lagras. Mot en sådan avgränsning talar dock att tillhandahållarna kan välja att inte lagra uppgifter i ett land t.ex. om landet inför regler som tillhandahållarna anser vara alltför betungande. Samma uppgifter kan dessutom finnas på många olika ställen i världen, och en uppgift kan också finnas i delar spridda över hela världen. Uppgifter som lagras i ett visst land behöver inte heller ha någon särskild koppling till kommunikation som ägt rum i det aktuella landet. Om en tillhandahållare skulle välja att i Sverige lagra uppgifter om all global kommunikation, kan det också ifrågasättas om en svensk lagringsskyldighet som omfattade alla dessa uppgifter skulle anses proportionell. Många stora tillhandahållare av Noik lagrar sina uppgifter utanför Sverige och en svensk lagringsskyldighet skulle då inte träffa dem. Att införa en lagringsskyldighet som bara träffar ett fåtal tillhandahållare framstår inte som meningsfullt.

Man skulle också kunna överväga om lagringsskyldigheten kan knytas till sådana Noik-konton som har någon viss koppling till Sverige, såsom att ett svenskt telefonnummer eller en svensk adress har angetts vid registreringen av kontot. Med hänsyn till de stora skillnader i vilka uppgifter som krävs vid registrering av Noik-konton hos olika tillhandahållare framstår denna anknytning som alltför vag och dessutom lätt att kringgå, t.ex. genom att en person lämnar oriktiga uppgifter vid registreringen.

Ett annat alternativ för en avgränsning av lagringsskyldigheten skulle kunna ta sikte på var deltagarna i kommunikationen befinner sig. Det finns annan lagstiftning som anknyter till om avsändare och mottagare befinner sig i Sverige. I lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet anges att inhämtning inte får avse signaler mellan en avsändare och en mottagare som båda befinner sig i Sverige. En förutsättning för detta alternativ är att tillhandahållarna har kunskap om var deltagarna i kommunikationen befinner sig. I vart fall vissa tillhandahållare av Noik har tillgång till uppgifter om kommunikationsutrustningens lokalisering, t.ex. uppgifter om gps-position.

Det finns dock vissa nackdelar med en avgränsning av lagringsskyldigheten som tar sikte på insamling av sådan lokaliseringsinformation. Användarna kan t.ex. stänga av funktioner som visar enhetens lokalisering. Tillhandahållarna av Noik skulle också behöva identifiera var alla kommunikationsutrustningar befinner sig för att avgöra om en lagringsskyldighet föreligger. En sådan identifiering skulle vara resurskrävande för tillhandahållarna och innebära ett stort integritetsintrång.

Ytterligare ett alternativ skulle kunna vara att lagringsskyldigheten knyts till sådan kommunikation som går till, från eller inom Sverige. Lagringsskyldighetens anknytning till Sverige blir enligt vår bedömning tydlig om enbart uppgifter om sådan kommunikation som i sin helhet eller till någon del skett i Sverige ska lagras.

Frågan är då hur tillhandahållare av Noik kan få kunskap om att kommunikationen har skett i Sverige, utan att behöva identifiera exakt var varje kommunikationsutrustning befinner sig.

Det finns i dag många olika lösningar för att lokalisera användares kommunikationsutrustning. Många mjukvarutjänster och webbplatser samlar in sådan information. Det finns inget krav på att tillhandahållare av Noik ska lokalisera var tjänsterna används men tillhandahållarna kan ha ett egenintresse av att veta detta, exempelvis för att kunna rikta reklam eller vid felsökning.

I den mån tillhandahållare av Noik inte har kunskap om huruvida kommunikationen går till, från eller inom Sverige skulle ett sätt för dem att få reda på det kunna vara att utgå från vilken ip-adress som kommunikationen kommer från eller ska till. Tillhandahållare av Noik måste nämligen, i vart fall i något skede, ha information om den ip-adress som användarens enhet använder för att koppla upp sig mot tjänsten för att kommunikationen ska kunna komma till stånd. Som framgår av avsnitt 9.3 är det oftast enkelt att fastställa i vilket land kommunikationen äger rum. Genom tillgången till de ip-adresser som används vid kommunikationen skulle tillhandahållare av Noik alltså på ett automatiserat sätt kunna inhämta uppgifter för att fastställa att kommunikationen till någon del sker i Sverige utan att behöva spåra användarens närmare lokalisering. Trots att uppgifter om i vilket land en ip-adress används inte alltid är 100-procentigt korrekt menar vi att träffsäkerheten är tillräcklig god för att kunna ligga till grund för att avgöra om en lagringsskyldighet föreligger eller inte.

Det kan också noteras att flera tillhandahållare av Noik i sina användarvillkor anger att de samlar in och behandlar uppgifter om ip-adresser och andra lokaliseringsuppgifter. Om tillhandahållarna redan har tillgång till uppgifter om att kommunikationen skickas från eller mottas i Sverige, behöver de förstås inte inhämta ytterligare uppgifter om detta.

Det finns visserligen, som vi berört ovan, möjligheter för användare att dölja sin egentliga ip-adress, exempelvis genom s.k. VPN-tjänster. När en VPN-tjänst används döljs användarens ip-adress för andra än VPN-leverantören. Tillhandahållaren av Noik har då endast tillgång till ip-adressen för den VPN-server som kommunikationen sker via. Det som då skulle styra lagringsskyldigheten är om kommunikationen sker via en VPN-server som är belägen i Sverige. Det finns som tidigare nämnts även andra sätt att dölja sin egentliga ip-adress (se avsnitt 9.3).

Av de alternativ som vi nu övervägt framstår det sistnämnda, dvs. att lagringsskyldigheten knyts till sådan kommunikation som går till, från eller inom Sverige, som den mest rimliga avgränsningen för en lagringsskyldighet.

Det kan konstateras att det nog kan innebära utmaningar för tillsynsmyndigheten att tillse att en lagringsskyldighet av detta slag efterföljs. Att regelefterlevnaden kan vara svår att kontrollera innebär dock inte att en lagringsskyldighet bör undvikas om den är proportionell och absolut nödvändig.

Med hänsyn till att det på relativt enkla sätt går att dölja sin ip-adress, kan det också ifrågasättas om regleringen blir effektiv. De flesta användare torde inte använda sig av verktyg för att dölja sin ip-adress. Utvecklingen synes dock gå mot att ip-adresser döljs i allt större utsträckning. Förekomsten av sådan teknik bör dock inte få någon avgörande betydelse för frågan om en lagringsskyldighet avgränsad via exempelvis ip-adresser. Vi menar att regleringen kan förväntas bli tillräckligt effektiv för att motivera en lagringsskyldighet, särskilt mot bakgrund av att flera tillhandahållare av Noik redan samlar in och behandlar flera olika typer av lokaliseringsuppgifter. Kontrollen av ip-adresser är alltså inte det enda sättet för tillhandahållare av Noik att utröna om kommunikationen har nödvändig anknytning till Sverige och det bör inte i lagstiftning anges en viss metod för att bedöma var kommunikationen sker. Den tekniska utvecklingen kan innebära att det framöver finns andra sätt för tillhanda-

hållare av Noik att få kunskap om huruvida kommunikationen till någon del sker i Sverige. För att lagstiftningen ska vara så teknikneutral som möjligt bör den ange att lagringsskyldigheten omfattar uppgifter om sådan kommunikation som skickas från eller mottas i Sverige.

Tillhandahållare som bör omfattas av lagringsskyldigheten

Utredningens förslag: Lagringsskyldigheten ska träffa den som tillhandahåller allmänt tillgängliga Noik i Sverige.

Utredningens bedömning: Tillhandahållare av allmänt tillgängliga Noik bör inte omfattas av en anmälningsplikt motsvarande den som föreskrivs i 2 kap. 1 § nya LEK.

Tillhandahållare av Noik omfattas inte av någon skyldighet att anmäla sin verksamhet enligt nya LEK. I övervägandena inför införandet av nya LEK gjordes bedömningen att anmälningsplikten inte bör gälla för tillhandahållare av Noik.[28] I skäl 44 i e-kodexen anges att Noik, till skillnad från andra typer av elektroniska kommunikationstjänster, inte utnyttjar allmänna nummerresurser och inte deltar i något allmänt säkerställt interoperabelt ekosystem. Det anges vidare att det därför har bedömts inte vara lämpligt att låta dessa typer av tjänster omfattas av den allmänna auktorisationsordningen. Av artikel 12.2 i e-kodexen följer att den allmänna auktorisationsordningen inte omfattar tillhandahållare av Noik. Dessa omfattas därmed inte heller av den möjlighet till anmälningskrav som ges i artikel 12.3 och som bara gäller företag som omfattas av den allmänna auktorisationen.

Vi gör ingen annan bedömning när det gäller möjligheten att införa en anmälningsplikt för tillhandahållare av Noik. Varken de brottsbekämpande myndigheterna eller PTS har heller gett uttryck för ett påtagligt behov av att låta tillhandahållare av Noik omfattas av skyldigheten att anmäla sin verksamhet. Vi föreslår därför inte att någon skyldighet att anmäla sin verksamhet ska införas för den som tillhandahåller Noik i Sverige.

Utan en skyldighet att anmäla sin verksamhet är det naturligtvis svårt för såväl brottsbekämpande myndigheter som för reglerings-

[28] Se prop. 2021/22:136 s. 127 f.

och tillsynsmyndigheten att veta vilka som tillhandahåller Noik i Sverige. Problemen i detta avseende ska dock inte överdrivas. Redan enligt gällande regler omfattas den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst (dvs. även en allmänt tillgänglig Noik) av reglerna om säkerhet i 8 kap. nya LEK (med undantag av bestämmelsen i 8 kap. 5 § om skyddsåtgärder vid lagring och annan behandling av trafikuppgifter m.m. för brottsbekämpande ändamål). Vidare omfattas tillhandahållare av sådana tjänster av bestämmelserna om integritetsskydd vid behandling av trafikuppgifter och lokaliseringsuppgifter i 9 kap. nya LEK (1–5 §§ och 7–9 §§). Tillhandahållare av Noik omfattas också av reglerna om uppgiftsskyldighet i 10 kap. nya LEK och av vissa regler om tillsyn och sanktionsavgifter enligt 11 respektive 12 kap. nya LEK. Tillhandahållare av Noik omfattas vidare av vissa bestämmelser om tjänster till slutanvändare i 7 kap. nya LEK. PTS har i vissa avseenden föreskriftsrätt i förhållande till tillhandahållare av Noik. Vilka som anses tillhandahålla Noik i Sverige får utvecklas i PTS reglerings- och tillsynsverksamhet och i praxis.

Mot denna bakgrund framstår det som rimligt att en lagringsskyldighet ska träffa den som tillhandahåller Noik i Sverige.

Den nu gällande lagringsskyldigheten för tillhandahållare av elektroniska kommunikationstjänster omfattar endast sådana tjänster som är *allmänt tillgängliga*, dvs. att det finns en allmän möjlighet att ansluta sig till tjänsten. Om tjänsten tillhandahålls öppet på marknaden och därmed är tillgänglig för alla som är villiga att följa villkoren för tillhandahållandet, tyder det på att tjänsten är allmänt tillgänglig. Vår bedömning är att även en lagringsskyldighet för tillhandahållare av Noik bör begränsas till allmänt tillgängliga tjänster. Om lagringsskyldigheten skulle gälla även sådana tjänster som inte är allmänt tillgängliga, skulle lagringsskyldigheten kunna träffa sådana kommunikationstjänster som t.ex. finns inom polisen och Försvarsmakten men även sådana tjänster som myndigheter, företag eller privatpersoner kan skapa för att använda bara inom en mycket begränsad krets. Det ska också noteras att många av de regler som införts i nya LEK, t.ex. de ovan nämnda reglerna om säkerhet och integritetsskydd vid behandling av trafik- och lokaliseringsuppgifter, enbart gäller för allmänt tillgängliga elektroniska kommunikationstjänster. Att införa en lagringsskyldighet även för icke allmänt tillgängliga Noik skulle innebära att regelverket i dessa avseenden måste ses över.

Det skulle inte heller vara rimligt att ålägga sådana tillhandahållare de skyldigheter som följer av bestämmelserna.

Sådana tjänster som möjliggör interpersonell och interaktiv kommunikation enbart som en extrafunktion av mindre betydelse och som är direkt kopplad till en annan tjänst omfattas som nämnts inte av definitionen av Noik. Att överväga en sådan skyldighet omfattas inte, som också sagts ovan, av våra direktiv. Någon lagringsskyldighet avseende tillhandahållare av sådana tjänster bör därför inte föreslås inom ramen för denna utredning. Som nämnts i avsnitt 9.3 bedömer vi, mot bakgrund av vad som uttalas i skäl 17 i e-kodexen, att utrymmet är mycket begränsat för vad som kan anses vara en sådan extrafunktion av mindre betydelse.

Det kan i detta sammanhang noteras att elektroniska kommunikationstjänster träffas av definitionen av informationssamhällets tjänster enligt artikel 1 i anmälningsdirektivet. Definitionen omfattar alla tjänster som vanligtvis utförs mot ersättning på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare. Bestämmelser om informationssamhällets tjänster finns bl.a. i e-handelsdirektivet. E-handelsdirektivet syftar till att säkerställa den fria rörligheten för informationssamhällets tjänster mellan medlemsstaterna och är införlivat i svensk rätt främst genom lagen (2002:562) om elektronisk handel och andra informationssamhällets tjänster.

Enligt artikel 1.5 b i e-handelsdirektivet ska direktivet dock inte tillämpas på frågor beträffande informationssamhällets tjänster som omfattas av direktiv 97/66/EG av den 15 december 1997 om behandling av personuppgifter och skydd för privatlivet inom telekommunikationsområdet. Det senare direktivet är ersatt av e-dataskyddsdirektivet. Enligt artikel 19 i e-dataskyddsdirektivet ska hänvisningar till det upphävda direktivet anses som hänvisningar till e-dataskyddsdirektivet.

Bestämmelserna i e-handelsdirektivet utgör således inte något hinder mot att ålägga den som tillhandahåller en allmänt tillgänglig Noik i Sverige, och som är etablerad i en annan medlemsstat, en lagringsskyldighet med anknytande regler.

Vi återkommer till frågan om våra förslag omfattas av anmälningsskyldighet för tekniska föreskrifter enligt anmälningsdirektivet i avsnitt 13.

Lagringsskyldighetens omfattning

Utredningens förslag: Lagringsskyldighetens omfattning för tillhandahållare av allmänt tillgängliga Noik ska motsvara vad som enligt våra förslag ska gälla för andra tillhandahållare av elektroniska kommunikationstjänster. Lagringsskyldigheten vid geografiskt riktad lagring ska omfatta uppgifter som genereras eller behandlas vid samtal eller meddelandehantering samt lokaliseringsuppgifter som inte är trafikuppgifter. Lagringsskyldigheten vid nationell säkerhetslagring och utökad riktad lagring får omfatta samma uppgifter.

Samma lagringstider ska gälla för uppgifterna oavsett om de lagras av tillhandahållare av Noik eller av andra tillhandahållare.

Lagringstiden ska räknas från den dag kommunikationen avslutades. Om tillhandahållarna saknar uppgift om när kommunikationen avslutades, ska lagringstiden räknas från den dag då uppgiften genererades.

I fråga om lokaliseringsuppgifter som inte är trafikuppgifter ska lagringstiden räknas från den dag uppgifterna genererades och i fråga om meddelanden hos en Noik ska lagringstiden räknas från den dag meddelandet skickades.

Dagens lagringsskyldighet enligt 9 kap. 19 § nya LEK omfattar uppgift om abonnemang och annan uppgift som angår ett särskilt meddelande, dvs. trafikuppgifter (se avsnitt 6.6.2), som är nödvändiga för vissa preciserade syften. Dessa är formulerade som uppgifter 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.

Skyldigheten att lagra uppgifter omfattar i dag och enligt våra förslag i avsnitten 6, 7 och 8 uppgifter som genereras eller behandlas i tillhandahållarens verksamhet. Det betyder att tillhandahållaren inte har någon skyldighet att införskaffa uppgifter som denne annars inte genererar eller behandlar. Däremot ska en uppgift lagras så fort den har funnits hos tillhandahållaren, även om det bara rör sig om en ytterst kort tid.[29] Se även avsnitt 7.3.6.

[29] Se prop. 2010/11:46 s. 77.

Många Noik motsvarar funktionsmässigt sådan telefonitjänst och meddelandehantering som tillhandahålls av teleoperatörerna. Utgångspunkten bör vara att en lagringsskyldighet för tillhandahållare av allmänt tillgängliga Noik ska omfatta motsvarande uppgifter och att samma princip ska gälla om att tillhandahållaren inte har någon skyldighet att införskaffa uppgifter som denne annars inte genererar eller behandlar. Det kan vara problematiskt att tillhandahållare av Noik har begränsad eller ibland ingen information om användaren av tjänsten. Vi bedömer dock att det i nuläget inte finns anledning att införa ett krav på identifiering av användaren (jfr avsnitt 9.3.6). Det skulle också vara förenat med svårigheter om ett sådant krav skulle gälla exempelvis endast för användare som i Sverige registrerar ett Noik-konto, eftersom användaren ofta kan välja att registrera uppgifter med koppling till ett annat land, t.ex. med angivande av ett utländskt mobilnummer.

Begreppet *telefonitjänst* i 1 kap. 7 § nya LEK kan dock inte användas beträffande Noik, eftersom en telefonitjänst i nya LEK definieras som en elektronisk kommunikationstjänst som innebär en möjlighet att ringa upp eller ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan.

I 1 kap. 7 § nya LEK definieras *meddelandehantering* som 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. Med *samtal* avses enligt samma lagrum en förbindelse genom en allmänt tillgänglig interpersonell kommunikationstjänst som möjliggör talkommunikation i båda riktningarna.

Begreppen samtal och meddelandehantering bör därför användas för att reglera lagringsskyldigheten för tillhandahållare av allmänt tillgängliga Noik. Därutöver ska, enligt våra förslag i avsnitt 7 och 8, lokaliseringsuppgifter som inte är trafikuppgifter (dvs. uppgifter som genereras utan att någon kommunikation äger rum) omfattas av geografiskt riktad lagring. Sådana uppgifter får också omfattas av nationell säkerhetslagring och utökad riktad lagring.

Vilka uppgifter om abonnemang, trafik- och lokaliseringsuppgifter som genereras och behandlas i tillhandahållarens verksamhet kan, som nämnts ovan, skilja sig åt mellan olika tjänster. Det är rimligt att anta att tillhandahållare av Noik i något skede har tillgång till uppgifter som är nödvändiga för att spåra och identifiera kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och

varaktighet för kommunikationen och typ av kommunikation. Vissa tillhandahållare har också tillgång till uppgifter om vilken kommunikationsutrustning som har använts. Genom tillgången till användarnas ip-adresser kan tillhandahållaren också normalt sett få tillgång till ungefärlig lokalisering av kommunikationsutrustningen. Till skillnad från teleoperatörerna har tillhandahållare av Noik inte alltid tillgång till lokaliseringsuppgifter via basstationer. I vart fall vissa tillhandahållare av Noik har emellertid tillgång till uppgifter om kommunikationsutrustningens lokalisering.

Det kan konstateras att i de fall tillhandahållaren har tillgång till lokaliseringsuppgifter, exempelvis kommunikationsutrustningens gps-position, kan dessa uppgifter vara mer specifika än vad lokaliseringsuppgifter är som fås genom att en mobiltelefon kopplar upp sig mot en viss cell på en basstation. Lokaliseringsuppgifter hos en tillhandahållare av Noik kan alltså innebära ett större integritetsintrång för enskilda. Den enskilde användaren kan dock välja att inte använda sig av sådana funktioner som visar kommunikationsutrustningens positionering, eftersom dessa funktioner normalt inte behövs för själva kommunikationstjänsten.

De brottsbekämpande myndigheternas stora nytta och deras påtagliga behov av uppgifter om elektronisk kommunikation föreligger, som tidigare nämnts, oberoende av vilken typ av tillhandahållare som ansvarar för kommunikationstjänsten. Vi har i avsnitt 6, 7 och 8 föreslagit regler om lagring i syfte att skydda den nationella säkerheten samt lämnat ett förslag på hur riktad lagring i syfte att bekämpa grov brottslighet skulle kunna utformas för de tillhandahållare som omfattas av dagens lagringsskyldighet. Våra förslag bygger, liksom dagens lagringsskyldighet, på att uppgifter ska lagras för vissa preciserade syften. Vi ser inget skäl att, för tillhandahållare av allmänt tillgängliga Noik, vare sig inskränka eller utvidga för vilka preciserade syften lagringsskyldigheten ska gälla. Detta oavsett om alla tillhandahållare av allmänt tillgängliga Noik genererar eller behandlar samtliga typer av uppgifter som kan omfattas av lagringsskyldighet. Om en viss typ av uppgift inte genereras eller behandlas i tillhandahållarens verksamhet, omfattas den inte av lagringsskyldigheten. Tillhandahållaren behöver alltså inte inhämta uppgiften för att uppfylla lagringsskyldigheten, se avsnitt 7.3.6.

Lagringsskyldigheten bör, som nämnts ovan, omfatta sådana uppgifter som genereras och behandlas vid samtal och meddelandehantering samt lokaliseringsuppgifter som inte är trafikuppgifter.

Våra förslag innebär alltså följande lagringsskyldighet för tillhandahållare av Noik när kommunikationen sker till, från eller inom Sverige:

- Skyldighet att lagra uppgifter om abonnemang och registrerad användare (se avsnitt 6),
- skyldighet att lagra de uppgifter som framgår av ett föreläggande om nationell säkerhetslagring såsom 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 (se avsnitt 7),
- skyldighet att lagra ovan uppräknade uppgifter i de kommuner som omfattas av geografiskt riktad lagring (se avsnitt 8), samt,
- skyldighet att lagra ovan uppräknade uppgifter i den mån de omfattas av föreläggande om utökad riktad lagring avseende plats, område, person eller teknik (se avsnitt 8).

Lagringsskyldighetens omfattning för tillhandahållare av allmänt tillgängliga Noik bör alltså motsvara vad som enligt våra förslag ska gälla för andra tillhandahållare av elektroniska kommunikationstjänster.

Tillhandahållare av Noik får i regel utgå från ip-adresser, och i förekommande fall uppgifter om gps-position eller motsvarande uppgifter, för att verkställa lagringsskyldigheten. I regel bör det inte föranleda större svårigheter för tillhandahållare av Noik att fastställa var en kommunikationsutrustning finns än vad som är fallet för traditionella teleoperatörer som utgår från uppgifter om telemastpositioner. Det har sin grund i att tillhandahållare av Noik ytterst måste ha förmåga att skicka information till och ta emot information från den som använder Noik. Det saknar således betydelse om förmedling av information sker med stöd av ip-adresser eller master för telekommunikation. Som vi redogjort för i avsnitt 9.3 kan det dock i vissa situationer vara svårt att fastställa om en kommunikationsutrustning finns inom ett område som omfattas av lagringsskyldigheten, särskilt

om den geografiska avgränsningen är snäv. Så kan framför allt vara fallet om en tillhandahållare av Noik föreläggs att lagra uppgifter avseende en viss plats.

Våra förslag innebär inte att tillhandahållarna ska inhämta ytterligare uppgifter för att kunna fastställa lagringsskyldigheten. Om en tillhandahållare av Noik varken med hjälp av ip-adress eller kommunikationsutrustningens lokaliseringsuppgifter kan fastställa om utrustningen finns i ett område som omfattas av riktad lagring, saknas det förutsättningar för lagring.

Vi påminner dock i detta sammanhang om att en tillhandahållare av Noik som behandlar en ip-adress för att förmedla sina tjänster inte kan undandra sig lagringsskyldighet genom att radera, förstöra eller maska trafikuppgifterna, ens om det sker automatiskt och omedelbart (se avsnitt 7.3.6). Detsamma gäller de lokaliseringsuppgifter som tjänsteleverantören har tillgång till.

Vi föreslår att samma lagringstider ska gälla för uppgifterna oberoende om de lagras av tillhandahållare av Noik eller av andra tillhandahållare. Lagringstiden för kommunikation via Noik bör också normalt räknas från den dag kommunikationen avslutades eller, i fråga om lokaliseringsuppgifter som inte är trafikuppgifter, från den dag uppgifterna genererades.

Att fastställa när kommunikation har avslutats vid tal- eller videomötestjänster bör vara oproblematiskt. Annorlunda förhåller det sig emellertid i fråga om meddelanden. Ett meddelande skickat via Noik kan, i motsats till traditionella meddelanden som skickats via en teleoperatör, tas emot vid flera olika tillfällen. Så kan exempelvis vara fallet om användaren har tjänsten kopplad till flera olika enheter, eller om användaren köper en ny enhet eller återställer en gammal enhet. Det skulle, åtminstone i teorin, kunna innebära att lagringstiden fortsätter löpa utan inskränkning i tid. Lagringstiden bör därför inte utgå från när ett meddelande togs emot med mindre än att tillhandahållare av Noik kan fastställa att det är första gången ett meddelande tas emot. En Noik kan emellertid, som framgår av avsnitt 9.3, vara utformad på många olika sätt. Det är dock inte självklart att alla Noik har särskild funktionalitet för att fastställa när ett meddelande har tagits emot för första gången. Det framstår som en alltför långtgående åtgärd att ställa krav att tillhandahållare av Noik ska utveckla sådan funktionalitet i sina tjänster.

Ett annat sätt att beräkna lagringstiden är att utgå från tidpunkten när ett meddelande skickades. Mot en sådan lösning talar att det kan uppstå situationer då lagringstiden redan har löpt ut när meddelandet mottas. Så kan exempelvis ske om mottagaren av ett meddelande inte tar del av detta förrän lång tid efter det skickades. Vi gör, trots detta, bedömningen att lagringstiden bör beräknas från tidpunkten när ett meddelande skickades. Det har sin grund i att det i de allra flesta fallen skulle vara oproblematiskt att fastställa hur lagringstiden ska beräknas. Härutöver vore alternativet att låta lagringstiden börja löpa på nytt varje gång ett meddelande tas emot vilket vore en oskälig börda på tillhandahållare av Noik.

Sammanfattning m.m. av våra förslag om en lagringsskyldighet för tillhandahållare av Noik

Vi föreslår sammanfattningsvis att tillhandahållare av allmänt tillgängliga Noik ska omfattas av skyldigheten att lagra vissa uppgifter om elektronisk kommunikation. Lagringsskyldigheten avser sådan 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 motsvara det vi föreslår ska gälla för övriga lagringsskyldiga, dvs. enligt våra förslag om lagring av abonnemangsuppgifter, nationell säkerhetslagring och riktad lagring.

För ett meddelade via Noik bör lagringstiden dock räknas från dagen då meddelandet skickades. Därefter ska uppgifterna genast utplånas om det inte dessförinnan har kommit in en begäran om utlämnande av uppgifter eller ett bevarandeföreläggande. I dessa fall ska den lagringsskyldige fortsätta lagra uppgifterna till dess de har lämnats ut eller, vid ett bevarandeföreläggande, tiden för bevarande har löpt ut. Detta bör regleras genom tillägg i 9 kap. 22 § andra stycket nya LEK.

Vi återkommer nedan till vilka övriga bestämmelser kopplade till skyldigheten att lagra och ge tillgång till uppgifter om elektronisk kommunikation som bör gälla för tillhandahållare av Noik.

9.6.2 En tystnadsplikt för tillhandahållare av Noik

Utredningens förslag: Tillhandahållare av Noik ska omfattas av sådan tystnadsplikt som enligt nya LEK gäller vid tillhandahållande av andra elektroniska kommunikationstjänster. Tystnadsplikten för uppgift om abonnemang, innehållet i ett elektroniskt meddelande och trafikuppgift ska gälla vid kommunikation som till någon del sker i Sverige. Tystnadsplikten som hänför sig till användningen av vissa hemliga tvångsmedel och andra åtgärder ska gälla för tillhandahållare av Noik i den mån åtgärderna kan eller genom våra förslag kommer att kunna vidtas hos sådana tillhandahållare.

Vi har ovan konstaterat att tillhandahållare av allmänt tillgängliga Noik bör omfattas av en skyldighet att lagra vissa uppgifter om elektronisk kommunikation i syfte att under föreskrivna förutsättningar ge de brottsbekämpande myndigheterna tillgång till uppgifterna. I detta avsnitt överväger vi om det bör gälla någon tystnadsplikt för tillhandahållare av Noik.

I 9 kap. 31 § nya LEK regleras en tystnadsplikt för den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst som inte är en Noik har fått del av eller tillgång till vissa närmare angivna uppgifter. Tystnadsplikten gäller för

- uppgift om abonnemang,
- innehållet i ett elektroniskt meddelande, och
- annan uppgift som angår ett särskilt elektroniskt meddelande (vi har i avsnitt 6.6.2 föreslagit att detta begrepp ska ersättas med begreppet trafikuppgift).

Tystnadsplikten 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. Tystnadsplikten i fråga om en uppgift om abonnemang och trafikuppgift gäller inte heller i förhållande till innehavaren av ett abonnemang som har använts för ett elektroniskt meddelande.

För ovan nämnda tillhandahållare regleras en tystnadsplikt i 9 kap. 32 § nya LEK för uppgifter som hänför sig till användning av vissa hemliga tvångsmedel och andra åtgärder för att i brottsbekämpande syfte hämta in uppgifter om elektronisk kommunikation.

Tystnadsplikten gäller även för en begäran enligt 9 kap. 33 § första stycket 2 nya LEK om utlämnande av uppgift om abonnemang, om begäran gäller brottslig verksamhet eller misstanke om brott, till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som har att ingripa mot brottet eller den brottsliga verksamheten. Tystnadsplikten gäller även för ett frysningsföreläggande enligt 27 kap. 16 § RB och för en begäran enligt 9 kap. 33 § fösta stycket 5 nya LEK om utlämnande av en uppgift om tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster. Tystnadsplikten gäller även för en angelägenhet som avser inhämtning av signaler i elektronisk form enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Bestämmelserna om tystnadsplikt fördes över från 6 kap. gamla LEK utan någon ändring i sak. Med hänsyn till att definitionen av elektronisk kommunikationstjänst i nya LEK utvidgades till att även omfatta Noik infördes i bestämmelserna om tystnadsplikt ett uttryckligt undantag för just sådana kommunikationstjänster. Regeringen anförde att bestämmelserna om tystnadsplikt inte omfattas av e-kodexen och att den ändrade definitionen av elektronisk kommunikationstjänst inte bör utvidga tillämpningsområdet för bestämmelserna till tillhandahållare av Noik utan närmare överväganden. Eftersom det saknades underlag för sådana överväganden menade regeringen att en utvidgning av tillämpningsområdet för bestämmelserna inte borde göras inom ramen för genomförandet av e-kodexen.[30]

Bestämmelserna om tystnadsplikt infördes redan i den äldre telelagen[31] i samband med bolagiseringen av Televerket. Tidigare fanns föreskrifter om sekretess för vissa uppgifter hos Televerket. Sekretess gällde bl.a. för uppgift som angår ett särskilt telefonsamtal eller ett annat meddelande och för uppgift som angår enskildas förbindelser med samfärdselverksamheten (t.ex. uppgifter om telefonnummer).[32] I den då gällande sekretesslagen fanns också bestämmelser om

[30] Se prop. 2021/22:136 s. 329.
[31] Telelagen (1993:597).
[32] Se dåvarande 9 kap. 8 § sekretesslagen (1980:100).

begränsningar i sekretessen, bl.a. att sekretessen inte hindrar att uppgifter om en enskilds adress, telefonnummer och arbetsplats lämnas ut till en myndighet om uppgiften behövs för delgivning och att sekretess i vissa fall inte hindrar att en uppgift som angår misstanke om brott lämnas till åklagarmyndighet, polismyndighet eller annan myndighet som har att ingripa mot brottet.[33]

När verksamheten i Televerket överfördes till aktiebolag var det nödvändigt att den reglering som behövs till skydd för den enskildes integritet utformades på ett annat sätt än genom bestämmelserna i den då gällande sekretesslagen. Regleringen av enskild verksamhet behövde bygga på bestämmelser om tystnadsplikt i stället för på bestämmelser om inskränkningar i offentlighetsprincipen.[34]

Bestämmelser om tystnadsplikt i enskild televerksamhet infördes i telelagen för uppgift om teleabonnemang, innehållet i ett telemeddelande och annan uppgift som angår ett särskilt sådant meddelande. När det gällde myndigheters behov av uppgifter om abonnemang för delgivning och i fråga om brottsutredande myndigheters behov av uppgifter som angår misstanke om brott och som omfattas av tystnadsplikten infördes i telelagen bestämmelser om en uppgiftsskyldighet. Det klargjordes också att prövningen av om en uppgift skall lämnas ut, till skillnad mot vad som gäller vid sekretessprövning, i samtliga fall ska göras av den begärande myndigheten, eftersom det inte bedömdes lämpligt att de enskilda teleföretagen skulle göra denna prövning.[35]

Reglerna om tystnadsplikt och uppgiftsskyldighet fördes över till gamla LEK med vissa ändringar i terminologin.

En tystnadsplikt enligt 9 kap. 31 § nya LEK

Som framgår av avsnitt 3 är skyddet för intrång i enskildas privatliv, inklusive enskildas kommunikation, reglerat i internationella konventioner, EU:s rättighetsstadga och svensk grundlag. Tystnadsplikten vid elektronisk kommunikation enligt 9 kap. 31 § nya LEK syftar till att skydda enskildas kommunikation mot obehörigt intrång. Vi ser inga skäl till att inte även tillhandahållare av Noik skulle omfattas av en sådan tystnadsplikt, i synnerhet eftersom Noik numera omfattas av definitionen elektronisk kommunikationstjänst i nya LEK.

[33] Se dåvarande 14 kap. 2 § tredje och fjärde styckena sekretesslagen (1980:100).
[34] Se prop. 1992/93:200 s. 162 f.
[35] Se a. prop. s. 163 f.

Behovet av skydd för enskildas kommunikation gör sig lika starkt gällande oavsett vem som tillhandahåller kommunikationstjänsten. Bestämmelserna i 9 kap. 31 § nya LEK bör därför gälla även för tillhandahållare av Noik och det undantag för sådana kommunikationstjänster som regleras i paragrafen bör tas bort. Vi har i avsnitt 7.3.9 föreslagit att tystnadsplikten ska avse även lokaliseringsuppgifter som inte är trafikuppgifter. Sådan tystnadsplikt bör gälla även för tillhandahållare av Noik.

Liksom i fråga om en lagringsskyldighet för tillhandahållare av Noik behöver en reglering av tystnadsplikten ha en viss anknytning till Sverige. Vi föreslår att samma anknytning till Sverige ska gälla för tystnadsplikten som för lagringsskyldigheten, dvs. att den knyts till sådan kommunikation som sker till, från eller inom Sverige. Tystnadsplikten ska alltså gälla för den som, i samband med tillhandahållande av Noik, har fått del av eller tillgång till uppgift om abonnemang, innehållet i ett elektroniskt meddelande och trafikuppgift när det gäller kommunikation som sker från eller mottas i Sverige samt för lokaliseringsuppgifter som inte är trafikuppgifter beträffande sådana uppgifter i Sverige.

Tystnadsplikten för tillhandahållare av Noik bör, liksom vid tillhandahållandet av andra elektroniska kommunikationstjänster, gälla för alla sådana tillhandahållare och alltså inte enbart för sådana som är allmänt tillgängliga.

En följd av vårt förslag om att tillhandahållare av Noik ska omfattas av tystnadsplikten är att det inte finns någon möjlighet för de brottsbekämpande myndigheterna att använda andra straffprocessuella tvångsmedel, såsom husrannsakan med efterföljande beslag, för att få åtkomst till sådana uppgifter som omfattas av tystnadsplikten, se avsnitt 5.2. Det finns dock inget som hindrar att ett beslut om husrannsakan används, dels för att få åtkomst till sådana uppgifter hos andra än de tillhandahållare som omfattas av tystnadsplikten, dels för att hos en tillhandahållare få åtkomst till andra uppgifter än de som omfattas av tystnadsplikten. Enligt vår uppfattning bör inte heller en tystnadsplikt för tillhandahållare Noik förhindra åtkomst till innehåll i en sådan tjänst genom användning av genomsökning på distans. Till skillnad mot vad som är fallet vid en husrannsakan hos en tillhandahållare av Noik, är det den vars inloggningsuppgifter eller utrustning som används, som är föremål för tvångsmedlet. Verkställigheten kan inte heller sägas ske hos tillhandahållaren av tjänsten.

En tystnadsplikt enligt 9 kap. 32 § nya LEK

Som nämnts ovan avser tystnadsplikten som regleras i 9 kap. 32 § nya LEK uppgifter som hänför sig till användning av vissa hemliga tvångsmedel och andra åtgärder för att i brottsbekämpande syfte hämta in uppgifter om elektronisk kommunikation. Tystnadsplikten enligt denna bestämmelse gäller även för uppgifter som hänför sig till inhämtning av signaler i elektronisk form enligt lagen om signalspaning i försvarsunderrättelseverksamhet. Tystnadsplikten enligt denna paragraf syftar till att skydda såväl den brottsbekämpande verksamheten respektive försvarsunderrättelseverksamheten som uppgifter om enskildas personliga och ekonomiska förhållanden som förekommer i sådan verksamhet.

Vi har i avsnitt 7.3.9 föreslagit att tystnadsplikten enligt 9 kap. 32 § nya LEK ska omfatta en angelägenhet om nationell säkerhetslagring. I avsnitt 8.3.7 har vi föreslagit motsvarande tystnadsplikt för en angelägenhet om utökad riktad lagring. Nedan följer en genomgång av de bestämmelser i offentlighets- och sekretesslagen som i offentlig verksamhet begränsar handlingsoffentligheten och yttrandefriheten för nu aktuella uppgifter. Tanken med genomgången är att belysa den närmare materiella innebörden av tystnadsplikten i 9 kap. 32 § nya LEK i förhållande till våra förslag.

Enligt 2 kap. 1 § TF har, till främjande av ett fritt meningsutbyte och en fri och allsidig upplysning och ett fritt konstnärligt skapande, var och en rätt att ta del av allmänna handlingar. Rätten får dock begränsas bl.a. om det krävs med hänsyn till rikets säkerhet eller dess förhållande till en annan stat eller en mellanfolklig organisation, intresset att förebygga eller beivra brott och skyddet för enskildas personliga eller ekonomiska förhållanden (2 kap. 2 § första stycket TF). En motsvarande reglering när det gäller yttrandefrihet finns i 2 kap. 1, 20 och 23 §§ RF.

Sekretess gäller för uppgift som hänför sig till förundersökning i brottmål eller till angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs (18 kap. 1 § OSL). I 18 kap. 2 § OSL regleras sekretessen i de brottsbekämpande myndigheternas underrättelseverksamhet. För uppgift som hänför sig till sådan verksamhet gäller sekretess bl.a. om det inte

står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas. Sekretessen enligt 18 kap. 1 och 2 §§ gäller i annan verksamhet än som där avses hos en myndighet för att biträda en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen med att förebygga, uppdaga, utreda eller beivra brott samt hos tillsynsmyndigheten i konkurs och hos Kronofogdemyndigheten för uppgift som angår misstanke om brott (18 kap. 3 § OSL). För uppgifter i verksamhet som avser rättsligt samarbete på begäran av en annan stat eller en mellanfolklig domstol, gäller sekretess bl.a. för uppgift som hänför sig till en angelägenhet som angår tvångsmedel, om det kan antas att det varit en förutsättning för den andra statens eller den mellanfolkliga domstolens begäran att uppgiften inte skulle röjas (18 kap. 17 § OSL).

I 35 kap. OSL regleras sekretess till skydd för enskild i verksamhet som syftar till att förebygga eller beivra brott, m.m. Enligt 35 kap. 1 § gäller sekretess bl.a. 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 angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott eller annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen.

I 15 kap. 2 § OSL regleras försvarssekretessen. Sekretess gäller för uppgift som rör verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs.

Enligt 38 kap. 4 § OSL gäller sekretess hos Försvarsmakten i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten samt hos Försvarets radioanstalt i underrättelse- och säkerhetsverksamheten för uppgift om en enskilds personliga eller ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider skada eller men.

Tystnadsplikten i 9 kap. 32 § nya LEK syftar alltså till att i enskild verksamhet skydda sådana uppgifter som i offentlig verksamhet om-

fattas av sekretess enligt de ovan nämna bestämmelserna i offentlighets- och sekretesslagen.

I den mån sådana hemliga tvångsmedel och andra åtgärder som regleras i 9 kap. 32 § nya LEK kan eller genom våra förslag kommer att kunna vidtas i förhållande till en tillhandahållare av Noik, är det rimligt och konsekvent att tystnadsplikten enligt 9 kap. 32 § nya LEK bör gälla för dessa tillhandahållare. Om ingen tystnadsplikt skulle gälla, finns det inte något rättsligt hinder mot att dessa tillhandahållare till obehöriga röjer sådana uppgifter som omfattas av dagens tystnadsplikt för andra tillhandahållare av elektroniska kommunikationsnät och elektroniska kommunikationstjänster. Det skulle kunna omintetgöra syftet med inhämtningen av uppgifterna, t.ex. om det blev känt vem som är föremål för inhämtningen. Det skulle också kunna innebära skada eller men för enskilda om uppgifter om deras personliga eller ekonomiska förhållanden röjs.

Tystnadsplikten enligt denna paragraf uppkommer endast i den mån svenska myndigheter har rätt att inhämta uppgifter med stöd av de bestämmelser som anges i paragrafen. I följande avsnitt prövar vi i vilken mån uppgifter om elektronisk kommunikation kan eller bör kunna inhämtas från tillhandahållare av Noik.

I likhet med 9 kap. 31 § nya LEK bör 9 kap. 32 § nya LEK gälla för alla tillhandahållare av Noik och alltså inte enbart för sådana som är allmänt tillgängliga.

Det ska i detta sammanhang noteras att den tystnadsplikt som följer av 9 kap. 31 och 32 §§ nya LEK i vissa avseenden inskränker meddelarfriheten, dvs. rätten enligt 1 kap. 1 och 7 §§ TF och 1 kap. 1 och 10 §§ YGL att meddela och offentliggöra uppgifter (se 44 kap. 4 § OSL).

Sammanfattning m.m. av våra förslag angående tystnadsplikt

Sammanfattningsvis föreslår vi att tystnadsplikten enligt 9 kap. 31 § nya LEK ska gälla för tillhandahållare av Noik när det gäller uppgifter om sådan kommunikation som sker till, från eller inom Sverige och när det gäller lokaliseringsuppgifter som inte är trafikuppgifter i Sverige. Vi vill för tydlighetens skull upprepa att tystnadsplikten för tillhandahållare av Noik innefattar även innehållet i ett elektroniskt meddelande.

Vi föreslår också att tystnadsplikten enligt 9 kap. 32 § nya LEK ska gälla för tillhandahållare av Noik i den mån de hemliga tvångsmedel och de andra åtgärder som avses i bestämmelsen kan eller genom våra förslag kommer kunna vidtas hos tillhandahållare av Noik. Vi har i avsnitt 7.3.9 och 8.3.7 föreslagit att tystnadsplikten enligt 9 kap. 32 § nya LEK ska omfatta angelägenheter om nationell säkerhetslagring och om utökad riktad lagring. Vi föreslår att denna tystnadsplikt ska gälla även för tillhandahållare av Noik.

Våra förslag förutsätter att en ändring görs i 9 kap. 31 § LEK så att även den som i samband med tillhandahållandet av Noik har fått tillgång till de i paragrafen angivna uppgifterna ska omfattas av förbudet mot att obehörigen föra vidare eller utnyttja det som han eller hon har fått del av eller tillgång till. Någon ändring behöver inte göras i 9 kap. 32 § nya LEK för att tillhandahållare av Noik ska omfattas av den där reglerade tystnadsplikten, eftersom bestämmelsen hänvisar till de tillhandahållare som regleras i 9 kap. 31 § nya LEK.

9.6.3 Åtkomsten till lagrade uppgifter hos tillhandahållare av Noik

Nedan överväger vi i vilken mån lagrade uppgifter om elektronisk kommunikation kan eller bör kunna hämtas in från tillhandahållare av Noik.

Med lagrade uppgifter avses alla uppgifter som finns lagrade av någon anledning, dvs. både sådana uppgifter som finns lagrade på grund av reglerna om datalagring i 9 kap. nya LEK och sådana som lagrats av annan anledning. Även sådana abonnemangs-, trafik- eller lokaliseringsuppgifter som tillhandahållaren lagrar för egna ändamål, som uppgifter som hos tillhandahållaren behandlas för fakturering, kan inhämtas med stöd av reglerna som medger åtkomst till uppgifter.[36] Uppgifter som lagras med stöd av 9 kap. 19 § nya LEK får dock behandlas endast för att lämnas ut för brottsbekämpande ändamål (se 9 kap. 21 § nya LEK). Våra förslag ovan innebär att motsvarande ska gälla för uppgifter som lagras i syfte att bekämpa grov brottslighet (enligt 9 kap. 19 c och 19 d §§ nya LEK). Vi har vidare föreslagit att uppgifter som lagras i syfte att skydda den nationella säkerheten (med stöd av 9 kap. 19 b § nya LEK) får behandlas endast för att läm-

[36] Se t.ex. SOU 2017:75 s. 283.

nas ut enligt den av oss föreslagna lagen om lagring och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda nationell säkerhet och att detta regleras i ett andra stycke i 9 kap. 21 § nya LEK.

Det kan redan här påpekas att uppgifterna inte nödvändigtvis kommer att vara lagrade i Sverige. Om de uppgifter som ska hämtas in av de brottsbekämpande myndigheterna inte lagras i Sverige, kan det uppstå en konflikt mellan de svenska reglerna om inhämtning av uppgifter och reglerna om utlämnande av uppgifter i det land som uppgifterna finns. Ett inhämtande av uppgifter kan kräva att någon form av rättslig hjälp begärs från detta land, för det fall en tjänsteleverantör inte vill samarbeta.

Vi har i avsnitt 5.3 redogjort för bestämmelserna som ger de brottsbekämpande myndigheterna tillgång uppgifter om elektronisk kommunikation. Vi återkommer i avsnitt 10.4.3 till frågan om en anpassningsskyldighet för tillhandahållare av Noik.

Tillgången till abonnemangsuppgifter m.m. hos tillhandahållare av Noik

Utredningens förslag: Skyldigheterna att lämna ut uppgifter om abonnemang m.m. med stöd av nya LEK ska gälla för samtliga tillhandahållare av elektroniska kommunikationsnät och elektroniska kommunikationstjänster.

I 9 kap. 33 § nya LEK föreskrivs en skyldighet för den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst som inte är en Noik att på begäran lämna ut uppgifter om abonnemang och i vissa fall trafikuppgifter till olika myndigheter och till regionala alarmeringscentraler. Som framgår av föregående avsnitt utgör denna bestämmelse ett undantag från den tystnadsplikt som gäller för tillhandahållarna.

Utlämnande av uppgifter i brottsbekämpande syfte

Enligt 9 kap. 33 § första stycket 2 nya LEK är tillhandahållare av elektroniska kommunikationsnät och elektroniska kommunikationstjänster som inte är Noik skyldiga att på begäran lämna ut uppgifter om

abonnemang som gäller brottslig verksamhet eller misstanke om brott till brottsbekämpande myndigheter. De brottsbekämpande myndigheternas tillgång till uppgifter enligt denna bestämmelse anses, som ovan nämnts, inte utgöra ett hemligt tvångsmedel. Uppgifter om abonnemang har inte ansetts vara särskilt integritetskänsliga, eftersom de endast ger uppgift om att personen är abonnent eller användare av en viss tjänst eller av en tillfällig identifierare såsom en dynamisk ip-adress vid en viss tidpunkt. De kan inte likställas med trafik- och lokaliseringsuppgifter, av vilka man kan dra mer precisa slutsatser om personers privatliv.

De brottsbekämpande myndigheterna har lika stor nytta och samma påtagliga behov av uppgifter om abonnemang oavsett vem som tillhandahåller den elektroniska kommunikationstjänsten. En skyldighet för tillhandahållare av Noik att lämna ut uppgifter om abonnemang till brottsbekämpande myndigheter innebär inte någon större inskränkning i den enskildes fri- och rättigheter än vad en sådan skyldighet för andra tillhandahållare av elektroniska kommunikationstjänster innebär. Skyldigheten att lämna ut abonnemangsuppgifter enligt den aktuella bestämmelsen bör därför omfatta även tillhandahållare av Noik. En annan sak är att tillhandahållare av Noik inte alltid har tillgång till sådana uppgifter om sina användare som teleoperatörerna har om sina användare, se avsnitt 9.3 ovan. Det kan i detta sammanhang noteras att det i artikel 18.1.b i Budapestkonventionen finns bestämmelser om att behöriga myndigheter i en stat ska kunna förelägga en tjänsteleverantör som erbjuder sina tjänster inom statens territorium att lämna ut sådana uppgifter om abonnemang som leverantören har i sin besittning eller under sin kontroll.

Vidare finns det, som vi nämnt ovan (se 9.6.1), i 9 kap. 33 § första stycket 5 nya LEK en skyldighet för den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst som inte är en Noik 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 föreläggande enligt 27 kap. 16 § RB till den myndighet som har meddelat föreläggandet. Som nämnts i avsnitt 5.3.1 infördes denna skyldighet och möjligheten att meddela ett bevarandeföreläggande i samband med Sveriges tillträde till Budapestkonventionen. Konventionen ställer krav på att lagrade datorbehandlingsbara uppgifter ska kunna säkras oavsett om en eller flera tillhanda-

hållare har deltagit i överföringen. Konventionsstaterna ska därför garantera att en tillräcklig mängd sådana trafikuppgifter ska kunna röjas för myndigheterna så att tillhandahållarna, och den vägmeddelandet överförts, ska kunna identifieras (artikel 17). Regeringen gjorde bedömningen att det i praktiken huvudsakligen kommer att vara sådana tillhandahållare av elektroniska kommunikationsnät eller kommunikationstjänster som omfattas av anmälningsplikten i LEK som blir aktuella för ett sådant utlämnande av uppgifter. Genom att begränsa kretsen till dessa aktörer blir det också, enligt vad regeringen uttalade, en möjlig och rimlig uppgift för den som begäran riktas mot att ta fram den efterfrågade informationen.[37]

Som vi tidigare konstaterat sker en allt större del av all elektronisk kommunikation genom Noik. Genom att utvidga skyldigheten att lämna information om vilka tillhandahållare som har deltagit vid överföringen av ett meddelade till att gälla även för tillhandahållare av Noik säkerställs att Sverige uppfyller Budapestkonventionens krav. För de brottsbekämpande myndigheterna skulle en sådan skyldighet kunna vara extra viktig i förhållande till tillhandahållare av Noik, eftersom dessa ofta inte ansvarar för själva överföringen av meddelandet. Exempelvis skulle en tillhandahållare av en e-posttjänst kunna lämna information om vilken annan tillhandahållare som har överfört ett e-postmeddelande. Det kan vidare konstateras att möjligheten att meddela ett bevarandeföreläggande också finns i förhållande till en tillhandahållare av Noik. Vi bedömer därför att även tillhandahållare av Noik (inte bara tillhandahållare av allmänt tillgängliga Noik) ska omfattas av skyldigheten att lämna information om vilka eventuella övriga tillhandahållare som deltagit vid överföringen av ett meddelade. Om tillhandahållaren av Noik inte har någon uppgift om vilka de övriga aktörerna är, kommer någon information inte att kunna lämnas ut, jfr avsnitt 5.3.1.

Utlämnande av uppgifter för andra syften än brottsbekämpning

Bestämmelsen i 9 kap. 33 § nya LEK omfattar även skyldigheter att lämna ut uppgifter i annat än brottsbekämpande syfte. Uppgifter om abonnemang ska således enligt bestämmelsens första stycke 1 lämnas ut till

[37] Se prop. 2020/21:72 s. 39.

- en myndighet som i ett särskilt fall behöver en sådan uppgift för delgivning, om det kan antas att den som söks för delgivning håller sig undan eller att det annars finns synnerliga skäl,
- Finansinspektionen, om uppgiften är av väsentlig betydelse för utredningen av en misstänkt överträdelse av EU:s marknadsmissbruksförordning eller om uppgiften är av väsentlig betydelse i ett ärende om tillsyn när det gäller vissa bestämmelser i lagen om betalningstjänster eller lagen om verksamhet med bostadskrediter,
- Konsumentombudsmannen, om uppgiften är av väsentlig betydelse i ett ärende om tillsyn enligt lagen om avtalsvillkor i konsumentförhållanden eller marknadsföringslagen, när det är fråga om en misstänkt överträdelse av unionslagstiftning som skyddar konsumenternas intressen enligt bilagan till EU:s förordning om samarbete mellan de nationella myndigheter som har tillsynsansvar för konsumentskyddslagstiftningen,
- Konsumentverket, om uppgiften är av väsentlig betydelse i ett ärende om tillsyn enligt lagen med kompletterande bestämmelser till EU:s geoblockeringsförordning,
- Kronofogdemyndigheten, om myndigheten behöver uppgiften i exekutiv verksamhet och uppgiften är av väsentlig betydelse för handläggningen av ett ärende,
- Läkemedelsverket, om uppgiften är av väsentlig betydelse i ett ärende om tillsyn när det gäller bestämmelserna om marknadsföring i läkemedelslagen,
- Polismyndigheten, om uppgiften behövs i samband med underrättelse, efterforskning eller identifiering vid olyckor eller dödsfall eller för att fullgöra en uppgift som avses i 12 § polislagen,
- Polismyndigheten eller en åklagarmyndighet, om uppgiften behövs i ett särskilt fall för att myndigheten ska kunna fullgöra en underrättelseskyldighet enligt 33 § lagen med bestämmelser om unga lagöverträdare, och
- Skatteverket, om uppgiften är av väsentlig betydelse för handläggningen av ett ärende som avser kontroll av skatt eller avgift eller rätt folkbokföringsort enligt folkbokföringslagen.

Enligt 9 kap. 33 § första stycket 3 nya LEK ska uppgift om abonnemang och annan uppgift som angår ett särskilt meddelande (dvs. trafikuppgift) lämnas till en regional alarmeringscentral som avses i lagen om verksamhet hos vissa regionala alarmeringscentraler. Slutligen ska uppgifter om abonnemang, trafikuppgift, och uppgift om i vilket geografiskt område en viss kommunikationsutrustning finns eller har funnits lämnas till Polismyndigheten, om 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 nya LEK).

De ovan nämnda myndigheterna, som får hämta in uppgifter om abonnemang med stöd av bestämmelsens första stycke 1, torde ha lika stor nytta och lika stort behov av uppgifterna oavsett vem som tillhandahåller kommunikationstjänsten. Utlämnande av dessa uppgifter från en tillhandahållare av Noik innebär inte heller något större integritetsintrång för den enskilde än vad ett motsvarande utlämnande från någon annan tillhandahållare av elektroniska kommunikationstjänster innebär. Detsamma gäller för uppgift om abonnemang och trafikuppgift som regionala alarmeringscentraler får hämta in och för sådana uppgifter som Polismyndigheten får hämta in i syfte att efterforska försvunna personer. Det bör poängteras att Polismyndighetens inhämtning av uppgifter som regleras i paragrafens första stycke 4 inte sker i brottsbekämpande syfte utan för att eftersöka försvunna personer när det kan befaras att det finns fara för personernas liv eller allvarlig risk för deras hälsa. Uppgifter som inhämtas enligt bestämmelsen ska alltså inte användas för andra syften. Enligt vår bedömning är det både rimligt och proportionellt att skyldigheterna att lämna ut uppgifter till de angivna myndigheterna och till regionala alarmeringscentraler ska gälla även för tillhandahållare av Noik. När det gäller skyldigheten att lämna ut lokaliseringsuppgifter till Polismyndigheten kan det noteras att tillhandahållare av Noik vanligen inte har tillgång till lokaliseringsuppgifter som härrör från teleoperatörernas basstationer, eftersom kommunikationen förmedlas över internet. Tillhandahållare av Noik kan dock ha tillgång till andra lokaliseringsuppgifter. Skyldigheten att lämna ut uppgifter enligt bestämmelsen gäller enbart uppgifter som tillhandahållaren har fått del av eller tillgång till. I den mån en tillhandahållare av Noik har tillgång till uppgift om i vilket geografiskt område en viss kommunikations-

utrustning finns eller har funnits, bör skyldigheten att lämna ut dessa uppgifter till Polismyndigheten även träffa tillhandahållare av Noik.

Vi föreslår alltså sammanfattningsvis att skyldigheterna 9 kap. 33 § nya LEK att lämna ut uppgifter ska gälla för samtliga tillhandahållare av elektroniska kommunikationsnät och elektroniska kommunikationstjänster – alltså, liksom i dag, även sådana som inte är allmänt tillgängliga. Undantaget för tillhandahållare av Noik i paragrafens första stycke bör därför tas bort. Regeln om ersättning i paragrafens andra stycke bör gälla även i förhållande till tillhandahållare av Noik.

Tillgången till trafik- och lokaliseringsuppgifter genom hemlig övervakning av elektronisk kommunikation

Utredningens bedömning: HÖK kan redan i dag användas för att få tillgång till uppgifter hos en tillhandahållare av Noik. En uppgift om ett unikt användarnamn eller en användaridentitet är en uppgift om abonnemang och utgör en sådan adress som en HÖK kan avse. Tillhandahållare av Noik omfattas emellertid inte av någon anpassningsskyldighet.

Genom hemlig övervakning av elektronisk kommunikation, dvs. HÖK kan trafikuppgifter och lokaliseringsuppgifter hämtas in (se avsnitt 5). Som bestämmelsen i 27 kap. 19 § första stycket RB är utformad finns det inget hinder mot att ett beslut om HÖK används för att få tillgång till uppgifter hos en tillhandahållare av Noik. Även beslut om HÖK med tillämpning av bestämmelserna i preventivlagen, lagen om särskild kontroll av vissa utlänningar, lagen om internationell rättshjälp i brottmål eller lagen om en europeisk utredningsorder kan användas för att få tillgång till uppgifter hos en tillhandahållare av Noik. Ett tillstånd till HAK ger automatisk tillgång till sådana uppgifter om utväxlade meddelanden som annars kräver beslut om HÖK (se 27 kap. 18 § tredje stycket RB).

Som nämnts ovan är det dock inte säkert att tillhandahållare av Noik på samma sätt som teleoperatörer har tillgång till uppgifter om vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område eller i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits.

Vid kommunikation genom Noik används användarnamn. Om användarnamnet inte är unikt är det kopplat till användarens användaridentitet (t.ex. en sifferkombination), se ovan avsnitt 9.3. En fråga som bör ställas är om en uppgift om ett användarnamn eller en användaridentitet är en abonnemangsuppgift enligt 9 kap. 31 § första stycket 1 nya LEK och som de brottsbekämpande myndigheterna har rätt att få tillgång till enligt 9 kap. 33 § första stycket 2 nya LEK. Som tidigare nämnts finns det varken i EU-rätten eller i nationell rätt någon definition av begreppet uppgift om abonnemang. Regeringen har uttalat att uppgifter om abonnemang som utgångspunkt kan definieras som uppgifter som identifierar abonnenten eller den registrerade användaren bakom ett visst nummer eller en viss adress, i motsats till uppgifter som redogör för hur numret eller adressen har använts.[38] Mot denna bakgrund menar vi att en uppgift om ett unikt användarnamn eller en användaridentitet är att betrakta som en abonnemangsuppgift. Om de brottsbekämpande myndigheterna har tillgång endast till ett icke unikt användarnamn, kan de alltså behöva vända sig till tillhandahållaren av Noik och begära att få tillgång till den unika användaridentiteten.

HÖK får, enligt 27 kap. 20 § första stycket 1 och 2 RB, endast avse ett telefonnummer eller *annan adress* eller en viss kommunikationsutrustning som under den tid tillståndet avser har någon viss koppling till den misstänkte. Eftersom telefonnummer inte används för att förmedla kommunikation via Noik, finns det anledning att överväga vad som ska anges som adress i en ansökan om HÖK för verkställighet hos en tillhandahållare av Noik. Om inhämtningen avser uppgifter om den misstänktes e-postkonto eller en viss ip-adress som använts av den misstänkte är det naturligt att det är e-postadressen respektive ip-adressen som ska anges. Frågan är om ett unikt användarnamn eller en användaridentitet kan anses vara en sådan *adress* som tvångsmedelsåtgärden kan avse. Rent språkligt kan det ifrågasättas om ett användarnamn eller en användaridentitet kan anses vara en adress. Före år 2012 skulle telemeddelandet, som då var det som avsågs med den hemliga övervakningen, befordras eller ha befordrats till eller från ett telefonnummer, en kod, eller annan teleadress. I motiven till den regleringen angavs att med teleadress avsågs en identifiering av den icke fysiska adress som ett telemeddelande skickas till eller från. Adressen kunde enligt motiven vara ett abonnemang, en

[38] Se prop. 2018/19:86 s. 93.

enskild anknytning, adressen för elektronisk post, en kod eller någon annan tillförlitlig identifieringsmetod.[39] Genom 2012 års reform ersattes begreppet teleadress med adress. Någon saklig ändring var inte avsedd. Eftersom paragrafen inte uttömmande anger vilka identifieringsmetoder som får användas, kan tvångsmedlet tillämpas oberoende av om det är fråga om en traditionell fysisk avgränsning eller om det gäller en av it-utvecklingen skapad ny möjlighet att identifiera vissa meddelanden.[40] Det unika användarnamnet eller användaridentiteten är det som faktiskt identifierar sändaren eller mottagaren av kommunikationen och utgör alltså en tillförlitlig identifieringsmetod. Vi menar därför att det unika användarnamnet eller användaridentiteten är att anse som en sådan adress som ett beslut om HÖK kan avse. Vi bedömer att det inte behöver göras några ändringar i 27 kap. 20 § första stycket 1 och 2 RB för att ett beslut om HÖK ska kunna avse en sådan adress som används vid kommunikation via Noik. Någon annan särskild författningsreglering behövs inte heller för att ge de brottsbekämpande myndigheterna tillgång till uppgifter om elektronisk kommunikation hos tillhandahållare av Noik genom HÖK.

Tillhandahållare av Noik omfattas emellertid inte av någon anpassningsskyldighet (se 9 kap. 29 och 29 b §§ nya LEK). Avsaknaden av en sådan anpassningsskyldighet medför att förutsättningarna för de brottsbekämpande myndigheterna att få tillgång till uppgifter från dessa tillhandahållare är begränsade. Vi återkommer i avsnitt 10 med överväganden och förslag om hur anpassningsskyldigheten för tillhandahållare av Noik bör utformas.

Tillgången till trafik- och lokaliseringsuppgifter med stöd av inhämtningslagen

Utredningens förslag: Uppgifter ska få inhämtas från tillhandahållare av Noik med stöd av beslut om inhämtning enligt inhämtningslagen.

Enligt lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, dvs. inhämtningslagen, får Polismyndigheten, Säkerhetspolisen

[39] Se prop. 1994/95:227 s. 21.
[40] Se Juno, kommentaren till RB 27:18.

och Tullverket i sin underrättelseverksamhet i hemlighet hämta in uppgifter om meddelanden som i ett elektroniskt kommunikationsnät har överförts till eller från ett telefonnummer eller annan adress, om vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område eller uppgifter om inom vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits. Lagen reglerar enbart inhämtning från den som enligt nya LEK tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst som inte är en Noik och ger inte stöd för de brottsbekämpande myndigheterna att hämta in uppgifter med hjälp av egna tekniska hjälpmedel.

Undantaget för inhämtning av uppgifter från tillhandahållare av Noik infördes som en följd av att begreppet elektronisk kommunikationstjänst fick en vidare innebörd i nya LEK och alltså omfattade även Noik. Ändringen gjordes för att inhämtningslagens tillämpningsområde inte skulle utvidgas utan överväganden.[41]

Utredningen som låg till grund för inhämtningslagen gjorde bedömningen att inhämtningen skulle ske från samma krets av leverantörer som omfattas av tystnadsplikten enligt nuvarande 9 kap. 31–32 §§ nya LEK.[42] Vi har ovan föreslagit att tillhandahållare av Noik ska omfattas av tystnadsplikt enligt dessa bestämmelser.

De myndigheter som får inhämta uppgifter enligt inhämtningslagen har lika stor nytta och lika stort behov av uppgifter om elektronisk kommunikation i sin underrättelseverksamhet oavsett vem som tillhandahåller kommunikationstjänsten. Inhämtningen av uppgifter från en tillhandahållare av Noik innebär inte heller något större integritetsintrång för den enskilde än vad en inhämtning av uppgifter från någon annan tillhandahållare av elektroniska kommunikationstjänster innebär. Det bör därför finnas en möjlighet att med tillämpning av inhämtningslagen inhämta uppgifter även från tillhandahållare av Noik. Det undantag för tillhandahållare av Noik som finns i 1 § inhämtningslagen bör därför tas bort. Liksom vid HÖK är det inte säkert att tillhandahållaren av Noik har tillgång till uppgifter om vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område eller i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits.

[41] Se prop. 2021/22:136 s. 375 f.
[42] Se SOU 2009:1 s. 175.

Tillgången till trafik- och lokaliseringsuppgifter genom hemlig dataavläsning

Utredningens bedömning: De brottsbekämpande myndigheterna kan redan i dag verkställa hemlig dataavläsning i informationssystem som innehas av tillhandahållare av Noik.

Hemlig dataavläsning, dvs. HDA, innebär att uppgifter, som är avsedda för automatiserad behandling, i hemlighet och med ett tekniskt hjälpmedel läses av eller tas upp i ett avläsningsbart informationssystem. Tvångsmedlet ger Polismyndigheten, Säkerhetspolisen, Tullverket och Ekobrottsmyndigheten möjligheter att avlyssna och övervaka personer som är misstänkta för eller förväntas begå allvarliga brott. Tillstånd till HDA får beviljas bl.a. för att läsa av och ta upp kommunikationsövervakningsuppgifter. Ett tillstånd till hemlig dataavläsning kan verkställas i informationssystem som innehas av tillhandahållare av Noik. Någon särskild författningsreglering behövs således inte för att ge de brottsbekämpande myndigheterna tillgång till uppgifterna genom HDA.

Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § nya LEK är på begäran av den verkställande myndigheten skyldig att medverka i samband med verkställandet av hemlig dataavläsning (24 § lagen om hemlig dataavläsning). Den som bedriver sådan verksamhet har också en tystnadsplikt för uppgifter som hänför sig till användning av hemlig dataavläsning (32 § lagen om hemlig dataavläsning). Vi återkommer i avsnitt 10.4.5 till frågor om medverkansskyldighet och tystnadsplikt vid HDA för tillhandahållare av Noik.

9.6.4 Krav på säkerhet och villkor för behandlingen av uppgifter m.m. för tillhandahållare av Noik

I detta avsnitt överväger vi vad som bör gälla för tillhandahållare av Noik avseende säkerhet för information och behandling av uppgifter.

Säkerhet

Utredningens förslag: Tillhandahållare av allmänt tillgängliga Noik ska omfattas av kraven på skyddsåtgärder vid lagring och annan behandling av uppgifter för brottsbekämpande ändamål. Uppgifter som omfattas av lagringsskyldighet får inte lagras utanför EU.

Utredningens bedömning: Det behövs inga ändringar i de regler om säkerhet som redan gäller för tillhandahållare av allmänt tillgängliga Noik.

Ett tillförlitligt och säkert utbyte av information via elektroniska kommunikationsnät och elektroniska kommunikationstjänster är centralt för marknadens aktörer och samhället i stort. En ökad komplexitet i nät och tjänster medför ökade risker för tekniska fel. Till detta kommer risker som beror på mänskliga misstag, väderpåverkan, olyckor och attacker. Säkerhet för nät och tjänster definieras som elektroniska kommunikationsnäts och elektroniska kommunikationstjänsters förmåga att vid en viss tillförlitlighetsnivå motstå händelser som undergräver tillgängligheten, autenticiteten riktigheten eller konfidentialiteten hos näten eller tjänsterna, hos lagrade, överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via dessa elektroniska kommunikationsnät eller elektroniska kommunikationstjänster.[43]

De flesta krav på säkerhet enligt 8 kap. nya LEK omfattar tillhandahållare av allmänt tillgängliga Noik. Sådana tillhandahållare ska vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att på ett lämpligt sätt hantera risker som hotar säkerheten i nät och tjänster. Åtgärderna ska säkerställa en nivå på säkerheten i nät och tjänster som är lämplig i förhållande till riskerna.

[43] Se 1 kap. 7 § nya LEK och artikel 2.21 i e-kodexen.

Åtgärder ska vidtas särskilt för att förebygga och minimera säkerhetsincidenters påverkan på användare och på andra nät och tjänster. Rätten för regeringen eller den myndighet som regeringen bestämmer att meddela ytterligare föreskrifter om säkerhetsåtgärderna och om undantag från skyldigheten att vidta sådana åtgärder gäller även i förhållande till allmänt tillgängliga Noik. Möjligheten för PTS att ålägga en tillhandahållare att på egen bekostnad låta ett oberoende kvalificerat organ utföra en säkerhetsgranskning gäller för allmänt tillgängliga Noik. Även skyldigheten att rapportera säkerhetsincidenter till PTS och att informera användare om konkreta och betydande hot om en säkerhetsincident gäller för tillhandahållare av allmänt tillgängliga Noik (8 kap. 1–4 §§). Vidare omfattas tillhandahållare av allmänt tillgängliga Noik av bestämmelserna om att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att uppgifter som behandlas i samband med tillhandahållandet av tjänsten skyddas. Åtgärderna ska vara ägnade att säkerställa en nivå på säkerheten som, med hänsyn till tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för integritetsincidenter. Tillhandahållare av allmänt tillgängliga Noik omfattas också av skyldigheterna att informera berörda abonnenter om särskilda risker för bristande skydd av behandlade uppgifter, att utan onödigt dröjsmål underrätta PTS och i vissa fall abonnenter och användare om integritetsincidenter och att föra en förteckning över integritetsincidenter (8 kap. 6–9 §§).

Den som är skyldig att lagra uppgifter enligt 9 kap. 19 § nya LEK 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 § nya LEK och som har förelagts enligt 27 kap. 16 § RB att bevara en viss lagrad uppgift (bevarandeföreläggande) ska avseende den uppgiften vidta samma åtgärder för att skydda uppgiften. Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om sådana skyddsåtgärder (8 kap. 5 § nya LEK).

Eftersom vi föreslår att tillhandahållare av allmänt tillgängliga Noik ska omfattas av reglerna om lagringsskyldighet, bör dessa tillhandahållare också omfattas av kraven på skyddsåtgärder vid lagring och annan behandling av uppgifter för brottsbekämpande ändamål enligt 8 kap. 5 § nya LEK. Detta kräver ingen ändring av den aktuella paragrafens första stycke, eftersom vi ovan föreslagit att tillhanda-

hållare som omfattas av lagringsskyldighet, dvs. även tillhandahållare av allmänt tillgängliga Noik, ska regleras i 9 kap. 19 § nya LEK. Eftersom vi inte föreslår att tillhandahållare av Noik ska omfattas av anmälningsplikten i 2 kap. 1 § nya LEK, behöver dock bestämmelsen ändras för att kraven på skyddsåtgärder ska gälla för tillhandahållare av Noik även beträffande uppgifter som omfattas av ett bevarandeföreläggande. Paragrafens andra stycke bör därför ändras så att den knyts till bestämmelserna i 9 kap. 19 § nya LEK i stället för de i 2 kap. 1 § nya LEK.

I 9 kap. 4 § nya FEK föreskrivs att den som är skyldig att lagra uppgifter enligt 9 kap. 19 § nya LEK ska vidta de åtgärder som krävs för att säkerställa att de lagrade uppgifterna är av samma kvalitet och föremål för samma säkerhet och skydd som vid den behandling som skett före lagringen. Den lagringsskyldige ska vidta de åtgärder som krävs för att skydda uppgifterna mot oavsiktlig eller otillåten förstöring och oavsiktlig förlust eller ändring. Sådana åtgärder ska även vidtas för att förhindra otillåten lagring av, behandling av eller tillgång till uppgifterna och otillåtet avslöjande av uppgifterna. Uppgifterna får göras tillgängliga endast för personal med särskild behörighet. Uppgifterna får inte lagras utanför EU. PTS får, efter att ha gett Integritetsskyddsmyndigheten, Polismyndigheten och Säkerhetspolisen tillfälle att yttra sig, meddela närmare föreskrifter om de åtgärder som ska vidtas enligt denna bestämmelse (9 kap. 5 § nya FEK).

Eftersom vi föreslår att tillhandahållare av allmänt tillgängliga Noik ska omfattas av lagringsskyldighet, bör dessa tillhandahållare omfattas även av de nu nämnda reglerna. Någon författningsändring behövs inte för att dessa tillhandahållare ska omfattas av bestämmelsen, eftersom paragrafen avser den som är skyldig att lagra uppgifter. Det kan naturligtvis vara förknippat med svårigheter för tillhandahållare av globala Noik att uppgifterna ska lagras just inom EU. I Tele2-domen konstaterade EU-domstolen att artikel 15.1 i e-dataskyddsdirektivet inte medger att medlemsstaterna avviker från kraven på att leverantörerna vidtar lämpliga tekniska och organisatoriska åtgärder för att säkerställa ett effektivt skydd av de lagrade uppgifterna mot riskerna för missbruk och otillåten tillgång till uppgifterna. Med hänsyn till mängden uppgifter, uppgifternas känsliga natur och risken för otillåten tillgång till uppgifterna måste leverantörerna av elektroniska kommunikationstjänster, enligt domstolen, garantera en särskilt hög skydds- och säkerhetsnivå genom lämpliga tekniska

och organisatoriska åtgärder. Domstolen uttalade att den nationella lagstiftningen i synnerhet måste föreskriva att lagringen sker inom unionen och att uppgifterna oåterkalleligen förstörs när deras lagringstid gått ut (p. 122 i domen). Även tillhandahållare av allmänt tillgängliga Noik måste därför se till att de uppgifter som omfattas av lagringsskyldighet också faktiskt lagras inom EU.

Vi påminner i detta sammanhang om att de krav som vi nu föreslår gällande lagring inom EU tar sikte på uppgifter som omfattas av e-dataskyddsdirektivet. I övrigt gäller andra regler, bl.a. EU:s dataskyddsförordning. Vi återkommer i avsnitt 13 till vilka konsekvenser lagringsskyldigheten har för tillhandahållare av allmänt tillgängliga Noik.

Villkor för behandlingen av uppgifter

Utredningens bedömning: Det behövs inga särskilda ändringar i de bestämmelser som reglerar villkoren att behandla uppgifter för tillhandahållare av allmänt tillgängliga Noik.

Den som tillhandahåller en allmänt tillgänglig Noik omfattas av skyldigheten att utplåna eller avidentifiera trafikuppgifter som har lagrats eller behandlats på något annat sätt när de inte längre behövs för att överföra ett elektroniskt meddelande. Detta gäller under förutsättning att uppgifterna avser användare som är fysiska personer eller abonnenter. Det gäller dock inte om uppgifterna sparas för viss angiven behandling (9 kap. 1 § nya LEK).

Trafikuppgifterna får exempelvis sparas om de 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 (9 kap. 1 § andra stycket nya LEK).

Även de uppgifter som krävs för abonnentfakturering och betalning av avgifter för samtrafik får behandlas till dess att fordran är betald eller preskription har inträtt och det inte längre lagligen går att göra invändningar mot faktureringen eller avgiften. Om den som

uppgifterna rör har samtyckt till det, får tillhandahållaren behandla trafikuppgifter för marknadsföringssyften eller för att tillhandahålla andra tjänster där uppgifterna behövs (9 kap. 2 § nya LEK).

Behandlingen av trafikuppgifter enligt 9 kap. 1 och 2 §§ nya LEK får utföras endast av den som har fått i uppdrag av tillhandahållaren att sköta fakturering, trafikstyrning, kundförfrågningar, marknadsföring av elektroniska kommunikationstjänster eller tillhandahållande av andra tjänster där uppgifterna behövs. Behandlingen ska begränsas till vad som är nödvändigt för verksamheten (9 kap. 3 § nya LEK).

De begränsningar för behandling av trafikuppgifter som följer av 9 kap. 1–3 §§ nya LEK gäller inte när en förvaltningsmyndighet eller en domstol behöver tillgång till uppgifterna för att lösa tvister, för elektroniska meddelanden som omfattas av ett frysningsföreläggande, för elektroniska meddelanden som omfattas av beslut om HAK, HÖK, tekniskt bistånd med sådan avlyssning eller övervakning, inhämtning enligt inhämtningslagen eller i den utsträckning uppgifterna behövs för att förhindra eller avslöja obehörig användning av en elektronisk kommunikationstjänst (9 kap. 4 § nya LEK).

Trafikuppgifter får även sparas för sådan behandling som anges i 9 kap. 19 § nya LEK, dvs. för att lagras för brottsbekämpande ändamål (se 9 kap. 1 § andra stycket nya LEK). Vi har i avsnitt 7.3.8 och 8.3.6 föreslagit ändring av 9 kap. 1 § nya LEK i anledning av våra förslag om nationell säkerhetslagring och lagring för att bekämpa grov brottslighet.

Vi bedömer att någon ytterligare ändring av 9 kap. 1 § inte behövs, eftersom det i 9 kap. 19 § nya LEK enligt våra förslag ska anges att även tillhandahållare av allmänt tillgängliga Noik ska lagra uppgifter enligt vad som anges i 9 kap. 19 a–19 d §§.

Lokaliseringsuppgifter som inte är trafikuppgifter och som rör användare som är fysiska personer eller abonnenter får behandlas endast sedan de har avidentifierats eller användaren eller abonnenten har gett sitt samtycke till behandlingen. Behandling får ske endast i den utsträckning och under den tid som krävs för tillhandahållandet av en tjänst där uppgifterna behövs. Lokaliseringsuppgifter får behandlas om de omfattas av ett beslut om inhämtning av uppgifter enligt 27 kap. RB eller inhämtningslagen (se 9 kap. 7 och 10 §§ nya LEK).

Vi har i avsnitt 7 och 8 föreslagit att lokaliseringsuppgifter som inte är trafikuppgifter ska omfattas av geografiskt riktad lagring och att sådana uppgifter får omfattas av såväl nationell säkerhetslagring

som utökad riktad lagring. Lokaliseringsuppgifter som ska lagras enligt 19 b–19 d §§ nya LEK får enligt våra förslag behandlas trots 7–9 §§.

Vi bedömer i likhet med ovan att någon ytterligare ändring inte behövs, eftersom tillhandahållare av allmänt tillgängliga Noik omfattas av lagringsskyldigheten enligt den av oss föreslagna 9 kap. 19 § nya LEK.

Enligt 9 kap. 21 § nya LEK får uppgifter som har lagrats enligt 9 kap. 19 § nya LEK därutöver behandlas endast för att lämnas ut enligt 9 kap. 33 § första stycket 2 eller 5 nya LEK, 27 kap. RB eller inhämtningslagen. Våra förslag ovan innebär att 9 kap. 21 § nya LEK ska ändras så att bestämmelsen i stället hänvisar till lagring enligt 9 kap. 19 c och 19 d §§ nya LEK (se avsnitt 8). Som nämnts ovan har vi också föreslagit att uppgifter som lagras i syfte att skydda den nationella säkerheten med stöd av 9 kap. 19 b § nya LEK får behandlas endast för att lämnas ut enligt den av oss föreslagna lagen om lagring och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda nationell säkerhet och att detta regleras i ett andra stycke i 9 kap. 21 § nya LEK.

Några andra ändringar i de bestämmelser som reglerar villkoren för behandling av uppgifter behövs inte för att tillhandahållare av allmänt tillgängliga Noik ska kunna omfattas av de skyldigheter att lagra och ge tillgång till uppgifter om elektronisk kommunikation som vi föreslagit ovan.

Sanktionsavgifter

Vi återkommer i avsnitt 10.5 till frågor om sanktionsavgifter för tillhandahållare av Noik.

10 En modernisering av anpassningsskyldigheten, m.m.

I detta avsnitt analyserar vi frågor om den s.k. anpassningsskyldighetens omfattning och om hur en reglering av denna skyldighet kan utformas på ett så tydligt, enhetligt, säkert och teknikneutralt sätt som möjligt. Sist i detta avsnitt överväger vi frågan om sanktionsavgifter i olika avseenden.

10.1 Inledning

Tillhandahållare av elektroniska kommunikationsnät och elektroniska kommunikationstjänster spelar en viktig roll när de brottsbekämpande myndigheterna hämtar in elektronisk kommunikation och uppgifter om sådan. För att underlätta för de brottsbekämpande myndigheterna har tillhandahållarna ålagts en anpassningsskyldighet. Skyldigheten innebär bl.a. att viss angiven verksamhet ska bedrivas så att beslut om HAK och HÖK kan verkställas och att det kan ske på ett sådant sätt att verkställandet inte röjs. Anpassningsskyldigheten innebär också ett krav på skyndsamhet och format vid utlämnandet av uppgifter. Den tekniska utvecklingen har medfört att regleringen av anpassningsskyldigheten till viss del har blivit oklar och ålderdomlig.

Det är angeläget att anpassningsskyldighetens omfattning är tydlig, modern och tillgodoser brottsbekämpningens behov. Samtidigt behöver regleringen vara välavvägd så att teknikutvecklingen främjas, nätsäkerheten bibehålls och företagen inte påförs orimliga bördor.

Enligt våra direktiv ska vi

- analysera anpassningsskyldighetens omfattning och ta ställning till hur en reglering kan utformas på ett så tydligt, enhetligt, säkert och teknikneutralt sätt som möjligt,

- analysera behovet av lagstiftning eller andra åtgärder i fråga om anpassningsskyldigheten så att hemliga tvångsmedel kan verkställas på ett effektivt sätt även i framtiden, och
- lämna förslag på de författningsändringar och andra åtgärder som bedöms nödvändiga.

10.2 Gällande rätt

Det finns två delar av anpassningsskyldigheten. Den första delen av anpassningsskyldigheten regleras i 9 kap. 29 § första stycket nya LEK och innebär att tillhandahållare ska bedriva verksamheten så att beslut om HAK och HÖK kan verkställas och så att verkställandet inte röjs. Anpassningsskyldigheten i denna del gäller endast för vissa verksamheter, nämligen verksamheter som innefattar tillhandahållande av

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

Bestämmelsen överfördes från 6 kap. 19 § gamla LEK till 9 kap. 29 § nya LEK utan någon ändring i sak. Begreppet allmänt kommunikationsnät ändrades till allmänt elektroniskt kommunikationsnät för att anpassas till terminologin i nya LEK.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § RF meddela närmare föreskrifter om frågor som gäller anpassningsskyldigheten och får i enskilda fall besluta om undantag från kravet (9 kap. 29 § andra stycket nya LEK).

I 9 kap. 13 § nya FEK anges att Post- och telestyrelsen får, efter samråd med Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket och Åklagarmyndigheten, meddela närmare föreskrifter som behövs för HAK och HÖK enligt 9 kap. 29 § nya LEK. Post- och telestyrelsen får också, enligt samma paragraf, i enskilda fall medge undantag från kravet på anpassningsskyldighet enligt 9 kap. 29 första stycket nya LEK. Sådana föreskrifter eller undantag har inte meddelats (inte heller enligt de tidigare gällande föreskrifterna i 36 § förordningen [2003:396] om elektronisk kommunikation).

Den andra delen av anpassningsskyldigheten, som föreskrivs i 9 kap. 29 b § nya LEK, reglerar krav på skyndsamhet och format vid utlämnandet av innehållet i eller uppgifter om elektronisk kommunikation samt lokaliseringsuppgifter som inte är trafikuppgifter (dvs. sådana lokaliseringsuppgifter som inte behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande). När den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § nya LEK lämnar ut uppgifter om abonnemang, uppgifter som avser innehållet i ett elektroniskt meddelande, andra uppgifter som angår ett särskilt elektroniskt meddelande eller lokaliseringsuppgifter som inte är trafikuppgifter till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott, ska det, 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 nya LEK). Vidare ska, vid sådant utlämnande, uppgifterna ordnas och göras tillgängliga i ett format som gör att de enkelt kan tas om hand (9 kap. 29 b § andra stycket nya LEK). Vi har i avsnitt 6.2.2 föreslagit att begreppet *annan uppgift som angår ett särskilt elektroniskt meddelande* ska ersättas med begreppet *trafikuppgift*.

Tillsynsmyndigheten får, om det finns särskilda skäl för det, i enskilda fall besluta om undantag från kravet på format när uppgifterna ska lämnas ut (9 kap. 29 b § tredje stycket nya LEK). Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om hur uppgifterna ska lämnas ut (9 kap. 29 b § fjärde stycket nya LEK).

Reglerna om anpassningsskyldighet när det gäller utlämnande av uppgifter ändrades den 1 augusti 2022.[1] Tidigare reglerades hela anpass-

[1] Se prop. 2021/22:183, bet. 2021/22: JuU34, rskr. 2021/22:432.

ningsskyldigheten i 6 kap. 19 § gamla LEK. Enligt paragrafens andra stycke skulle innehållet i och uppgifter om avlyssnade eller övervakade meddelanden göras tillgängliga så att informationen enkelt kunde tas om hand.

Vidare fanns tidigare en särskild bestämmelse om att den som var skyldig att lagra uppgifter enligt 6 kap. 16 a § gamla LEK skulle bedriva verksamheten så att uppgifterna utan dröjsmål kunde lämnas ut och så att verkställandet av utlämnandet inte röjdes. Uppgifterna skulle göras tillgängliga på ett sådant sätt att informationen enkelt kunde tas om hand (6 kap. 16 f § gamla LEK).

Den 1 maj 2021 infördes en bestämmelse som innebar bl.a. att kravet i 6 kap. 16 f § gamla LEK skulle gälla på motsvarande sätt för en uppgift som omfattades av ett föreläggande om bevarande som hade meddelats med stöd av 27 kap. 16 § RB (6 kap. 16 g § gamla LEK).

Ändringarna när det gäller skyldigheter vid utlämnande av uppgifter, som infördes den 1 augusti 2022, innebär bl.a. följande.

- Den särskilda anpassningsskyldigheten i 6 kap. 16 f § gamla LEK, som gällde för den som var lagringsskyldig, har ingen motsvarighet i nya LEK.
- Ett skärpt krav på i vilken form uppgifter ska lämnas ut till brottsbekämpande myndigheter har införts.
- En utvidgning har skett av de typer av uppgifter som omfattas av kraven på format och skyndsamhet vid utlämnande. Kraven gäller alltså inte bara för innehållet i och uppgifter om avlyssnade eller övervakade meddelanden utan för alla typer av uppgifter som omfattas av tillhandahållarnas tystnadsplikt enligt 9 kap. 31 § första stycket nya LEK samt för lokaliseringsuppgifter som inte är trafikuppgifter.
- En utvidgning har gjorts avseende de tillhandahållare som omfattas av kraven på format och skyndsamhet vid utlämnande av uppgifter. Regleringen omfattar alla som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § nya LEK.
- Skyndsamhetskravet vid utlämnande av uppgifter har utvidgats till att omfatta inte bara sådana uppgifter som lagras för brottsbekämpande ändamål och uppgifter som omfattas av ett föreläggande om bevarande utan även uppgifter som lagras för tillhanda-

hållarnas egna ändamål. Skyndsamhetskravet gäller även för uppgifter som inhämtas i realtid.

Dessutom har rätten till ersättning utvidgats till att omfatta samma typer av uppgifter som bestämmelserna om format och skyndsamhet. De nya bestämmelserna om ersättning gäller också när uppgifter hämtas in av brottsbekämpande myndigheter för andra ändamål än brottsbekämpning, t.ex. när Polismyndigheten hämtar in uppgifter för att eftersöka en försvunnen person. Rätten till ersättning gäller för den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § nya LEK, oavsett vilket lagligt stöd som finns för utlämnandet (se 9 kap. 29 a § nya LEK).

I 27 kap. 25 § första stycket RB finns en bestämmelse om verkställighet av beslut om HAK och HÖK. Där anges att de tekniska hjälpmedel som behövs för avlyssningen eller övervakningen får användas när tillstånd till dessa tvångsmedel har lämnats. Med detta avses bl.a. att de tekniska hjälpmedlen får anslutas, underhållas och återtas. Regleringen anses innebära en förpliktelse för tillhandahållare att i viss utsträckning medverka till att tvångsmedelsbesluten kan verkställas.[2] I 9 § lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen) finns en motsvarande bestämmelse.

10.3 Frågans tidigare behandling

Anpassningsskyldigheten infördes redan i den äldre telelagen (1993:597) som trädde i kraft i juli 1996. Anpassningsskyldigheten träffade enbart sådana leverantörer som beviljats tillstånd att inom ett allmänt tillgängligt telenät tillhandahålla telefonitjänst till fast nätanslutningspunkt, mobil teletjänst eller nätkapacitet, om verksamhetens omfattning ansågs vara betydande.

I fråga om den närmare innebörden av anpassningsskyldigheten angavs i förarbetena bl.a. följande.

Anpassningsskyldigheten innebär i praktiken främst ett krav på leverantören att i sin verksamhet använda sig av tekniska hjälpmedel som har vissa egenskaper. Leverantörerna ska använda sig av sådan maskinell utrustning och sådana datorprogram som erfordras för att

[2] Se prop. 1995/96:180 s. 22.

tillgodose de krav som riktas mot dem. Sådana personella och organisatoriska dispositioner måste vidtas som krävs för att hantera hjälpmedlen. De begärda uppgifterna bör hållas tillgängliga inom viss tid, på visst sätt och på viss plats så att de enkelt kan tas om hand.

Kravet innebär att om teleoperatören kodar, komprimerar eller krypterar telemeddelandena måste dessa levereras i klartext. Det låter sig knappast göras att fastställa standardiserade normer som ska gälla för samtliga operatörer som omfattas av kravet på anpassning. En operatör med ett mycket stort antal abonnenter kan behöva tillhandahålla system med större kapacitet än en operatör som har ett förhållandevis litet antal abonnenter. De olika tekniska lösningar som används i moderna telesystem kan också föranleda att den avvägning mellan effektivitet och ekonomi som måste göras utfaller olika i de enskilda fallen om varje operatör kan bedömas för sig. En inte alltför handfast reglering är nödvändig om inte varje teknisk landvinning på teleområdet ska behöva leda till författningsändringar.

Regeringen angav också att det kan finnas skäl att göra skillnad på krav som riktas mot en teleoperatör vid införande av ett nytt telesystem och krav på anpassningar av redan befintliga telesystem som lagstiftningen inledningsvis ger upphov till. Några mer preciserade anvisningar om vad som bör krävas av varje operatör ansågs inte behöva anges direkt i lag eller annan författning. I stället ansåg regeringen att PTS i egenskap av tillsynsmyndighet borde ges möjlighet att, inom ramen för myndighetens befogenheter att meddela tillståndsvillkor och föreskrifter, avgöra vilka åtgärder som ska vidtas för att bestämmelserna ska uppfyllas. När det gäller anpassningen i befintliga system angav regeringen att det i första hand bör ankomma på de brottsbekämpande myndigheterna och operatörerna att komma överens om vad som behöver göras.[3]

Utredningen om elektronisk kommunikation

Utredningen om elektronisk kommunikation föreslog i sitt delbetänkande *Lag om elektronisk kommunikation* (SOU 2002:60) att reglerna i telelagen angående hemlig teleavlyssning och hemlig teleövervakning skulle överföras till den föreslagna nya lagen om elektronisk kommunikation. I betänkandet uttalades att de tjänster som

[3] Se prop. 1995/96:180 s. 25 ff.

i praktiken träffades av anpassningsskyldigheten torde vara fast telefoni och mobil telefoni. För att skyldigheten inte skulle drabba mindre operatörer oskäligt betungande föreslogs att den skulle omfatta de som tillhandahåller allmänna telefonnät eller allmänt tillgängliga telefonitjänster.[4]

Enligt regeringens bedömning innebar emellertid de ändringar som Utredningen om elektronisk kommunikation föreslagit att tillhandahållande av vissa nät och tjänster som omfattades av anpassningsskyldigheten skulle komma att falla utanför denna. Det gällde dels tillhandahållande av sådan nätkapacitet som inte avser ett allmänt telefonnät men väl ett allmänt kommunikationsnät som inte enbart är avsett för utsändningar till allmänheten av program i ljudradio m.m. enligt yttrandefrihetsgrundlagen, dels vissa elektroniska kommunikationstjänster till mobil nätanslutningspunkt. Regeringen angav som exempel att den anpassningsskyldighet som enligt telelagen gällde för tillstånden att bedriva tredje generationens mobiltelefoni (UMTS) skulle komma att avsevärt begränsas. Vidare ansåg regeringen att det med hänsyn till den något ändrade terminologin i den nya lagen behövde klargöras att telefonitjänst till fast nätanslutningspunkt innefattar förutom överföring av lokala, nationella och internationella samtal även telefax samt datakommunikation med viss angiven lägsta datahastighet, som medger funktionell tillgång till internet. Sådan datakommunikation benämndes enligt telelagen datakommunikation via låghastighetsmodem. Det angavs vidare att utredningens förslag samtidigt innebar en utvidgning av tillämpningsområdet genom att verksamheten inte behöver ha viss omfattning för att omfattas.[5] Regeringen uttalade också att frågan om anpassningsskyldighetens omfattning i förhållande till det nya regelverket på området för elektronisk kommunikation var komplicerad och krävde en fördjupad analys som inte kunde göras inom ramen för det aktuella lagstiftningsärendet. Frågan skulle därför i stället behandlas i ett annat sammanhang. I avvaktan på sådan ytterligare utredning av anpassningsskyldigheten angavs att skyldighetens omfattning enligt den nya lagen borde ansluta så nära som möjligt till den omfattning som gällde enligt telelagen. Avsikten var alltså inte att låta skyldigheten

[4] Se SOU 2002:60 s. 505 f.
[5] Se prop. 2002/03:110 s. 267 ff.

omfatta fler och ej heller färre verksamheter än vad som omfattades enligt dåvarande regler.[6]

Beredningen för rättsväsendets utveckling

Beredningen för rättsväsendets utveckling hade bl.a. i uppdrag att göra en översyn av vilka verksamheter som bör omfattas av anpassningsskyldigheten och denna skyldighets förhållande till rättegångsbalkens regler om hemlig teleavlyssning och hemlig teleövervakning. Beredningen föreslog i sitt delbetänkande *Tillgång till elektronisk kommunikation i brottsutredningar m.m.* (SOU 2005:38) att anpassningsskyldigheten i 6 kap. 19 § gamla LEK skulle utvidgas till att omfatta verksamheter som avser ett allmänt tillhandahållande av ett elektroniskt kommunikationsnät eller tjänster inom ett sådant nät.[7] Det föreslogs också att dåvarande Rikspolisstyrelsen skulle få möjlighet att föreskriva om undantag från anpassningsskyldigheten. Någon ändring vad gäller omfattningen av själva anpassningsskyldigheten ansågs inte vara nödvändig. I betänkandet föreslogs också att det i 27 kap. RB skulle föras in en bestämmelse som anger att en enskild (i praktiken en operatör) ska vara skyldig att genast på begäran av en brottsutredande myndighet medverka vid verkställighet av beslut om avlyssning eller övervakning. Skyldigheten att medverka skulle enligt förslaget ses helt skild från anpassningsskyldigheten och innebära att operatörerna vidtar andra åtgärder efter begäran om aktiv medverkan vid verkställighet av tvångsmedelsbesluten. Som exempel skulle det kunna det röra sig om att lämna information om funktioner, tillhandahålla teknisk utrustning eller vidta de personella eller organisatoriska dispositioner som är nödvändiga för verkställighet inom kort tid av tvångsmedelsbeslut.[8] Förslagen har inte lett till lagstiftning.

Datalagringsdirektivet

Bestämmelsen i 6 kap. 16 f § gamla LEK, om att den som var skyldig att lagra uppgifter skulle bedriva verksamheten så att uppgifterna utan dröjsmål kunde lämnas ut och så att verkställandet av utlämnandet

[6] Se a. prop. s. 269.
[7] Se SOU 2005:38 s. 272 ff.
[8] Se a.a. s. 339 ff.

inte röjdes, infördes när Europaparlamentets och rådets direktiv 2006/24/EG om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG (datalagringsdirektivet) genomfördes i Sverige. Regeringen uttalade i samband med detta att den föreslagna lagringsskyldigheten omfattar fler leverantörer än de som är anpassningsskyldiga enligt 6 kap. 19 § gamla LEK och att skyldigheten att lagra trafikuppgifterna därför bör förenas med en anpassningsskyldighet som innebär att samtliga de lagringsskyldiga leverantörernas verksamhet ska bedrivas på ett sådant sätt att de lagrade uppgifterna enkelt kan överföras till och användas av de brottsbekämpande myndigheterna. Regeringen anförde vidare att detta innebär att myndigheterna utan ansträngning ska kunna ta del av informationen även om den skulle vara exempelvis krypterad eller komprimerad och att uppgifterna alltid måste överlämnas på ett sådant sätt att säkerheten och skyddet för uppgifterna inte eftersätts.[9]

Andra ändringar och överväganden

Bestämmelsen om anpassningsskyldighet i 6 kap. 19 § gamla LEK ändrades språkligt i samband med att begreppen telemeddelande, hemlig teleavlyssning och hemlig teleövervakning ersattes av begreppen meddelande, hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. Någon ändring i sak var dock inte avsedd.[10]

I departementspromemorian Registrering av kontantkort, m.m. (Ds 2020:12) konstaterade utredaren att bestämmelserna om anpassningsskyldighetens omfattning i 6 kap. 19 § gamla LEK har blivit oklar och ålderdomlig till följd av den teknikutveckling som pågått länge och som fortfarande pågår samt att det vore önskvärt att bestämmelsen förtydligades och formulerades på ett så teknikneutralt sätt som möjligt. Utredaren ansåg också att det vore lämpligt att utforma bestämmelserna om anpassningsskyldighet och lagringsskyldighet så att de träffar samma aktörer, men lämnade inget förslag i denna del.

[9] Se prop. 2010/11:46 s. 50.
[10] Se prop. 2011/12:55 s. 63 f. och 143.

I samband med införandet av nya LEK fördes reglerna om anpassningsskyldighet över från 6 kap. 19 § gamla LEK till 9 kap. 29 § nya LEK utan någon ändring i sak.[11] Som nämnts ovan delades anpassningsskyldigheten därefter upp i två olika paragrafer, 9 kap. 29 och 29 b §§, och ändringar infördes i den senare paragrafen, som avser skyndsamhet och format vid utlämnande av uppgifter.[12]

Det kan slutligen nämnas att Utredningen om utökade möjligheter att använda hemliga tvångsmedel (Ju 2020:20) i sitt slutbetänkande *Bättre möjligheter att verkställa frihetsberövanden* (SOU 2022:50) har föreslagit att kraven på skyndsamhet och format vid utlämnande av uppgifter enligt 9 kap. 29 b § nya LEK även ska omfatta utlämnande av uppgifter i syfte att kunna lokalisera personer som är dömda och eftersöks för verkställighet samt personer som missköter sin anmälningsskyldighet enligt lagen om särskild kontroll av vissa utlänningar.

10.4 Överväganden och förslag

10.4.1 Verksamheter som bör omfattas av anpassningsskyldigheten

Utredningens förslag: Anpassningsskyldigheten ska omfatta den som bedriver verksamhet som ska anmälas enligt LEK. Ett undantag ska dock gälla för tillhandahållare av maskin-till-maskin-tjänster.

I detta avsnitt behandlar vi frågan hur anpassningsskyldigheten bör utformas när det gäller de traditionella teleoperatörerna. I avsnitt 10.4.3. behandlar vi frågan om en anpassningsskyldighet för tillhandahållare av Noik.

Anpassningsskyldigheten i 9 kap. 29 § första stycket nya LEK innebär alltså att tillhandahållare av viss angiven verksamhet ska bedriva verksamheten så att beslut om HAK och HÖK kan verkställas och så att verkställandet inte röjs. Anpassningsskyldigheten gäller endast för verksamhet som innefattar tillhandahållande av

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

[11] Se prop. 2021/22:136 s. 329 och 508.
[12] Se prop. 2021/22:183.

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 viss angiven lägsta datahastighet som medger funktionell tillgång till internet, eller

   b) en allmänt tillgänglig elektronisk kommunikationstjänst till mobil nätanslutningspunkt.

Det har såväl i tidigare utredningar som till oss framhållits att bestämmelsen är otydlig i flera avseenden. Från både brottsbekämpande myndigheter och teleoperatörer har det framförts att det råder en viss osäkerhet när det gäller vilka verksamheter som omfattas av bestämmelsen. I bestämmelsen används vissa begrepp som definieras i andra bestämmelser i nya LEK. Vissa av definitionerna har ändrats utan att det har föranlett någon ändring av den aktuella bestämmelsen. I 1 kap. 7 § nya LEK finns vissa definitioner. En *elektronisk kommunikationstjänst* definieras som en tjänst som vanligen tillhandahålls mot ersättning via elektroniska kommunikationsnät och som – med undantag för dels tjänster i form av tillhandahållande av innehåll som överförs med hjälp av elektroniska kommunikationsnät och elektroniska kommunikationstjänster, dels tjänster som innebär utövande av redaktionellt ansvar över sådant innehåll – är en

1. internetanslutningstjänst enligt artikel 2.2 i Europaparlamentets och rådets förordning (EU) 2015/2120 av den 25 november 2015 om åtgärder rörande en öppen internetanslutning och slutkundsavgifter för reglerad kommunikation inom EU och om ändring av direktiv 2002/22/EG och förordning (EU) nr 531/2012,
2. interpersonell kommunikationstjänst, eller
3. tjänst som utgörs helt eller huvudsakligen av överföring av signaler, såsom överföringstjänster som används för tillhandahållande av maskin-till-maskin-tjänster eller för rundradio.

En *telefonitjänst* definieras som en elektronisk kommunikationstjänst som innebär en möjlighet att ringa eller ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan.

Ett *samtal* definieras som en förbindelse genom en allmänt tillgänglig interpersonell kommunikationstjänst som möjliggör talkommunikation i båda riktningarna.

Som nämnts ovan framhöll regeringen redan inför att gamla LEK trädde i kraft år 2003 att det, med hänsyn till den ändrade terminologin i gamla LEK, fanns behov av att klargöra att det med telefonitjänst till fast nätanslutningspunkt i detta sammanhang avsågs såväl överföring av lokala, nationella och internationella samtal som telefax och datakommunikation med viss angiven lägsta datahastighet, som ger funktionell tillgång till internet.

Det kan konstateras att terminologin i 9 kap. 29 § första stycket nya LEK, främst vad gäller tillhandahållande av en allmänt tillgänglig telefonitjänst till en fast nätanslutningspunkt, är ålderdomlig och stämmer dåligt överens med definitionerna i lagen.

Den tekniska utvecklingen innebär att tjänster kan tillhandahållas på fler sätt och att gränserna för olika typer av tjänster flyter ihop. Teknikutvecklingen, tillsammans med den nu ålderdomliga terminologin, har gjort och gör att det är svårt att klargöra vilka verksamheter som omfattas av anpassningsskyldigheten.

Anpassningsskyldigheten är i praktiken ofta en förutsättning för att beslut om HAK och HÖK över huvud taget ska kunna verkställas. Bestämmelserna om HAK och HÖK är teknikneutrala och således inte begränsade till en viss typ av teknik för att befordra meddelanden. Enligt reglerna får meddelanden avlyssnas eller övervakas om de överförs eller har överförts i ett elektroniskt kommunikationsnät till eller från ett telefonnummer eller annan adress. Om det är fråga om fast telefoni, mobiltelefoni eller internet har alltså ingen betydelse för frågan om meddelandet som sådant kan träffas av tvångsmedelsregleringen. Trots att den legala möjligheten finns att avlyssna eller övervaka ett visst meddelande, medför avsaknaden av anpassningsskyldighet för vissa verksamheter att tvångsmedelsbesluten sannolikt inte kan verkställas.

HAK och HÖK får inte avse meddelanden som endast överförs eller har överförts i ett elektroniskt kommunikationsnät som med hänsyn till sin begränsade omfattning och omständigheterna i övrigt får anses vara av mindre betydelse från allmän kommunikationssyn-

punkt (27 kap. 20 § tredje stycket RB). Enligt förarbetena avses med elektroniskt kommunikationsnät av mindre betydelse från allmän kommunikationssynpunkt bl.a. system för snabbtelefoner, porttelefoner, pc-nät och liknande utrustning inom eller intill en bostad samt hörselslingor för hörselskadade och interna system för personsökning i form av fasta installationer. Även interna kommunikationer på mindre arbetsplatser, via t.ex. pc-nät, utgör nät av mindre betydelse. Motsatsen gäller vanligtvis beträffande sådana telenät som är uppkopplade mot och används för kommunikation via allmänt tillgängliga telenät eller större företagsnät. Detsamma gäller fristående datorer som är försedda med modem och datorer i t.ex. små interna nätverk som via andra nätverk kommunicerar med varandra eller med t.ex. elektroniska anslagstavlor, informationsdatabaser eller andra informationssystem.[13]

För att säkerställa att beslut om HAK och HÖK kan verkställas fullt ut skulle anpassningsskyldigheten behöva gälla för all verksamhet som avser tillhandahållande av elektroniska kommunikationsnät och elektroniska kommunikationstjänster i sådana nät, med undantag av sådana nät som får anses vara av mindre betydelse från allmän kommunikationssynpunkt. En sådan avgränsning skulle dock innebära att anpassningsskyldigheten träffar ett mycket stort antal tillhandahållare, även sådana som tillhandhåller nät och tjänster som inte är allmänt tillgängliga.

För att minska risken för otydligheter anser vi att anpassningsskyldigheten bör knytas till sådana begrepp som regleras i nya LEK.

I våra direktiv anges att det inbördes förhållandet mellan lagringsskyldigheten och anpassningsskyldigheten kan leda till tolkningsproblem. Lagringsskyldigheten enligt 9 kap. 19 § nya LEK gäller för de tillhandahållare som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § samma lag. De som ska anmäla sin verksamhet enligt den bestämmelsen är tillhandahållare av allmänna elektroniska kommunikationsnät som vanligen tillhandahålls mot ersättning och av allmänt tillgängliga elektroniska kommunikationstjänster. Skyldigheten att anmäla verksamheten gäller inte för tillhandahållare av Noik eller för verksamhet som består enbart i överföring av signaler via tråd för utsändning till allmänheten av program som avses i 1 kap. 2 § YGL (2 kap. 1 § första och andra styckena nya LEK). Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om

[13] Se prop. 1994/95:227 s. 27 och 31.

ytterligare undantag från kravet på anmälan (2 kap. 1 § tredje stycket nya LEK).

Även om det är svårt att tydligt klargöra vilka verksamheter som omfattas av anpassningsskyldigheten kan det sammanfattningsvis konstateras att denna skyldighet och den nu gällande lagringsskyldigheten till vissa delar träffar olika verksamheter. När det gäller tillhandahållande av allmänna elektroniska kommunikationsnät omfattar lagringsskyldigheten endast sådana som vanligen tillhandahålls mot ersättning medan ett sådant krav inte gäller för att omfattas av anpassningsskyldigheten. Vid tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster gäller anpassningsskyldigheten fullt ut för sådana tjänster till en mobil nätanslutningspunkt medan det finns begränsningar när det gäller tjänster till en fast nätanslutningspunkt (se avsnitt 10.3 10.3angående tillkomsten av och överväganden om anpassningsskyldighetens utformning).

Mot bakgrund av den snabba tekniska utvecklingen bör anpassningsskyldighetens omfattning anges på ett så teknikneutralt sätt som möjligt, t.ex. utan att viss typ av överföringsteknik med viss lägsta datahastighet anges i författningstexten.

Anpassningsskyldigheten bör som nyss nämnts knytas till sådana begrepp som regleras i nya LEK. Vi anser att anpassningsskyldigheten i 9 kap. 29 § första stycket nya LEK som utgångspunkt bör träffa samma aktörer som omfattas av skyldigheten att anmäla sin verksamhet i 2 kap. 1 § nya LEK och därmed av de som omfattas av den nu gällande lagringsskyldigheten i 9 kap. 19 § nya LEK. Vi har i avsnitt 9.6.1 föreslagit att tillhandahållare av allmänt tillgängliga Noik ska omfattas av reglerna om lagring av abonnemangsuppgifter, om nationell säkerhetslagring och om riktad lagring. Vi återkommer i avsnitt 10.4.3 till frågan om en anpassningsskyldighet för tillhandahållare av Noik.

Vi kan inte se några skäl till att anpassningsskyldigheten i dag borde vara mer begränsad när det gäller elektroniska kommunikationstjänster som tillhandahålls till fast nätanslutningspunkt än till mobil nätanslutningspunkt, eftersom tillgång till internet och datakommunikation sedan länge kan ges såväl till fast som mobil nätanslutningspunkt.

När det gäller tillhandahållare av allmänna elektroniska kommunikationsnät bör anpassningsskyldigheten, liksom skyldigheten att anmäla sin verksamhet enligt 2 kap. 1 § nya LEK, gälla beträffande

sådana tjänster som vanligen tillhandahålls mot ersättning. I praktiken tillhandahålls tjänster av här aktuellt slag i princip alltid mot någon form av ersättning.

Som nämnts ovan kan en elektronisk kommunikationstjänst bestå av en internetanslutningstjänst, en interpersonell kommunikationstjänst eller en tjänst som helt eller huvudsakligen utgörs av överföring av signaler, såsom överföringstjänster som används för tillhandahållande av maskin-till-maskin-tjänster eller för rundradio. Rundradio innebär distribution av signaler för ljudradio (radio) och bilder (television) avsedda för en större allmänhet.[14] Vad som utgör en tjänst som helt eller huvudsakligen utgörs av överföring av signaler är inte alltid lätt att avgöra i praktiken. I EU-domstolens praxis har tillhandahållandet av ett baspaket via kabel ansetts utgöra en elektronisk kommunikationstjänst i den mån tjänsten i huvudsak omfattar överföring av tv-sändningar genom kabelnätet till konsumenternas mottagare (se dom UPC Nederland, C-518/11, p. 44 och 47). Överföringen av signaler behöver inte ske i tillhandahållarens nät, utan det väsentliga är om tillhandahållaren är ansvarig gentemot slutanvändarna för den överföring av signaler som säkerställer att slutanvändarna tillhandahålls den tjänst som de abonnerar på (se dom UPC DTH, C-475/12, p. 43).[15] Det finns ingen skyldighet att anmäla sådan verksamhet som enbart består i överföring av signaler via tråd för utsändning till allmänheten av program som avses i 1 kap. 2 § YGL (se 2 kap. 1 § första och andra styckena nya LEK). Liksom tidigare bör anpassningsskyldigheten inte omfatta sådan verksamhet.

Det finns dock skäl att överväga om samtliga övriga tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster (som inte är Noik) bör omfattas av anpassningsskyldigheten eller om vissa tillhandahållare ska undantas från denna skyldighet. Det kan konstateras att den delen av anpassningsskyldigheten, som reglerar kravet på skyndsamhet och format vid utlämnandet av uppgifter, sedan den 1 augusti 2022 omfattar alla tillhandahållare som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § nya LEK (se 9 kap. 29 b § nya LEK). Det finns enligt vår bedömning inte skäl att undanta några allmänt tillgängliga elektroniska kommunikationstjänster som består av internetanslutningstjänster eller interpersonella kommunikations-

[14] Se http://www.ne.se/uppslagsverk/encyklopedi/lång/rundradio. Hämtat den 20 april 2023.
[15] Se prop. 2021/22:136 s. 123.

tjänster från anpassningsskyldigheten enligt 9 kap. 29 § första stycket nya LEK.

Det kan dock ifrågasättas om allmänt tillgängliga maskin-till-maskin-tjänster bör omfattas av den nu aktuella delen av anpassningsskyldigheten. Med maskin-till-maskin-tjänster avses tjänster som omfattar automatisk överföring av data och information mellan enheter eller mjukvarubaserade tillämpningar med liten eller ingen mänsklig medverkan.[16] Tjänsterna kan exempelvis användas för övervakning, mätning, styrning, transport och logistik i bl.a. bilar, tåg, elmätare, hemlarm och gräsklippare.[17] De brottsbekämpande myndigheterna har uttryckt att det finns ett visst behov av att kunna inhämta lokaliseringsuppgifter från tillhandahållare av maskin-till-maskin-tjänster som används i bilar. I takt med att allt fler föremål kan kopplas upp mot internet kan också behovet av att kunna inhämta uppgifter från sådana tjänster öka, t.ex. som alternativ till traditionell spaning.

Man skulle visserligen kunna tänka sig att införa en anpassningsskyldighet enbart för vissa typer av maskin-till-maskintjänster förutsatt att det finns ett tillräckligt behov av det. Det finns dock en risk för att en sådan differentiering av anpassningsskyldigheten ger upphov till nya tolkningsproblem gällande gränserna för vilka tjänster som omfattas av skyldigheten. Eftersom de brottsbekämpande myndigheternas behov av åtkomst till uppgifter från maskin-till-maskin-tjänster i nuläget avser främst lokaliseringsuppgifter avseende fordon och då behovet inte framstår som påtagligt, anser vi att det skulle vara oproportionerligt att ha en anpassningsskyldighet för tillhandahållare av sådana tjänster. Vi föreslår därför att tillhandahållare av maskin-till-maskin-tjänster generellt sett inte ska omfattas av anpassningsskyldigheten i 9 kap. 29 § första stycket nya LEK.

Även om tillhandahållare av maskin-till-maskin-tjänster, enligt vårt förslag, inte ska vara skyldiga att anpassa sin verksamhet så att beslut om HAK och HÖK kan verkställas så omfattas de av skyldigheten att lämna ut abonnemangsuppgifter m.m. enligt 9 kap. 33 § nya LEK. De bör därför omfattas av kraven på skyndsamhet och format vid utlämnandet av uppgifter och rätten till ersättning vid sådant utlämnande. Tillhandahållare av allmänt tillgängliga maskin-till-maskin-tjänster bör alltså även fortsättningsvis omfattas av anpassnings-

[16] Se prop. 2021/22:136 s. 407.
[17] Se promemorian Registrering av kontantkort, m.m., Ds.2020:12 s. 51.

skyldigheten vid utlämnande av uppgifter enligt 9 kap. 29 b § nya LEK och rätten till ersättning enligt 9 kap. 29 a § nya LEK.

Sammanfattningsvis föreslår vi att anpassningsskyldigheten i 9 kap. 29 § första stycket nya LEK ska omfatta alla tillhandahållare av elektroniska kommunikationsnät och elektroniska kommunikationstjänster som ska anmälas enligt 2 kap. 1 § nya LEK förutom sådana som tillhandahåller maskin-till-maskin-tjänster.

Om anpassningsskyldigheten bestäms på detta sätt, får man enligt oss en rimlig avvägning avseende vilka tillhandahållare som ska vara anpassningsskyldiga enligt 9 kap. 29 § första stycket nya LEK. En sådan reglering skulle också minska risken för tolkningsproblem, eftersom den förhåller sig till samma terminologi som nya LEK i övrigt. Regleringen skulle dessutom vara mer teknikneutral.

Vårt förslag innebär att vissa ytterligare tillhandahållare än i dag kommer att omfattas av anpassningsskyldigheten i 9 kap. 29 § första stycket nya LEK, nämligen tillhandahållare av vissa allmänt tillgängliga elektroniska kommunikationstjänster till fast nätanslutningspunkt. Anpassningsskyldigheten för tillhandahållare av sådana tjänster skulle alltså gälla utan de begränsningar som finns i dag, t.ex. gällande internetanslutningstjänster. Tillhandahållare av maskin-till-maskin-tjänster till mobil nätanslutningspunkt omfattas av nu gällande anpassningsskyldighet. Vårt förslag innebär att sådana tillhandahållare inte längre ska omfattas av anpassningsskyldighet i 9 kap. 29 § första stycket nya LEK. Slutligen innebär vårt förslag att anpassningsskyldigheten för tillhandahållare av allmänna elektroniska kommunikationsnät endast ska gälla beträffande sådana tjänster som vanligen tillhandahålls mot ersättning.

Anpassningsskyldigheten innebär att tillhandahållarna måste anpassa sina system så att tvångsmedelsbesluten kan verkställas. Den innebär också att tillhandahållarna måste ha en organisation och en bemanning för att se till att tvångsmedlen kan verkställas utan dröjsmål. Vi återkommer till dessa frågor i vår konsekvensanalys, avsnitt 13. Möjligheten för regeringen eller den myndighet regeringen bestämmer att meddela närmare föreskrifter om anpassningsskyldigheten och att i enskilda fall besluta om undantag från kravet på anpassningsskyldighet bör gälla även i förhållande till tillhandahållare som genom våra förslag träffas av anpassningsskyldigheten.

10.4.2 Utformningen av anpassningsskyldigheten

Utöver frågan om vilka verksamheter som bör omfattas av anpassningsskyldigheten finns det anledning att överväga hur skyldigheten ska komma till uttryck i författningsregleringen. Vi kan konstatera att det i vissa fall finns olika uppfattningar om innebörden av nuvarande reglering. Även den tekniska utvecklingen ger anledning att överväga behovet av justeringar i regleringen (se avsnitt 10.4.1). I detta avsnitt överväger vi därför frågor om hur anpassningsskyldigheten bör utformas.

Inhämtning enligt inhämtningslagen

Utredningens förslag: Anpassningsskyldigheten ska uttryckligen omfatta även beslut om inhämtning enligt inhämtningslagen.

Enligt 9 kap. 29 § första stycket nya LEK ska en verksamhet bedrivas så att beslut om HAK och HÖK kan verkställas och så att verkställandet inte röjs. Anpassningsskyldigheten anses även gälla vid beslut om inhämtning med stöd av inhämtningslagen.[18]

Inhämtningslagen ger brottsbekämpande myndigheter befogenhet att i underrättelseverksamhet hämta in uppgifter om elektronisk kommunikation från den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst som inte är en Noik. Vi har i avsnitt 9.6.3 föreslagit att inhämtning av uppgifter med tillämpning av inhämtningslagen även ska få ske från tillhandahållare av Noik.

Det är en viss skillnad mellan bestämmelserna i 1 § inhämtningslagen och 27 kap. 19 § RB när det gäller tillstånd till HÖK i realtid. Enligt inhämtningslagen får nämligen inhämtningen av uppgifter om meddelanden (trafikuppgifter) endast avse uppgifter som *har* överförts, dvs. historiska uppgifter. I övrigt motsvaras de uppgifter som får hämtas in enligt inhämtningslagen av de uppgifter som får hämtas in inom ramen för ett tillstånd till HÖK enligt 27 kap. 19 § RB. Det kan i detta sammanhang nämnas att Utredningen om preventiva tvångsmedel

[18] Se t.ex. direktiven till denna utredning s. 10 och promemorian Registrering av kontantkort, m.m., Ds. 2020:12, s. 121 f.

(Ju 2021:15) har i uppdrag att ta ställning till om, och i så fall på vilket sätt, tillämpningsområdet för inhämtningslagen bör utvidgas.[19]

Det har till oss framförts att det i vissa fall har ifrågasatts om anpassningsskyldigheten gäller vid beslut om inhämtning enligt inhämtningslagen. Enligt vår uppfattning måste anpassningsskyldigheten rimligen omfatta såväl tillstånd som har sin grund i rättegångsbalkens regler som i inhämtningslagens. I annat fall hade bestämmelsen ändrats i samband med att inhämtningslagen infördes. I förtydligande syfte föreslår vi att bestämmelsen i 9 kap. 29 § första stycket nya LEK uttryckligen ska ange att anpassningsskyldigheten omfattar även beslut enligt inhämtningslagen.

Frågor om kryptering m.m.

Utredningens bedömning: Nuvarande föreskrifter om anpassningsskyldighet innefattar en skyldighet för tjänsteleverantörerna att se till att de brottsbekämpande myndigheterna kan tillgodogöra sig uppgifter om och innehållet i meddelanden oavsett ny teknik och nya tillämpningar. Något förtydligande av föreskrifterna behövs därför inte.

Den tekniska och samhälleliga utvecklingen har medfört svårigheter att använda hemliga tvångsmedel. Informationen som ska avlyssnas eller övervakas är ofta krypterad. Dels finns möjlighet att på egen hand köpa programvara för att kryptera meddelanden, dels är det mycket vanligt att t.ex. tillhandahållare av kommunikationstjänster har inbyggda funktioner som utför kryptering. Krypteringstjänster har i stor utsträckning ett legitimt syfte och möjliggör för användare att kunna kommunicera med varandra utan risk för att utomstående ska kunna ta del av innehållet. Men krypteringen för också med sig att de brottsbekämpande myndigheterna ofta inte kan ta del av innehållet i kommunikationen med mindre än att tillhandahållaren av tjänsten har funktioner för detta.

[19] Se tilläggsdirektiv till Utredningen om preventiva tvångsmedel, dir. 2022:32.

Internationell roaming m.m.

En fråga som enligt våra direktiv kan ha betydelse för anpassningsskyldigheten är hur internationell roaming sker. Roaming innebär att en användares kommunikationsutrustning, t.ex. en mobiltelefon, kopplas upp mot ett mobilnät som tillhör en annan operatör än den som användaren har abonnemang hos. Roaming inom EU/EES reglerades tidigare genom ett antal förordningar, bl.a. den s.k. roamingförordningen (Europaparlamentets och Rådets förordning [EU] 531/2012). Denna förordning ändrades genom införandet av den s.k. TSM-förordningen (Europaparlamentets och Rådets förordning [EU] 2015/2120). Sedan den 1 juli 2022 gäller en omarbetning av förordningen – Europaparlamentets och rådets förordning (EU) 2022/612 av den 6 april 2022 om roaming i allmänna mobilnät i unionen. Förordningen gäller till och med den 30 juni 2032.

Internationell roaming innebär alltså att en användares utrustning kopplas upp mot ett mobilnät som tillhör en leverantör i ett annat land när användaren befinner sig i det landet. I 4G-nätet använder sig leverantörerna av en teknisk lösning som innebär att all kommunikation sker med hemleverantörens IMS (IP Multimedia Subsystem, dvs. en arkitektur för ip-baserade tjänster i mobiltelefonisystemet). Detta kallas Home Routing, dvs. trafiken dirigeras hem.

En person med ett utländskt abonnemang som befinner sig i Sverige och använder 4G-nätet utnyttjar alltså endast delar av infrastrukturen i det svenska mobilnätet medan all kommunikation sker genom hemleverantörens IMS. En följd av detta är att i princip all trafik genom 4G-nätet från en användare med ett utländskt abonnemang som befinner sig i Sverige förblir krypterad och blir oläslig för såväl de svenska operatörerna som de svenska brottsbekämpande myndigheterna.

Internationell roaming kan såväl i 4G-nätet som 5G-nätet ske enligt flera olika standarder. Till skillnad från 2G- och 3G-näten, där det besökta landets telefoniväxlar kommer åt kommunikationen, gör Home Routing det tekniskt omöjligt för nationella brottsbekämpande myndigheter i det besökta landet att bereda sig tillgång till användarens kommunikation.

Problemet för de brottsbekämpande myndigheterna med s.k. S8 Home Routing i 4G-nätet kommer även finnas i 5G-nätet men då benämnas N9 Home Routing.

Inom EU finns för närvarande inte något initiativ som syftar till att hantera problematiken. Däremot har GSMA (en sammanslutning som bl.a. samordnar och informerar om internationell roaming) tagit fram en rekommendation för hur man kan lösa frågor om internationell roaming och brottsbekämpande myndigheters åtkomst till information.

Polismyndigheten har i en skrivelse i mars 2019 till de fyra stora teleoperatörerna och till PTS, klargjort sin ståndpunkt i frågan om internationell roaming. I skrivelsen anger Polismyndigheten bl.a. att den teleoperatör som har för avsikt att ingå ett roamingavtal med en utländsk operatör måste säkerställa att meddelandena kan levereras så att brottsbekämpande myndigheter enkelt ska kunna ta hand om signalerna vid HAK och HÖK, dvs. både metadata om meddelanden och innehållet i meddelanden. Det innebär enligt Polismyndigheten att den utländska operatören i roamingavtal ska förbinda sig att inte aktivera egen kryptering.

Enligt Polismyndigheten finns det bland teleoperatörerna olika inställningar till frågan om anpassningsskyldighet vid internationell roaming. Det finns inte, såvitt känt, något ställningstagande i denna fråga från någon tillsynsmyndighet inom EU.

5G-nätet m.m.

I våra direktiv anges att introduktionen av 5G kan medföra behov av förändringar av anpassningsskyldigheten.

Den teknikutveckling som 5G innebär kommer att möjliggöra mobilnät med betydligt högre dataöverföringshastigheter, kortare fördröjningar i nätverk, högre kapacitet och avsevärt högre täthet av enheter än tidigare men även större fokus på integritet och kryptering. 5G kan exempelvis medföra tillämpningar av flera krypterings- och autentiseringsprocesser. De tjänster som ofta förknippas med 5G är tillämpningar inom det som kallas ”sakernas internet” (eng. internet of things), där föremål kopplas upp och kommunicerar via internet. Det kan t.ex. röra sensorer, mätare och liknande i kontroll- och säkerhetssystem i både hem-, kontors-, industri och offentlig miljö, självstyrande fordon, fjärrstyrda robotar och avancerade tillämpningar för artificiell intelligens.

Det finns två versioner av 5G, nämligen 5G NSA (non stand alone) och 5G SA (stand alone). 5G NSA, som används redan i dag, går genom 4G-nätets centrala infrastruktur men med nya radiobasstationer. 5G SA innebär en ny central infrastruktur (corenät) som använder som använder nya identifierare och nya format på lokaliseringsuppgifter. 5G SA kommer att innebära en förtätning av basstationer som kan ge mer precisa lokaliseringsuppgifter. 5G SA har en inbyggd möjlighet till så kallad totalsträckskryptering (eng. end-to-end encryption). Sådan kryptering skulle väsentligt försvåra för de brottsbekämpande myndigheterna att få tillgång till elektronisk kommunikation trots domstolsbeslut om tillstånd till HÖK eller HAK. 5G SA innebär en komplex struktur som är helt olik dagens mobilnät.

Särskilt om kryptering av identifierare

Det kommer också att vara möjligt att kryptera identifierare (alltså uppgifter som gör det möjligt att identifiera enheter och användare) i 5G-nätet. Varje elektronisk kommunikationstjänst behöver kunna kopplas till en abonnent. Abonnenten måste vara en identifierbar fysisk eller juridisk person. I 5G-nätet kommer temporära identifieringsparametrar, SUCI (eng. Subscription Concealed Identifier) kunna kopplas till en permanent identifieringsparameter, SUPI (eng. Subscription Permanent Identifier). SUPI i 5G-nätet är motsvarigheten till IMSI-nummer i 4G-nätet. Förenklat kan man säga att IMSI-nummer i 4G ibland färdas öppet över det luftburna nätet medan SUPI i 5G-nätet aldrig färdas öppet över nätet, utan omvandlas till en temporär identifierare i form av SUCI och blir på så sätt anonymiserad. En sådan kryptering skulle göra det närmast omöjligt för brottsbekämpande myndigheter att identifiera enskilda enheter eller var vissa personer, såsom misstänkta gärningsmän, befinner sig. Kringinformation (metadata) som normalt är tillgänglig via HÖK, såsom plats, datum, tid, samtalslängd, samtal och motpart, skulle därmed kunna gå förlorad för brottsbekämpande myndigheter.

Krypteringen av identifierare påverkar de brottsbekämpande myndigheternas möjlighet att använda bl.a. s.k. IMSI-catchers. En IMSI-catcher är ett tekniskt hjälpmedel för identifiering av mobila elektroniska kommunikationsutrustningar som närmast kan betraktas som

en portabel basstation för mobiltelefoni (falsk basstation). En IMSI-catcher kan presentera uppgifter om vilka IMSI- och IMEI-nummer som finns i närheten av IMSI-catchern. I detta avseende finns det likheter med den information som man kan få tillgång till vid s.k. basstationstömningar genom HÖK.

Användningen av en IMSI-catcher skiljer sig dock på flera sätt från en HÖK. För det första är användningen av IMSI-catchers en oreglerad polisiär arbetsmetod som stöds av principen om att avlyssning av etern är fri (se 9 kap. 27 § andra stycket p. 3 nya LEK). För det andra används IMSI-catchers som ett operativt spaningshjälpmedel snarare än ett verktyg för inhämtning av bevisning. För det tredje omfattar inhämtningen av uppgifter genom en IMSI-catcher inte trafikuppgifter utan endast uppgifter om identifierare, alltså abonnemangsuppgifter.

Genom att kombinera användandet av en IMSI-catcher med traditionell fysisk spaning är det möjligt att ta reda på vilka kommunikationsutrustningar och abonnemang en viss person använder sig av, eller var personen befinner sig.[20]

Användningen av IMSI-catchers syftar huvudsakligen till att inhämta sådan information som är nödvändig för att senare kunna begära beslut om HAK och HÖK.

Att SUPI omvandlas till SUCI innebär att de brottsbekämpande myndigheterna inte utan tillhandahållarnas hjälp kommer kunna lokalisera och identifiera kommunikationsutrustningar med hjälp av en motsvarighet till en IMSI-catcher eller på annat sätt. Därmed minskar möjligheterna för myndigheterna att få tillstånd till HAK och HÖK avseende relevanta adresser kopplade till en misstänkt gärningsman. För att de brottsbekämpande myndigheterna ska kunna identifiera den elektroniska kommunikationsutrustningen behövs teleoperatörernas hjälp att koppla ihop temporära SUCI med permanenta SUPI.

Våra överväganden

Bestämmelsen i 9 kap. 29 § första stycket nya LEK är enligt vår uppfattning tydlig när det gäller kravet på att beslut om HAK och HÖK ska kunna verkställas. Regleringen lämnar inget utrymme för olika tolkningar.

[20] Se betänkandet Särskilda spaningsmetoder, SOU 2010:103, s. 295 ff.

I förarbetena till bestämmelsen om anpassningsskyldighet anfördes bl.a. följande.

Anpassningsskyldigheten innebär att innehållet i meddelandet måste göras tillgängligt samtidigt som det förmedlas eller i vart fall i omedelbar anslutning till att det förmedlas. Det är också nödvändigt att polisen kan identifiera meddelandet. Likaså finns ett behov av att det avlyssnade meddelandet görs tillgängligt för polisen på ett sådant sätt och på en sådan plats att det enkelt kan tas om hand av polisen. Detta innebär att om teleoperatören, av effektivitetsskäl eller andra skäl, kodar eller komprimerar telemeddelandena, dessa måste levereras i klartext. Detsamma gäller för krypterade meddelanden. En förutsättning i det sistnämnda fallet är givetvis att det är teleoperatören som tillhandahåller krypteringssystemet och att teleoperatören har möjlighet att dekryptera meddelandet. Teleoperatörerna bör alltså inte kunna avkrävas telemeddelandena i klartext om abonnenten själv komprimerar eller krypterar sina meddelanden.[21]

Även dessa förarbetsuttalanden ger ett starkt stöd för att de aktörer som träffas av bestämmelsen har en skyldighet att bedriva verksamheten på sådant sätt att krypterade uppgifter kan lämnas ut till de brottsbekämpande myndigheterna i läsbar form när krypteringsmöjligheten tillhandahålls av den anpassningsskyldige aktören.

Den tekniska utvecklingen har inneburit att det i dag finns andra aktörer än teleoperatören eller abonnenten som kan kryptera eller på andra sätt göra uppgifterna otillgängliga för de brottsbekämpande myndigheterna. Frågan är om någon anpassningsskyldighet föreligger när det inte är teleoperatören själv som tillhandahåller krypteringsmöjligheten.

Vi menar att man vid kryptering m.m. som tillhandahålls av tredje part måste se till vilken av parterna, dvs. teleoperatören eller abonnenten, som har möjliggjort sådan kryptering. I de fall abonnenten anlitar någon annan för att kryptera uppgifter, kan teleoperatören inte anses vara ansvarig för att dekryptera dessa. I realiteten torde det inte ens vara möjligt för teleoperatören. Om teleoperatören, som en del i tillhandahållandet av tjänsten, ingår avtal med annan, måste det dock anses åligga teleoperatören att säkerställa att kravet på anpassningsskyldighet kan uppfyllas. När en svensk teleoperatör exempelvis ingår roamingavtal med en utländsk operatör om att tillåta den utländska operatörens kunder att nyttja det svenska kommunikations-

[21] Se prop. 1995/96:180 s. 27.

nätet, måste alltså teleoperatören säkerställa att uppgifterna vid tvångsmedelsanvändningen kan levereras i läsbar form till de brottsbekämpande myndigheterna både när det gäller uppgifter om meddelanden och innehållet i meddelanden. Annars uppfyller teleoperatören inte sin anpassningsskyldighet.

Även i de fall teleoperatören för sina kunder möjliggör totalsträckskryptering eller annat som förhindrar verkställighet av de aktuella tvångsmedlen åligger det operatören att göra uppgifterna tillgängliga för brottsbekämpande myndigheter i läsbar form. Vi menar att detta gäller även om krypteringslösningen ingår i den standard som tillämpas, såsom den krypteringsmöjlighet som finns i 5G SA. Även om abonnenten själv kan välja att använda krypteringsmöjligheten eller inte är det teleoperatören som har anslutit sina tjänster till 5G och således möjliggjort krypteringen. Teleoperatörerna måste i dessa fall kunna tillämpa lösningar så att exempelvis ett beslut om HAK kan verkställas, antingen genom att krypteringen i dessa fall slås av eller genom att avlyssningsuppgifterna dekrypteras. Det räcker alltså inte att uppgifter från tvångsmedelsanvändningen lämnas ut i krypterad form, ens om dekrypteringsnycklar tillhandahålls. All trafik till eller från en användarutrustning eller en unik identifierare måste kunna avlyssnas, oberoende av nätverk eller nätverkskonfiguration.

Vi menar alltså att nuvarande föreskrifter om anpassningsskyldighet innefattar en skyldighet för teleoperatörerna att se till att de brottsbekämpande myndigheterna kan tillgodogöra sig meddelanden oavsett om de är krypterade eller förmedlade genom roaming, så länge det är teleoperatören som har möjliggjort denna kryptering eller roaming.

Det kan ifrågasättas om reglerna om anpassningsskyldighet är rimliga för teleoperatörerna mot bakgrund av den teknikutveckling som varit efter det att reglerna tillkom och om de därför bör ändras i något avseende. Det ställs olika krav på teleoperatörerna som i vissa avseenden kan förefalla oförenliga. Teleoperatörerna har t.ex. skyldigheter när det gäller att bedriva samtrafik och att göra tjänster interoperabla med andra tillhandahållares tjänster.[22] Det finns också krav på teleoperatörerna att vidta åtgärder för att hantera risker som hotar säkerheten i nät och tjänster och för att säkerställa ett skydd för behandlade uppgifter.[23] Bland de åtgärder som vidtas i syfte att skydda

[22] Se 5 kap. nya LEK.
[23] Se 8 kap. nya LEK.

uppgifterna är användningen av olika krypteringslösningar. Samtidigt innebär teleoperatörernas anpassningsskyldighet vid internationell roaming att de i roamingavtal måste kunna säkerställa att uppgifterna vid tvångsmedelsanvändningen kan levereras i läsbar form till de brottsbekämpande myndigheterna, vilket kan innebära krav på att viss kryptering slås av. Särskilt för små teleoperatörer kan det vara svårt att vid ingående av roamingavtal ställa krav på att utländska operatörer ska se till att uppgifterna kan tillhandahållas utan viss kryptering. Såväl Polismyndigheten som vissa teleoperatörer har emellertid till oss uppgett att det finns standarder som möjliggör ett verkställande av tvångsmedelsbeslut även beträffande personer med utländska abonnemang som befinner sig i Sverige, att sådana standarder inte innebär att kommunikationen förmedlas helt utan kryptering och att det pågår ett arbete för att förbättra sådana standarder. För att dessa standarder ska kunna tillämpas måste de dock regleras i respektive roamingavtal. Om den utländske operatören vägrar att gå med på sådana villkor, t.ex. för att lagstiftningen i aktuellt land kräver att kommunikationen är krypterad på visst sätt, kan följden bli att den svenske operatören inte kan erbjuda sina kunder att använda sitt abonnemang i det landet och att utländska abonnenter inte kan använda denne operatörs nät i Sverige.

Även beträffande krypterings- och autentiseringsprocesser som möjliggörs i 5G-nätet kan det vara svårt för den enskilde operatören att ta fram lösningar som möjliggör dekryptering eller motsvarande av de uppgifter som omfattas av tvångsmedelsbeslut. Utan att gemensamma standarder tas fram och tillämpas, som möjliggör verkställighet av tvångsmedelsbeslut, skulle operatörerna alltså kunna vara förhindrade att t.ex. ansluta sig till 5G SA.

Anpassningsskyldigheten kan alltså i vissa avseenden innebära en stor utmaning för teleoperatörerna. Det är därför mycket angeläget att det så snabbt som möjligt tas fram och tillämpas internationella standarder som möjliggör för brottsbekämpande myndigheter att i läsbar form kunna få del av uppgifter som omfattas av tvångsmedelsbeslut när nya nät, standarder, tillämpningar eller annan ny teknik introduceras. Situationen är dock inte unik för Sverige. Lagstiftare, myndigheter och teleoperatörer ställs inför samma frågor också i andra länder. Vi menar att Sverige bör arbeta aktivt för att det inom EU ska påbörjas ett arbete med gemensamma standarder.

Vårt uppdrag syftar till att säkerställa att de brottsbekämpande myndigheternas tillgång till information förbättras och upprätthålls över tid i takt med teknikutvecklingen och förändrade kommunikationsvanor, samtidigt som respekten för mänskliga rättigheter säkerställs. Mot denna bakgrund framstår det inte som rimligt att nu införa lättnader i anpassningsskyldigheten på grund av att den tekniska utvecklingen har gjort det svårare för teleoperatörerna att uppfylla sin anpassningsskyldighet. En grundläggande princip bör vara att det är tekniken som ska följa lagstiftningen och inte lagstiftningen som ska följa tekniken.

De brottsbekämpande myndigheterna behöver ha tillgång till ändamålsenliga och verkningsfulla verktyg för att kunna förhindra, upptäcka, utreda och lagföra brott. Brottsligheten är i förändring, liksom kriminellas handlingssätt och hur de kommunicerar. Tillgång till information och bevisning från elektroniska kommunikationer är ofta av stor betydelse i utredningar av allvarlig brottslighet. Som tidigare nämnts har den tekniska utvecklingen och nya kommunikationsmönster gjort att mycket av den information som tidigare varit tillgänglig för brottsbekämpande myndigheter inte längre går att komma åt. Bekämpning av allvarlig brottslighet är ett viktigt allmänt intresse i ett demokratiskt samhälle. Vi menar därför att en rimlig utgångspunkt är att brottsbekämpande myndigheter ska kunna förebygga och utreda brott samt samla bevis som kan leda till åtal även vid införande av ny teknik, nya lösningar och nya kommunikationsnät. Detta gäller även om det bara är en liten del av all kommunikation som faktiskt är föremål för beslut om hemliga tvångsmedel.

Eftersom det finns olika uppfattningar om hur långt anpassningsskyldigheten sträcker sig skulle det kunna finnas anledning att överväga om bestämmelserna språkligt bör förtydligas utan att ändras i sak.

Ett förtydligande skulle exempelvis kunna införas i 9 kap. 29 § första stycket nya LEK om att verksamheten, *oavsett nya tekniska lösningar eller överenskommelser*, ska bedrivas så att beslut om HAK, HÖK och inhämtning enligt inhämtningslagen kan verkställas och så att verkställandet inte röjs. Detta är emellertid enligt vår mening redan innebörden av den aktuella bestämmelsen. Att föreslå förtydliganden av detta eller liknande slag kan öppna för tolkningsproblem, t.ex. genom oriktiga motsatsslut. Enligt vår uppfattning bör det därför inte införas något sådant förtydligande i bestämmelsen.

Vidare skulle det kunna övervägas om ett förtydligande bör göras i 9 kap. 29 b § andra stycket nya LEK avseende i vilken form som uppgifterna ska lämnas ut, t.ex. att *uppgifterna ska vara läsbara för de mottagande myndigheterna även om innehållet i och uppgifter om meddelandet skickas i krypterad form*. Men även här menar vi att paragrafen ska förstås på detta sätt och att den inte bör ge utrymme för missförstånd. Här kan argumenteras mot förtydliganden på samma sätt som ovan. I detta sammanhang kan också hänvisas till vad som anges i förarbetena till ändringen i den del av anpassningsskyldigheten som avser krav på skyndsamhet och format vid utlämnande av uppgifter, som trädde i kraft i augusti 2022. Regeringen anförde där att kravet i 9 kap. 29 b § andra stycket nya LEK inte enbart innebär att uppgifter som lämnas ut ska göras tillgängliga på ett sådant sätt att de är läsbara, vilket i princip var fallet redan med den tidigare regleringen. Uppgifterna ska även vara sammanställda på ett sådant strukturerat sätt att de enkelt kan komma till användning i det brottsbekämpande arbetet. Enligt regeringen kan ett sätt att uppfylla kravet vara att använda sig av i förväg överenskomna format baserade på etablerade standarder.[24]

Ytterligare en fråga, som har att göra med den ovan redovisade användningen av IMSI-catchers, är om teleoperatörerna bör ha någon form av omedelbar skyldighet att medverka till identifieringen av mobila elektroniska kommunikationsutrustningar när permanenta identifieringsparametrar förvandlas till temporära identifieringsparametrar i den luftburna delen av 5G-nätet. Som nämnts ovan försvinner möjligheten för de brottsbekämpande myndigheterna att kunna identifiera kommunikationsutrustningar genom motsvarigheten till IMSI-catchers vid förvandlingen av identifieringsparametrarna. Endast teleoperatören, som har tillgång till dekrypteringsnycklar, kan koppla de temporära parametrarna med de permanenta.

Som framgår av avsnitt 6 har vi föreslagit att uppgifter om abonnemang som genereras och behandlas i tjänsteleverantörernas verksamhet ska lagras. Det innefattar även kopplingen mellan tillfälliga och permanenta identifierare. I avsnitt 7 har vi föreslagit att uppgifter om kopplingen mellan tillfälliga och permanenta identifierare ska kunna omfattas av ett beslut om nationell säkerhetslagring. I avsnitt 8 har vi föreslagit att kopplingen mellan tillfälliga och permanenta identifierare ska omfattas av geografiskt riktad lagring och att dessa upp-

[24] Se prop. 2021/22:183 s. 50 och 74.

gifter kan omfattas av utökad riktad lagring. Uppgifterna kommer således att lagras en viss tid.

De brottsbekämpande myndigheterna har framhållit den stora nyttan och det påtagliga behovet i den brottsbekämpande verksamheten av att omedelbart kunna identifiera kommunikationsutrustningen. Utan en sådan möjlighet minskar möjligheten att ens kunna ansöka om HAK och HÖK. Det är alltså fråga om de brottsbekämpande myndigheternas *omedelbara* tillgång till en typ av abonnemangsuppgift.

De brottsbekämpande myndigheternas problem med att inte kunna identifiera kommunikationsutrustningar genom en kommande form av IMSI-catchers är visserligen en följd av krypteringen i 5G-nätet. Det är emellertid inte en fråga om att teleoperatörerna ska anpassa sin verksamhet så att beslut om vissa hemliga tvångsmedel kan verkställas.

En lösning skulle kunna vara att teleoperatörerna i nära realtid lämnar ut uppgift om kopplingen mellan den tillfälliga identifieraren som är av intresse för de brottsbekämpande myndigheterna och den permanenta identifieraren. Ett sådant utlämnande torde förutsätta att utlämnandet sker elektroniskt. De brottsbekämpande myndigheterna har också tagit upp frågan om ett elektroniskt utlämnande av andra abonnemangsuppgifter från teleoperatörer till brottsbekämpande myndigheter. Myndigheterna menar att ett sådant utlämnande skulle spara tid och kostnader för teleoperatörerna och kunna effektivisera den brottsbekämpande verksamheten. Frågan om och hur ett elektroniskt utlämnande av uppgifter om abonnemang ska ske omfattas inte av våra direktiv.

Redan i dag finns dock möjlighet för PTS att meddela ytterligare föreskrifter om hur uppgifter ska lämnas ut enligt 9 kap. 29 b § nya LEK (se 9 kap. 13 § 3 nya FEK). Som nämnts ovan gäller kravet på skyndsamhet och format enligt 9 kap. 29 b § nya LEK även vid utlämnande av abonnemangsuppgifter och vår ståndpunkt ovan är att dessa krav gäller oavsett ny teknik och nya tillämpningar. Det finns också krav på att tillhandahållaren vidtar de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling (se 8 kap. 5 § nya LEK) och på tystnadsplikt vid en begäran om utlämnande av uppgift om abonnemang enligt 9 kap. 33 § första stycket 2 nya LEK (se 9 kap. 32 § 5 nya LEK).

Enligt vår bedömning finns det ingenting som hindrar att ett elektroniskt utlämnande av uppgifter om abonnemang kommer till stånd genom överenskommelser mellan de brottsbekämpande myndigheterna och teleoperatörerna. Att meddela närmare föreskrifter om hur uppgifterna ska lämnas ut eller att se över överenskommelser mellan de brottsbekämpande myndigheterna och teleoperatörerna i takt med den tekniska utvecklingen, exempelvis när det gäller realtidslösningar eller annat elektroniskt utlämnande av uppgifter, är en angelägen uppgift för berörda aktörer.

Sammanfattningsvis föreslår vi inga ändringar eller förtydliganden av själva utformningen av anpassningsskyldigheten i 9 kap. 29 § första stycket eller 9 kap. 29 b § nya LEK.

10.4.3 En anpassningsskyldighet för tillhandahållare av Noik

Utredningens förslag: Tillhandahållare av allmänt tillgängliga Noik ska omfattas av en skyldighet att bedriva verksamheten så att beslut om HAK, HÖK och inhämtning enligt inhämtningslagen kan verkställas och så att verkställandet inte röjs. Samma tillhandahållare ska också omfattas av skyldigheterna att utan dröjsmål lämna ut uppgifter till brottsbekämpande myndigheter samt att ordna uppgifterna och göra dem tillgängliga i ett format som gör att de enkelt kan tas om hand.

Vi har i tidigare avsnitt föreslagit att tillhandahållare av allmänt tillgängliga Noik ska omfattas av lagringsskyldighet enligt 9 kap. 19 a–19 d §§ nya LEK såvitt gäller samtal och meddelanden med anknytning till Sverige. Vi har vidare föreslagit att tillhandahållare av Noik ska omfattas dels av den tystnadsplikt för uppgifter om abonnemang, innehållet i ett elektroniskt meddelande och trafikuppgifter (annan uppgift som angår ett särskilt elektroniskt meddelande) som föreskrivs i 9 kap. 31 § nya LEK när det gäller kommunikation som till någon del sker i Sverige, dels av den tystnadsplikt som hänför sig till användningen av vissa hemliga tvångsmedel m.m. enligt 9 kap. 32 § nya LEK. Vi har också föreslagit att skyldigheten att i brottsbekämpande syfte lämna ut uppgifter om abonnemang och om vilka övriga tillhandahållare av elektroniska kommunikationsnät eller kommunikationstjänster som har deltagit vid överföringen av ett meddelande

som omfattas av ett föreläggande enligt 27 kap. 16 § RB (enligt 9 kap. 33 § första stycket 2 och 5 nya LEK) ska gälla även för tillhandahållare av Noik. Vi har också föreslagit att inhämtning av trafik- och lokaliseringsuppgifter med tillämpning av inhämtningslagen ska få ske från tillhandahållare av Noik. Vi har konstaterat att trafik- och lokaliseringsuppgifter redan enligt dagens reglering om HÖK kan inhämtas hos tillhandahållare av Noik. Det kan vidare konstateras att det inte finns något hinder mot att uppgifter om innehållet i ett meddelande hämtas in från tillhandahållare av Noik genom ett beslut om HAK.

Frågan är i vad mån tillhandahållare av Noik bör omfattas av en anpassningsskyldighet av motsvarande slag som teleoperatörerna har. Som nämnts ovan är anpassningsskyldigheten i praktiken ofta en förutsättning för att beslut om HAK, HÖK och inhämtning enligt inhämtningslagen över huvud taget ska kunna verkställas. Utgångspunkten måste rimligen vara att en sådan anpassningsskyldighet bör gälla med hänsyn till den stora nytta och det påtagliga behov som de brottsbekämpande myndigheterna har när det gäller tillgång till uppgifter om elektronisk kommunikation (se avsnitt 5.5).

I samband med införandet av nya LEK konstaterade regeringen att anpassningsskyldigheten för allmänt tillgängliga elektroniska kommunikationstjänster gäller för den som tillhandahåller en sådan tjänst till en mobil nätanslutningspunkt. Regeringen anförde att, eftersom tillhandahållandet av Noik inte sker till en mobil nätanslutningspunkt, de i dagsläget inte omfattas av bestämmelserna om anpassningsskyldighet. Noik tillhandahålls nämligen oberoende av huruvida den underliggande internettjänsten är fast eller mobil.[25]

När det gäller skyldigheten att bedriva verksamheten så att beslut om de angivna hemliga tvångsmedlen kan verkställas och så att verkställandet inte röjs kan inledningsvis konstateras att de stora tillhandahållarna av Noik i Sverige, såsom Google, Meta, Apple och Microsoft, är globala bolag som tillhandahåller sina tjänster i många olika länder. Dessa bolag har inte sitt säte i Sverige och deras verksamhet styrs till övervägande del av regler i andra länder. Det kan därför finnas skäl att överväga hur långt svensk legislativ jurisdiktion sträcker sig när det gäller att reglera sådana bolags verksamhet.

Som framgår av avsnitt 5.4.1 finns det inget hinder för en stat att utöva lagstiftande eller dömande makt över personer och egendom

[25] Se prop. 2021/22:136 s. 329.

som befinner sig utomlands och över händelser som äger rum utanför statens territorium, så länge det handlar om egna medborgare eller egendom som har en länk till staten och förutsatt att det inte råder något folkrättsligt förbud mot ett sådant utövande av jurisdiktion. Liksom beträffande frågan om en svensk skyldighet för tillhandahållare av allmänt tillgängliga Noik att lagra uppgifter om elektronisk kommunikation med svensk anknytning, torde det inte finnas något hinder mot att i Sverige stifta lagar som ställer krav på sådana tillhandahållare att bedriva sin verksamhet på visst sätt. Detta gäller under förutsättning att det handlar om verksamhet med viss anknytning till Sverige, såsom att tjänsten tillhandahålls här. Vi menar alltså att vi i nationell författning kan ställa krav på utländska tillhandahållare som erbjuder olika slags varor och tjänster i landet under förutsättning att kraven är nödvändiga i ett demokratiskt samhälle för att tillgodose ett allmänt intresse och att kraven är proportionerliga i förhållande till det syfte som ska tillgodoses. Det vore vidare en orimlig konkurrensfördel för utländska tillhandahållare om dessa inte skulle kunna träffas av sådana krav som åligger inhemska tillhandahållare när det gäller samma sorts varor eller tjänster som tillhandahålls i Sverige. Det finns också många exempel på svenska krav som ställs även på utländska aktörer som tillhandahåller varor och tjänster i Sverige. Som exempel kan nämnas att de krav som ställs vid förmedling av korttidsboende via onlinetjänsten Airbnb. Ett annat exempel är krav enligt taxitrafiklagen (2012:211) som ställs vid taxitjänster som förmedlas av onlinetjänsten Uber. Däremot torde det inte vara möjligt att här reglera sådan verksamhet som inte har någon anknytning till Sverige, exempelvis regler om hur en utländsk tillhandahållare av Noik ska bedriva sin verksamhet i andra länder.

Bekämpning av allvarlig brottslighet är ett viktigt allmänt intresse i ett demokratiskt samhälle. Rimliga krav måste därför kunna ställas på dem som i Sverige tillhandahåller elektroniska kommunikationsnät- och tjänster för att tillgodose de brottsbekämpande myndigheternas berättigade behov av att kunna ta del av uppgifter som är nödvändiga för att förebygga, upptäcka, förhindra, utreda och beivra allvarliga brott.

En annan fråga är om en tillhandahållare av Noik kan eller vill följa en reglering som innebär att verksamheten ska bedrivas så att beslut om vissa angivna tvångsmedel kan verkställas, exempelvis om den svenska regleringen inte är förenlig med tillhandahållarens affärs-

modell eller är svår att förena med krav i andra länder. En konsekvens av en nationell sådan reglering kan därför bli att tillhandahållaren väljer att inte tillhandahålla sina tjänster i Sverige. Med tanke på att den tekniska utvecklingen inte är unik för Sverige finns det dock anledning att tro att anpassningskrav kommer att ställas på sådana tillhandahållare också i andra länder.

Vidare kan det i vissa avseenden vara förenat med svårigheter att kontrollera om tillhandahållaren efterlever regleringen, t.ex. när det gäller kravet på att verkställandet av tvångsmedelsbesluten inte röjs för obehöriga. På samma sätt som vi har resonerat i frågan om en lagringsskyldighet för tillhandahållare av Noik bör dock inte eventuella svårigheter att kontrollera att skyldigheter uppfylls innebära att man avstår från att införa nödvändiga och proportionerliga skyldigheter.

Det kan vidare vara förenat med svårigheter att hantera eventuella tillhandahållare som vägrar att följa reglerna om att bedriva verksamheten så att tvångsmedelsbesluten kan verkställas. Tillsynsmyndigheten kan förelägga tillhandahållaren att fullgöra en sådan skyldighet men för att verkställa beslut om viten eller sanktionsavgifter hos tillhandahållare i andra länder behövs möjligheter till rättslig hjälp. Huruvida rättslig hjälp kan ges beror på i vilket land åtgärden ska verkställas och t.ex. vilka avtal Sverige har med det landet.

Som nämnts tidigare är kommunikation genom Noik ofta krypterad på ett sådant sätt att informationen inte är möjlig att läsa i klartext, vare sig av tillhandahållaren eller av den som har tillstånd till HAK. Även uppgifter om meddelanden (dvs. trafikuppgifter), t.ex. vem som kommunicerar med vem samt när och var detta sker, kan vara krypterade. Man kan därför ställa sig frågan om det är rimligt att tillhandahållare av Noik ska behöva ändra sina tjänster i detta avseende för att tillgodose ett svenskt krav på att kunna verkställa vissa tvångsmedelsbeslut. Vi menar att det är lika rimligt att ställa ett sådant krav på tillhandahållare av Noik som på traditionella teleoperatörer. En tillhandahållare av Noik torde dessutom ha lättare att anpassa sin verksamhet, eftersom denne helt självständigt kan utveckla sin tjänst medan teleoperatörerna ofta är beroende av hur tillverkare av telekomutrustning bygger sina produkter och hur internationella standarder för t.ex. interoperabilitet utformas.

En anpassningsskyldighet vid totalsträckskryptering skulle kunna genomföras på olika vis. Skyldigheten skulle t.ex. kunna bestå i att tillhandahållaren inför en försvagning i krypteringen och informerar

myndigheterna om denna försvagning, eller att tillhandahållaren inför en dold bakdörr i sin tjänst. Vi menar dock att sådana alternativ inte är acceptabla eftersom de skulle innebära en generell försvagning av informationssäkerheten för kommunikation som förmedlas genom tjänsten. Efter vad vi inhämtat under utredningen, skulle det emellertid vara fullt möjligt för tillhandahållare av Noik att ändra sina tjänster så att kraven på säkerhet och skyddet för kommunikationen tillgodoses, även om en anpassningsskyldighet införs. För en tjänst där totalsträckskryptering erbjuds skulle tillhandahållaren exempelvis kunna välja att utforma tjänsten så att totalsträckskryptering där bara sändare och mottagare kan läsa meddelanden endast används mellan konton som vid tidpunkten för kommunikationen inte omfattas av ett beslut om HAK. Om något av de konton som kommunicerar omfattas av ett beslut om HAK, skulle däremot endast sådan kryptering användas som tillåter att behörig myndighet kan ta del av trafiken i klartext. Med fördel skulle arrangemanget även kunna utformas så att endast myndighet och Noik tillsammans kan aktivera sådan avlyssning. Det betyder naturligtvis inte att skyddet för kommunikationen helt skulle sättas ur spel. Kryptering kan ändå behövas för att skydda kommunikationen i förhållande till externa aktörer, men den får inte vara sådan att den hindrar användningen av hemliga tvångsmedel. Detta tillvägagångssätt skulle minimera riskerna för att någon utomstående tar del av kommunikationen olovligen, samtidigt som hemliga tvångsmedel ändå kan verkställas i enlighet med lag. Tjänsten skulle dock behöva utformas på ett sätt som gör att avsändare och mottagare, så långt det är möjligt, inte kan avgöra om avlyssning sker.

Enligt vår bedömning skulle ett alternativ som det sistnämna vara acceptabelt ur såväl integritetsskydds- som informationssäkerhetsperspektiv. Kommunikation skulle skyddas mot avlyssning utom i de fall när staten har en lagstadgad rätt att ta del av kommunikationen. Det bör dock betonas att utformningen av de tekniska lösningarna för att genomföra anpassningsskyldigheten bäst görs av tillverkarna själva.

Efter genomförd anpassningsskyldighet ligger det i både myndigheternas och tillhandahållarnas intresse att tjänsten är så väl skyddad som möjligt mot avlyssning från obehöriga. Det skulle inte heller finnas något skäl för myndigheterna att i förhållande till tillhandahållare hemlighålla information som myndigheterna har om tekniska sårbarheter i tjänsterna, vilket däremot skulle vara fallet om uppgifter endast kunde inhämtas genom hemlig dataavläsning.

Vi bedömer att området också är lämpat för internationell standardisering, exempelvis när gäller hur en begäran om HAK hos en tillhandahållare av Noik ska utformas, liksom i vilka format uppgifterna ska överföras från tillhandahållarna till myndigheterna.

Ett synsätt som innebär att själva syftet med totalsträckskryptering är att uppgifterna inte ska kunna vara åtkomlig alls, inte ens för brottsbekämpande myndigheter, åsidosätter det allmänna intresset i demokratiska samhällen att kunna förebygga, upptäcka, förhindra, utreda och beivra allvarliga brott, inklusive sådana brott som hotar själva det demokratiska systemet och den nationella säkerheten.

Det kan i detta sammanhang nämnas att kommissionens förslag till förordning för att bekämpa sexuella övergrepp mot barn, om förslaget antas, kommer innebära att bl.a. tillhandahållare av Noik får en skyldighet att spåra, anmäla och rapporterna innehåll när det gäller sexuella övergrepp mot barn.[26] Tillhandahållare av Noik måste alltså i sådant fall kunna ta del av innehållet i meddelanden även om kommunikationen är krypterad. Som vi nämnt i avsnitt 9.4.2 har förslaget väckt debatt i Sverige under våren 2023.

Mot bakgrund av det nu anförda anser vi att tillhandahållare av Noik bör omfattas av anpassningsskyldigheten som föreskrivs i 9 kap. 29 § första stycket nya LEK. Med hänsyn till den tekniska utvecklingen bör det, liksom i nu gällande reglering, inte i lagen anges hur anpassningsskyldigheten ska uppfyllas. Liksom för tillhandahållare av andra elektroniska kommunikationstjänster bör en anpassningsskyldighet för tillhandahållare av Noik begränsas till att gälla enbart för sådana tjänster som är allmänt tillgängliga.

Vidare bör tillhandahållare av allmänt tillgängliga Noik omfattas av skyldigheterna i 9 kap. 29 b § nya LEK. Bestämmelsen innebär att uppgifter som gäller brottslig verksamhet eller misstanke om brott ska lämnas ut till brottsbekämpande myndigheter utan dröjsmål och på ett sådant sätt att utlämnandet inte röjs. Uppgifterna ska också ordnas och göras tillgängliga i ett format som gör att de enkelt kan tas om hand. Som nämnts tidigare omfattar dessa skyldigheter alla typer av uppgifter som omfattas av tystnadsplikten i 9 kap. 31 § nya LEK, dvs. uppgifter om abonnemang, innehållet i ett elektroniskt meddelande och trafikuppgifter (dvs. annan uppgift som angår ett sär-

[26] Se Proposal for a Regulation of the European Parliament and the Council laying down rules to prevent and combat child sexual abuse (COM (2022) 209 final) och Faktapromemoria 2021/22: FPM99.

skilt elektroniskt meddelande), men även lokaliseringsuppgifter som inte är trafikuppgifter enligt 9 kap. 29 b § tredje stycket nya LEK. Eftersom lokaliseringsuppgifter som inte är trafikuppgifter nu omfattas av tystnadsplikten enligt den av oss föreslagna ändringen i 9 kap. 31 § första stycket, behövs ingen särreglering i 29 b § tredje stycket.

Vi har beträffande lagringsskyldigheten och tystnadsplikten avseende kommunikationsuppgifterna för tillhandahållare av Noik föreslagit att dessa skyldigheter ska gälla endast vid sådan kommunikation som till någon del sker i Sverige. När det däremot gäller regleringen om de brottsbekämpande myndigheternas åtkomst till uppgifter om elektronisk kommunikation behövs ingen motsvarande begränsning. Vilka uppgifter som dessa myndigheter får hämta in styrs i stället av de bestämmelser som reglerar åtkomsten. Även dataskyddsregleringen påverkar myndigheternas möjlighet att inhämta och på annat sätt behandla uppgifter. De brottsbekämpande myndigheterna får nämligen behandla personuppgifter bara om det är nödvändigt för att kunna utföra sina brottsbekämpande uppgifter.[27] Vidare får personuppgifter behandlas bara för särskilda, uttryckligt angivna och berättigade ändamål.[28] Inte heller vid en reglering av anpassningsskyldigheten behövs, enligt vår uppfattning, någon nationell anknytning eftersom den avser verkställigheten av beslut enligt viss åtkomstreglering. Någon bestämmelse om att anpassningsskyldigheten enbart ska gälla vid sådan kommunikation som till någon del sker i Sverige behövs således inte och bör därför inte införas.

Sammanfattningsvis föreslår vi att den som i Sverige tillhandahåller allmänt tillgängliga Noik ska omfattas dels av skyldigheten att bedriva sin verksamhet så att beslut om HAK, HÖK och inhämtning enligt inhämtningslagen kan verkställas och så att verkställandet inte röjs, dels av skyldigheten om skyndsamhet och format vid utlämnande av uppgifter som gäller brottslig verksamhet eller misstanke om brott. Detta bör regleras genom att det i 9 kap. 29 § första stycket nya LEK hänvisas till den som är lagringsskyldig enligt 9 kap. 19 § nya LEK i stället för till den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § nya LEK. Även bestämmelsen i 9 kap. 29 b § nya LEK bör ändras på motsvarande sätt. Några ändringar i föreskrifterna i 27 kap. 25 § första stycket RB eller 9 § preventivlagen behövs inte, eftersom

[27] Se t.ex. 2 kap. 1 § brottsdatalagen (2018:1177) och 2 kap. 1 § lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter.
[28] Se t.ex. 2 kap. 3 § brottsdatalagen och 2 kap. 3 § lagen om Säkerhetspolisens behandling av personuppgifter.

dessa endast anger att de tekniska hjälpmedel som behövs vid HAK och HÖK får användas.

Anpassningsskyldigheten bör inte omfatta historiska uppgifter om kommunikation som skett före ikraftträdandet. Vi föreslår att det införs en övergångsbestämmelse med detta innehåll.

Vilka konsekvenser en svensk anpassningsskyldighet (och andra skyldigheter som vi föreslagit ovan) får för tillhandahållare av Noik, för det allmänna, för enskilda och för näringslivet beror på hur tillhandahållare av Noik väljer att förhålla sig till den svenska regleringen. Tillhandahållarna kan som sagt välja att inte längre tillhandahålla sina tjänster i Sverige, vilket inte bara innebär konsekvenser för tillhandahållarna själva utan även t.ex. för deras användare som kan behöva använda någon annan kommunikationstjänst. Om tillhandahållare av Noik väljer att tillhandahålla sina tjänster i Sverige, kommer våra förslag att innebära ekonomiska och andra konsekvenser för såväl dem som andra. Vi återkommer i avsnitt 13 till konsekvenserna av våra förslag.

10.4.4 Rätten till ersättning för tillhandahållare av Noik

Utredningens förslag: Tillhandahållare av allmänt tillgängliga Noik ska ha rätt till ersättning vid utlämnande av uppgifter till brottsbekämpande myndigheter.

I 9 kap. 29 a § nya LEK regleras rätten till ersättning för den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § nya LEK. Rätten till ersättning gäller för kostnader som uppstår när uppgifter om abonnemang, innehållet i ett elektroniskt meddelande, trafikuppgifter och lokaliseringsuppgifter som inte är trafikuppgifter lämnas ut till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott. Bestämmelserna om ersättning gäller också när uppgifter hämtas in av brottsbekämpande myndigheter för andra ändamål än brottsbekämpning, t.ex. när Polismyndigheten hämtar in uppgifter för att eftersöka en försvunnen person. I de fall det är särskilt föreskrivet ska ersättningen beräknas enligt schablon. Det är den myndighet som har begärt uppgifterna som ska betala ersättningen.

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

Eftersom vi föreslår att tillhandahållare av allmänt tillgängliga Noik ska omfattas av en lagringsskyldighet och vissa skyldigheter när det gäller brottsbekämpande myndigheters åtkomst till uppgifter om elektronisk kommunikation, bör dessa tillhandahållare också omfattas av reglerna om ersättning i 9 kap. 29 a § nya LEK. En ändring av paragrafen bör därför göras så att den hänvisar till den som är lagringsskyldig enligt 9 kap. 19 § nya LEK i stället för till den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § nya LEK. Ytterligare en förändring som följer av våra förslag är att det inte behövs någon särreglering i 29 a § andra stycket i fråga om lokaliseringsuppgifter som inte är trafikuppgifter. De omfattas nu av tystnadsplikten enligt den av oss föreslagna ändringen i 9 kap. 31 § första stycket, se avsnitt 10.4.3.

10.4.5 Medverkansskyldighet för tillhandahållare av Noik vid hemlig dataavläsning

Utredningens bedömning: Tillhandahållare av Noik bör inte omfattas av en skyldighet att medverka vid hemlig dataavläsning.

I lagen om hemlig dataavläsning föreskrivs en skyldighet för den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § nya LEK att på begäran medverka i samband med verkställighet av hemlig dataavläsning. Den som medverkar har rätt till ersättning för kostnader som uppstår vid sådan medverkan. Ersättningen ska betalas av den verkställande myndigheten (24 § lagen om hemlig dataavläsning). Vid införandet av lagen anförde regeringen att det med hänsyn till det begränsade antal fall av hemlig dataavläsning det förväntas bli fråga om inte finns skäl att i nuläget införa en anpassningsskyldighet för operatörerna i likhet med den som finns i LEK.[29] Det är inte närmare reglerat vad en medverkan ska avse. Av förarbetena till bestämmelsen framgår att medverkan kan avse t.ex. att en operatör identifierar vilka tjänster en specifik användare har och vilka förbindelser den använder, ger råd avseende vilka tekniska hjälpmedel som kan användas, tillhandahåller möjlighet att installera tekniska hjälpmedel i

[29] Se prop. 2019/20:64 s. 179.

operatörens nät för verkställighet eller bistår med andra liknande stödåtgärder.[30]

Den som i samband med verksamhet som ska anmälas enligt 2 kap. 1 § nya LEK har fått del av eller tillgång till en uppgift som hänför sig till användning av hemlig dataavläsning, får inte obehörigen föra vidare eller utnyttja det han eller hon fått del av eller tillgång till (32 § lagen om hemlig dataavläsning). Bestämmelsen innebär att vem som helst kan omfattas av tystnadsplikten, så länge han eller hon har fått del av eller tillgång till uppgifterna i samband med verksamhet som avses i bestämmelsen. Uppgifter som kan bli föremål för tystnadsplikten kan vara hänförliga till bl.a. tekniken som används vid verkställighet, personen som ska bli föremål för åtgärden, informationssystemet som innehåller uppgifterna som ska läsas av eller den brottsbekämpande myndigheten som ansvarar för verkställighet. Bestämmelsen omfattar varje uppgift som direkt eller indirekt gäller användning av hemlig dataavläsning.[31]

Frågan är om tillhandahållare av allmänt tillgängliga Noik bör omfattas av bestämmelserna om medverkansskyldighet, rätt till ersättning och tystnadsplikt vid verkställighet av hemlig dataavläsning.

Från de brottsbekämpande myndigheterna har det framhållits att, om tillhandahållare av Noik omfattas av en anpassningsskyldighet vid beslut om HAK, HÖK och inhämtning enligt inhämtningslagen, behovet av att använda hemlig dataavläsning och därmed behovet av en medverkan från dessa aktörer minskar. Hemlig dataavläsning är en ingripande och resurskrävande åtgärd som bara ska tillämpas när det finns synnerliga skäl för det. Kan samma information inhämtas på ett mindre integritetskänsligt sätt ska hemlig dataavläsning inte användas. Med hänsyn till att vi ovan har föreslagit att tillhandahållare av allmänt tillgängliga Noik ska omfattas av anpassningsskyldigheten såväl enligt 9 kap. 29 § första stycket som 9 kap. 29 b § nya LEK anser vi att en medverkansskyldighet vid hemlig dataavläsning inte bör införas. Detta ställningstagande grundar sig också på den omständigheten att en sådan skyldighet skulle kunna försätta tillhandahållare av Noik i en svår sits. Om en brottsbekämpande myndighet upptäcker sårbarheter i tillhandahållarens tjänst som skulle kunna nyttjas vid hemlig dataavläsning, skulle en medverkansskyldighet och en därtill kopplad tystnadsplikt kunna innebära att tillhandahållaren genom

[30] Se a. prop. s. 237.
[31] Se a. prop. s. 244.

myndigheten får kännedom om en sårbarhet som de varken får åtgärda eller berätta om. Vi föreslår därför inte någon medverkansskyldighet, rätt till ersättning eller tystnadsplikt vid hemlig dataavläsning för tillhandahållare av Noik.

10.5 Sanktionsavgifter

Utredningens förslag: Ändringar ska göras i föreskrifterna om sanktionsavgifter i nya LEK så att de även avser *dels* den som inte bedriver sin verksamhet så att beslut om inhämtning enligt inhämtningslagen kan verkställas, *dels* den som inte lagrar uppgifter om elektronisk kommunikation på föreskrivet sätt.

Utredningens bedömning: Föreskrifterna om sanktionsavgifter bör även avse tillhandahållare av allmänt tillgängliga Noik som inte uppfyller vissa andra skyldigheter. Någon ändring i föreskrifterna om sanktionsavgifter behöver inte göras för att dessa tillhandahållare ska omfattas av regleringen.

I detta avsnitt överväger vi i vilka avseenden reglerna om sanktionsavgifter bör ändras, inte enbart med anledning av våra förslag om ändringar av anpassningsskyldigheten.

Enligt 12 kap. 1 § första stycket 12 nya LEK ska tillsynsmyndigheten ta ut en sanktionsavgift av den som inte bedriver sin verksamhet så att beslut om HAK och HÖK kan verkställas och så att verkställandet inte röjs i enlighet med 9 kap. 29 § första stycket nya LEK och föreskrifter som har meddelats i anslutning till det stycket. Eftersom vi föreslår att anpassningsskyldigheten i 9 kap. 29 § första stycket nya LEK uttryckligen ska ange att även beslut om inhämtning enligt inhämtningslagen ska omfattas av bestämmelsen bör en följdändring göras i 12 kap. 1 § första stycket 12 nya LEK så att även brister i detta avseende träffas av föreskrifterna om sanktionsavgifter.

Dessutom bör möjligheten till sanktionsavgifter i detta avseende gälla också i förhållande till tillhandahållare av allmänt tillgängliga Noik som inte bedriver sin verksamhet så att beslut om HAK, HÖK och inhämtning enligt inhämtningslagen kan verkställas och så att verkställandet inte röjs. Eftersom vi föreslår att denna skyldighet för tillhandahållare av Noik ska regleras i samma stycke som skyldig-

heten för andra tillhandahållare, dvs. i 9 kap. 29 § första stycket nya LEK behövs ingen ändring göras i 12 kap. 1 § första stycket 12 nya LEK för att dessa tillhandahållare ska omfattas av bestämmelsen.

Tillhandahållare av Noik bör, som en följd av våra förslag, också träffas av föreskrifterna om sanktionsavgifter när det gäller att vidta skyddsåtgärder enligt 8 kap. 5 § nya LEK eller föreskrifter som meddelats med stöd av den paragrafen (12 kap. 1 § första stycket 7 nya LEK), att ordna uppgifter och göra dem tillgängliga i ett format som gör att de enkelt kan tas om hand i enlighet med 29 kap. 29 b § andra stycket nya LEK eller föreskrifter som meddelats i anslutning till det stycket (12 kap. 1§ första stycket 13 nya LEK) och att lämna ut en uppgift enligt 9 kap. 33 § nya LEK (12 kap. 1 § första stycket 15 nya LEK). Några ändringar i nu nämnda föreskrifter i 12 kap. nya LEK behövs inte för att tillhandahållare av Noik ska omfattas av dessa.

Ytterligare en fråga som bör övervägas är om sanktionsavgifter ska kunna tas ut även i förhållande till den som inte uppfyller kraven på att lagra uppgifter enligt 9 kap. 19 a–d §§ och 22 § nya LEK. Skyldigheten att lagra uppgifter om elektronisk kommunikation är samhällsviktig och en bristande efterlevnad av regleringen riskerar att få stora konsekvenser för den brottsbekämpande verksamheten. Utan tillgång till sådana uppgifter som omfattas av eller kan omfattas av lagringsskyldighet kan brottsbekämpande myndigheter över huvud taget inte utreda vissa typer av brott och i andra fall kan förundersökningar behöva läggas ned i brist på bevis.

Även i underrättelseverksamheten kan tillgången till uppgifter om elektronisk kommunikation vara avgörande exempelvis för att aktörer, platser och tidpunkter ska kunna kopplas samman och ge ett tillräckligt underlag för att inleda förundersökning. Det är mycket viktigt för det allmänna att det finns starka incitament att följa lagringsskyldigheten. Vi bedömer att möjligheten för tillsynsmyndigheten att genom förelägganden förenade med vite förmå tillhandahållare att fullgöra sin lagringsskyldighet inte innebär en tillräcklig drivkraft för den som av kostnadsskäl inte vill lagra uppgifter. Sanktionsavgiften skapar alltså ett incitament att undvika överträdelser. Vi anser därför att sanktionsavgifter bör kunna tas ut även vid bristande uppfyllnad av skyldigheterna att lagra uppgifter, alltså även när det gäller tillhandahållare av allmänt tillgängliga Noik.

Vi föreslår därför att det i 12 kap. 1 § första stycket nya LEK förs in en ny punkt med innebörden att tillsynsmyndigheten ska besluta att ta ut en sanktionsavgift av den som inte lagrar uppgifter i enlighet med 9 kap. 19 a–d och 22 §§ och föreskrifter som har meddelats i anslutning till dessa paragrafer.

11 Vissa frågor om exekutiv jurisdiktion

11.1 Inledning[1]

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 inom andra staters territorier, t.ex. att använda hemliga tvångsmedel där.

Elektroniskt lagrade uppgifter kan finnas i flera stater samtidigt eller ständigt förflyttas mellan stater. I Sverige har de folkrättsliga principerna traditionellt tolkats så att svenska brottsbekämpande myndigheter saknar jurisdiktion om uppgifter lagras elektroniskt på annan plats än i Sverige eller om det är okänt var uppgifterna lagras.

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. Det finns därför skäl att se över förutsättningarna, inklusive de folkrättsliga aspekterna, för att införa en särskild lagreglering för exekutiv jurisdiktion i förhållande till elektronisk information som finns utanför Sverige. Enligt våra direktiv ska vi

- analysera de folkrättsliga frågorna om exekutiv jurisdiktion i förhållande till elektroniska uppgifter utanför Sverige, och i denna analys även göra en jämförelse med rättsläget i andra relevanta länder,

[1] Högsta domstolen har den 30 mars 2023 förklarat att genomsökning på distans får ske även om den eftersökta informationen kan vara lagrad i utlandet (se Högsta domstolens beslut i mål Ö 5686-22). Beslutet meddelades efter det att utredningen haft sitt slutsammanträde och avsnitt 11 fått sin utformning. Vi har gjort bedömningen att texterna i avsnittet ändå bör vara kvar, bl.a. därför att vår ansats var något bredare än Högsta domstolens. Vissa justeringar i avsnittet har dock gjorts med anledning av Högsta domstolens beslut.

- ta ställning till om det bör införas en särskild lagreglering för territorialitetsprincipen vid exekutiv jurisdiktion som också tar hänsyn till andra anknytningsfaktorer än var data lagras, och
- vid behov lämna förslag på de författningsändringar och andra åtgärder som bedöms nödvändiga.

11.2 Folkrättsliga källor

För att analysera de jurisdiktionsfrågor som ryms inom vårt uppdrag måste hänsyn tas till de folkrättsliga källor som bestämmer ramen för varje stats jurisdiktion. Det kan inledningsvis konstateras att folkrätten inte är statisk. Den är ständigt i förändring. I artikel 38 i Internationella domstolens stadga, som ofta anses ge uttryck för vilka de folkrättsliga källorna är, anges följande källor.[2]

– Allmänna eller speciella internationella överenskommelser (traktat).
– Internationell sedvänja.
– Allmänna, av de civiliserade folken erkända, rättsgrundsatser.
– Rättsliga avgöranden och de olika ländernas mest sakkunniga författares lärosatser, såsom hjälpmedel för fastställande av gällande rätt.

Internationella överenskommelser är mellanstatliga avtal. Genom att ingå ett traktat inskränks den egna suveräniteten till förmån för avtalet. Det finns dock möjlighet att genom reservationer begränsa skyldigheten att följa de förpliktelser som stadgas i avtalet.

Om ett förhållande inte regleras av ett traktat, kan en stat hänvisa till internationell sedvanerätt. Sedvanerätten skiljer sig från traktat bl.a. genom att vara bindande för alla stater med undantag för det fall då en stat konsekvent motsätter sig sedvanan.[3]

För etablering av internationell sedvanerätt ska två kriterier vara uppfyllda:

- det ska finnas en allmän och enhetlig praxis mellan stater, och
- denna praxis ska av staterna anses vara förpliktigande.

[2] Se Bring m.fl., Sverige och folkrätten, Juno version 6, s. 29 och 30.
[3] Se Linderfalk, Folkrätten i ett nötskal, 2 uppl., s. 77 ff.

Man brukar tala om sedvanerättens objektiva och subjektiva element, dvs. å ena sidan staternas kontinuerliga praxis som är objektivt iakttagbar, och å andra sidan en rättsövertygelse från staternas sida att denna praxis är juridiskt bindande.[4] En förändring av internationell sedvanerätt innebär ofta att stater i ett initialt skede bryter mot en etablerad regel.

Allmänna rättsgrundsatser tar sikte på rättsliga principer av allmän karaktär som genomsyrar rättssystemen i ett stort antal stater, exempelvis principer såsom ne bis in idem och pacta sunt servanda.[5]

Slutligen finns de subsidiära rättskällorna domstolspraxis och doktrin som i egentlig mening inte är att betrakta som rättskällor utan som medel för fastställande av gällande rätt.[6]

11.3 Exekutiv jurisdiktion

Som framgår av avsnitt 11.2 kan en stats jurisdiktion utövas genom rätten att stifta lagar och andra regler (legislativ jurisdiktion), rätten att tillämpa lagstiftningen eller skipa rätt (judiciell jurisdiktion) och rätten att verkställa åtgärder eller förverkliga beslut som fattats inom ramen för lagstiftning och rättskipning (exekutiv jurisdiktion).

Den viktigaste inskränkningen som folkrätten ålägger en stat är att inte utöva makt inom en annan stats territorium. Det finns dock inte något hinder för en stat att utöva lagstiftande eller dömande makt över personer och egendom som befinner sig utomlands och över händelser som äger rum utanför statens territorium, så länge det inte finns något folkrättsligt förbud. Däremot kan verkställighet av nationella lagar och domar (den exekutiva jurisdiktionen) äga rum endast inom det egna territoriet.[7]

Den traditionella utgångspunkten i folkrätten är att det råder ett förbud för stater att vidta verkställighetsåtgärder inom andra staters territorier, t.ex. att använda straffprocessuella tvångsmedel där. Detta följer av den s.k. icke-interventionsprincipen. Staters befogenhet att utöva verkställighetsåtgärder endast inom sitt territorium utgår från den s.k. territorialitetsprincipen. Principerna uppfattas dock inte på

[4] Se Bring, m.fl., Sverige och folkrätten, Juno version 6, s. 31.
[5] Se a.a., s. 33.
[6] Se a.a., s. 34.
[7] Se a.a., s. 107.

samma sätt av alla stater.[8] Tanken med dessa principer är att ingen stat ska kränka en annan stats territoriella integritet (suveränitet). Om ett visst föremål av betydelse som bevisning i en utredning i Sverige exempelvis finns i en lokal i USA, är de svenska brottsbekämpande myndigheterna därför förhindrade att hämta föremålet i lokalen. I stället är myndigheterna som utgångspunkt hänvisade till att begära hjälp av amerikanska brottsbekämpande myndigheter, i första hand genom en begäran om internationell rättslig hjälp.

Förutsättningarna för exekutiv jurisdiktion har vuxit fram i den fysiska världen. Det är oftast enkelt att konstatera var fysiska saker finns förvarade. I den digitala världen ser förhållandena annorlunda ut. Elektroniska uppgifter kan finnas lagrade i flera stater samtidigt eller ständigt vara på väg mellan stater. I många fall är det inte möjligt ens för en tjänsteleverantör av elektronisk kommunikation att tala om var uppgifterna finns i varje givet ögonblick. När detta trots allt är möjligt kan förhållandena ändras på bråkdelen av en sekund.

I Sverige har territorialitetsprincipen och icke-interventionsprincipen när det gäller elektroniska uppgifter traditionellt tolkats så att svenska brottsbekämpande myndigheter saknar jurisdiktion om uppgifter lagras elektroniskt på annan plats än i Sverige eller om det är okänt var uppgifterna lagras, s.k. *loss of location*. Det innebär exempelvis att det tidigare inte har ansetts tillåtet för svenska brottsbekämpande myndigheter att under en förundersökning, där man känner till den misstänkes inloggningsuppgifter, logga in på dennes internetbaserade kommunikationstjänst om tjänsteföretagets servrar kan finnas utanför Sverige.[9] De svenska brottsbekämpande myndigheterna var hänvisade till att i stället begära internationell rättslig hjälp eller utfärda en europeisk utredningsorder för att få fram information som lagrats i utlandet, om man inte kan få fram den på frivillig väg. Denna uppfattning kommer till uttryck i bl.a. promemorian Brott och brottsutredning i IT-miljö[10] och i betänkandet *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet*.[11]

Tidigare har även i praxis funnits en restriktiv syn på möjligheterna att hämta in uppgifter vid loss of location. Högsta förvaltningsdomstolen avslog i april 2021 en begäran om bevissäkring av handlingar

[8] Se prop. 2021/22 :119 s. 85 f.
[9] Se SOU 2017:89 s. 444.
[10] Se Ds 2005:6 s. 282.
[11] Se SOU 2017:89 s. 465.

som lagrats i en molntjänst.[12] Domstolen konstaterade att det saknas bestämmelser om bevissäkring i form av eftersökande och omhändertagande av handlingar som är lagrade i molntjänster och vars fysiska lagringsplats inte är möjlig att lokalisera. Domstolen framhöll vidare att det inte fanns något lagstöd för att bifalla Skatteverkets ansökan om bevissäkring i den del som gäller handlingar lagrade i de aktuella molntjänsterna.

Högsta domstolen har dock i beslut den 30 mars 2023 gjort bedömningen att genomsökning på distans får ske även om den eftersökta informationen kan vara lagrad i utlandet.[13] Enligt domstolen är bestämmelserna om genomsökning på distans utformade så att de medger eftersökning av information som finns lagrad utanför Sverige och det finns inte några folkrättsliga hinder mot sådan eftersökning. Högsta domstolen konstaterade samtidigt att genomsökningen måste ske inom ramen för en svensk brottsutredning, att den måste vidtas med användning av utrustning som finns i Sverige och att genomsökningen ska ske på ett sådant sätt att den eftersökta informationen inte raderas eller på annat sätt påverkas till sitt innehåll.

11.4 Regler i svensk rätt om internationellt straffrättsligt samarbete

Det internationella straffrättsliga samarbetet innebär att stater hjälper varandra med åtgärder avseende utredning av brott, lagföring för brott och verkställighet av domar och slutliga beslut. Sverige har genom flera internationella överenskommelser åtagit sig att samarbeta med andra stater på det straffrättsliga området. Inom EU har en rad rättsakter antagits för att reglera och underlätta det straffrättsliga samarbetet mellan medlemsstaterna. Dessa rättsakter har införlivats i svensk rätt genom nationell lagstiftning eller är direkt tillämpliga i Sverige.

11.4.1 Lagen om internationell rättslig hjälp i brottmål

Genom lagen (2000:562) om internationell rättslig hjälp i brottmål (LIRB) och förordningen (2000:704) om internationell rättslig hjälp i brottmål har innehållet i flera internationella överenskommelser

[12] Se HFD 2021 ref. 23.
[13] Högsta domstolens beslut 30 mars 2023 i mål Ö 5686-22.

som Sverige är bundet av implementerats. LIRB är tillämplig på samarbete som tar sikte på rättsliga förfaranden som gäller utredning om och lagföring för brott. Lagen gäller inte om lagen (2017:1000) om en europeisk utredningsorder är tillämplig.

Enligt 1 kap. 2 § LIRB kan rättslig hjälp lämnas för bl.a. kvarstad, beslag samt husrannsakan och andra åtgärder som avses i 28 kap. rättegångsbalken, HAK, HÖK, och HDA.

Tillstånd till nämnda tvångsmedel lämnas under samma förutsättningar som gäller för motsvarande åtgärder under en svensk förundersökning, enligt rättegångsbalken eller annan lag eller författning, med beaktande av de särskilda bestämmelser som finns i lagen om internationell rättslig hjälp i brottmål (2 kap. 1 §). Vid prövningen om åtgärden kan vidtas i Sverige ska gärningen bedömas enligt svensk rätt och de svenska strafftrösklarna gäller. Det föreligger ett krav på dubbel straffbarhet avseende nämnda tvångsmedel (2 kap. 2 §).

Det finns vissa allmänna regler som gäller för samtliga prövningar av ansökningar om rättslig hjälp från andra länder. En ansökan ska enligt dessa bestämmelser avslås om ett bifall till ansökan skulle kränka Sveriges suveränitet, medföra fara för rikets säkerhet eller strida mot svenska allmänna rättsprinciper eller andra väsentliga intressen. Ansökan får vidare avslås om gärningen har karaktär av ett politiskt brott, gärningen utgör ett militärt brott, om inte gärningen motsvarar även annat brott enligt svensk lag vilket inte är ett militärt brott, det i Sverige har meddelats dom eller beslut om åtalsunderlåtelse eller straffvarning beträffande gärningen, eller omständigheterna annars är sådana att ansökan inte bör bifallas. Om åklagaren eller domstolen finner att ansökan bör avslås på någon av de nu angivna grunderna ska ansökan överlämnas till regeringen som beslutar i frågan (2 kap. 14 och 15 §§).

Svenska åklagares möjligheter att begära rättslig hjälp utomlands är i huvudsak oreglerad, eftersom möjligheterna att få rättslig hjälp av andra stater främst styrs av dessa staters internationella åtaganden och nationella lagstiftning. LIRB hindrar inte att en svensk åklagare ansöker om rättslig hjälp utomlands i den utsträckning den andra staten tillåter det (se 1 kap. 7 § LIRB).

Angående lagen om internationell rättslig hjälp i brottmål, se även avsnitt 5.4.2.

11.4.2 Lagen om en europeisk utredningsorder

Lagen (2017:1000) om en europeisk utredningsorder (EUO) genomför Europaparlamentets och rådets direktiv 2014/41/EU av den 3 april 2014 om en europeisk utredningsorder på det straffrättsliga området.

Enligt 1 kap. 3 § EUO avses med en europeisk utredningsorder antingen

- ett beslut i Sverige som innebär att en utredningsåtgärd ska vidtas i en annan medlemsstat i syfte att inhämta bevisning och som har meddelats av en åklagare eller domstol under en förundersökning eller rättegång i brottmål, eller
- ett beslut i en annan medlemsstat som innebär att en utredningsåtgärd ska vidtas i Sverige i syfte att inhämta bevisning och som har utfärdats eller godkänts av en domare, domstol, undersökningsdomare eller allmän åklagare i ett straffrättsligt förfarande eller i ett annat förfarande avseende straffbara gärningar som inleds vid en administrativ eller rättslig myndighet, när ett beslut i ett sådant annat förfarande kan leda till ett förfarande inför en domstol som är behörig att handlägga brottmål.

I 1 kap. 4 § EUO anges vad en utredningsåtgärd enligt lagen ska avse eller motsvara. Där framgår att bl.a. beslag, kvarhållande av försändelse enligt 27 kap. 9 § RB, en åtgärd enligt 27 kap. 15 § RB eller ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § RB, husrannsakan och andra åtgärder enligt 28 kap. RB (bl.a. genomsökning på distans), HAK, HÖK och hemlig dataavläsning är utredningsåtgärder som avses i lagen.

En utredningsorder som utfärdas i Sverige

En europeisk utredningsorder får enligt 2 kap. 1, 3 och 4 §§ EUO utfärdas i Sverige av åklagare om de förutsättningar som gäller för att vidta utredningsåtgärden under en svensk förundersökning är uppfyllda och åtgärden är nödvändig och proportionerlig. Dessutom krävs, när det är fråga om hemliga tvångsmedel, enligt 2 kap. 5 § EUO att domstol har lämnat tillstånd till att utfärda ordern. Enligt 2 kap. 6 § EUO ska det i utredningsordern anges om några särskilda form-

krav eller förfaranden ska iakttas av den behöriga myndigheten i den andra medlemsstaten vid verkställighet av utredningsordern.

Erkännande och verkställighet i Sverige av en utländsk utredningsorder

När det gäller erkännande och verkställighet i Sverige av en europeisk utredningsorder gäller enligt 3 kap. 1 § EUO att en utredningsorder som sänds över från en annan medlemsstat ska erkännas och verkställas i Sverige om vissa särskilda förutsättningar enligt lagen är uppfyllda och inte annat följer av lagen.

För hemliga tvångsmedel ställs i 3 kap. 4 § EUO som en särskild förutsättning upp att en utredningsorder får erkännas och verkställas endast om den gärning som avses i utredningsordern motsvarar ett brott enligt svensk lag och om övriga förutsättningar som gäller för en motsvarande åtgärd i en svensk förundersökning är uppfyllda.

Bland de obligatoriska vägransgrunderna i 3 kap. 5 § EUO nämns att utredningsordern skulle medföra fara för Sveriges säkerhet. En annan obligatorisk vägransgrund är att utredningsåtgärden inte motsvarar en åtgärd som anges i 1 kap. 4 § EUO. Detta gäller dock inte om en annan utredningsåtgärd kan vidtas som ger motsvarande resultat som den åtgärd som utredningsordern avser.

Underrättelse till annan medlemsstat

I 4 kap. 12–16 §§ EUO finns särskilda regler om underrättelse till annan medlemsstat och om underrättelse från annan medlemsstat till Sverige när HAK, HÖK eller hemlig dataavläsning enligt 2 § första stycket 1–3 lagen om hemlig dataavläsning (dvs. tillstånd för att läsa av eller ta upp kommunikationsavlyssningsuppgifter, kommunikationsövervakningsuppgifter och platsuppgifter) kan ske på den andra statens territorium utan bistånd från denna.

Bestämmelserna tar sikte på fall då en person, som tillsammans med den utrustning som är föremål för åtgärden, befinner sig på ett annat lands territorium och från vilket tekniskt bistånd inte behövs för genomförandet av åtgärden.[14] Typfallet torde vara när den som

[14] Se artikel 31 i Europaparlamentets och rådets direktiv 2014/41/EU av den 3 april 2014 om en europeisk utredningsorder på det straffrättsliga området.

är föremål för en åtgärd rör sig över gränsen och då använder samma mobiltelefon under sin resa. I sådana fall finns det möjlighet för det land i vars territorium åtgärden ska utföras att motsätta sig fortsatt verkställighet av tvångsmedlet.

Angående lagen om en europeisk utredningsorder, se även avsnitt 5.4.2.

11.4.3 Andra författningar som rör internationell rättslig hjälp om bevisinhämtning

Det finns andra författningar än ovan nämnda lagen om internationell rättslig hjälp i brottmål och lagen om en europeisk utredningsorder som kan aktualiseras vid rättslig hjälp. En sådan är lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar. Den lagen innehåller bestämmelser om gemensamma utredningsgrupper, kontrollerade leveranser och brottsutredningar med användning av skyddsidentitet i Sverige. Lagen gäller inte när lagen om en europeisk utredningsorder är tillämplig.

När det gäller inhämtande av information angående bankkonton och banktransaktioner finns enligt flera författningar på finansmarknadsområdet en skyldighet för olika finansiella företag att lämna ut uppgifter om enskildas förhållanden, om det behövs vid utredning av brott i ett inhemskt eller internationellt ärende (t.ex. 2 kap. 20 § lagen om [2004:46] värdepappersfonder).

I lagen (2005:500) om erkännande och verkställighet inom Europeiska unionen av frysningsbeslut regleras ett samarbete som syftar till att säkerställa att bevismaterial inte försvinner, men även en framtida verkställighet av beslut om beslag och förverkande. Lagen gäller inte om lagen om en europeisk utredningsorder, Europaparlamentets och rådets förordning (EU) 2018/1805 av den 14 november 2018 om ömsesidigt erkännande av beslut om frysning och beslut om förverkande, eller lagen (2020:968) med kompletterande bestämmelser till EU:s förordning om ömsesidigt erkännande av beslut om frysning och beslut om förverkande är tillämplig.

11.5 Arbetet inom Europarådet

11.5.1 Budapestkonventionen

I november 1996 beslutade Europarådets straffrättsliga styrkommitté (CDPC) att uppdra åt en expertkommitté att utreda frågor rörande it-relaterad brottslighet. Efter beslut i ministerrådet påbörjades arbetet med en konvention om it-relaterad brottslighet. Europarådets konvention om it-relaterad brottslighet (ETS nr 185, nedan kallad Budapestkonventionen) antogs av ministerrådet den 8 november 2001 och öppnades för undertecknande den 23 november 2001 samt trädde i kraft den 1 juli 2004.

Budapestkonventionen har tre huvudsyften. Det första är att åstadkomma en tillnärmning av ländernas nationella straffrätt beträffande vissa gärningar. Det andra är att säkerställa att det finns nationella processrättsliga bestämmelser som tillgodoser behovet av att utreda och lagföra de brott som behandlas i konventionen och andra brott som begås med hjälp av datorer samt att kunna ta till vara bevisning i elektronisk form. Det tredje är att lägga grunden för ett snabbt och effektivt internationellt samarbete vid bekämpningen av it-relaterade brott.

Ett tilläggsprotokoll öppnades för undertecknande i januari 2003 och trädde i kraft den 1 mars 2006. Tilläggsprotokollet kriminaliserar gärningar av rasistisk och främlingsfientlig natur begångna med hjälp av datorsystem.

Hittills har 67 stater ratificerat konventionen.[15] Även stater som inte är medlemmar i Europarådet har anslutit sig till och ratificerat konventionen, t.ex. Australien, Japan, Kanada och USA. Sverige undertecknade konventionen samma dag som den upprättades och ratificerade konventionen med tilläggsprotokoll den 28 april 2021. Sverige är sedan den 1 augusti 2021 part till konventionen. Sverige har avgett förklaringar om förbehåll i några avseenden. Sverige har bl.a. förbehållit sig rätten att endast tillämpa insamling i realtid av trafikuppgifter på de brott och brottstyper som avses i 27 kap. 19 § tredje stycket RB. Vidare har Sverige förbehållit sig rätten att inte tillämpa insamling i realtid av trafikuppgifter och avlyssning av innehållsuppgifter på meddelanden som överförs inom en tjänsteleverantörs datorsystem som

[15] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures. Hämtat den 20 april 2023.

dels drivs för en sluten användargrupp, dels inte använder allmänna kommunikationsnät och inte är anslutet till ett annat datorsystem.

Den 1 maj 2021 trädde lagändringar som behövdes för tillträdet i kraft.[16] Ändringarna innebär bl.a. att den som innehar en viss elektronisk uppgift som behövs i en brottsutredning kan föreläggas att bevara uppgiften, s.k. bevarandeföreläggande.[17] Dessutom är den som erbjuder elektroniska kommunikationsnät och tjänster skyldig att lämna ut information om vilka som deltagit vid överföringen av ett meddelande som omfattas av ett bevarandeföreläggande.[18] Åtgärderna kan också användas i det internationella straffrättsliga samarbetet.[19]

I Budapestkonventionens artikel 32 finns bestämmelser som gäller staters möjlighet att bereda sig tillgång till uppgifter som lagrats inom andra fördragsslutande staters territorium. Enligt artikel 32 får en fördragsslutande stat utan tillstånd från en annan sådan stat

a) bereda sig åtkomst till lagrade datorbehandlingsbara uppgifter som är allmänt tillgängliga (öppna källor), oavsett var uppgifterna befinner sig geografiskt, eller

b) genom ett datorsystem inom sitt territorium bereda sig åtkomst till eller ta emot lagrade datorbehandlingsbara uppgifter som finns hos annan fördragsslutande stat, om den förstnämnda staten erhåller lagligt och frivilligt samtycke av den person som har laglig rätt att röja uppgifterna för staten via det datorsystemet.

Artikeln medför i sig inte några egentliga förpliktelser utan är att betrakta som en överenskommelse om att tillåta en annan fördragsslutande stat att utan underrättelse eller tillstånd ta del av datorbehandlingsbara uppgifter som tekniskt sett finns på det egna territoriet.[20]

Det ska också noteras att det i Budapestkonventionens artikel 18.1.b finns bestämmelser om att behöriga myndigheter i en stat ska kunna förelägga en tjänsteleverantör som erbjuder sina tjänster inom statens territorium att lämna ut sådana abonnemangsuppgifter

[16] Se prop. 2020/21:72, bet. 2020/21:JuU16, rskr. 2020/21:234.
[17] Se 27 kap. 16 och 16 a §§ RB.
[18] Se 9 kap. 33 § första stycket 5 lagen (2022:482) om elektronisk kommunikation.
[19] Se 1 kap. 2 §, 2 kap. 1 och 2 §§ och 4 kap. 24 c § lagen (2000:562) om internationell rättslig hjälp i brottmål samt 1 kap. 4 §, 2 kap. 16 a §, 3 kap. 5 och 33 a §§ 4 kap. 1 och 2 §§ lagen (2017:1000) om en europeisk utredningsorder.
[20] Se SOU 2013:39 s. 196.

som leverantören har i sin besittning eller under sin kontroll. Detta gäller oavsett var uppgifterna rent faktiskt är lagrade.[21]

11.5.2 Fortsatt arbete inom Europarådet

Inom Europarådet har det inrättats en särskild kommitté med anledning av Budapestkonventionen, Cybercrime Convention Committee (T-CY), vars uppdrag bl.a. är att underlätta tillämpningen och genomförandet av konventionen, vara en plattform för utbytande av information mellan konventionens parter och överväga eventuella ändringar av konventionen. Olika arbetsgrupper har knutits till kommittén. Nedan följer en redogörelse för arbetet i två av dessa grupper.

Transbordergruppens kartläggning

Den s.k. Transbordergruppen redovisade i en rapport 2012 tillämpningen (avseende åren 2009 och 2010) i ett antal olika länder av gränsöverskridande tillgång till elektroniskt lagrade uppgifter. Utredningen om hemlig dataavläsning har sammanfattat kartläggningen på följande sätt.[22]

> Exempel 1) Gränsöverskridande tillgång till uppgifter vid rannsakan
>
> Vid en rannsakan mot en misstänkt person påträffas en påslagen dator. Den brottsbekämpande myndigheten får, av den misstänkte, nödvändiga inloggningsuppgifter för att komma åt uppgifter som lagras elektroniskt på annan plats än lokalt i datorn men som kan tillgängliggöras från datorn.
>
> I de flesta stater som ingick i kartläggningen var det tillåtet för den brottsbekämpande myndigheten att från den misstänktes dator direkt bereda sig tillgång till uppgifter som lagras på annan plats om det inte var uppenbart i vilken stat uppgifterna lagrades. De flesta stater tillät också användning av inloggningsuppgifter erhållna från den misstänkte för sådan direkt tillgång. Om det däremot stod klart att uppgifterna lagras i annan stat än den egna, kunde brottsbekämpande myndigheter i sju länder[23] bereda sig tillgång till uppgifterna medan detta i tio länder[24] då inte var tillåtet, såvida inte den misstänkte själv frivilligt samarbetar i enlighet med vad som gäller enligt artikel 32. I nästan alla stater gjorde det ingen skillnad för frågan om rätten till gränsöverskridande tillgång till

[21] Se TCY Guidance Note # 10 om artikel 18 i Budapestkonventionen (T-CY (2015)16), https://rm.coe.int/16806f943e. Hämtat den 20 april 2023.
[22] Se SOU 2017:89 s. 469 ff.
[23] Finland, Portugal, Polen, Chile, Montenegro, Japan och USA.
[24] Tjeckien, Litauen, Tyskland, Sverige, Turkiet, Bosnien och Hercegovina, Japan, Ungern, Estland och Nederländerna.

uppgifterna om det var brådskande eller förelåg en risk för att informationen skulle kunna försvinna. I vissa stater fanns krav på underrättelse till annan stat.

Exempel 2) Gränsöverskridande tillgång till uppgifter med lagligt erhållna inloggningsuppgifter

Den brottsbekämpande myndigheten har på ett lagligt sätt erhållit inloggningsuppgifter till en tjänst med påstått olagligt innehåll eller graverande (eng. incriminating) bevisning.

De flesta svarande staterna kunde i detta fall bereda sig tillgång till uppgifterna från de brottsbekämpande myndigheternas egna datorer om det inte var uppenbart var uppgifterna lagrades. Även om det stod klart att uppgifterna lagrades utanför den egna staten kunde fortfarande de flesta[25] stater bereda sig sådan tillgång från de egna datorerna.

Exempel 3) Gränsöverskridande tillgång till uppgifter med särskild mjukvara eller tekniska metoder

Under en brottsutredning har den brottsbekämpande myndigheten fått kännedom om ett datorsystem med påstått olagligt innehåll eller graverande bevisning.

Brottsbekämpande myndigheter i vissa stater var, enligt den inhemska lagstiftningen, med hjälp av mjukvara eller andra tekniska metoder tillåtna att skaffa sig tillgång på distans till information om uppgifterna om det inte var uppenbart i vilken stat uppgifterna lagrades. I majoriteten av dessa stater var det dock endast tillåtet under mycket speciella förhållanden. Om det stod klart att det informationssystem som åtgärden skulle riktas mot fanns i en annan stat än den egna var sådana åtgärder endast tillåtna i några få svarande länder.[26]

Exempel 4) Gränsöverskridande tillgång till uppgifter med samtycke

Under en brottsutredning får den brottsbekämpande myndigheten lagligen och frivilligt samtycke från en person att bereda sig tillgång till elektroniska uppgifter som tillhör denne och kan utgöra viktig bevisning men som lagras i en annan stat än den egna.

Brottsbekämpande myndigheter i nästan alla svarande stater kunde i detta fall bereda sig tillgång till och genom nedladdning (eng. download) säkra bevisningen om den person som lämnat sitt samtycke fysiskt fanns i den egna staten. Om personen fanns i staten där uppgifterna lagrades var det fortfarande tillåtet i de flesta svarande stater, medan det i några var otillåtet alternativt tveksamt eller krävde ytterligare förutsättningar eller inte var tydligt reglerat. I de flesta stater var det i detta fall också av betydelse att den som erbjöd tillgången hade rätt att avslöja uppgifterna i den stat där dessa lagrades.

[25] De enda undantagen utgjordes av Tjeckien, Litauen, Sverige, Ungern, Estland och Nederländerna.
[26] Bosnien och Hercegovina, Japan och eventuellt Chile.

Exempel 5) Information erhållen från tjänsteleverantör

Under en brottsutredning måste den brottsbekämpande myndigheten komma åt teknisk information som rör en misstänkt från en internetbaserad tjänstetillhandahållare.

I alla svarande stater gällde att tjänsteleverantören, om uppgifterna avsåg en person i den egna staten samt lagrades och administrerades där, var skyldig att förse den brottsbekämpande myndigheten med uppgifterna. Om uppgifterna däremot avsåg en person i den egna staten men fanns lagrade och administrerades i en annan stat krävdes i de flesta fall internationell rättslig hjälp (mutual legal assistance, MLA). Det gällde också om informationen gällde en person i en annan stat som hade gjort sig skyldig till brott i den egna staten om uppgifterna lagrades och administrerades i en annan stat. Det konstaterades också att många stater upplevde stora problem, både tekniska och juridiska, med att samla in uppgifter som lagrades i en annan stat.

Molnbevisgruppens arbete

Cloud Evidence Group (nedan kallad Molnbevisgruppen) redovisade i slutet av år 2016 en rapport med alternativ och rekommendationer till hur man kan gå vidare med frågor som gäller tillgång till molnlagrad bevisning.

I Molnbevisgruppens rapport[27] diskuteras bl.a. frågor om exekutiv jurisdiktion vid loss of location-situationer. Där anges att det är långt i från klart vilka regler som gäller i fråga om möjligheten för brottsbekämpande myndigheter att bereda sig tillgång till uppgifter som lagrats i molnet. Enligt rapporten är det möjligt att vid molnlagring och loss of location, till skillnad från vad som är fallet i den fysiska världen där fysiska ting endast kan finnas på ett ställe samtidigt, argumentera för andra relevanta anknytningspunkter än platsen där lagring sker för att avgöra vilket land som har exekutiv jurisdiktion. Förutom den stat där uppgifterna finns lagrade eller servern finns skulle exekutiv jurisdiktion enligt rapporten kunna tillkomma exempelvis en stat där tjänsteleverantören har sitt säte, en stat där tjänsteleverantören har en filial, en stat där den misstänkte har träffat avtal om molntjänsten, en stat där den misstänkte finns eller en stat där den misstänkte är medborgare.

En av slutsatserna i rapporten var att det behövs ett gemensamt internationellt ramverk som minskar risker för mellanstatliga kon-

[27] Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, https://rm.coe.int/16806a495e. Hämtat den 20 april 2023.

flikter och stärker skyddet för enskilda, inklusive deras säkerhet. En sådan lösning skulle enligt Molnbevisgruppen t.ex. kunna fokusera mindre på var elektroniskt lagrade uppgifter finns och i stället mer på var personen som innehar informationen och en eventuell målsägande finns. Enligt Molnbevisgruppen skulle de brottsbekämpande myndigheterna med en sådan lösning lagligen och gränsöverskridande kunna bereda sig tillgång till elektroniskt lagrade uppgifter oavsett var de är lagrade så länge det finns förutbestämda begränsningar av när så får ske.

Inför de rekommendationer som Molnbevisgruppen lämnade konstaterade den inledningsvis att internationell rättslig hjälp är den primära vägen för stater att få del av elektronisk bevisning som lagras i andra stater än den egna och att möjligheterna till sådan rättslig hjälp måste uttömmas för att nya och innovativa förslag till lösningar avseende jurisdiktionsfrågorna ska kunna få bred acceptans. De förslag som enligt Molnbevisgruppen bör tas upp till förnyat övervägande vid utarbetandet av ett nytt tilläggsprotokoll till Budapestkonventionen var följande.

- Gränsöverskridande direktåtkomst till uppgifter utan samtycke då de brottsutredande myndigheterna på laglig väg fått fram inloggningsuppgifter till en molntjänst.
- Gränsöverskridande direktåtkomst till uppgifter utan samtycke i god tro eller i nödsituationer eller under liknande omständigheter.
- Tillmätande av andra anknytningsfaktorers betydelse vid bedömningen av territorialitetsprincipen och därmed också av jurisdiktionsfrågan.

Ett andra tilläggsprotokoll till Budapestkonventionen

I juni 2017 antog Cybercrime Convention Committee (T-CY) ett förslag med villkor för utarbetande av ett andra tilläggsprotokoll till Budapestkonventionen.[28] Den 17 november 2021 antogs protokollet av Europarådets ministerkommitté.[29] Protokollet öppnades för under-

[28] Se Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b. Hämtat den 20 april 2023.
[29] Se Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, https://rm.coe.int/1680a49dab. Hämtat den 20 april 2023.

tecknande den 12 maj 2022. Sverige, tillsammans med ett 20-tal andra stater, undertecknade protokollet samma dag. Den 15 november 2021 tillsattes en arbetsgrupp med uppdraget att titta särskilt på frågan om loss of location-situationer. I gruppens mandat[30] ligger dock inte att ta fram ett utkast till ett nytt instrument. Arbetsgruppen har ännu inte (april 2023) redovisat sitt uppdrag.

I tilläggsprotokollet finns bl.a. regler som gör det möjligt för brottsbekämpande myndigheter i en stat att

- rikta en framställning till en enhet som tillhandahåller tjänster för domännamnsregistrering i en annan stat om information som enheten innehar eller kontrollerar, för att identifiera vem som är registrerad innehavare av ett domännamn (artikel 6),
- utfärda en order direkt till en tjänsteleverantör i en annan stat i syfte att få till stånd utlämnande av specificerade, lagrade abonnemangsuppgifter i den tjänsteleverantörens besittning eller kontroll, om abonnemangsuppgifterna behövs för den utfärdande partens specifika brottsutredningar eller straffrättsliga förfaranden (artikel 7),
- utfärda en order som ska överlämnas som en del av en framställning till en annan part i syfte att få en tjänsteleverantör på den anmodade partens territorium att ta fram specificerade och lagrade abonnemangs- och trafikuppgifter som finns i den tjänsteleverantörens besittning eller under dennes kontroll och som krävs för partens specifika brottsutredningar eller straffrättsliga förfaranden (artikel 8).

Protokollet innehåller också regler om påskyndat utlämnande av lagrade datorbehandlingsbara uppgifter i en nödsituation (artikel 9) samt regler om förfaranden vid ömsesidig rättslig hjälp i nödsituationer (artikel 10) och för förfaranden för internationellt samarbete i avsaknad av tillämpliga internationella avtal (artikel 11 och 12). Bestämmelser om villkor och garantier finns i artikel 13 och 14. Protokollet träder i kraft den första dagen i den månad som följer efter utgången av en period om tre månader efter den dag då fem parter till konventionen har uttryckt sitt samtycke till att vara bundna av protokollet.

[30] Se Cybercrime Convention Committee (T-CY), 25th Plenary Meeting of the T-CY, 15 November 2021 (virtual meeting), Meeting report, https://rm.coe.int/0900001680a49f74/. Hämtat den 20 april 2023.

11.6 Arbetet inom Europeiska unionen

Även inom EU pågår arbete som gäller it-relaterad brottslighet och åtkomst till elektroniska uppgifter. År 2016 efterlyste rådet konkreta åtgärder för att göra det rättsliga samarbetet effektivare och förbättra samarbetet mellan medlemsstaternas myndigheter och tjänsteleverantörer baserade i länder utanför EU. Vidare efterlystes förslag till lösningar på problemet med att fastställa och verkställa jurisdiktion i cyberrymden. I juni 2017 presenterade kommissionen, i ett s.k. non-paper[31], olika tänkbara lösningar i arbetet med e-bevisning och jurisdiktion i cyberspace. När det gäller loss of location angavs bl.a. att ett antal medlemsstater redan i dag har möjlighet att få tillgång till och i vissa fall kopiera sådan information direkt från datasystem.

11.6.1 Förslaget till förordning om tillgång till e-bevisning m.m.

Kommissionen presenterade i april 2018 ett förslag till förordning om europeiska utlämnande- och bevarandeorder för elektroniska bevis i straffrättsliga förfaranden, den s.k. e-bevisningsförordningen (COM(2018) 225). Förslagets övergripande syfte är att skapa ett nytt ändamålsenligt regelverk som kompletterar befintlig lagstiftning och effektiviserar gränsöverskridande inhämtning av elektronisk bevisning. För en något närmare beskrivning, se avsnitt 9.4.

Samtidigt presenterade kommissionen ett förslag till direktiv om utseende av en rättslig företrädare för insamling av bevisning i straffrättsliga förfaranden (COM(2018) 226). För att förenkla samarbetet mellan myndigheterna och tjänsteleverantörerna föreslås att vissa tjänsteleverantörer ska vara skyldiga att utse en rättslig företrädare (Legal Representative) inom unionen. Förslagen är fortfarande föremål för förhandlingar.

[31] Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, https://data.consilium.europa.eu/doc/document/ST-15072-2016-REV-1/en/pdf. Hämtat den 20 april 2023.

11.7 Frågans tidigare behandling

Såväl Utredningen om hemlig dataavläsning som Beslagsutredningen har i sina betänkanden uppmärksammat frågan om exekutiv jurisdiktion i förhållande till elektroniska uppgifter.[32]

Utredningen om hemlig dataavläsning konstaterade att det aldrig uttryckligen i svenska lagar nämns att det ska föreligga exekutiv jurisdiktion för Sverige för att myndigheter ska få vidta åtgärder mot enskilda. Utredningen pekade på att det i de lagar som reglerar det internationella samarbetet visserligen finns regler som ger svenska myndigheter vissa möjligheter att agera även när det inte finns jurisdiktion med sedvanlig tillämpning av territorialitetsprincipen, t.ex. reglerna om direktöverföring vid hemlig avlyssning av elektronisk kommunikation.

Utredningen menade att det på mycket goda grunder finns anledning att ifrågasätta den svenska hållningen avseende territorialitetsprincipen vid frågor om exekutiv jurisdiktion när det gäller utredningar som tangerar ”det digitala rummet”. Enligt utredningens uppfattning finns följande tre skäl till att tillämpa territorialitetsprincipen för exekutiv jurisdiktion på det sätt som nu sker i Sverige.

– Förutsebarhet uppnås genom att tillämpa samma princip i den fysiska och den digitala världen för att bestämma vem eller vilka som har jurisdiktion.
– En ändrad svensk uppfattning om när exekutiv jurisdiktion ska anses föreligga kan leda till risk för konflikter med andra stater.
– Inhämtning av uppgifter direkt från en annan stat skulle kunna innebära en risk för att den som verkställer åtgärden gör sig skyldig till brott i den andra staten (t.ex. dataintrång).

Utredningens argument för ett annat synsätt än det nuvarande i frågan om när Sverige ska anses ha jurisdiktion kan sammanfattas på följande sätt.

- Även en ändrad hållning skulle kunna vara förutsägbar, givet att den manifesteras tydligt.
- Det framstår som tämligen märkligt att svenska brottsbekämpande myndigheter inte ska kunna samla in elektroniskt lagrade uppgifter när en brottsutredning pågår i Sverige och riktas mot

[32] Se SOU 2017:89 s. 479 ff. och SOU 2017:100 s. 374 och 375.

en person som befinner sig i landet samt avser ett brott som begåtts i riket och trots att uppgifterna kan tillgängliggöras i Sverige utan att någon risk t.ex. för informationssäkerheten uppstår i den stat där uppgifterna lagras.

- Artikel 32 i Budapestbrottskonventionen tillåter en konventionspart att genom ett informationssystem inom sitt territorium samla in uppgifter som finns lagrade i annan stat när det finns frivilligt samtycke av den som äger eller disponerar informationen. Detta faktum talar i viss mån för att användande av inloggningsuppgifter för att bereda sig tillgång till uppgifter på ett användarkonto på en internettjänst inte utgör en kränkning av den andra statens suveränitet.
- En rad stater har infört unilaterala lösningar som innebär att inloggning från den egna staten med lagligen erhållna inloggningsuppgifter för inhämtning av uppgifter som lagras i en annan stat eller på okänd plats är tillåtet, vilket talar för att det inte utgör en kränkning av den andra statens suveränitet.
- Det bör inte vara särskilt svårt för Sverige att hitta en tolkning av territorialitetsprincipen som kan accepteras av oss själva även när andra stater gör samma tolkning beträffande uppgifter som lagras här. Ett införande av motsvarande möjlighet i Sverige som införts i andra länder, torde alltså inte leda till några mellanstatliga konflikter.

Mot det anförda kan, enligt utredningen, hållas att slutsatserna är behäftade med viss osäkerhet. Detta i synnerhet eftersom artikel 32 har varit föremål för internationella diskussioner under lång tid utan att någon enighet i frågan har kunnat uppnås. Alla världens länder är inte heller anslutna till Budapestkonventionen. Dessutom är utgångspunkten för Budapestkonventionen att platsen för lagring fortfarande är den relevanta faktorn när rättslig hjälp ska begäras. Att platsen för lagring är en relevant faktor även vid elektroniskt lagrade uppgifter framgår också i de rapporter som redovisats från såväl Europarådet som EU, där ju vikten av internationellt rättsligt samarbete understryks. Utredningen ansåg dock att risken för mellanstatliga konflikter inte nämnvärt bör öka genom att förändra den svenska hållningen när det är fråga om t.ex. situationer när det inte helt kan klarläggas var uppgifter lagras eller då det finns akut behov av att få

del av information, t.ex. på grund av en nödsituation eller på grund av att uppgifterna annars kommer försvinna.

Trots de starka skäl som finns för att ändra den svenska tolkningen av territorialitetsprincipen vid exekutiv jurisdiktion kom Utredningen om hemlig dataavläsning fram till slutsatsen att det inte framstår som lämpligt att göra det lagstiftningsvägen inom ramen för den utredningen. Utredningen menade att frågan i stället bör analyseras i särskild ordning och i ett sådant perspektiv att samtliga rättsområden som berörs av den beaktas. Utredningen framhöll också att frågan om en ändrad hållning avseende territorialitetsprincipen kan prövas av domstol i samband med tillståndsprövning för hemlig dataavläsning när åtgärden ska avse användarkonton till internetbaserade tjänster.

Beslagsutredningen påpekade att de förmodade fördelarna av den av utredningen föreslagna möjligheten till undersökning på distans skulle minska avsevärt om sådan undersökning bara får äga rum i fall där man vet att informationen är lagrad i Sverige. Beslagsutredningen kom, i likhet med Utredningen om hemlig dataavläsning, fram till att en tolkning av territorialitetsprincipen som enbart tar sikte på den stat där elektronisk information finns lagrad inte är anpassad till it-miljön och att det finns anledning att fokusera på vilka andra anknytningsmoment som bör kunna grunda jurisdiktion. Utredningen menade att detta ställningstagande inte lämpar sig för lagstiftning, utan de närmare förutsättningarna för jurisdiktion bör i stället utmejslas i rättspraxis.

11.8 Internationell utblick

De brottsbekämpande myndigheternas behov av att få tillgång till elektronisk information lagrad i andra stater har lett till att flera stater har infört möjligheter att inhämta sådan. Det finns dock stora skillnader när det gäller hur staterna förhåller sig till information som är lagrad i utlandet.

11.8.1 Nationell praxis i vissa länder

Belgien

I det s.k. Yahoo!-målet, som avgjordes av den belgiska kassationsdomstolen i december 2015 prövades frågan om skyldigheten för en webbmejl-leverantör etablerad i USA, att lämna ut digitalt lagrad information till en brottsbekämpande myndighet i Belgien.[33] Den brottsbekämpande myndigheten hade ställt sin begäran om utlämnande av den elektroniska informationen direkt till Yahoo!, som varken hade säte eller dotterbolag i Belgien. Bolaget motsatte sig begäran och gjorde gällande att den belgiska myndigheten inte kunde utöva exekutiv jurisdiktion utanför Belgiens territorium. Den belgiska kassationsdomstolen konstaterade att det var tillräckligt att Yahoo! tillhandahöll den aktuella tjänsten inom Belgiens territorium och att begäran om det digitala materialet därför inte kunde anses transnationell. Bolagets vägran att lämna ut materialet ansågs utgöra ett brott inom belgiskt territorium.

USA

I ett mål mellan Microsoft Corp. och USA prövades frågan om skyldigheten för ett amerikanskt bolag att lämna ut e-postmeddelanden som lagrades på servrar i Irland. Amerikanska myndigheter hade med stöd av ett domstolsbeslut riktat sig till Microsoft för att få del av bl.a. innehållet i e-postmeddelanden. Microsoft motsatte sig att lämna ut innehållet i meddelandena med hänvisning till att amerikanska myndigheter inte var behöriga att besluta om utlämnande av information som lagras i andra länder. Vid en prövning i andra instans år 2016 ogiltigförklarades domstolsbeslutet om utlämnande av den elektroniska informationen.[34] Domstolen påpekade att de avsedda e-postmeddelandena var skickade eller mottagna av en irländsk medborgare, inom irländskt territorium via en tjänst som marknadsförts och tillhandahållits på Irland. Det framhölls också att beslag generellt ska anses ha ägt rum på den plats där e-post-meddelanden är lagrade och vid den tidpunkt en kopiering av bevismaterialet sker. Domen kom aldrig att prövas av högsta instans (Supreme Court) efter-

[33] Yahoo! Inc [2015] Court of Cassation of Belgium, Nr. P.13.2082.N.
[34] United States Courts of Appeals for the Second Circuit, No. 14-2985.

som ett nytt domstolsbeslut fattats med stöd av senare tillkommen lagstiftning.[35]

I februari 2015 fick amerikanska myndigheter enligt ett domstolsbeslut beslagta en barnpornografisk webbplats, Playpen. Webbplatsen fanns tillgänglig endast via Tor-nätverket, som döljer användarnas ip-adresser. De amerikanska myndigheterna tog över och drev webbplatsen under två veckor för att kunna identifiera användarnas riktiga ip-adresser och därmed användarna. Utredningen resulterade i flera rättsfall där det bevismaterial som myndigheterna kommit över bedömdes vara otillåtet och således avvisades.[36] Eftersom Tor-nätverket dolde användarnas geografiska position kunde myndigheterna inte vid tillfället då åtgärden vidtogs ha haft vetskap om huruvida de befann sig inom en annan stats territorium eller inte.

Danmark

I dansk rätt finns det inga särskilda regler om genomsökning av utrustning eller om att under en husrannsakan ta del av externt lagrad information. Højesteret har i en dom den 10 maj 2012 (Sag 129/2011) ansett reglerna om hemlig husrannsakan tillämpliga på genomsökning av profiler på Facebook och Messenger, trots att dessa var lagrade på servrar i utlandet. I ärendet hade polisen fått tillgång till den misstänktes lösenord genom telefonavlyssning och använde dessa för att vid flera tillfällen logga in på den misstänktes Facebook- och Messengerkonton. Polisen kunde där undersöka de upplysningar och meddelanden som vid respektive inloggningstillfälle fanns på hans profiler, inklusive mottagna och avsända meddelanden. Højesteret konstaterade att man från vilken dator som helst kunde bereda sig tillgång till profilerna. Det ansågs inte röra sig om meddelanden under befordran, eftersom de fanns lagrade på profilerna och var tillgängliga med hjälp av lösenorden. Det var därför fråga om en husrannsakan. Højesteret konstaterade att det handlade om en brottslighet som omfattades av dansk jurisdiktion, att utredningen genomfördes av danska myndigheter och att åtgärden kunde vidtas utan hjälp av utländska myndigheter. Vid sådant förhållande ansågs det inte ha någon betydelse att de aktuella profilerna var lagrade på servrar i utlandet.

[35] Clarifying Lawful Overseas Use of Data Act (”US CLOUD Act”), https://www.congress.gov/bill/115th-congress/house-bill/4943/text. Hämtat den 20 april 2023.
[36] Se t.ex. United States v. Kreuger, 809 F3d 316 (1st Cir. 2017).

Norge

Norska Høyesterett har den 28 mars 2019 (HR-2019-619-A) meddelat dom i fråga som rörde norsk polis möjlighet att ladda ned information från servrar utomlands.[37] Bakgrunden var att det hade fattats beslut om husrannsakan hos ett norskt bolag. Det fanns inte någon misstanke om att brottet hade begåtts av någon inom bolaget. Den specifika frågan i målet var om norsk polis kunde tillåtas, att från företagets kontorslokaler i Oslo, ladda ner elektronisk information som lagrades i annat land, eller om en sådan tvångs-åtgärd föll utanför norska myndigheters jurisdiktion.

Det elektroniska materialet avsåg dels källkoder som fanns lagrade på en server i USA tillhörande annat bolag, dels utdrag från bolagets tekniska direktörs e-postkonto hos Google, som fanns lagrat på servrar någonstans i Nederländerna, Finland, Belgien eller Island. Det norska företaget överklagade beslutet om husrannsakan till Høyesterett och argumenterade för att norska myndigheter saknade möjlighet att verkställa beslutet eftersom detta i så fall skulle kränka andra staters suveränitet.

Høyesterett resonerade i domen kring problematiken vid loss of location och de rättsliga frågor som den tekniska utvecklingen aktualiserar vid tvångsmedel som riktas mot lagringsplatser i molnet. I domen hänvisas till den danska domen från 2012 samt till den svenska utredningen om hemlig dataavläsning. När det gäller övriga europeiska länder gjordes i domen en kort genomgång av praxis i rapporter från expertgrupper i Europarådet 2012 och 2016 samt från en arbetsgrupp under EU-kommissionen från 2018. Høyesterett sammanfattade detta på följande sätt:

> (58) Gjennomgangen viser at det ikke er etablert noen folkerettslig sedvane på dette området. Etter det opplyste finnes også lite retts-praksis som kan tjene til veiledning.
>
> (59) Likevel er det av interesse at mange land i praksis synes å godta en slik ransaking som i saken her. Det er heller ikke opplyst noe om mellomstatlige reaksjoner knyttet til at et lands myndigheter gjennom tvangsmidler overfor rettssubjekter på eget territorium har fått tilgang til materiale lagret i en annen stat.
>
> *(60) Utgangspunkt for vurderingen av om suverenitetsprinsippet er krenket.*
>
> (61) Så lenge det ikke finnes noen internasjonal konsensus, eller anvendelige konvensjonsbestemmelser, må norske rettsanvendere på selv-

[37] Referatet hämtat från Åklagarmyndighetens rättsliga vägledning 2022:13, Territorialitetsprincipen vid HDA.

> stendig grunnlag ta stilling til om bruk av tvangsmidler krenker en annen stats suverenitet. Ved vurdering av om norske myndigheters tvangsjurisdiksjon begrenses av suverenitetsprinsippet ved ransaking av et datasystem med lagringsenheter utenlands, kan det etter mitt skjønn være hensiktsmessig å ta utgangspunkt i en overordnet vurdering som denne: Griper den aktuelle ransakingen inn i en annen stats eksklusive tvangsjurisdiksjon på en slik måte at denne statens suverenitet krenkes?

Høyesterett konstaterade därefter bl.a.:

- att husrannsakansbeslutet hade verkställts på norskt territorium, i ett norskt företags kontorslokaler i Oslo i syfte att få tillgång till företagets datorsystem,
- att det elektroniska materialet har gjorts tillgängligt genom bruk av tvångsmedel mot ett norskt företag med kontor i Norge och att det alltså inte var tal om att norska myndigheter på egen hand trängt sig in i material som fanns lagrat i utlandet,
- att husrannsakansbeslutet endast gav tillgång till material som företaget själv hade lagrat och att företaget själv fritt kunde komma åt materialet från det utländska lagringsstället och
- att materialet fanns i behåll på den utländska servern; inga förändringar skulle göras, t.ex. radering eller någon spärr, och ett eventuellt beslag skulle göras tilltillgängligt genom kopiering till polisens egna lagringsenheter i Norge.

Under sådana förhållanden ansåg Høyesterett inte att det aktuella husrannsakansbeslutet berörde en annan stat på ett sådant sätt att det innebär en kränkning av suveränitetsprincipen, varför företagets överklagande ogillades.

11.8.2 Nationell lagstiftning i vissa länder

Vissa länder har lagstiftat om transnationell insamling av digitalt lagrade bevis. Nedan följer en presentation av utvald nationell lagstiftning på området.

Belgien

Enligt belgisk straffprocessuell lagstiftning, kan brottsbekämpande myndigheter kopiera, frysa eller ta bort digitalt lagrad information förutsatt att ett beslut om husrannsakan har fattats.[38] Bestämmelsen tar särskilt sikte på digitalt lagrad information som finns tillgänglig på den plats som husrannsakan omfattar. Om ett genomsökande av exempelvis en dator som finns på platsen skulle leda till upptäckten av externt lagrat digitalt material måste den brottsbekämpande myndigheten ansöka om ytterligare tillstånd för att få samla in det materialet. Detsamma gäller om det initialt påträffade datorsystemet är kopplat till ett datorsystem som inte finns på platsen om det senare ska utforskas. Ett sådant tillstånd kan utfärdas under förutsättning att

- det är nödvändigt för att avslöja sanningen i förhållande till det brott som föranledde husrannsakan, och
- andra åtgärder bedöms oproportionerliga eller det finns risk att beviset utan tillståndet kan försvinna.

Förfarandet är begränsat till datorsystem och information som finns direkt tillgängligt via det initiala datorsystemet. Om det skulle visa sig att informationen finns lagrad inom en annan stats territorium, får informationen bara kopieras. I sådant fall ska berörd stat också informeras.

Tyskland

I Tyskland omfattas, såvitt vi kunnat få fram, genomsökning av datorsystem och beslag av digitalt material av de traditionella straffprocessuella reglerna kring husrannsakan.[39] Särskilda bestämmelser som tillåter att myndigheter i ett senare skede utforskar datorsystem som de kommit över via traditionell husrannsakan har dock införts.[40] Efterforskandet kan ske via myndighetens egna datorer. Skulle ett datorsystem ge åtkomst till separata datorsystem och digitalt material inom en annan stat kan myndigheten utforska, ladda ner eller kopiera även dessa, förutsatt att det föreligger en risk att materialet

[38] Se art. 39bis och 88ter Code d'instruction criminelle (CIC).
[39] Sec. 98(1) och sec. 105(1) Strafprozeßordnung.
[40] Sec. 110(3) Strafprozeßordnung.

går förlorat och att det är av betydelse för utredningen. Rättslig hjälp ska i första hand tillämpas om materialets geografiska position kan bestämmas.

USA

I USA har införts en möjlighet att i domstolsbeslut förordna om efterforskande och beslag av digitalt material lagrat i datorsystem.[41] Åtgärden får vidtas på distans. Åtgärden kan avse datorsystem både inom och utom den brottsbekämpande myndighetens distrikt. Vidare kan åtgärden nyttjas för att få åtkomst till material vars geografiska position har dolts med tekniska hjälpmedel. Åtgärden får dock inte vidtas utanför det egna territoriet.

Enligt den ovan nämnda s.k. US CLOUD Act är amerikanska tjänsteleverantörer i regel skyldiga att på begäran av amerikanska myndigheter lämna ut elektroniska uppgifter, oavsett var uppgifterna är lagrade.

Portugal

I Portugal har, såvitt vi kunnat få fram, införts en lagstiftning som utvidgar de traditionella straffprocessuella tvångsmedlen. Brottsbekämpande myndigheter får, vid undersökning av ett datorsystem i Portugal, utvidga efterforskandet till ett externt datorsystem som finns tillgängligt via den första datorn.[42] Bestämmelsen är oberoende av den fysiska positionen av det material som efterforskas och samlas in, även om den berörda staten har identifierats.

11.8.3 Förhandlingar mellan EU och USA om ett avtal om tillgång till e-bevisning

Vissa amerikanska tjänsteleverantörer samarbetar i dag med europeiska brottsbekämpande myndigheter avseende utlämnande av vissa typer av elektroniska uppgifter. Detta samarbete bygger på frivillighet och avser endast utlämnande av mindre känsliga uppgifter. En

[41] Rule 41 United States Federal Rules of Criminal Procedure.
[42] Art. 15(5) Cybercrime Law.

fråga som aktualiserats i samband med förhandlingarna om e-bevisningsförordningen är de motstridiga skyldigheter som kan uppstå för tjänsteleverantörer som är underkastade såväl EU-rätten som amerikansk lagstiftning. Skyldigheten enligt US CLOUD Act för amerikanska tjänsteleverantörer att på begäran från amerikanska myndigheter lämna ut elektronisk information oavsett var den är lagrad kan stå i strid med de skyldigheter som tjänsteleverantören, som erbjuder sina tjänster inom EU, har enligt EU:s dataskyddslagstiftning eller den kommande e-bevisningsförordningen.

Kommissionen gavs i juni 2019 ett mandat av rådet att på EU:s vägnar förhandla om ett avtal med USA om underlättande av tillgång till e-bevisning i straffrättsliga förfaranden. År 2019 skickade kommissionen ut en enkät om gränsöverskridande tillgång till lagrad elektronisk bevisning till samtliga medlemsstater, med frågor bl.a. om vilka kriterier respektive stat använder för att avgöra om en tjänsteleverantör faller under statens jurisdiktion så att en inhemsk begäran om tillgång till elektronisk information kan skickas till leverantören. Svaren på denna enkät visar på tydliga skillnader mellan staterna när det gäller vilka kriterier (anknytningsfaktorer) som används.

Flera stater som svarat på enkäten uppgav att den relevanta anknytningsfaktorn är platsen där tjänsteleverantören har sitt säte. I vissa av dessa länder var det tillräckligt för jurisdiktion att leverantören har en filial inom territoriet. Flera andra länder svarade att den relevanta anknytningsfaktorn är platsen där leverantören verkar eller erbjuder sina tjänster. Av de stater som svarat på enkäten var det enbart Sverige som uttryckligen angett att den relevanta anknytningsfaktorn är platsen där informationen lagras.

11.9 Överväganden och förslag

11.9.1 Behovet av åtkomst till elektronisk information oavsett var informationen lagras

Utredningens bedömning: De brottsbekämpande myndigheterna har ett påtagligt behov av tillgång till elektronisk information även när informationen är lagrad utanför Sverige.

Informationstekniken har utvecklats på ett lavinartat sätt under de senaste decennierna. Som framgår av avsnitt 9.6.1 präglas dagens samhälle av att sådan teknik genomsyrar i stort sett alla sektorer. En mycket stor andel av den svenska befolkningen har tillgång till internet och använder regelbundet internet med hjälp av bl.a. datorer, smarttelefoner eller surfplattor. Vi har i samma avsnitt redogjort för att den it-relaterade brottsligheten har ökat kraftigt sedan början av 2000-talet.

Tillgången till internet har inte bara gjort det enkelt för människor över hela världen att kommunicera och dela information, utan har också lett till en utveckling där allt fler enskilda väljer att använda it-lösningar som inte finns på den egna datorn. Att använda någon annans dataresurs och infrastruktur har kommit att kallas för molntjänster[43] från engelskans cloud computing. Molntjänster kan användas för såväl bearbetning av data som för lagring och delning.

Det har gjort det möjligt för enskilda att bl.a. lagra elektronisk information i externa lagringsutrymmen. Informationen sparas då på en eller flera av tjänsteleverantörens servrar. Användaren kan sedan få tillgång till den externt lagrade informationen från i princip vilken utrustning som helst med internetåtkomst.

Det finns i dag otaliga tjänsteleverantörer som erbjuder lagringstjänster, i vilka användarna kan ladda upp t.ex. fotografier, filmklipp, textdokument eller andra typer av filer på ett användarkonto. Förutom tjänster för enbart lagring och delning finns andra typer av molntjänster. Exempel på sådana är ordbehandlings- och textredigeringsprogram, grafiska verktyg, sociala medier och olika kommunikationstjänster. Typiskt för dessa är att uppgifterna, dvs. användargenererade data och kommunikationsuppgifter, lagras hos tjänsteleverantören.

Möjligheten att lagra information externt har många fördelar, inte minst för att användarna på så vis kan frigöra lagringsutrymme, säkerhetskopiera informationen eller dela den med andra. Samtidigt innebär den externt lagrade informationen utmaningar för de brottsbekämpande myndigheterna. Bevismaterial förekommer i dag ofta i elektronisk form och allt oftare lagras den externt, i t.ex. en molntjänst, i stället för lokalt i t.ex. den misstänktes dator eller mobiltelefon. De brottsbekämpande myndigheterna har ett stort behov av att

[43] Begreppet finns definierat i 2 § 7 p. lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

kunna inhämta sådan information, även när den lagras på externa servrar.

De flesta stora tjänsteföretag lagrar uppgifterna också på andra ställen än i Sverige. Även om tjänsteleverantören har servrar i Sverige är sannolikheten stor att det inte går att klarlägga att just de eftersökta uppgifterna lagras i Sverige i det ögonblick som verkställighet ska ske. Elektroniskt lagrade uppgifter kan nämligen finnas i flera stater samtidigt eller ständigt förflyttas mellan stater. En och samma fil kan också vara uppdelad och lagrad på olika servrar i olika länder.

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.

I de fall det kan fastställas i vilket land den elektroniska informationen finns lagrad kan de brottsbekämpande myndigheterna vända sig till det landet med en begäran om rättslig hjälp eller, i tillämpliga fall, en europeisk utredningsorder. Sådana åtgärder kan dock vara tidsödande och risken finns att den elektroniska informationen raderas, förvanskas eller flyttas till ett annat land under handläggningstiden. Det är inte heller säkert att det landet som begäran eller utredningsordern skickas till i praktiken har bättre möjligheter att komma åt den elektroniska informationen, exempelvis om innehållet är krypterat.

Om det däremot inte går att fastställa var den elektroniska informationen lagras, finns det inget land att vända sig till med en begäran om hjälp. I loss of location-fall kan konsekvensen bli att de brottsbekämpande myndigheterna över huvud taget inte kan få tillgång till relevant elektronisk bevisning.

Som framgått ovan har frågan om hur man ska hantera brottsbekämpande myndigheters tillgång till uppgifter som lagras utanför den egna jurisdiktionen diskuterats under lång tid inom såväl Europarådet som EU. Vissa länder har hanterat svårigheterna att komma åt informationen genom egna lösningar. I några länder har frågan lösts genom lagstiftning och i vissa andra genom praxis.

I Sverige finns det ingen lagstiftning som klargör i vilken utsträckning brottsbekämpande myndigheter kan bereda sig tillgång till elektronisk information som lagras på andra platser än i Sverige. Det finns dock, som nämnts ovan, bestämmelser i lagen om en europeisk utredningsorder och i lagen om internationell rättslig hjälp i brottmål, som

reglerar vad som gäller vid tvångsmedelsanvändning när den person eller den utrustning som tvångsmedlet avser befinner sig i en annan stat.

En möjlighet till exekutiv jurisdiktion som enbart tar sikte på den stat där elektronisk information finns lagrad är, som framgår av det ovan sagda, inte anpassad till dagens förhållanden. Det vore naturligtvis en stor fördel om frågan om hur man ska hantera brottsbekämpande myndigheters tillgång till elektronisk information som lagras utanför den egna jurisdiktionen löstes i internationell samverkan i stället för att varje enskild stat skapar egna lösningar. Det står dock klart att de förslag som nu förhandlas inte kommer lösa alla de svårigheter som finns när det gäller åtkomst till elektroniskt lagrad information. Det är också högst osäkert när förslagen kommer att implementeras. Man skulle emellertid kunna se förslagen som ett steg i riktningen mot att lagringsplatsen inte ska vara det avgörande rekvisitet för tillgången till elektronisk information.

Brottsbekämpande myndigheter behöver få tillgång till elektronisk information som är eller kan vara lagrad utanför Sverige i större omfattning än i dag.

Vi menar att det mot bakgrund av den snabba tekniska utvecklingen av elektroniska kommunikations- och lagringstjänster och internationaliseringen av dessa finns ett påtagligt behov av ett utrymme att utöva exekutiv jurisdiktion med utgångspunkt i andra anknytningsmoment än just lagringsplatsen. Vi återkommer nedan till om det finns förutsättningar för detta.

11.9.2 En grundläggande förutsättning för exekutiv jurisdiktion

Utredningens bedömning: Exekutiv jurisdiktion i förhållande till elektronisk information som finns utanför Sverige kan bara vara aktuell när de brottsbekämpande myndigheterna utan bistånd kan skaffa sig tillgång till informationen från en plats där de är behöriga att verka.

Det är i dag endast genom de straffprocessuella tvångsmedlen hemlig dataavläsning och genomsökning på distans som sådan åtkomst är möjlig.

Vi har i avsnitt 5 redogjort för regleringen gällande de brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation såväl inom som utanför en förundersökning. I avsnitt 5 har vi också redovisat regleringen om hemlig dataavläsning respektive genomsökning på distans. Utöver dessa tvångsmedel kan brottsbekämpande myndigheter få tillgång till elektronisk information genom husrannsakan, beslag, edition, exhibition, kvarhållande av försändelse, penningbeslag, hemlig kameraövervakning och hemlig rumsavlyssning. Det bör i detta sammanhang nämnas att elektronisk information också frivilligt kan lämnas ut till de brottsbekämpande myndigheterna.

Vår ståndpunkt är att exekutiv jurisdiktion bara kan komma i fråga såvitt gäller sådan elektronisk information som de brottsbekämpande myndigheterna utan bistånd från någon utomstående kan skaffa sig tillgång till från en plats där de är behöriga att verka, dvs. främst inom Sverige.

En längre gående jurisdiktion skulle riskera att komma i konflikt med folkrätten, jfr avsnitt 11.9.3. Vidare finns det knappast praktiska förutsättningar att sträcka ut jurisdiktionen längre än till elektronisk information som faktiskt är åtkomlig. I de fall någon form av bistånd behövs från en annan stat eller från t.ex. en tjänsteleverantör i en annan stat för att få tillgång till den elektroniska informationen kan frågan inte lösas genom att föreskriva eller påstå att Sverige har exekutiv jurisdiktion i förhållande till informationen. När sådant bistånd behövs är de brottsbekämpande myndigheterna hänvisade till att begära rättslig hjälp eller att, i tillämpliga fall, utfärda en europeisk utredningsorder. Om den elektroniska informationen däremot är tillgänglig från Sverige utan bistånd skulle informationen under vissa förutsättningar kunna anses ha en sådan anknytning till Sverige att svenska nationella bestämmelser får tillämpas vid inhämtning av informationen.

Vid hemlig dataavläsning och genomsökning på distans kan de brottsbekämpande myndigheterna på egen hand bereda sig tillgång till elektronisk information lagrad i andra stater. Vid båda dessa tvångsmedel handlar det om inhämtning av elektronisk information som finns i ett avläsningsbart informationssystem. Ett avläsningsbart informationssystem kan avse både fysiska och immateriella lagringsplatser. Med fysiska lagringsplatser avses att informationen är lagrad på själva enheten, t.ex. på lagringsmedia i en persondator, mobiltelefon, surfplatta, smart armbandsur eller en server som har beslagtagits

eller påträffats vid husrannsakan eller kroppsvisitation. Med immateriella lagringsplatser avses att informationen är lagrad på lagringsmedia i en extern enhet, vanligen en server. På enheten är informationen avgränsad för användaren och åtkomst till informationen ges i regel genom ett användarkonto till den tjänst som tillhandahålls, exempelvis en molntjänst för fillagring, en extern kommunikationstjänst eller andra typer av molntjänster som vi beskrivit föregående avsnitt. Det som är aktuellt för våra överväganden är framför allt tillgång till elektronisk information som finns på immateriella lagringsplatser.

När det gäller tillgång till uppgifter som finns lokalt lagrade på t.ex. en mobiltelefon som finns i en annan stat uppstår inte samma problematik gällande var informationen är lagrad. I de senare fallen bör de brottsbekämpande myndigheterna även fortsatt vara hänvisade till att begära rättslig hjälp från den stat där den elektroniska kommunikationsutrustningen finns eller, i tillämpliga fall, underrätta den staten i enlighet med 4 kap. 16 § lagen om en europeisk utredningsorder.

Vid hemlig dataavläsning får tekniska hjälpmedel användas för att läsa av eller ta upp informationen i ett avläsningsbart informationssystem. Vid genomsökning på distans får handlingar i det avläsningsbara informationssystemet eftersökas endast om de brottsbekämpande myndigheterna kommer åt informationen genom autentisering i informationssystemet. Eftersom den eftersökta informationen på immateriella lagringsplatser ofta lagras utanför Sverige eller på okänd plats, föreligger en osäkerhet om huruvida informationen får hämtas trots att myndigheterna genom dessa tvångsmedel utan bistånd kan bereda sig tillgång till den. Såväl Utredningen om hemlig dataavläsning som Beslagsutredningen konstaterade i sina betänkanden att förslagen till de båda tvångsmedlen hemlig dataavläsning respektive genomsökning på distans (av utredningen benämnt undersökning på distans) skulle få en begränsad effektivitet om den nuvarande svenska tolkningen av territorialitetsprincipen vid exekutiv jurisdiktion vidhålls.[44]

Enligt vår bedömning är inga andra tvångsmedel än hemlig dataavläsning och genomsökning på distans relevanta i detta sammanhang, eftersom de i praktiken inte medger att myndigheterna på egen hand bereder sig tillgång till elektronisk information i ett annat land.

Den som vid en *husrannsakan* eller efter ett *beslag* söker igenom innehållet i en elektronisk kommunikationsutrustning anses inte få

[44] Se SOU 2017:89 s. 465 och SOU 2017:100 s. 308.

bereda sig tillgång till annan information än sådan som finns lagrad i utrustningen. Det finns nämligen inget lagstöd för att eftersöka information som inte i fysisk mening finns vare sig på platsen för husrannsakan eller i det beslagtagna föremålet.[45] Det är alltså inte tillåtet att hämta information från applikationer (appar) och meddelandetjänster i en beslagtagen mobiltelefon eller dator i de fall informationen inte är lagrad i utrustningen. I dessa fall kan i stället genomsökning på distans ske för att få tillgång till informationen.

Varken genom ett *editions- eller exhibitionsföreläggande* eller ett beslut om *kvarhållande av försändelse* eller *penningbeslag* kan de brottsbekämpande myndigheterna själva bereda sig tillgång till elektronisk information i ett annat land. Den som har en skriftlig handling eller ett föremål som kan antas vara av betydelse som bevis är som huvudregel skyldig att lägga fram handlingen eller föremålet. Ett föreläggande om edition eller exhibition handlar just om att förmå den som innehar en skriftlig handling att förete denna eller att tillhandahålla föremålet för syn.

Reglerna om kvarhållande av försändelse ger en möjlighet för de brottsbekämpande myndigheterna att hos ett befordringsföretag beslagta enskilda försändelser under befordran till eller från en person utan personens vetskap. Det kan i detta sammanhang noteras att elektronisk post som förmedlas via ett elektroniskt kommunikationsnät inte räknas som försändelse utan som ett elektroniskt meddelande. För sådana meddelanden tillämpas reglerna om hemliga tvångsmedel på teleområdet.[46]

Egendom i form av pengar, fordran eller annan rättighet som skäligen kan antas vara föremål för brott enligt lagen (2014:307) om straff för penningtvättbrott, eller ett motsvarande värde, får tas i beslag (penningbeslag). Penningbeslag får dock avse endast sådan egendom som finns tillgänglig. Om penningbeslaget avser en fordran eller annan rättighet, ska gäldenären eller annan förpliktad meddelas förbud att fullgöra sin förpliktelse till någon annan än Polismyndigheten.

Både *hemlig kameraövervakning* och *hemlig rumsavlyssning* är tvångsmedel som kräver teknisk utrustning på den plats som övervakas respektive avlyssnas. Det är alltså inte möjligt för brottsbekämpande myndigheter att bereda sig tillgång till sådana övervaknings- och avlyssningsuppgifter utan bistånd från det aktuella landet.

[45] Se prop. 2021/22:119 s. 75 med där gjorda hänvisningar.
[46] Se Lindberg, Straffprocessuella tvångsmedel, 5:e uppl. s. 529.

Teoretiskt skulle brottsbekämpande myndigheter själva kunna bereda sig tillgång till elektronisk information i andra länder vid HÖK och HAK. Dessa tvångsmedel omfattar nämligen såväl inhämtning av uppgifter från teleoperatörer som inhämtning genom egna tekniska medel som de brottsbekämpande myndigheterna förfogar över. Vid inhämtning genom egna tekniska medel skulle myndigheterna alltså i teorin kunna komma åt information i andra länder. I praktiken verkställs dock dessa tvångsmedel i de allra flesta fall hos eller med bistånd av teleoperatören. Ett undantag från det nu sagda är i de fall det t.ex. kommer in sms till en beslagtagen mobiltelefon. Om HAK beviljas för att ta del av innehållet i ett sådant meddelande krävs normalt sett ingen medverkan från teleoperatören. I sådana fall handlar det dock inte om information som finns på okänd plats eller i ett annat land. När den person som är föremål HAK eller HÖK lämnar svenskt territorium kan i vissa fall uppgifter fortsatt inhämtas genom tvångsmedlet. När de brottsbekämpande myndigheterna upptäcker detta ska de dock antingen avbryta tvångsmedelsanvändningen eller tillämpa relevanta bestämmelser om rättslig hjälp.

Inhämtning av uppgifter med stöd av inhämtningslagen reglerar enbart inhämtning från den som enligt lagen om elektronisk kommunikation tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och som inte är en Noik och ger alltså inte stöd för de brottsbekämpande myndigheterna att hämta in uppgifter med hjälp av egna tekniska hjälpmedel. Vi har i avsnitt 9.6.3 föreslagit att inhämtning med stöd av inhämtningslagen ska få ske även från tillhandahållare av Noik. Detta påverkar dock inte de brottsbekämpande myndigheternas möjligheter att inhämta uppgifter på annat sätt än från tillhandahållaren. De brottsbekämpande myndigheterna kan alltså inte med stöd av inhämtningslagen på egen hand bereda sig tillgång till elektronisk information som lagras i andra länder.

Sammanfattningsvis är alltså vår bedömning att det endast är de straffprocessuella tvångsmedlen hemlig dataavläsning och genomsökning på distans som är av relevans för våra överväganden om möjligheterna till extraterritoriell inhämtning av elektronisk information. Genom dessa båda tvångsmedel kan de brottsbekämpande myndigheterna utan bistånd från utomstående bereda sig tillgång till elektronisk information som är eller kan vara lagrad utanför Sverige.

11.9.3 Folkrättsliga överväganden

Utredningens bedömning: Det finns inte några folkrättsliga hinder mot att de brottsbekämpande myndigheterna inhämtar elektronisk information som är eller kan vara lagrad utanför Sverige under förutsättning att myndigheterna utan bistånd kan skaffa sig tillgång till uppgifterna, att inhämtningen inte innebär 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.

Den traditionella utgångspunkten i folkrätten är, som nämnts ovan, att det råder ett förbud för stater att vidta verkställighetsåtgärder inom andra staters territorier, till exempel att använda straffprocessuella tvångsmedel där.

Den traditionella svenska tolkningen av icke-interventionsprincipen och territorialitetsprincipen vid verkställighet av tvångsmedel är att svenska brottsbekämpande myndigheter inte har rätt att ta del av elektronisk information som är lagrad i andra stater. Detta gäller även om ägaren eller innehavaren av informationen finns i Sverige och även om det finns andra faktorer som anknyter till Sverige. Det finns flera exempel på länder som gör en annan tolkning av dessa principer men en hållning i linje med den traditionella svenska tolkningen synes ha varit utgångspunkten i förhandlingarna inom såväl Europarådet som EU.

Ett undantag från denna hållning, och som också manifesteras i Budapestkonventionen, gäller allmänt tillgänglig information på t.ex. en hemsida som var och en får ta del av (jfr artikel 32 a i Budapestkonventionen). Enligt artikel 32 b i Budpestkonventionen, är det också tillåtet att genom ett datorsystem inom det egna landets territorium bereda sig åtkomst till eller ta emot lagrade datorbehandlingsbara uppgifter som finns hos en annan konventionsstat, om den person som har laglig rätt att röja uppgifterna ger sitt lagliga och frivilliga samtycke. Sverige är, som redan nämnts i avsnitt 11.5.1, sedan den 1 augusti 2021 part till Budapestkonventionen.

Vid hemlig dataavläsning är det inte aktuellt att inhämta något samtycke från den person som har laglig rätt att röja uppgifterna, eftersom åtgärden sker just i hemlighet och ofta mot den person som har sådan rätt. När det gäller genomsökning på distans finns det ett

uttryckligt förbud mot att åberopa den misstänktes samtycke för att besluta om åtgärden (se 28 kap. 1 § tredje stycket och 10 i § RB). I förarbetena anges att regleringen inte utgör ett hinder mot att ett eventuellt samtycke hämtas in och läggs till grund för jurisdiktion vid verkställighet av genomsökning på distans enligt artikel 32 b i Budapestkonventionen, om uppgifterna som eftersöks finns i en annan fördragsslutande stat. Regeringen bedömde att ett samtycke som grundar jurisdiktion enligt Budapestkonventionen inte är oförenligt med reglerna som förbjuder att samtycke läggs till grund för ett beslut om genomsökning på distans.[47]

Ytterligare ett undantag från hållningen att brottsbekämpande myndigheter inte har rätt att ta del av elektronisk information som är lagrad i andra stater finns i Budapestkonventionens artikel 18.1.b. Enligt denna artikel får behöriga myndigheter i en stat förelägga en tjänsteleverantör, som erbjuder sina tjänster inom den statens territorium, att lämna ut sådana abonnemangsuppgifter som leverantören har i sin besittning eller under sin kontroll. Detta gäller alltså oavsett var uppgifterna rent faktiskt är lagrade.[48]

Det står alltså klart att svenska brottsbekämpande myndigheter har möjlighet att ta del av elektronisk information som lagras på andra ställen än i Sverige i den utsträckning som Budapestkonventionen medger det.

Frågan är om det finns några folkrättsliga hinder mot att de brottsbekämpande myndigheterna inhämtar elektronisk information som är eller kan vara lagrad utanför Sverige när detta kan göras utan bistånd t.ex. från den berörda staten eller från tjänsteleverantören.

Folkrätten består, som framgått ovan (se avsnitt 11.2), främst av överenskommelser (traktat) och internationell sedvanerätt. Utöver Budapestkonventionen och dess andra tilläggsprotokoll finns det inga breda internationella rättsakter som reglerar frågan om exekutiv jurisdiktion för att i brottsbekämpande syfte få åtkomst till elektronisk information som lagras i en annan stat. Inom EU pågår visserligen förhandlingar när det gäller förslag till en förordning om tillgång till e-bevisning (COM(2018)225) och ett direktiv om utseende av företrädare för insamling av e-bevisning (COM(2018)226). Vidare har kommissionen ett uppdrag att förhandla med USA om ett avtal

[47] Se prop. 2021/22:119 s. 85 och 86.
[48] Se TCY Guidance Note # 10 om artikel 18 i Budapestkonventionen (T-CY (2015)16), https://rm.coe.int/16806f943e. Hämtat den 20 april 2023.

som rör tillgång till elektronisk bevisning. Vad slutresultatet av dessa förhandlingar kommer att innebära och när det kan vara klart är dock ovisst.

Sverige har sannolikt begränsade möjligheter att på egen hand träffa bilaterala (eller multilaterala) överenskommelser med andra stater om gränsöverskridande åtkomst till elektronisk information eftersom detta område numera torde falla under exklusiv EU-kompetens.

Det kan också konstateras att det inte finns någon internationell sedvanerätt på nu aktuellt område att hänvisa till (jfr också Norska Høyesteretts uttalande om detta i domen den 28 mars 2019, se avsnitt 11.8.2). Som framgår ovan (se avsnitt 11.2) ska det, för etablering av internationell sedvanerätt, finnas en allmän och enhetlig praxis mellan stater och denna praxis ska av staterna anses vara förpliktigande. Med hänsyn till de stora skillnaderna i hur olika stater förhåller sig till frågan om åtkomst till elektronisk information som lagras utanför den egna statens territorium kan inte ens den första delen av kravet, dvs. en allmän och enhetlig praxis, anses vara uppfyllt.

I vissa länder finns tämligen omfattande möjligheter att inhämta elektronisk information som lagras på andra ställen än i den egna staten och några protester mot eller konflikter på grund av detta synes inte ha uppkommit. Det kan här noteras att det endast var Sverige som, bland de medlemsstater inom EU som år 2019 svarade på den ovannämnda enkäten om gränsöverskridande tillgång till lagrad elektronisk bevisning, uttryckligen angav att den enda relevanta anknytningsfaktorn är platsen där informationen lagras (se avsnitt 11.8.3). Man skulle därför kunna säga att folkrätten med avseende på åtkomst till elektroniskt lagrad information håller på att förändras och att Budapestkonventionens andra tilläggsprotokoll och förslaget till e-bevisförordning utgör exempel på en sådan förändring.

Svaret på frågan om det finns några folkrättsliga hinder mot att den exekutiva jurisdiktionen knyts till möjligheten för de brottsbekämpande myndigheterna att utan bistånd kan skaffa sig tillgång till informationen beror, enligt vår uppfattning, på hur pass stort intrånget i andra staters suveränitet är. Ju större intrånget är i den andra statens suveränitet desto större är risken för konflikter med den andra staten eller att den som verkställer åtgärden skulle kunna göra sig skyldig till brott i den andra staten. Vi menar att utgångspunkten måste vara att ett intrång i den berörda statens suveränitet inte får vara annat än obetydligt.

En omständighet att beakta när det gäller intrånget i andra staters suveränitet är om tillgången påverkar andra staters möjlighet att få tillgång till informationen eller om den svenska tillgången kan medföra andra risker för informationssäkerheten i system i andra stater. Med informationssäkerhet avses i detta sammanhang att elektroniskt lagrad information skyddas så att den alltid finns där när den behövs (tillgänglighet), att man kan lita på att den är korrekt och inte manipulerad eller förstörd (riktighet) och att endast behöriga personer får ta del av den (konfidentialitet).[49]

De brottsbekämpande myndigheternas tillgång till elektroniskt lagrad information bör därför vara begränsad på så sätt att de enbart ska ha rätt att ta del av informationen, och inte att ändra eller radera den. Denna begränsning bör endast gälla vid själva åtkomsten till informationen. När myndigheterna väl har fått tillgång till informationen får den naturligtvis bearbetas och på andra sätt behandlas.[50] Vi menar att detta redan följer av regleringen om hemlig dataavläsning och genomsökning på distans. Hemlig dataavläsning innebär att uppgifterna får läsas av eller tas upp. Vid hemlig dataavläsning som gäller kommunikationsavlyssnings- eller kommunikationsövervakningsuppgifter får meddelanden som överförs eller har överförts i ett elektroniskt kommunikationsnät även hindras från att nå fram. Det finns dock ingen rätt att ändra eller radera uppgifter i det avläsningsbara informationssystem som uppgifterna hämtas in från. Genomsökning på distans innebär att söka efter lagrade handlingar. En handling som påträffas vid en genomsökning på distans får kopieras om den skäligen kan antas ha betydelse för utredning om brott eller om förverkande av utbyte av brottslig verksamhet enligt 36 kap. 1 b § brottsbalken.[51] Någon rätt att ändra eller radera handlingar som påträffas vid genomsökning på distans finns alltså inte.

Vidare bör den svenska åtkomsten innebära att endast behöriga tjänstemän, som har ett behov av tillgång till uppgifterna för att utföra sina arbetsuppgifter, får tillgång till informationen. En sådan princip finns redan för de brottsbekämpande myndigheterna enligt

[49] Jfr 2 § första stycket 2 lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och se www.informationssakerhet.se som Myndigheten för samhällsskydd och beredskap ansvarar för men som flera myndigheter står bakom.
[50] Jfr prop. 2021/22:119 s. 80.
[51] Se 27 kap. 17 a § RB.

gällande dataskyddsreglering.[52] Dessutom skyddas uppgifter om enskildas personliga och ekonomiska förhållanden av sekretess.[53]

Utöver risken för att själva informationen förändras eller raderas måste beaktas om inhämtningen innebär någon risk för att informationssystemen på något sätt kan komma till skada.

När det gäller genomsökning på distans, där åtkomsten till det avläsningsbara informationssystemet sker genom autentisering, dvs. på samma sätt som när en behörig användare hade kommit åt systemet, torde det inte finnas några risker för skador på informationssystemet som informationen hämtas från. Sådan inhämtning kan därför sägas innebära ett mycket obetydligt intrång i den berörda statens suveränitet.

Vid verkställighet av hemlig dataavläsning som sker i Sverige får de tekniska hjälpmedel som behövs för avläsningen och upptagningen användas. Om det är nödvändigt får systemskydd brytas eller kringgås och tekniska sårbarheter utnyttjas. Det finns därför krav på aktsamhet som innebär att någon olägenhet eller skada inte får förorsakas utöver vad som är absolut nödvändigt, när ett beslut om hemlig dataavläsning verkställs. Aktsamhetskravet innebär också att informationssäkerheten i andra avläsningsbara informationssystem än det tillståndet avser inte får åsidosättas, försämras eller skadas till följd av verkställigheten. Vidare innebär kravet att den verkställande myndigheten, när verkställigheten avslutas, ska vidta de åtgärder som behövs för att informationssäkerheten i det avläsningsbara informationssystem som tillståndet avser ska hålla minst samma nivå som vid verkställighetens början. Dessutom föreskrivs att ett tekniskt hjälpmedel som har använts ska tas bort, avinstalleras eller annars göras obrukbart så snart det kan ske efter att tiden för tillståndet har gått ut eller tillståndet upphävts (25 § lagen om hemlig dataavläsning). I förarbetena till lagen om hemlig dataavläsning uttalas att vid tillstånd till hemlig dataavläsning som avser användarkonton eller på motsvarande sätt avgränsade delar av kommunikationstjänster, lagringstjänster eller liknande tjänster är allt vid sidan av den definitionen att se som utanför informationssystemet. Det innebär exempelvis att allt innehåll på den tjänst som användarkontot tillhör men som inte kan tillgängliggöras genom användarkontot, t.ex. andras använ-

[52] Se t.ex. 2 kap. 1 § och 3 kap. 6 § brottsdatalagen (2018:1177).
[53] Se 35 kap. 1 § offentlighets- och sekretesslagen (2009:400).

darkonton och den fysiska infrastrukturen för tjänsten, omfattas av aktsamhetskravet.[54]

Enligt vår uppfattning bör, för att hemlig dataavläsning ska få användas beträffande elektronisk information som är eller kan vara lagrad utanför Sverige, en förutsättning vara att någon skada inte får åsamkas heller på det avläsningsbara informationssystem som tillståndet avser. Att tillåta sådan skada skulle, enligt oss, innebära ett inte obetydligt intrång i den berörda statens suveränitet. Ett sådant utvidgat aktsamhetskrav skulle alltså innebära att de brottsbekämpande myndigheterna inte får använda sig av teknik eller metoder som bedöms kunna orsaka skada på det avläsningsbara informationssystem som tillståndet avser. Tillgången till uppgifter i informationssystemet genom autentisering torde, liksom vid genomsökning på distans, inte innebära några risker för skador. Vidare skulle det vara möjligt att genom t.ex. hemlig dataavläsning bereda sig tillgång till inloggningsuppgifter som finns lagrade i Sverige för att sedan, med hjälp av dessa uppgifter, inhämta information som är eller kan vara lagrad utanför Sverige, genom antingen hemlig dataavläsning eller genomsökning på distans.

Slutligen måste tydliga och lämpliga förutsättningar fastställas för i vilka fall tillgång till informationen kan medges. Vi återkommer till denna fråga nedan.

Under ovan nämnda förutsättningar bedömer vi att intrånget i andra staters suveränitet skulle vara mycket begränsat och knappast torde kunna ge upphov till några invändningar från andra stater. Dessutom torde Sverige kunna acceptera att andra stater bereder sig tillgång till information som lagras i Sverige under motsvarande omständigheter. Såvitt känt har Sverige inte heller framfört några protester mot de länder som i praxis eller lagstiftning har infört möjligheter till extraterritoriell inhämtning av elektronisk information. Vår slutsats är således att det inte finns några folkrättsliga hinder mot att de brottsbekämpande myndigheterna inhämtar elektronisk information som är eller kan vara lagrad utanför Sverige under förutsättning att myndigheterna utan bistånd kan skaffa sig tillgång till uppgifterna, att åtgärden inte innebär mer än ett obetydligt intrång i en annan stats suveränitet att inhämtningen inte bedöms kunna orsaka någon skada på det avläsningsbara informationssystem som tvångsmedlet avser. Den självständiga tillgången till informationen utgör alltså en

[54] Se prop. 2019/20:64 s. 239.

relevant anknytningsfaktor för jurisdiktion, vilket innebär att svenska nationella bestämmelser får tillämpas vid inhämtning av sådan information. Detta innebär, enligt vårt sätt att se på saken, att bestämmelserna om tillstånd från en annan stat till gränsöverskridande hemlig dataavläsning i 4 kap. 28 h § lagen om internationell rättslig hjälp i brottmål och om underrättelse om hemlig dataavläsning i 4 kap. 12 § lagen om en europeisk utredningsorder inte skulle bli tillämpliga i de fall inhämtningen sker med stöd av den av oss föreslagna lagen.

11.9.4 Omfattningen av exekutiv jurisdiktion bör klargöras genom att lagfästas

Utredningens bedömning: Omfattningen av exekutiv jurisdiktion i förhållande till elektronisk information som är eller kan vara lagrad utanför Sverige bör klargöras genom att förutsättningarna framgår av lag.

Som vi har konstaterat ovan är det endast möjligt för de brottsbekämpande myndigheterna att utan bistånd få tillgång till elektronisk information som är eller kan vara lagrad utanför Sverige genom hemlig dataavläsning och genomsökning på distans. De båda straffprocessuella tvångsmedlen är relativt nya och lagen om hemlig dataavläsning är tidsbegränsad. Vi menar dock att dessa omständigheter inte talar mot en möjlighet till exekutiv jurisdiktion beträffande elektronisk information som finns eller kan finnas utanför Sverige. Såsom både Beslagsutredningen och Utredningen om hemlig dataavläsning konstaterade, behövs en sådan möjlighet för att de båda tvångsmedlen ska kunna användas på ett effektivt sätt vid inhämtning av uppgifter från immateriella lagringsplatser. Som nämnts ovan är det nämligen vanligt att det inte går att fastställa att uppgifterna i dessa fall lagras enbart i Sverige. Såväl Beslagsutredningen som Utredningen om hemlig dataavläsning menade att det finns anledning att ifrågasätta om just lagringsplatsen är den mest relevanta grunden för jurisdiktion när det gäller elektronisk information lagrad i utlandet eller på okänd plats men kom till slutsatsen att frågan får överlämnas till rättspraxis.

Som framgår av avsnitt 11.9.3 är vår bedömning att folkrätten under vissa förutsättningar inte hindrar att brottsbekämpande myn-

digheter redan i dag, genom ovan nämnda tvångsmedel, inhämtar elektronisk information som är eller kan vara lagrad utanför Sverige.

Högsta domstolens har nu konstaterat att bestämmelserna om genomsökning på distans medger eftersökning av information som finns lagrad utanför Sverige. Något avgörande finns emellertid inte som tar sikte på HDA. Vi menar att det i lag bör klargöras att exekutiv jurisdiktion av här beskrivet slag är tillåten under förutsättning att vissa villkor, som vi tar upp i nästa avsnitt, är uppfyllda. På det sättet tillgodoses de brottsbekämpande myndigheternas behov av informationen samtidigt som förutsättningarna blir tydliga för envar, inte minst för de befattningshavare som ska ansöka eller pröva frågan om tillstånd till de aktuella tvångsmedlen.

11.9.5 Närmare om lagregleringen

Utredningens förslag: En reglering av inhämtning genom straffprocessuella tvångsmedel av elektronisk information som är eller kan vara lagrad utanför Sverige ska gälla såväl under förundersökning som i underrättelseverksamhet.

I regleringen ska anges att inhämtningen får avse endast sådan information som de brottsbekämpande myndigheterna utan bistånd kan få tillgång till informationen i det avläsningsbara informationssystem som tvångsmedlet avser. Vidare ska det anges att inhämtningen av informationen inte får innebära mer än ett obetydligt intrång i en annan stats suveränitet och att inhämtningen inte får bedömas kunna orsaka någon skada på det avläsningsbara informationssystem som tvångsmedlet avser.

Regleringen ska ske i en ny lag benämnd lagen om inhämtning av elektronisk information som är eller kan vara lagrad utanför Sverige vid användning av straffprocessuella tvångsmedel.

Utredningens bedömning: Regleringen ska gälla beträffande brott som svensk domstol är behörig att döma över och brottslig verksamhet som innefattar brott som svensk domstol är behörig att döma över.

Regleringen ska gälla såväl under förundersökning som i underrättelseverksamhet

En särskild fråga är om regleringen av möjligheten att inhämta elektronisk information lagrad utanför Sverige bör gälla både under en förundersökning och i underrättelseverksamhet. Genomsökning på distans kan beslutas endast inom ramen för en förundersökning. Däremot kan hemlig dataavläsning användas såväl inom som utanför en förundersökning.

Underrättelseverksamheten är till stora delar oreglerad, vilket kan tala mot att regleringen ska gälla i sådan verksamhet. Mot detta kan invändas att just tvångsmedelsanvändningen är reglerad på ett likartat sätt såväl inom som utom förundersökning. Exempelvis ska beslut om tillstånd till hemlig dataavläsning i båda fallen fattas av domstol och offentligt ombud ska i båda fallen närvara vid rättens sammanträde.

Det kan vidare konstateras att både lagen om internationell rättslig hjälp i brottmål och lagen om en europeisk utredningsorder är tillämpliga endast under förundersökning eller lagföring av brott och inte i underrättelseverksamhet. Å andra sidan ska den nu aktuella regleringen inte avse internationell samverkan utan rent nationell lagstiftning om jurisdiktion för svenska myndigheter. Det är alltså en principiell fråga om när elektroniskt lagrad information ska få inhämtas från svenskt territorium. Eftersom svensk lagstiftning tillåter hemlig dataavläsning såväl inom en förundersökning som i underrättelseverksamhet bör, enligt vår uppfattning, principen vara densamma i båda fallen.

Övriga förutsättningar för inhämtning av informationen

Som framgår ovan har det i vissa länder fastställts bestämmelser om när transnationell inhämtning av elektronisk information är tillåten (se avsnitt 11.8.2). Frågan är vilka förutsättningar som bör föreligga enligt en sådan reglering i Sverige.

Vi har ovan kommit fram till att regleringen enbart kan omfatta sådan elektronisk information som svenska brottsbekämpande myndigheter utan bistånd har tillgång till med stöd av relevanta straffprocessuella tvångsmedel och att sådan tillgång i dagsläget endast är möjlig genom hemlig dataavläsning och genomsökning på distans.

De brottsbekämpande myndigheterna bör få använda dessa tvångsmedel bara från en plats där de är behöriga att verka, dvs. främst i Sverige. Vi har också bedömt att de brottsbekämpande myndigheternas tillgång bör vara begränsad till att enbart ta del av informationen, och inte att på något sätt ändra eller radera den, vilket redan följer av regleringen om hemlig dataavläsning och genomsökning på distans. Vi har vidare bedömt att endast behöriga befattningshavare, som har ett behov av tillgång till uppgifterna för att utföra sina arbetsuppgifter, bör ha tillgång till informationen och konstaterat att en sådan princip redan gäller för de brottsbekämpande myndigheterna enligt dataskyddsregleringen. Vi har också funnit att inhämtningen inte får innebära mer än ett obetydligt intrång i den berörda statens suveränitet och att den inte får bedömas kunna orsaka någon skada på det informationssystem som tvångsmedlet avser. Vi har slutligen bedömt att regleringen bör gälla såväl inom en förundersökning som i underrättelseverksamhet.

Nästa fråga är vilka ytterligare förutsättningar som ska föreligga för att de brottsbekämpande myndigheterna ska få inhämta information som är eller kan vara lagrad utanför Sverige. Det kan exempelvis övervägas om förutsättningarna bör vara att brottet eller den brottsliga verksamheten har ägt rum i Sverige, att gärningsmannen eller målsäganden är svenska medborgare eller att någon av dessa är bosatta i Sverige. Vi anser dock att regleringen bör följa bestämmelserna om vilka brott som svenska domstolar är behöriga att döma över, eftersom dessa också sätter gränserna för svenska förundersökningar och i förlängningen även den underrättelseverksamhet som sker i brottsbekämpande syfte.

Svensk domstol är enligt 2 kap. 1 § BrB behörig att döma över brott som begåtts i Sverige. I vissa fall krävs dock åtalsförordnande för brott som begåtts i Sverige, t.ex. om brottet har begåtts av en utlänning på ett utländskt fartyg och riktat sig mot en utlänning eller mot ett utländskt intresse (se 2 kap. 2 § BrB). Svensk domstol är i vissa fall behörig att döma över brott som begåtts utanför Sverige (2 kap. 3 § BrB). Dessa fall baseras i huvudsak på de olika folkrättsliga anknytningsprinciperna:

- den s.k. flaggstatsprincipen (att brottet begåtts på t.ex. ett fartyg eller luftfartyg under svensk flagg),
- den aktiva personalitetsprincipen (att brottet begåtts av någon som vid gärningstillfället var svensk medborgare eller hade hemvist i Sverige),
- den passiva personalitetsprincipen (brottet har riktat sig mot en svensk medborgare eller någon annan som har hemvist i Sverige, eller mot en svensk juridisk person),
- den s.k. statsskyddsprincipen (att brottet har riktat sig mot Sveriges säkerhet, allmän verksamhet eller annat av rättsordningen särskilt skyddat svenskt intresse),
- principen om härledd jurisdiktion (i de fall då domsrätten på något sätt härleds från en annan stat som har domsrätt med stöd av sedvanliga regler) och
- universalitetsprincipen (domsrätt över vissa internationella brott oberoende av var och av vem brottet har begåtts).

Det finns också bestämmelser i annan lagstiftning om svensk domstols behörighet att döma över vissa brott som begåtts utanför Sverige (dessa bestämmelser anges i 2 kap. 4 § BrB). För vissa brott som begåtts utanför Sverige krävs dubbel straffbarhet för svensk domstols behörighet (detta krävs vid domsrätt som grundas på den aktiva eller passiva personalitetsprincipen eller på principen om härledd jurisdiktion (se 2 kap. 5 § BrB). I vissa fall får åtal väckas utan åtalsförordnande när brottet begåtts utanför Sverige, t.ex. om brottet begåtts i Danmark, Finland, Island eller Norge (se 2 kap. 7 § BrB). Det finns vidare regler om i vilken utsträckning en tidigare utländsk dom utgör hinder för lagföring i Sverige (ne bis in idem-principen; se 2 kap. 9 § BrB). De begränsningar av svensk domstols behörighet och tillämpligheten av svensk lag som följer av allmän folkrätt eller av en internationell överenskommelse som är bindande för Sverige ska iakttas (2 kap. 12 § BrB).

Vi menar alltså att en reglering om inhämtning av elektronisk information, som är eller kan vara lagrad utanför Sverige, ska gälla i samtliga fall när svensk domstol är behörig att döma över brottet respektive när den brottsliga verksamheten innefattar brott som svensk domstol är behörig att döma över och under de förutsättningar som

vi tidigare nämnt. En annan sak är att föreskrifterna om respektive tvångsmedel ställer upp specifika förutsättningar för i vilka fall tvångsmedlen får användas. Enligt vår bedömning behöver det i regleringen inte uttryckligen anges att svensk domstol ska vara behörig att döma över brottet. Den domstol eller den befattningshavare som prövar frågan om tvångsmedelsanvändning har, som alltid, att pröva sin egen behörighet. Dessa ska alltså också pröva de folkrättsligt grundade begränsningarna i den svenska kompetensen, t.ex. bestämmelser om immunitet, vilket i princip även kan innebära hinder mot användning av straffprocessuella tvångsmedel.[55] Vidare behöver det inte, enligt vår bedömning, i regleringen anges att de brottsbekämpande myndigheterna får inhämta uppgifterna endast från en plats de är behöriga att verka, eftersom detta är utgångspunkten för all myndighetsutövning, inklusive användning av straffprocessuella tvångsmedel.

I regleringen bör det dock uttryckligen anges dels att inhämtningen endast får avse sådan information som myndigheterna utan bistånd kan skaffa sig tillgång till i det avläsningsbara informationssystem som tvångsmedlet avser, dels att inhämtningen inte får bedömas kunna orsaka någon skada på det informationssystem som åtgärden avser. Beslut om hemlig dataavläsning med stöd av vårt förslag torde i nuläget visserligen endast kunna avse immateriella lagringsplatser. Vårt förslag bör dock vara av mer principiellt slag och som tar höjd för såväl ändringar i tvångsmedelslagstiftningen som nya tekniska lösningar. Regleringen bör därför inte begränsas till inhämtning från immateriella lagringsplatser.

Som vi angett ovan bör inhämtningen aldrig få innebära mer än ett obetydligt intrång i en annan stats suveränitet. Detta bör uttryckligen anges i regleringen. Vi bedömer visserligen att inhämtning under de förutsättningar som vi ovan föreslagit normalt sett inte innebär mer än ett obetydligt intrång i den berörda statens suveränitet. Men det bör ändå göras en proportionalitetsbedömning av intrånget i den berörda statens suveränitet. I motsats till hemlig dataavläsning avseende exempelvis ett användarkonto till en utländsk lagringstjänst, som typiskt sett endast utgör ett sådant obetydligt intrång, torde hemlig dataavläsning avseende en mobiltelefon i en annan stat anses innebära ett inte obetydligt intrång i den berörda statens suveränitet. Vidare skulle användningen av ett framtida straffprocessuellt tvångsmedel kunna medföra sådana beaktansvärda risker för informations-

[55] Se prop. 2020/21:204 s. 158 och 159 med där angivna hänvisningar.

säkerheten att det innebär mer än ett obetydligt intrång i den berörda statens suveränitet.

Man skulle också kunna överväga om en förutsättning för att få inhämta elektronisk lagrad information bör vara att tjänsten, i vilken informationen som ska inhämtas lagras, tillhandahålls i Sverige. Vi har dock svårt att se något egentligt skäl för en sådan förutsättning. För det första kan det vara vanskligt att bedöma huruvida en tjänst kan anses tillhandahållas i Sverige. För det andra kan tjänsten, även om det bedöms att den inte tillhandahålls i Sverige, t.ex. för att den inte riktar sig till användare här, ändå vara tillgänglig för användare här. De brottsbekämpande myndigheternas möjlighet att, genom t.ex. hemlig dataavläsning, på egen hand få tillgång till information på ett användarkonto i en sådan tjänst, påverkas inte av att tjänsten inte anses tillhandahållas i Sverige.

Mot bakgrund av att inhämtningen ska ske med stöd tvångsmedelsregleringen finns det inte heller skäl att överväga exempelvis om särskilda regler ska gälla i nödsituationer eller i annars särskilt brådskande fall. Vi finner inte heller skäl att på något annat sätt begränsa möjligheten att med stöd av straffprocessuella tvångsmedel inhämta elektroniskt lagrad information oavsett i vilka länder informationen rent faktiskt lagras. Vi återkommer i nästa avsnitt till frågor om rättssäkerhetsgarantier m.m.

Regleringen ska ske i en ny lag

En reglering av nu aktuellt slag skulle kunna implementeras i svensk rätt på olika sätt. Exempelvis skulle regleringen kunna finnas i anslutning till bestämmelserna om svensk domstols behörighet i 2 kap. BrB. Vi anser dock inte att en specifik reglering om inhämtning av elektroniskt lagrad information passar särskilt bra bland brottsbalkens bestämmelser om i vilka fall svenska domstolar är behöriga att döma över brott. Ett annat alternativ är att regleringen införs i anslutning till regleringen av respektive relevant tvångsmedelsreglering, dvs. i lagen om hemlig dataavläsning respektive i 28 kap. RB. En fördel med en reglering i dessa lagar är att den är lätt tillgänglig för tillämparen. Vi anser emellertid att det bästa vore att en reglering av detta slag görs i en ny särskild lag som gäller generellt för inhämtning av elektronisk information genom straffprocessuella tvångsmedel. Lagen

skulle då också gälla om det införs andra tvångsmedel som ger de brottsbekämpande myndigheterna möjlighet att på egen hand få tillgång till elektroniskt lagrad information. Vi föreslår att lagen ska benämnas lagen om inhämtning av elektronisk information som är lagrad utanför Sverige vid användning av straffprocessuella tvångsmedel.

11.9.6 Rättssäkerhetsgarantier m.m.

Utredningens bedömning: De rättssäkerhetsgarantier som gäller enligt respektive tvångsmedelsreglering är tillräckliga.

Det bör inte införas någon underrättelseskyldighet till de stater som den inhämtade informationen lagras i.

För att skydda personers integritet och för att upprätthålla en hög grad av rättssäkerhet innehåller reglerna om straffprocessuella tvångsmedel ett antal kontrollmekanismer och rättssäkerhetsgarantier. Detta gäller särskilt för de hemliga tvångsmedlen, där den berörde inte är medveten om tvångsmedelsanvändningen. Det finns således regler om bl.a. förhandskontroll, underrättelseskyldighet, tillsyn och begränsningar i rätten att använda överskottsinformation. Dessutom gäller ändamålsprincipen, behovsprincipen och proportionalitetsprincipen vid all tvångsmedelsanvändning, se avsnitt 5.2.

Hemlig dataavläsning

I lagen om hemlig dataavläsning föreskrivs bl.a. följande. Frågor om hemlig dataavläsning ska prövas av domstol på ansökan av åklagare eller Säkerhetspolisen (14 §). Under vissa förutsättningar får tillstånd ges av åklagaren i avvaktan på rättens beslut. Om åklagaren har gett tillstånd till hemlig dataavläsning ska han eller hon utan dröjsmål anmäla beslutet till rätten som skyndsamt ska pröva ärendet. Om åklagarens beslut har verkställts innan rätten gjort sin prövning, ska rätten pröva om det har funnits skäl för åtgärden. Om rätten finner att det saknats sådana skäl, får de uppgifter som lästs av eller tagits upp inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden eller för någon annan som uppgifterna avser (17 §).

När en ansökan eller anmälan om hemlig dataavläsning har kommit in till rätten, ska rätten så snart som möjligt utse ett offentligt ombud i ärendet och hålla ett sammanträde. Vid sammanträdet ska den som gjort ansökan eller anmälan och det offentliga ombudet närvara (16 §).

När rätten har beslutat i frågor om hemlig dataavläsning ska den skyndsamt underrätta Säkerhets- och integritetsskyddsnämnden (SIN) om beslutet (21 §).

Hemlig dataavläsning får inte avse ett avläsningsbart informationssystem som stadigvarande används eller är särskilt avsett att användas i viss verksamhet där tystnadsplikt gäller, exempelvis verksamhet som bedrivs av advokater och läkare (se 11 §).

Det finns även regler om hur överskottsinformation ska hanteras, om granskning, bevarande och förstörande av upptagningar och upptecknin gar och om skyldighet att underrätta den enskilde om användningen av hemlig dataavläsning (se 28–31 §§).

SIN:s uppdrag omfattar att utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel. SIN ska också, på begäran av en enskild, kontrollera om han eller hon har utsatts för hemliga tvångsmedel och om tvångsmedelsanvändningen och verksamhet som hänger samman med sådan användning har varit i enlighet med lag eller annan författning.[56] Även Riksdagens ombudsmän och Justitiekanslern utövar tillsyn över de brottsbekämpande myndigheternas verksamhet. Integritetsskyddsmyndigheten utövar tillsyn över myndigheternas personuppgiftsbehandling.

Genomsökning på distans

Ett beslut om genomsökning på distans, som alltså inte är ett hemligt tvångsmedel, får meddelas av undersökningsledaren, åklagaren eller rätten. En polisman får vidta åtgärden även utan sådant beslut, om det är fara i dröjsmål och genomsökningen inte kan antas bli av stor omfattning eller medföra synnerlig olägenhet för den som drabbas av åtgärden. Om genomsökningen kan antas bli av stor omfattning eller medföra synnerlig olägenhet för den som drabbas av åtgärden bör åtgärden, om det inte är fara i dröjsmål, inte vidtas utan rättens beslut. Rätten får ta upp frågan om genomsökning på distans på be-

[56] Se 1 och 3 §§ lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet.

gäran av undersökningsledaren eller åklagaren. Efter åtalet får rätten även på yrkande av målsäganden eller självmant ta upp en sådan fråga (28 kap. 10 d § RB).

Genomsökning på distans får inte avse handlingar med uppgifter som enligt 27 kap. 2 § RB hindrar beslag (dvs. handlingar som kan antas innehålla uppgifter som en befattningshavare eller någon annan som avses i 36 kap. 5 § RB inte får höras som vittne om, och handlingen innehas av honom eller henne eller den som tystnadsplikten gäller till förmån för). I de fall det vid genomsökningen påträffas handlingar med uppgifter som omfattas av beslagsförbudet, ska genomsökningen omedelbart avbrytas i den del den avser sådana uppgifter (28 kap. 10 c § RB).

Det finns även regler i fråga om rätt till närvaro vid genomsökning på distans (se 28 kap. 10 e § RB). Om en genomsökning på distans har utförts utan att den som drabbats av åtgärden har varit närvarande ska han eller hon, så snart det kan ske utan men för utredningen, underrättas om åtgärden (28 kap. 10 g § RB). Den som har drabbats av åtgärden har också rätt att på begäran få ett bevis om åtgärden. Beviset ska även innehålla uppgift om det brott som misstanken avser (28 kap. 10 h § RB).

Som nämnts ovan får den misstänktes samtycke inte åberopas för beslut om genomsökning på distans, om inte den misstänkte själv har begärt att åtgärden ska vidtas (28 kap. 10 i § RB).

De brottsbekämpande myndigheternas verksamhet står under Riksdagens ombudsmäns och Justitiekanslerns tillsyn. Integritetsskyddsmyndigheten utövar tillsyn över bl.a. myndigheternas personuppgiftsbehandling.

Vår bedömning

Vi bedömer att vårt förslag i fråga om exekutiv jurisdiktion i förhållande till elektronisk information som är eller kan vara lagrad utanför Sverige inte ger upphov till mer än ett obetydligt intrång i andra staters suveränitet och att förslaget ligger inom ramen för vad som kan anses folkrättsligt tillåtet. Det har inte heller under utredningen framkommit att vårt förslag skulle ge upphov till något ytterligare intrång i enskildas integritet eller några andra risker än vad som är fallet vid inhämtning av elektronisk information lagrad i Sverige. Vi

bedömer därför att det inte behövs några ytterligare kontrollmekanismer eller rättssäkerhetsgarantier än de ovan nämnda när tvångsmedelsanvändningen avser inhämtning av information som är eller kan vara lagrad utanför Sverige. Vi föreslår därför inte att några nya sådana ska införas.

En särskild fråga är om det bör finnas en skyldighet att underrätta den eller de stater i vilka den inhämtade informationen lagras om inhämtningen. En sådan underrättelseskyldighet kan endast vara aktuell i de fall de brottsbekämpande myndigheterna vet i vilket eller vilka land informationen lagras. Eftersom informationen kan vara lagrad på många ställen samtidigt och dessutom ständigt byta lagringsplats kan en underrättelseskyldighet vara besvärlig att uppfylla. Med hänsyn till utformningen av våra förslag, som enligt vår uppfattning innebär att intrånget i andra staters suveränitet blir mycket begränsat, anser vi att någon underrättelseskyldighet inte bör införas.

Som vi redogjort för ovan (avsnitt 11.4.2), finns det i lagen om en europeisk utredningsorder (EUO) bestämmelser om underrättelse till en annan medlemsstat vid vissa beslut om hemliga tvångsmedel. Om beslut har meddelats i Sverige om hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter, kommunikationsövervakningsuppgifter eller platsuppgifter i en annan medlemsstat från vilken det inte behövs något bistånd för att genomföra åtgärden, ska åklagaren underrätta den medlemsstaten om beslutet. Bestämmelsen tar, som tidigare nämnts, sikte på fall då den person, tillsammans med den kommunikationsutrustning som är föremål för åtgärden, befinner sig på ett annat lands territorium och från vilket tekniskt bistånd inte behövs för genomförandet av åtgärden. Underrättelsen ska lämnas innan avläsningen påbörjas, om det vid denna tidpunkt är känt att telefonnumret, adressen eller den elektroniska kommunikationsutrustningen kommer att användas eller finnas i den andra medlemsstaten. I annat fall ska underrättelse lämnas så fort åklagaren får kännedom om detta, även om det sker efter det att avläsningen är avslutad (se 4 kap. 16 § EUO). Som nämnts ovan (avsnitt 11.9.3) blir dock varken bestämmelserna i denna lag eller i lagen om internationell rättslig hjälp i brottmål tillämpliga när den av oss föreslagna lagen tillämpas. Vid tillämpning av den föreslagna lagen ska nämligen tvångsmedelsanvändningen ske med stöd av svenska nationella bestämmelser.

12 Ikraftträdande- och övergångsbestämmelser

12.1 Ikraftträdande och övergångsbestämmelser

Utredningens förslag: De föreslagna reglerna om inhämtning av elektronisk information som är lagrad utanför Sverige vid användning av straffprocessuella tvångsmedel ska träda i kraft den 1 juli 2024. Övriga föreslagna regler ska träda i kraft den 1 juli 2025.

Det ska införas en övergångsbestämmelse för trafik- och lokaliseringsuppgifter som lagrats innan de nya reglerna träder i kraft.

Den nya regleringen bör träda i kraft så snart som möjligt. Det bör dock beaktas att förslagen rör komplexa frågor inom ett viktigt område och att beredningen i Regeringskansliet därför måste tillåtas ta viss tid. I fråga om reglerna om inhämtning av elektronisk information som är lagrad utanför Sverige vid användning av straffprocessuella tvångsmedel bedömer vi att förslagen bör kunna träda i kraft den 1 juli 2024.

Övriga förslag kommer sannolikt att medföra tidskrävande anpassningar av it-stöd för de som träffas av anpassnings- och lagringsskyldigheten, se avsnitt 13.1. Tillhandahållarna behöver enligt vår bedömning få tillräckligt med tid för att kunna ställa om sina system. Vi bedömer därför att förslagen i betänkandets övriga delar bör träda i kraft tidigast den 1 juli 2025.

I fråga om lagring av trafik- och lokaliseringsuppgifter krävs en övergångsbestämmelse för de uppgifter som lagrats enligt 9 kap. 19 § nya LEK när de av oss föreslagna reglerna träder i kraft. Utan en övergångsbestämmelse skulle redan lagrade uppgifter annars behöva gallras vid ikraftträdande av de nya reglerna. Vi föreslår därför att trafik- och lokaliseringsuppgifter som redan finns lagrade när de nya reglerna träder i kraft ska lagras enligt 9 kap. 22 § nya LEK i dess nuvarande lydelse.

13 Förslagens konsekvenser

13.1 Inledning

De krav som ställs på redovisningen av vilka konsekvenser som förslagen i betänkanden kan få framgår av 14–16 §§ kommittéförordningen (1998:1474). Kraven innebär i sammandrag följande. Om förslagen i betänkandet påverkar kostnaderna eller intäkterna för staten, kommuner, regioner, företag eller andra enskilda, ska en beräkning av dessa konsekvenser redovisas i betänkandet. Om förslagen innebär samhällsekonomiska konsekvenser i övrigt, ska dessa redovisas. När det gäller kostnadsökningar och intäktsminskningar för staten, kommuner eller regioner, ska även en finansiering föreslås. Om förslagen i ett betänkande har betydelse för det kommunala självstyret, ska konsekvenserna i det avseendet anges i betänkandet. Detsamma gäller när ett förslag har betydelse för brottsligheten och det brottsförebyggande arbetet, för sysselsättning och offentlig service i olika delar av landet, för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags, för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen.

Utöver det angivna följer det av våra direktiv att vi ska beskriva vilka konsekvenser de förslag som lämnas har för det nationella och internationella skyddet för mänskliga rättigheter, inklusive den personliga integriteten, och för möjligheterna att kommunicera på ett säkert sätt.

Problembeskrivningar, behov, det vi önskar uppnå och alternativa lösningar framgår av respektive avsnitt i betänkandet. Där redovisar vi också vår bedömning av hur förslagen förhåller sig till EU-rätten och Sveriges åtaganden när det gäller mänskliga rättigheter. Vad som angetts i dessa avsnitt upprepas i huvudsak inte i det följande.

13.2 Vilka berörs av våra förslag?

Utredningens bedömning: Enskilda personer, tillhandahållare av allmänna elektroniska kommunikationsnät som vanligen tillhandahålls mot ersättning och allmänt tillgängliga elektroniska kommunikationstjänster, Polismyndigheten, Säkerhetspolisen, Tullverket, SIN, PTS, Åklagarmyndigheten, Ekobrottsmyndigheten, allmänna domstolar, Kustbevakningen och Försvarsmakten berörs av våra förslag.

Vi har i betänkandet lämnat förslag om reformerade regler om lagring av elektronisk information och tillgång till sådana uppgifter i anledning av senare praxis från EU-domstolen. Vi föreslår nya regler om lagring för att skydda den nationella säkerheten och en möjlig modell av lagring för att bekämpa grov brottslighet. Våra förslag omfattar även en lagringsskyldighet för tillhandahållare av Noik, en modernisering av anpassningsskyldigheten och en reglering av inhämtning genom straffprocessuella tvångsmedel av elektronisk information, som är eller kan vara lagrad utanför Sverige. Nedan beskriver vi på ett övergripande plan hur enskilda personer, tillhandahållare och myndigheter berörs av våra förslag.

- De trafik- och lokaliseringsuppgifter som genereras när enskilda använder sig av allmänna elektroniska kommunikationsnät och elektroniska kommunikationstjänster kan komma att lagras i en större utsträckning än i dag i syfte att bekämpa hot mot den nationella säkerheten. Sådana uppgifter kan även komma att lagras för att bekämpa den grova brottsligheten.
- Traditionella teleoperatörer och tillhandahållare av Noik behöver anpassa sina system så att lagring kan ske och uppgifter kan lämnas ut till de brottsbekämpande myndigheterna. De nya formerna av lagring innebär att teleoperatörerna och tillhandahållarna av Noik kommer att ha fler kontakter än i dag med de brottsbekämpande myndigheterna och med PTS.
- Säkerhetspolisen får nya arbetsuppgifter när det gäller handläggningen av ärenden om nationell säkerhetslagring och ärenden om utökad riktad lagring avseende områden, platser, personer, utrustning och abonnemang. Handläggningen förutsätter samråd och

kontakter med bl.a. Försvarsmakten och de som bedriver säkerhetskänslig verksamhet.

- SIN:s uppdrag utökas. Nämnden får en ny delegation, Datalagringsdelegationen, som ska överpröva Säkerhetspolisens beslut om nationell säkerhetslagring när dessa överklagas. Handläggning av ärenden om nationell säkerhetslagring medför också krav på ett mer omfattande kanslistöd hos SIN. Nämnden får vidare ett nytt tillsynsområde när det gäller beslut om utökad riktad lagring.
- Polismyndigheten och Tullverket får nya arbetsuppgifter i form av beslut om utökad riktad lagring avseende områden, platser, personer, utrustning och abonnemang. Handläggningen förutsätter samråd och kontakter med berörda parter.
- Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten och Ekobrottsmyndigheten får, efter tillstånd till hemlig dataavläsning eller genomsökning på distans, utan biträde från utomstående bereda sig tillgång till elektronisk information som är eller kan vara lagrad utanför Sverige. Kustbevakningen får samma möjlighet vad gäller genomsökning på distans. Åklagare vid Åklagarmyndigheten och Ekobrottsmyndigheten får därigenom hantera angelägenheter om hemlig dataavläsning och genomsökning på distans i fler situationer än tidigare genom tydligare bestämmelser om jurisdiktion. Samtidigt minskar behovet av HDA när användning av HAK och HÖK kan beslutas mot tillhandahållare av Noik.
- PTS får en ny arbetsuppgift som rör beslut om geografiskt riktad lagring. Myndighetens tillsyn och möjlighet att utfärda sanktionsavgifter enligt nya LEK utökas.
- Allmänna domstolar får hantera ärenden om hemlig dataavläsning och genomsökning på distans i fler situationer än tidigare.
- Försvarsmakten är skyldig att medverka då Säkerhetspolisen begär samråd i angelägenheter om nationell säkerhetslagring.
- Ett offentligt ombud ska bevaka enskildas intressen i ärenden om nationell säkerhetslagring.

13.3 Om marknaden för tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster och tillhandahållare av Noik

De företag som är relevanta för förslagen består av två grupper av tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster, de traditionella mobiloperatörerna och tillhandahållare av Noik. Vi kan inte förutse några omedelbara konsekvenser för andra bolag. Vi berör därför inte andra företag i detta avsnitt.

Tillhandahållare av allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster som inte är Noik

Antalet tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster uppgick under år 2021 till cirka 600 företag.[1] De fyra största aktörerna, Telia Company, Tele2, Telenor och Hi3G (Tre), hade sammanlagt 96 procent av abonnemangen inom mobila tjänster.

I fråga om fast bredband stod de tre största operatörerna, Telia Company, Telenor och Tele2, tillsammans för 68 procent av abonnemangen. De fem största operatörerna inom fiberabonnemang var Telia Company, Telenor, Bahnhof, Tele2 och Bredband2, som tillsammans hade 87 procent av dessa abonnemang. Gruppen ”övriga” hade 12,7 procent av abonnemangen och där ingick cirka 180 aktörer. Störst i gruppen övriga var Allente med 2 procent. Marknadsandelarna på fasta bredbandsabonnemang inkluderar abonnemang på xDSL, kabel-tv, fiber, samt tekniker såsom satellit och fast radio/radiolänk.

I fråga om fast telefoni hade Telia Company störst marknadsandel sett till antalet abonnemang, motsvarande 41,6 procent. Näst störst var Tele2 med 16,3 procent följt av Telavox och Telenor med 12,9 respektive 6,7 procent. Gruppen ”övriga” består av drygt 100 aktörer och störst i den gruppen var WX3.

Under år 2021 uppgick intäkterna avseende slutkunder för telekommunikation till 49,2 miljarder kronor. Här ingår mobila samtals- och datatjänster, fasta internettjänster, fasta samtalstjänster och data-

[1] Enligt PTS rapport ”Svensk telekommarknad 2021”, PTS-ER-2022:22.

kommunikationstjänster till slutkunder, men däremot inte intäkter från tv-abonnemang, roaming eller mjukvarutjänster.

Särskilt om tillhandahållare av allmänt tillgängliga Noik

Tillhandahållare av Noik omfattas inte av reglerna om anmälningsplikt enligt 2 kap. 1 § nya LEK. Det är därför svårt att uppskatta hur många företag som tillhandahåller allmänt tillgängliga nummeroberoende elektroniska kommunikationstjänster i Sverige. Vidare kan företagen ha hemvist i olika länder samtidigt som deras tjänster tillhandahålls globalt. Sådana tjänster kan också uppstå och försvinna i stor omfattning på relativt kort tid. Många av dessa företag har inte säte i Sverige.

Det är emellertid inte svårt att identifiera de för tillfället största aktörerna. De är Apple, Google, Microsoft, Tencent och Meta (tidigare Facebook).

Enligt webbsajten www.statista.com används Noik av flera miljarder användare varje månad. Enbart Whatsapp, som ägs av Meta och är den mest använda tjänsten, hade cirka två miljarder månatliga användare.[2]

I likhet med marknaden för tillhandahållare av allmänt tillgängliga kommunikationstjänster kan det konstateras att ett fåtal tillhandahållare av Noik står för en stor andel av den totala användningen.

13.4 Konsekvenser

Utredningens bedömning: Våra förslag om lagring av uppgifter om abonnemang, nationell säkerhetslagring och riktad lagring ökar risken något för intrång i den personliga integriteten jämfört med i dag. Den ökade risken för integritetsintrång är nödvändig och proportionerlig för att skydda den nationella säkerheten och för att bekämpa den grova brottsligheten.

Förslagen om modernisering av anpassningsskyldigheten och om exekutiv jurisdiktion bedöms inte påverka risken för intrång i den personliga integriteten på ett nämnvärt sätt.

[2] Se https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/. Hämtat den 20 april 2023.

Lagring av uppgift om abonnemang, nationell säkerhetslagring, lagringsskyldighet också för tillhandahållare av allmänt tillgängliga Noik, modernisering av anpassningsskyldigheten och bestämmelser om exekutiv jurisdiktion kommer att vara klart positiva för brottsbekämpningen. Förslag om riktad lagring kan ibland komma att försvåra det brottsbekämpande arbetet. Sammantaget kommer förslagen att vara till fördel för brottsbekämpningen.

De tekniska anpassningar som behövs för en förändrad lagringsskyldighet leder till kostnadsökningar för tillhandahållarna. Denna kostnadsökning ska de själva stå för. Förslagen kan ha en viss påverkan på konkurrensen mellan företag.

Polismyndigheten, Säkerhetspolisen, och Tullverket kommer att behöva ytterligare resurser.

Förslagen kan ha en viss påverkan på miljön. Förslagen kan påverka jämställdheten mellan kvinnor och män. Förslagen bedöms inte få några ytterligare sådana konsekvenser som anges i kommittéförordningen. Förslagen medför inga skyldigheter enligt EU:s anmälningsdirektiv för tekniska föreskrifter.

13.4.1 Samhällspolitiska konsekvenser

Skyddet för den personliga integriteten

Genom våra förslag kommer fler aktörer än tidigare att lagra uppgifter om enskilda och elektronisk kommunikation. Vi föreslår lagring av uppgifter om abonnemang (avsnitt 6), nationell säkerhetslagring (avsnitt 7), lagring av trafik- och lokaliseringsuppgifter i syfte att bekämpa grov brottslighet (avsnitt 8) och lagringsskyldighet för tillhandahållare av Noik (avsnitt 9).

Uppgifter om abonnemang ska som huvudregel lagras ett år efter det att ett abonnemang har upphört. Förslaget omfattar även tillhandahållare av Noik. Det innebär att antalet uppgifter som lagras blir fler. Begreppet uppgift om abonnemang har samma innebörd som tidigare.

Våra förslag medför därför i denna del något ökade risker för den personliga integriteten. Men det ska då framhållas att uppgifter om abonnemang inte är lika integritetskänsliga som trafik- och lokaliseringsuppgifter samt att uppgifterna omfattas av tystnadsplikt. Tillgång till uppgift om abonnemang får endast medges för vissa särskilt författningsreglerade ändamål (se 9 kap. 33 § nya LEK).

Trafik- och lokaliseringsuppgifter lagras för två övergripande syften. Det ena syftet är att skydda den nationella säkerheten (nationell säkerhetslagring), det andra är för att bekämpa grov brottslighet (geografiskt riktad lagring och utökad riktad lagring). En nyhet jämfört med tidigare är att tillhandahållare av Noik ska lagra trafik- och lokaliseringsuppgifter. Kommunikation via exempelvis Whatsapp, Imessage, Messenger och Telegram kommer alltså inte längre vara undantagen från lagring.

På ett övergripande plan kan man beskriva konsekvenserna för den personliga integriteten på följande sätt.

Vid *nationell säkerhetslagring* ökar risken för integritetsintrång. Men sådan lagring kan bara förekomma när det föreligger ett allvarligt hot mot Sveriges säkerhet.

Vid *geografiskt riktad lagring* ökar risken för integritetsintrång för dem som är bosatta i kommuner där det finns en förhöjd risk för grov brottslighet medan risken generellt blir lägre i övriga kommuner.

Vid *utökad riktad lagring* ökar risken för integritetsintrång för personer som blir föremål för beslut om utökad riktad lagring eller personer som befinner sig i områden eller platser som omfattas av beslut om utökad riktad lagring. Härutöver ökar risken för integritetsintrång för personer som dömts för grova brott, för personer som är eller har varit föremål för hemliga tvångsmedel samt för personer som använder sig av utrustning eller abonnemang som har koppling till grova brott eller sådan brottslig verksamhet som innefattar sådana brott. För alla andra minskar risken för integritetsintrång.

Vi menar att dock att bedömningen av konsekvenserna för den personliga integriteten bör göras genom en samlad bedömning.

När det gäller påverkan på den personliga integriteten bör man inledningsvis hålla isär frågan om lagring från frågan om tillgången till trafik- och lokaliseringsuppgifter. Lagringen av trafik- och lokaliseringsuppgifter innebär inte att de brottsbekämpande myndigheterna per automatik får tillgång till uppgifterna. Lagringen skapar bara, förenklat uttryckt, förutsättningar för framtida användning av hemliga tvångsmedel. Men generellt påverkar både lagringen av och tillgången till trafik- och lokaliseringsuppgifter den personliga integriteten.

Med våra förslag kommer tillhandahållarna sannolikt att lagra fler trafik- och lokaliseringsuppgifter än tidigare. Uppgifterna kommer vidare att lagras under en längre tid jämfört med dagens reglering. En ny uppgiftskategori, lokaliseringsuppgifter som inte är trafikupp-

gifter, kommer att bli föremål för lagring. Med sådana avses uppgifter om position som genererats i en användares utrustning oberoende av att den aktivt används för kommunikation, t.ex. gps-positioner.

Uppgifter om rörelsemönster är särskilt integritetskänsliga. Förslag om en lagringsskyldighet för sådana uppgifter ökar risken för integritetsintrång. Det bör dock framhållas att den tekniska utvecklingen har lett till att sådana uppgifter redan i dag lagras av operatörerna. Exempelvis lämnar en modern mobiltelefon vid samtal eller datatrafik kontinuerlig uppgift om plats när den används i ett traditionellt telenät. Uppgifterna lagras förvisso inte i syfte att bekämpa brottslighet men kan inhämtas för att bekämpa grov brottslighet. Vårt förslag om att utöka lagringen till att även omfatta lokaliseringsuppgifter som inte är trafikuppgifter leder med andra ord inte till en avsevärd risk för ökat integritetsintrång.

Vi kan således konstatera att det med våra förslag uppstår en risk för ökat intrång i den personliga integriteten i och med att tillhandahållarna kommer att bevara uppgifterna en längre tid jämfört med i dag och för att de brottsbekämpande myndigheterna, efter beslut om hemliga tvångsmedel, kan få tillgång till fler uppgifter än vad som hade varit fallet om det inte fanns en skyldighet att lagra uppgifterna. Vi återkommer dock nedan om begränsningar genom bl.a. förslagen om riktad lagring. Uppgifterna är också integritetskänsliga och ger en samlad bild över vem som kommunicerade med vem, när kommunikationen ägde rum, var de som använde enheterna befann sig, hur de förflyttade sig och vilken typ av kommunikation det var fråga om.

Bedömning av risken för ett ökat integritetsintrång bör även ske mot bakgrund av att tillhandahållarna inte ska samla in ytterligare uppgifter i anledning av våra förslag. Tydligare uttryckt innebär våra förslag alltså att tillhandahållarna ska bevara vissa uppgifter som redan förekommer i deras verksamhet, så att de brottsbekämpande myndigheterna senare ska ha bättre möjligheter att bekämpa brottslighet som innefattar hot mot den nationella säkerheten och annan grov brottslighet. Som en principiell utgångspunkt har vi slagit fast att tillhandahållarna enligt våra förslag inte ska ha någon skyldighet att införskaffa uppgifter som inte genereras eller behandlas i deras verksamhet. Om en användare exempelvis stänger av funktioner i sin utrustning som leder till att tillhandahållarna inte får del av vissa uppgifter, exempelvis gps-positioner, kommer sådana uppgifter heller inte att bli föremål för lagring. En annan sak är att det finns en bortre

gräns för användarens möjlighet till sådana anpassningar, då en enhet till slut blir obrukbar om all funktionalitet stängs ned.

Ytterligare en aspekt som påverkar vår bedömning är den tekniska utvecklingen och förändrade kommunikationsvanor. Som vi tidigare har beskrivit använder sig en stor andel av befolkningen numera av kommunikationslösningar som inte omfattas av datalagring. Så var det inte tidigare. Tidigare var det huvudsakliga sättet för elektronisk kommunikation samtal och meddelanden i de traditionella teleoperatörernas regi. Det fanns då större förutsättningar att lagra elektronisk kommunikation. Över tid har alltså mängden av uppgifter som lagras blivit mindre trots att tillgången till olika slags kommunikationsmedel har ökat. Vid bedömningen av om våra förslag medför en ökad lagring bör även detta beaktas.

När vi väger samman alla aspekter i fråga om risker för den personliga integriteten gör vi bedömningen att våra förslag om datalagring rent generellt ökar riskerna något för intrång i den personliga integriteten om det jämförs med dagens regler.

Vi övergår nu till frågan om de åtgärder som vi föreslår för att minska riskerna för den personliga integriteten. I dag finns strikta regler som syftar till att skydda den personliga integriteten i såväl tillhandahållarnas som de brottsbekämpande myndigheternas verksamhet. Vid bedömningen av våra förslag bör man alltså även beakta det regelverk som redan finns på plats. Vi har härutöver föreslagit en rad olika åtgärder för att minska riskerna för den personliga integriteten. Syftet har varit att förslagen, sett utifrån ett helhetsperspektiv, inte ska leda till integritetsinskränkningar som är mer långtgående än behövligt. För en utförlig redogörelse av våra förslag i frågor om lagring m.m. hänvisas till avsnitt 6, 7, 8 och 9. Sammanfattningsvis kan följande sägas om förslagen.

Uppgift om abonnemang som genereras och behandlas i tillhandahållarnas verksamhet ska som huvudregel lagras i ett år efter det att abonnemanget upphörde att gälla. Lagringsskyldigheten omfattar även tillhandahållare av allmänt tillgängliga Noik. Det medför en ökad lagring i fråga om mängden uppgifter. Begreppets innebörd är detsamma som tidigare. Uppgifterna omfattas även av samma tystnadsplikt som gäller i dag. Tillgång medges endast för författningsreglerade ändamål.

Nationell säkerhetslagring får inte beslutas förrän det föreligger ett allvarligt hot mot Sveriges säkerhet som är verkligt och aktuellt eller förutsebart. Ett föreläggande om lagring för den nationella säker-

heten ska begränsas till vad som är absolut nödvändigt för syftet med lagringen. Ett offentligt ombud ska bevaka enskildas intressen och ombudet får överklaga ett beslut om nationell säkerhetslagring. SIN ska överpröva Säkerhetspolisens beslut vid ett överklagande. Tillgång till uppgifter som lagrats för den nationella säkerheten får 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.

Lagring i syfte att bekämpa grov brottslighet ska vara riktad mot grov brottslighet. Lagringen ska ske i kommuner där risken för grova brott och grov brottslighet är högre jämfört med andra kommuner. Enligt våra beräkningar omfattar den geografiskt riktade lagringen nu mindre än hälften av Sveriges yta och cirka 70 procent av befolkningens bostadsorter. Det bör sättas i relation till nuvarande regler om lagring som är mer långtgående.

Utökad riktad lagring ska vara begränsad till vad som är absolut nödvändigt för att bekämpa grov brottslighet. Ytterligare en begränsning är att lagringen endast får omfatta brottsutsatta områden, skyddsvärda platser och personer som är eller varit föremål för hemliga tvångsmedel eller dömts för grova brott, samt viss utrustnings- eller abonnemangsidentitet. SIN ska utöva tillsyn i fråga om de brottsbekämpande myndigheternas användning av beslut om utökad riktad lagring. Med våra förslag sker inte datalagring i alla situationer. Trafik- och lokaliseringsuppgifter ska i dessa fall raderas så snart de inte är nödvändiga för tillhandahållarens verksamhet. Ur integritetsperspektiv är en sådan uppgiftsminimering positiv och minskar integritetsintrånget. Vi återkommer i nästa avsnitt om den påverkan en sådan reglering får för brottsbekämpningen.

Det är vår sammantagna bedömning att de åtgärder vi har föreslagit är tillräckliga för att uppnå en bra balans mellan intresset av att främja brottsbekämpningen och intresset av att enskildas personliga integritet inte kränks på ett sätt som inte är godtagbart.

Konsekvenser för brottsligheten och det brottsförebyggande arbetet

I fråga om nya modeller för lagring gör vi följande bedömning. Med våra förslag kommer lagringen av uppgifter att variera. Nationell säkerhetslagring kommer att vara generell och odifferentierad. Vid geo-

grafiskt riktad lagring sker lagring i kommuner med förhöjd risk för förekomst av grova brott och grov brottslighet. Utökad riktad lagring sker efter beslut från de behöriga myndigheterna. När lagring sker, kommer lagringen att omfatta fler uppgifter än i dag och tillhandahållare av allmänt tillgängliga Noik kommer att omfattas av lagringsskyldigheten. Kommunikation via exempelvis appar som Whatsapp, Imessage, Messenger och Telegram kommer att omfattas av lagring. Lagringstiden kommer att vara längre och mer enhetlig. Det medför att uppgifter som lagras ger en samlad bild i fråga om kommunikation och rörelsemönster. De brottsbekämpande myndigheterna får i sådana situationer tillgång till ett bättre underlag. Detta kommer att främja uppklarning av grov brottslighet, bl.a. narkotika- och våldsbrottslighet. Även underrättelseverksamheten kommer att främjas genom våra förslag.[3]

Att brottsutredning och underrättelseverksamhet främjas förutsätter dock att lagring sker. När förutsättningar inte finns för lagring för brottsbekämpande syften kommer mängden uppgifter vara mindre än med nuvarande ordning. De brottsbekämpande myndigheterna kan då enbart få tillgång till sådana uppgifter som operatörerna lagrar för egna ändamål. Den anpassning som vi föreslår i anledning av EU-rätten får som konsekvens att lagringen inte omfattar samtliga användare. Vi har anledning att tro att den modell av lagring som vi föreslår i vissa situationer kan komma att få en negativ inverkan på de brottsbekämpande myndigheternas förmåga att klara upp brottsligheten. Det gäller dock endast i områden där geografiskt riktad lagring inte sker.

De brottsbekämpande myndigheterna har gett tydliga exempel på situationer där avsaknad av trafik- och lokaliseringsuppgifter skulle leda till minskade möjligheter att bekämpa brottslighet. De har också påpekat att det kan uppstå stötande effekter där gärningsplatsen kan få inverkan på förutsättningarna för att lösa brott på ett annat sätt än tidigare. Vi saknar skäl att ifrågasätta dessa uppgifter. Vi har i avsnitt 8 redovisat våra överväganden kring de negativa effekterna av våra förslag och vilka åtgärder som krävs för att motverka dessa.

Våra förslag om riktad lagring bygger på behovet av anpassningar till EU-rätten. Vi har gjort bedömningen att vi bör lägga fram förslag om riktad lagring, så att det finns alternativ vid den fortsatta beredningen. Bedömningen av konsekvenserna av våra förslag bör därför

[3] Jfr SOU 2017:75 s. 297–299 och prop. 2018/19:86 s. 108 och 109.

göras i förhållande till alternativa former av datalagring som inte är generella och odifferentierade. Jämfört med sådana alternativ gör vi bedömningen att våra förslag ger goda förutsättningarna för lagring av trafik- och lokaliseringsuppgifter.

Vi har förutom förslag om lagring även föreslagit modernisering av anpassningsskyldigheten och förtydligat under vilka förhållanden de brottsbekämpande myndigheterna får inhämta elektronisk information som är eller kan vara lagrad utanför Sverige. Dessa förslag ökar effektiviteten vad gäller såväl arbetet inom underrättelseverksamheten som möjligheterna att klara upp brott.

Antalet fall av användande av hemliga tvångsmedel vid utlänningskontroll är få. Vi bedömer att den användningen inte kommer att påverkas av våra förslag på ett märkbart sätt.[4]

Våra förslag om en anpassning till EU-rätten och lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet kan ibland komma att försvåra det brottsbekämpande arbetet eftersom sådan lagringsskyldighet inte kommer vara generell. Däremot kommer våra förslag om nationell säkerhetslagring, möjligheten att över huvud taget lagra fler typer av uppgifter och under längre tid än i dag att vara klart positiva för brottsbekämpningen. Brottsbekämpningen kommer också att klart gynnas av förslagen om lagringsskyldighet och anpassningsskyldighet för tillhandahållare av Noik, om en tydligare anpassningsskyldighet för de traditionella teleoperatörerna och om en möjlighet för de brottsbekämpande myndigheterna att inhämta elektronisk information som är eller kan vara lagrad utanför Sverige. Enligt vår mening kommer våra förslag sammantaget att vara till fördel för brottsbekämpningen.

Frågor om miljö och jämställdhet

Som vi beskriver nedan kan våra förslag om lagring medföra inköp av lagringsmedia och en ökad energikonsumtion i serverhallar där lagringen ska verkställas, vilket kan ha viss påverkan på miljön. Vi kan emellertid inte närmare beräkna eller bedöma en sådan miljöpåverkan.

Ett av de sex delmålen i den svenska jämställdhetspolitiken är att mäns våld mot kvinnor ska upphöra. Mäns våld mot kvinnor och våld i nära relationer pekas ut som det tydligaste uttrycket för bris-

[4] Jfr SOU 2017:75 s. 300.

tande jämställdhet mellan kvinnor och män.[5] Det finns även en överrepresentation av män vid annan brottslighet. Brottsbekämpning är därför viktig även för jämställdheten mellan kvinnor och män. Som framgår ovan främjar en del av våra förslag brottsbekämpningen. Det är dock svårt att göra några säkra uttalanden om våra förslag kommer att medföra några positiva eller negativa effekter för jämställdheten mellan kvinnor och män.

13.4.2 Konsekvenser för företagen

Konkurrens

Vi bedömer att våra förslag kommer att få en viss påverkan i frågan om konkurrens mellan tillhandahållarna. Som vi har redogjort för i avsnitt 13.3 består marknaden för telekommunikation av ett stort antal aktörer som får antas ha olika förutsättningar att anpassa it-stöd och organisation. Även om både små och stora aktörer måste anpassa sig till ett förändrat regelverk finns det anledning att anta att de brottsbekämpande myndigheterna i första hand kommer att vända sig till de största tillhandahållarna när beslut om lagring fattas. Detsamma torde gälla när tillgång begärs till uppgifter genom beslut om hemliga tvångsmedel. Våra förslag kan falla ut så att belastningen på de små aktörerna blir mindre jämfört med de stora aktörerna. Samtidigt kan det vara svårare för ett mindre bolag att klara av att bära ökade kostnader. Det går därför inte att dra några säkra slutsatser i frågor om konkurrens mellan små och stora aktörer.

När det gäller tillhandahållare av Noik kan bolagen ha en viss konkurrensfördel genom att dessa typiskt sett inte har investerat i egen infrastruktur för elektronisk kommunikation i Sverige. Tillhandahållare av Noik kommer således i vissa situationer inte att påverkas av lagringsskyldigheten i samma utsträckning som de traditionella teleoperatörerna. Med våra förslag blir dock reglerna konkurrensneutrala i den meningen att lagringsskyldigheten gäller alla tillhandahållare.

[5] Se https://jamstalldhetsmyndigheten.se/mans-vald-mot-kvinnor/fakta-och-statistik/. Hämtat den 20 april 2023.

Kostnader

Vi bedömer att våra förslag kommer att vara kostnadsdrivande för dem som ska verkställa lagringen och de som måste anpassa sina it-stöd så att tvångsmedelsbeslut ska kunna verkställas. Vi har då även beaktat att it-stöd rent generellt behöver kontinuerlig översyn och uppdateringar.

I fråga om lagringsskyldigheten kommer en stor del av kostnaderna sannolikt att bestå i olika anpassningar av it-stöd. Tillhandahållare behöver framöver kunna lagra fler typer av uppgifter och ha förmåga att hantera olika typer av lagring. Med våra förslag kan tillhandahållarna också behöva lagra uppgifter med utgångspunkt från ett beslut. Eftersom besluten kan se olika ut, kommer bolagen att behöva ha förmågan att differentiera både vilka uppgifter som ska lagras och lagringstiden. Härutöver behöver tillhandahållarna kunna skilja på om uppgifter är lagrade för den nationella säkerheten eller om lagring sker för att bekämpa grov brottslighet. Enligt uppgift från teleoperatörerna saknas i dag tekniskt stöd för den typen av urvalsmekanism. En sådan skulle därför behöva utvecklas från grunden.

Den svenska modellen för lagring är dessutom en nyhet för tillhandahållare av Noik. Det torde i sig kräva viss särskild anpassning till svenska förhållanden.

Teleoperatörerna har uppgett att lagring av lokaliseringsuppgifter som inte är trafikuppgifter skulle medföra mycket stora kostnader för bolagen, sett till mängden uppgifter. Kostnaden för inköp av lagringsmedia är i och för sig lägre i dag än när datalagringsskyldigheten infördes. Lagring av uppgifterna innebär trots detta sannolikt ytterligare kostnader i form av ökad energikostnad i serverhallar och kostnad för personal som ska sköta driften. Vi förutser också en ökning av kostnader i fråga om den praktiska hanteringen som en konsekvens av beslut om nationell säkerhetslagring och utökad riktad lagring.

Även i fråga om anpassningsskyldigheten medför våra förslag nya kostnader för tillhandahållare av vissa allmänt tillgängliga elektroniska kommunikationstjänster till fast nätanslutningspunkt. Denna grupp kommer att behöva anpassa sina it-stöd så att tvångsmedelsbeslut kan verkställas. Verkställigheten kräver också en sådan organisation och bemanning så att tvångsmedel kan verkställas utan dröjsmål. Sammantaget bedömer vi att förslagen driver kostnader utöver vad som annars skulle blivit fallet om våra förslag inte genomfördes.

Finansiering

Frågan är hur de ökade kostnaderna ska fördelas. Den nuvarande modellen för kostnadsfördelning mellan det allmänna och operatörerna innebär att operatörerna står för kostnader för anpassning, drift och underhåll och de brottsbekämpande myndigheterna betalar en 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 (prop. 2010/11:46 s. 67). Förutom att vila på detta principiella ställningstagande har en sådan modell för kostnadsfördelning även samhällsekonomiska fördelar. Den part som har möjlighet att påverka kostnaden har nämligen också ett ansvar för den. På detta sätt nyttjas operatörernas tekniska och administrativa kompetens på området, samtidigt som de har ett tydligt incitament att hålla nere kostnader för anpassning och drift. Med denna modell får de brottsbekämpande myndigheterna dessutom incitament att inhämta trafik- och lokaliseringsuppgifter bara då de anser det vara en effektiv metod som kan förväntas föra utredningsarbetet framåt. En sådan modell har tidigare bedömts som samhällsekonomiskt kostnadseffektiv (prop. 2010/11:46 s. 68). Starka skäl talar enligt vår mening för att den gällande modellen för kostnadsfördelning inte bör frångås.

Mot det kan anföras att tillhandahållarna behövde förändra sitt it-stöd så sent som 2019 till följd av de ändringar som då gjordes i bestämmelserna om datalagring. Ändringarna handlade om att differentiera lagringstiden och upphörande av lagring av vissa uppgifter, vilket jämfört med de förslag vi nu föreslår får bedömas som en mindre omfattande ändring.

Ett på nytt förändrat regelverk efter relativt kort tid kan mot denna bakgrund uppfattas som betungande. Därför kan det finnas anledning att överväga om leverantörerna till någon del ska kompenseras för de relativt stora förändringarna som vi nu föreslår. Det kan exempelvis nämnas att i Danmark har tillhandahållarna erhållit viss ersättning i anledning av genomförande av regler om riktad lagring. Överväganden kring en statlig subvention av de it-utvecklingskostnader som våra förslag medför är emellertid en komplex fråga. Inom ramen för vårt uppdrag och med det underlag vi har bedömer vi dock inte att det finns anledning att föreslå någon sådan kompensation. Under

alla förhållanden behöver en sådan fråga utredas särskilt. Den kan inte tas upp i vår utredning.

Sammantaget anser vi alltså att den gällande modellen för kostnadsfördelningen inte ska frångås. Det innebär att tillhandahållarna alltjämt ska stå för anpassningskostnader, drift och underhåll. Det allmänna ska ersätta operatörerna för de kostnader som hänför sig till utlämnande av uppgifter i enskilda ärenden.

13.4.3 Konsekvenser för myndigheter

Polismyndigheten

Polismyndigheten har påtalat att det är svårt att göra en exakt beräkning av de kostnader som följer av förslagen. Förslagen medför enligt myndigheten en årlig kostnad om cirka 28 miljoner kronor, varav 12 miljoner kronor avser anpassning av tekniska system och 16 miljoner kronor avser ökade personalkostnader. I kostnaderna för teknik inryms hyra av säkra förbindelser till de ytterligare tillhandahållare som träffas av anpassningsskyldigheten samt livscykelkostnader, inklusive avskrivningar, för teknisk utrustning. De redovisade kostnaderna ryms inte inom befintliga budgetramar. Kostnaderna fördelar sig enligt Polismyndigheten på följande sätt.

Förslaget om exekutiv jurisdiktion

Förslaget kommer sannolikt leda till fler fall där Polismyndigheten kan verkställa HDA eller genomsökning på distans men inte i sådan omfattning att det får någon ekonomisk påverkan för myndigheten. Förslaget kan i enskilda fall leda till effektivare resursanvändning eftersom andra, mer kostsamma, spaningsåtgärder inte behöver vidtas i vissa fall när information kan tillgås med stöd av den nya lagen.

Förslaget om nationell säkerhetslagring

De ekonomiska konsekvenserna av nationell säkerhetslagring är svåra att förutse och någon uppskattning av kostnader kan inte lämnas.

Förslagen om geografisk riktad lagring och utökad riktad lagring

De ekonomiska konsekvenserna i fråga om geografiskt riktad lagring är svårbedömda. När trafik- och lokaliseringsuppgifter inte lagras i områden som inte omfattas av geografiskt riktad lagring försämras förutsättningarna för brottsbekämpning. Viss brottslighet blir inte utredd och behovet av resurser minskar. I vissa situationer leder brist på lagrade trafik- och lokaliseringsuppgifter till en ökad användning av hemliga tvångsmedel och andra utredningsåtgärder. Kostnaden ökar i sådana situationer då bl.a. analytiker, utredare och teknisk personal tas i anspråk.

Förslaget om utökad riktad lagring medför omfattande kostnader för Polismyndigheten i form av analyser, utredningsarbete och beslut för att skapa förutsättningar för datalagring i de delar av landet som inte omfattas av geografiskt riktad lagring. Polismyndigheten beräknar kostnaderna för detta till cirka 8 miljoner kronor årligen.

Förslaget om lagringsskyldighet för tillhandahållare Noik och en modernisering av anpassningsskyldigheten

Förslaget medför att uppgifter kan inhämtas från fler tillhandahållare. Det medför utvecklingskostnader för Polismyndighetens tekniska system. En anpassning av myndighetens tekniska system bedöms uppgå till cirka 12 miljoner kronor årligen. Vidare medför förslagen personella kostnader om 8 miljoner kronor årligen. Ytterligare kostnader kan uppkomma om Polismyndigheten behöver anpassa sina tekniska system till många tillhandahållare av Noik eller om olika tekniska standarder behöver användas.

Säkerhetspolisen

Förslagen medför enligt Säkerhetspolisen en total årlig kostnad för myndigheten som uppgår till cirka 30 miljoner kronor, varav 10 miljoner avser personalkostnader och 20 miljoner avser kostnader för teknik. I kostnaderna för teknik inryms hyra av säkra förbindelser till de ytterligare tillhandahållare som träffas av anpassningsskyldigheten samt livscykelkostnader, inklusive avskrivningar, för teknisk utrustning. De kostnader som redovisas ryms inte inom befintliga

budgetramar. Kostnaderna fördelar sig enligt Säkerhetspolisen på följande sätt.

Förslaget om exekutiv jurisdiktion

Förslaget kommer sannolikt leda till fler fall där Säkerhetspolisen kan verkställa HDA eller genomsökning på distans men inte i sådan omfattning att det får någon ekonomisk påverkan. Förslaget kan i enskilda fall leda till effektivare resursanvändning eftersom andra, mer kostsamma, spaningsåtgärder inte behöver vidtas i vissa fall när information kan tillgås med stöd av den nya lagen.

Förslaget om nationell säkerhetslagring

Genom förslaget får Säkerhetspolisen en ny uppgift med tillhörande administration. Förslaget innebär också kostnader för utbildning och genomförande. Varje ärende om nationell säkerhetslagring innebär att underlag ska tas fram och föredras vid ett sammanträde till vilket ett offentligt ombud ska kallas att närvara. Säkerhetspolisen ska även bemöta eventuella överklaganden från det offentliga ombudet och ska närvara vid kontrollorganets sammanträde i ärendet. Såsom förslaget är utformat är det fråga om ett begränsat antal ärenden, men ärendenas karaktär medför att ett betydande arbete kommer att krävas inför ett beslut.

Förslaget medför sannolikt även en ökning av antalet framställningar om verkställighet av beslut om tillstånd till hemliga tvångsmedel inklusive beslut enligt inhämtningslagen. Omfattningen av ökningen är dock svår att bedöma.

Sammantaget bedömer Säkerhetspolisen att kostnaderna kommer att uppgå till årligen 3 miljoner kronor.

Förslaget om geografiskt riktad lagring och utökad riktad lagring

Förslaget om geografiskt riktad lagring som beslutas av PTS föranleder inga direkta kostnader för Säkerhetspolisen. Förslaget såvitt avser utökad riktad lagring innebär nya arbetsuppgifter med tillhörande handläggning, administration, samråd och beslutsfattande. Vissa be-

slut om utökad riktad lagring är sannolikt av enklare slag och kräver ingen nämnvärd analys eller bedömning. Det gäller främst i fråga om beslut om utökad riktad lagring avseende en skyddsvärd plats som grundas på om platsen är ett skyddsobjekt eller en sådan plats där det bedrivs säkerhetskänslig verksamhet enligt säkerhetsskyddslagen. I nämnda fall bör det inte heller vara fråga om särskilt många beslut per år, eftersom besluten får gälla i upp till tre år. Även om varje ny arbetsuppgift medför en viss ökad kostnad för en myndighet är kostnaden för denna del av förslaget inte av sådan omfattning att den påverkar Säkerhetspolisen i någon större utsträckning.

I fråga om beslut om utökad riktad lagring avseende en skyddsvärd plats som bedöms vara särskilt betydelsefull från brottsbekämpningssynpunkt krävs en större arbetsinsats från myndigheten. Det handlar t.ex. om att identifiera sådana platser, göra en analys av platsens betydelse från brottsbekämpningssynpunkt, samråda med övriga beslutande myndigheter samt ta fram underlag för själva beslutet och administration kring detta.

Mot bakgrund av att den geografiskt riktade lagringen – utifrån den ögonblicksbild som förslaget nu resulterar i – undantar en mycket stor del av Sveriges yta, ställs höga krav på de analyser, bedömningar och samråd som de brottsbekämpande myndigheterna måste göra inför beslut om utökad riktad lagring avseende skyddsvärda platser. De höga kraven innebär att såväl tid som andra resurser behöver läggas för att åstadkomma en mer träffsäker lagring av uppgifter utifrån geografiska parametrar. Den arbetsinsats som krävs för detta bedöms vara omfattande. Samtliga platser som behöver analyseras och bedömas kommer sannolikt inte att omfattas av ett beslut om utökad riktad lagring. Att beräkna kostnaden utifrån antalet beslut framstår därför inte som rimligt. Kostnaden bör i stället beräknas utifrån den arbetsinsats som förslaget kräver inför ett beslut. Eftersom förslaget innebär att platser behöver analyseras och bedömas löpande samt att beslut ska upphävas så snart det inte längre finns skäl, är det inte fråga om en punktinsats utan om en ny kontinuerlig och löpande arbetsuppgift för myndigheten. Myndigheten kommer att behöva lägga omfattande resurser på detta arbete.

Förslaget om utökad riktad lagring avseende utrustnings- och abonnemangsidentitet innebär sannolikt många fler beslut eller fler objekt som omfattas av ett beslut. Likt det ovan anförda om skyddsvärda platser borde kostnadsberäkningen inte utgå från antalet beslut

utan från den arbetsinsats som myndigheten behöver göra inför besluten. Arbete som behöver göras handlar t.ex. om att identifiera vilken utrustnings- eller abonnemangsidentitet som bör omfattas av ett beslut, bedöma om den använts vid eller skäligen kan antas komma till användning vid ett grovt brott eller vid grov brottslig verksamhet samt göra lämplighetsavvägningar utifrån bl.a. sekretess och säkerhetsskydd såväl inför samråd med övriga brottsbekämpande myndigheter inför beslutet. För att åstadkomma en mer träffsäker lagring av uppgifter krävs en arbetsinsats som är såväl omfattande som tidskrävande. Det är också, precis som angetts ovan om beslut gällande skyddsvärda platser, en ny löpande arbetsuppgift för myndigheten och inte någon punktinsats. Sammantaget bedömer Säkerhetspolisen att kostnaderna årligen kommer att uppgå till 4 miljoner kronor.

Förslaget om lagringsskyldighet för tillhandahållare Noik och en modernisering av anpassningsskyldigheten

Förslaget medför att uppgifter kan inhämtas från fler tillhandahållare. Det medför vissa initiala kostnader för att upprätta kontaktvägar och kommunikationskanaler för inhämtning av uppgifter från nya tillhandahållare, sådana som inte tidigare har omfattats av skyldigheten att medverka vid verkställighet av beslut om hemliga tvångsmedel. Det innebär en ökad mängd uppgifter som kommer in till Säkerhetspolisen. Därmed uppkommer en viss ökning av kostnader för att kunna omhänderta och hantera dessa uppgifter. Till detta kommer kostnaderna för verkställande av beslut enligt inhämtningslagen hos tillhandahållare av Noik. För användning av hemliga tvångsmedel i realtid krävs säkra förbindelser mellan Säkerhetspolisen och tillhandahållare av Noik. Sådana lösningar finns redan i drift för de teleoperatörer som i dag har motsvarande anpassningsskyldighet. En exakt bedömning av de kostnader som kommer att bli aktuella är svår att göra, men uppskattningsvis kommer cirka 20 miljoner kronor att krävas årligen. Kostnader bör kunna fördelas mellan de brottsbekämpande myndigheterna. Sammantaget bedömer Säkerhetspolisen att kostnaderna årligen kommer att uppgå till 23 miljoner kronor.

Tullverket

Förslagen medför enligt Tullverket en total årlig kostnadsökning för myndigheten som uppgår till cirka 20 miljoner kronor, varvid 5 miljoner kronor avser personella resurser och cirka 15 miljoner kronor avser kostnader för teknikanpassningar. Kostnaderna fördelar sig enligt Tullverket på följande sätt.

Förslaget om nationell säkerhetslagring

De ekonomiska konsekvenserna av nationell säkerhetslagring är svåra att förutse och någon uppskattning av kostnader kan inte lämnas.

Förslaget om geografiskt riktad lagring och utökad riktad lagring

Utökad riktad lagring innebär nya arbetsuppgifter för Tullverket med tillkommande kostnader för att utveckla nya rutiner. För att motverka de negativa effekterna av geografiskt riktad lagring behöver Tullverket fatta beslut som kräver omfattande analyser. Med hänsyn till att geografiskt riktad lagring inte täcker stora delar av Sverige krävs sannolikt många beslut. De nya arbetsuppgifterna kräver att Tullverket identifierar platser, områden, personer, utrustning och abonnemang där det finns behov av utökad riktad lagring. Tullverket behöver även samråda med andra myndigheter inför beslut och sedermera omprövning av beslut. De tillkommande arbetsuppgifterna ryms inte inom befintliga budgetramar och kräver resursförstärkning, såväl för implementeringskostnader som för löpande kostnader. Baserat bl.a. på antal underrättelseärenden per år beräknar Tullverket att kostnaderna uppgår till minst två årsarbetskrafter, motsvarande cirka 1,7 miljoner kronor.

Förslagen om lagringsskyldighet för tillhandahållare av Noik och en modernisering av anpassningsskyldigheten

Tullverket gör bedömningen att förslaget kommer att ge upphov till behov av resursförstärkning för underrättelse- och tullkriminalavdelningen. Förslaget medför också vissa initiala kostnader för att upprätta kontaktvägar och kommunikationskanaler för inhämtning av

uppgifter från tillhandahållare som inte tidigare har omfattats av skyldigheten att medverka vid verkställighet av beslut om hemliga tvångsmedel. Tullverket gör bedömningen att antalet ärenden hos myndigheten där ansökan om inhämtning till åklagare eller begäran om HÖK via åklagare inte kommer att öka nämnvärt. Däremot bedömer Tullverket att antalet framställningar om uppgiftslämnande av trafik- och lokaliseringsuppgifter kommer att öka. Även den totala mängden trafik- och lokaliseringsuppgifter som kommer in till Tullverket kommer att öka. Baserat på antalet ansökningar om inhämtningar och HÖK-beslut som Tullverket handlägger görs bedömning att förslagen kommer innebära behov av en resursförstärkning om knappt en årsarbetskraft. I nuläget beräknas den kostnaden till cirka 3,4 miljoner kronor.

Tullverket kommer, i likhet med Polismyndigheten och Säkerhetspolisen, att ha kostnader för verkställande av hemliga tvångsmedel i realtid och andra teknikanpassningar. Tullverket har svårt att göra en exakt beräkning av kostnaderna men uppskattar att denna kostnad kommer att uppgå till cirka 15 miljoner årligen, varav cirka 5 miljoner kronor avser drift- och supportkostnader och cirka 10 miljoner kronor avser delfinansiering av de myndighetsgemensamma tekniska förmågorna.

Åklagarmyndigheten och Ekobrottsmyndigheten

Åklagarmyndigheten har beskrivit svårigheterna med att göra en säker ekonomisk prognos. Förslagen kan i vissa fall resultera i att åklagare kan komma att använda hemlig övervakning av elektronisk kommunikation i en större omfattning jämfört med i dag. Det kommer att leda till att utredningar kan drivas längre, vilket i sig är kostnadsdrivande. I andra fall kommer avsaknaden av trafik- och lokaliseringsuppgifter att leda till minskad användning av hemliga tvångsmedel och utredningar. Det resulterar i färre kontakter med Polismyndigheten och domstol. I sådana situationer finns inte arbetsuppgifter för åklagare och administrativ personal, vilket kommer att minska kostnaderna för myndigheten. Åklagarmyndigheten har sammantaget gjort bedömningen att de ekonomiska konsekvenserna av förslagen kommer att rymmas inom befintliga budgetramar.

Ekobrottsmyndigheten har erinrat om att myndigheten, till skillnad från Åklagarmyndigheten, har en egen funktion för avlyssning och övervakning av elektronisk kommunikation. Ekobrottsmyndigheten har gjort bedömningen att de ekonomiska konsekvenserna av förslagen kommer att rymmas inom befintliga budgetramar.

Säkerhets- och integritetsskyddsnämnden

SIN har uppgett att förslagen kommer att medföra omfattande implementeringskostnader. En ny organisation måste byggas upp med rutiner för en ny delegation. De nya arbetsuppgifterna ställer även nya krav på möteslokaler och medför kostnader för hantering av säkerhetsskyddskänsligt material. Det löpande arbetet med Datalagringsdelegationen kommer att medföra behov av kanslistöd. Detsamma gäller det nya tillsynsområdet där en stor mängd underrättelser behöver hanteras. Sammantaget bedömer SIN att förslagen medför kostnadsökningar om cirka 3 miljoner kronor årligen. Kostnaderna motsvarar en och en halv årsarbetskraft för föredragande, en årsarbetskraft för kanslistöd samt ökade lokalkostnader och anpassning till de särskilda behov som Datalagringsdelegationens verksamhet kommer att kräva.

Utöver de resursbehov som framgår ovan kan det på sikt uppkomma ytterligare behov av tillskott till nämndens verksamhet när omfattningen av den nya verksamheten tydliggörs.

Post- och telestyrelsen

PTS har för utredningen redovisat att kostnadsökningar i anledning av utredningens förslag om geografiskt riktad lagring kommer att rymmas inom befintliga budgetramar. Övriga konsekvenser för myndigheten av utredningens förslag består i att myndigheten får utökade uppgifter i form av att behöva ge vägledning och även bedriva tillsyn, eftersom de olika formerna av lagringsskyldighet som införs är nya och nya aktörer berörs av skyldigheterna. För dessa utökade uppgifter har PTS i budgetunderlag för åren 2024–2026 begärt resursförstärkningar. De kostnadsökningar som följer av förslagen i betänkandet ryms i det begärda anslaget.

Allmänna domstolar, Försvarsmakten och Kustbevakningen

Vår bedömning är att våra förslag har högst marginell påverkan på de allmänna domstolarnas, Försvarsmaktens och Kustbevakningens verksamhet. Uppkomna kostnader i dessa verksamheter bör rymmas inom befintliga budgetramar.

Kommuner och regioner

Angelägenheter om lagring av trafik- och lokaliseringsuppgifter i syfte att bekämpa grov brottslighet och hot mot den nationella säkerheten faller utanför kommunernas verksamhet och därigenom även den kommunala självstyrelsen. Den omständigheten att vi utgår från kommunerna som geografisk avgränsning i förslag om geografiskt riktad lagring saknar betydelse vid bedömningen av denna fråga.

Finansiering

Våra förslag medför ökade kostnader för Polismyndigheten, Säkerhetspolisen, Tullverket och SIN. De uppgifter om kostnader som myndigheterna har redovisat är behäftade med viss osäkerhet. Det saknas underlag för oss att föreslå en närmare finansiering av förslagen. Vi gör dock bedömningen att de ökade kostnaderna inte ryms inom ramen för befintliga budgetanslag för respektive myndighet.

13.4.4 Övriga konsekvenser

Ingen anmälningsskyldighet för tekniska föreskrifter

Enligt anmälningsdirektivet har medlemsstater en skyldighet att offentligt tillkännage om en ny nationell teknisk föreskrift har antagits. Direktivet är dock inte tillämpligt på teletjänster (se artikel 1.3 i ramdirektivet). Ramdirektivet har numera ersatts av e-kodexen som införlivats i Sverige genom nya LEK, se avsnitt 4.3.

Frågan om anmälningsskyldighet för tekniska föreskrifter behandlades i Utredningen Datalagring – brottsbekämpning och integritet (SOU 2017:75). Där konstaterades att någon anmälningsskyldighet inte uppkom i anledning av de föreslag som lämnades i fråga om data-

lagring.[6] Vi gör ingen annan bedömning. Någon anmälningsskyldighet kommer således inte att uppkomma med anledning av de föreslag vi lämnar.

Inga övriga konsekvenser

Förslagen bedöms inte få några ytterligare sådana konsekvenser som anges i kommittéförordningen (1998:1474).

[6] Se SOU 2017:75 s. 305.

14 Författningskommentar

14.1 Förslaget till lag (2024:000) om inhämtning av elektronisk information som är lagrad utanför Sverige vid användning av straffprocessuella tvångsmedel

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.

Genom denna paragraf och övriga paragrafer i lagen klargörs möjligheten till exekutiv jurisdiktion avseende åtkomst till elektronisk information som är lagrad utanför Sverige. Övervägandena finns i avsnitt 11.9.5.

Att informationen är lagrad utanför Sverige innebär att den finns eller är sparad utomlands. Lagen gäller även om det är oklart var informationen lagras. Lagen gäller såväl inom som utom förundersökningar beträffande brott som svensk domstol är behörig att döma över eller brottslig verksamhet som innefattar brott som svensk domstol är behörig att döma över, dvs. sådana brott eller sådan brottslig verksamhet som svenska myndigheter får bekämpa.

Av paragrafen framgår att lagen är tillämplig vid de brottsbekämpande myndigheternas användning av straffprocessuella tvångsmedel. Någon uttrycklig begränsning görs inte till vissa straffprocessuella tvångsmedel. De straffprocessuella tvångsmedel som lagen i dag kan tillämpas på är hemlig dataavläsning och genomsökning på distans.

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.

I paragrafen föreskrivs att de brottsbekämpande myndigheterna endast får inhämta sådan information som de utan bistånd kan skaffa sig tillgång till. Övervägandena finns i avsnitt 11.9.5.

Med att utan bistånd skaffa sig tillgång menas att den brottsbekämpande myndigheten kan bereda sig tillgång till de aktuella uppgifterna som lagras utanför Sverige i ett avläsningsbart informationssystem, t.ex. ett konto på en lagringstjänst eller en kommunikationsutrustning, utan hjälp från utomstående, t.ex. tillhandahållaren av lagringstjänsten eller någon annan stat. Detta påverkar dock inte på vilket sätt myndigheterna kan få tillgång till t.ex. de inloggningsuppgifter eller den mobiltelefon som används för att komma åt informationen, vilket alltså kan ske med hjälp från utomstående.

Paragrafen förutsätter att inhämtningen görs från en plats där den brottsbekämpande myndigheten är behörig att verka, i praktiken Sverige. För att de brottsbekämpande myndigheterna ska kunna skaffa sig tillgång till informationen, ställs i 3 § upp vissa villkor för inhämtningen.

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.

Paragrafen ger uttryck för den försiktighetsprincip som måste råda då information som är eller kan vara lagrad utanför Sverige inhämtas av svenska brottsbekämpande myndigheter. Övervägandena finns i avsnitt 11.9.5.

Paragrafen innehåller två rekvisit som begränsar möjligheterna till inhämtning av elektronisk information, nämligen att inhämtningen inte får innebära mer än ett obetydligt intrång i en annan stats suveränitet och att inhämtningen inte får bedömas orsaka någon skada på det informationssystem som tvångsmedlet avser.

Utgångspunkten är att inhämtningen inte får innebära annat än ett obetydligt intrång i den berörda statens suveränitet. Detta gäller även om det inte är klarlagt i vilken eller vilka stater den elektroniska informationen lagras. En inhämtning av elektroniska uppgifter som lagras i ett annat land innebär i många fall ett intrång i den statens suveränitet. Men är intrånget inte mer än obetydligt, får det tolereras. Utöver den proportionalitetsbedömning som alltid ska göras vid användning av tvångsmedel, ska en proportionalitetsbedömning göras av intrånget i den berörda statens suveränitet. Vid denna bedömning

kan bl.a. beaktas hur känsliga de uppgifter som den brottsbekämpande myndigheten vill inhämta kan vara. Ju viktigare uppgifterna är för brottsbekämpningen, desto mer utrymme finns det för att bedöma ett intrång som godtagbart. En inhämtning som medför beaktansvärda risker för informationssäkerheten innebär normalt mer än ett obetydligt intrång och är därför inte tillåtet. Med informationssäkerhet avses i detta sammanhang att elektroniskt lagrad information skyddas så att den alltid finns där när den behövs (tillgänglighet), att man kan lita på att den är korrekt och inte manipulerad eller förstörd (riktighet) och att endast behöriga personer får ta del av den (konfidentialitet).

Hemlig dataavläsning, med de begränsningar som följer av denna lag, och genomsökning på distans bör emellertid normalt inte innebära några beaktansvärda risker för informationssäkerheten, eftersom informationen fortfarande är tillgänglig på användarkontot och inga ändringar får göras i informationen. Tillgång till uppgifter på ett användarkonto genom inloggning på kontot eller i övrigt normal åtkomst till tjänsten bör som huvudregel anses vara ett obetydligt intrång i andra staters suveränitet.

Vidare framgår att information inte får inhämtas, om inhämtningen kan bedömas orsaka någon skada på det informationssystem som tvångsmedlet avser. Vid exempelvis hemlig dataavläsning får tekniska hjälpmedel användas, systemskydd brytas och tekniska sårbarheter utnyttjas om det är nödvändigt. Sådana åtgärder kan, när det gäller information som finns i ett annat land än Sverige, vara förbjudna redan av det skälet att användningen av åtgärden skulle innebära ett för stort intrång i det aktuella landets suveränitet. Men även om bedömningen görs att så inte är fallet, kan åtgärden vara förbjuden eftersom den kan orsaka skada på det informationssystem som tvångsmedlet avser. I 25 § lagen (2020:62) om hemlig dataavläsning finns en bestämmelse om aktsamhetskrav när beslut om hemlig dataavläsning verkställs. Enligt paragrafen får någon olägenhet eller skada inte förorsakas utöver vad som är absolut nödvändigt. Vidare får, enligt samma paragraf, informationssäkerheten i andra avläsningsbara informationssystem än det tillståndet avser inte åsidosättas, försämras eller skadas. Regeln i 3 § sträcker sig alltså längre. Detta innebär att den tänkta åtgärden inte får vidtas om bedömningen görs att den kan orsaka någon skada på det aktuella informationssystemet. Denna stränga syn ger uttryck för den försiktighetsprincip som ska

tillämpas när information som är eller kan vara lagrad utanför Sverige inhämtas av svenska brottsbekämpande myndigheter.

14.2 Förslaget till lag (2025:000) om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet

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

Paragrafen anger syftet med lagen. Övervägandena finns i avsnitt 7.2.2 och 7.3.3. Lagen reglerar förutsättningarna för lagring av och tillgång till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

Med uttrycket uppgifter om elektronisk kommunikation avses uppgift om abonnemang samt trafik- och lokaliseringsuppgifter, dvs. de uppgifter som framgår av 9 kap. 31 § första stycket 1 och 3 nya LEK. Även lokaliseringsuppgifter som inte är trafikuppgifter omfattas av regleringen genom en ny fjärde punkt i 9 kap. 31 § första stycket samma lag. Med lokaliseringsuppgifter som inte är trafikuppgifter avses exempelvis satellitpositioneringsuppgifter som genererats i utrustningen.

Uttrycket Sveriges säkerhet saknar legaldefinition. Det används synonymt med uttrycken riket säkerhet och nationell säkerhet i bl.a. offentlighets- och sekretesslagen (2009:400), säkerhetsskyddslagen (2018:585), lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter och lagen (2022:700) om särskild kontroll av vissa utlänningar. Uttrycket har här samma innebörd. Viss vägledning i fråga om innebörden kan hämtas från rekommendationer från Rådet för de europeiska advokatsamfunden (CCBE). Där anges att nationell säkerhet kan förstås som statens inre och yttre säkerhet, och bestå av ett eller flera av följande element:

- statens suveränitet,
- integriteten hos dess territorium, dess institutioner och dess kritiska infrastruktur,
- skyddet av statens demokratiska ordning,

• skydd av dess medborgare och invånare mot allvarliga hot mot liv, hälsa och mänskliga rättigheter och

• uppförande och främjande av dess utrikesförbindelser och engagemang för fredlig samexistens mellan nationer.

Ytterligare vägledning kan hämtas genom i den brottskatalog som anges i 11 §.

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.

Paragrafen anger förutsättningarna för nationell säkerhetslagring, förfarandet före beslut och giltighetstiden av ett föreläggande om nationell säkerhetslagring. Paragrafen innehåller också en upplysning om att det i nya LEK finns regler som berör tillhandahållarna. Övervägandena framgår av avsnitt 7.3.1, 7.3.3 och 7.3.6.

Av *första stycket* framgår att Säkerhetspolisen ska bedöma hotet mot den nationella säkerheten och får besluta om nationell säkerhetslagring. Med nationell säkerhetslagring menas en lagring av trafik- och lokaliseringsuppgifter som är generell och odifferentierad och som sker i syfte att skydda den nationella säkerheten.

För lagring krävs att det föreligger ett allvarligt hot mot Sveriges säkerhet som är verkligt och aktuellt eller förutsebart. Omständigheter som kan vara av betydelse vid bedömningen av hotet mot den nationella säkerheten är t.ex. om det inträffar ett terrordåd, förekomsten av allvarliga och skadliga cyberangrepp, förhöjd terrorhotsnivå i Sverige, hot om ett väpnat angrepp mot Sverige eller om andra

jämförbara allvarliga hot mot Sveriges inre eller yttre säkerhet föreligger. Uttrycket Sveriges säkerhet beskrivs i 1 §.

Säkerhetspolisen ska samråda med Försvarsmakten vad gäller hotet mot den nationella säkerheten. Säkerhetspolisen får också, i den mån myndigheten bedömer det lämpligt och nödvändigt, inhämta information från andra myndigheter och organ som kan antas ha relevant kunskap om omständigheter av betydelse för bedömningen av hotet mot Sveriges säkerhet. Säkerhetspolisen får även samråda med andra myndigheter i fråga om vilka tillhandahållare som ska omfattas av ett föreläggande och om lagringsskyldighetens omfattning. Säkerhetspolisens inhämtning av information eller samråd kan ske utan särskilda formkrav men med iakttagande av tillämpliga regler i verksamheten, bl.a. gällande sekretess och personuppgiftsbehandling.

Andra stycket reglerar dels hur lång tid ett föreläggande om nationell säkerhetslagring får gälla, dels när ett föreläggande kan förlängas eller ska upphävas. Ett föreläggande får gälla i högst ett år. Tiden tar sikte på giltigheten av det föreläggande som reglerar lagringsskyldigheten för tillhandahållarna. Det är alltså inte samma sak som tiden som de lagrade uppgifterna ska finnas kvar (se tredje stycket).

Om Säkerhetspolisen gör bedömningen att hotet mot den nationella säkerheten kvarstår efter ett år, får myndigheten förlänga lagringsskyldigheten genom ett nytt föreläggande. Även det nya föreläggandet blir då föremål för kontroll enligt 8–10 §§. Säkerhetspolisen ska enligt bestämmelsen löpande ompröva om hotet består och upphäva lagringsskyldigheten om det inte längre finns skäl för nationell säkerhetslagring.

Tredje stycket lämnar upplysning om att det finns bestämmelser i nya LEK om lagringsskyldighetens omfattning och hur lång tid trafik- och lokaliseringsuppgifter 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.

Paragrafen ger uttryck för den proportionalitetsprincip som gäller vid nationell säkerhetslagring. Övervägandena framgår av avsnitt 7.3.1. Syftet med bestämmelsen är att begränsa de negativa konsekvenser

som ett beslut om nationell säkerhetslagring kan innebära. En första förutsättning är att det ska vara absolut nödvändigt för att skydda Sveriges säkerhet att meddela ett föreläggande enligt 2 §. Vidare ska föreläggandet begränsas till vad som är absolut nödvändigt i vissa angivna avseenden.

Enligt *första punkten* ska en bedömning göras avseende vilka tillhandahållare som ska omfattas av lagringsskyldigheten. I bedömningen ingår exempelvis vilken förmåga tillhandahållaren har att verkställa ett beslut om nationell säkerhetslagring. Även andra faktorer får tas med i bedömningen, exempelvis tillhandahållarens förmåga att hantera känslig information.

Enligt *andra punkten* ska en bedömning göras avseende föreläggandets giltighetstid. Vid bedömningen ska beaktas att trafik- och lokaliseringsuppgifter genereras kontinuerligt, samtidigt som lagringstiden i vissa fall räknas från den tidpunkt då uppgifterna genererades. Uppgifter kan därför fortsätta vara lagrade även efter föreläggandets giltighetstid.

Enligt *tredje punkten* ska en bedömning göras avseende lagringsskyldighetens omfattning av olika uppgiftstyper. Vilka uppgifter som kan omfattas av lagringsskyldigheten framgår av 9 kap. 19 b § nya LEK.

Offentligt ombud

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

Paragrafen anger att det i ärenden om nationell säkerhetslagring ska finnas ett offentligt ombud som ska bevaka enskildas intressen. Övervägandena finns i avsnitt 7.3.4.

Med enskilda åsyftas här inte bara enskilda fysiska personer utan även tillhandahållare enligt 9 kap. 19 § nya LEK. Uttrycket enskildas intressen kan avse såväl personliga, ekonomiska som andra förhållanden.

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 erfaren-

het. 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.

Paragrafen innehåller bl.a. föreskrifter om för vilken tid ett offentligt ombud ska förordnas, om kvalifikationskrav för offentliga ombud och om hur regeringen ska inhämta förslag på lämpliga ombud. Övervägandena finns i avsnitt 7.3.4.

Av *första stycket* framgår att regeringen ska förordna en person som ska tjänstgöra som ordinarie offentligt ombud under högst tre år. Regeringen ska även förordna 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.

Av *andra stycket* framgår de krav som ställs på ett offentligt ombud. Kraven motsvarar i huvudsak vad som gäller för offentliga ombud enligt 27 kap. 26 § rättegångsbalken. Det krävs således att ett offentligt ombud ska vara svensk medborgare samt ha varit ordinarie domare, vara eller ha varit advokat eller ha motsvarande juridisk erfarenhet. Med det sistnämnda avses personer som genom sin utbildning, meriter och erfarenhet har tillräckliga kvalifikationer i frågor som bl.a. rör rättssäkerhetsgarantier och angelägenheter om nationell säkerhet. Ett offentligt ombud får inte vara i konkurstillstånd eller ha förvaltare enligt 11 kap. 7 § föräldrabalken.

Enligt *tredje stycket* ska regeringen hämta in förslag på lämpliga personer från Domarnämnden och Sveriges advokatsamfund. Inget hindrar förstås regeringen från att inhämta förslag och relevant information om lämpliga personer även från annat håll.

I *fjärde stycket* finns en reglering som tillåter det offentliga ombudet att slutföra ett uppdrag i ett visst ärende som är pågående när förordandet upphör.

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.

Paragrafen reglerar rätten till ersättning till det offentliga ombudet och rätten att överklaga Säkerhetspolisens beslut om ersättning. Övervägandena finns i avsnitt 7.3.4.

Regleringen motsvarar vad som gäller för offentliga ombud enligt rättegångsbalken. I första hand beslutar Säkerhetspolisen om ersättning till det offentliga ombudet. Om det offentliga ombudet överklagar Säkerhetspolisens beslut om nationell säkerhetslagring, beslutar SIN om ersättning till det offentliga ombudet även avseende det arbete som utförts i ärendet innan det överklagades. Ett offentligt ombud får överklaga Säkerhetspolisens beslut om ersättning till SIN trots att beslutet om nationell säkerhetslagring inte har överklagats.

7 § Den som förordnats som offentligt ombud får inte obehörigen röja vad han eller hon har fått kännedom om i angelägenhet om nationell säkerhetslagring.

Paragrafen reglerar tystnadsplikt för det offentliga ombudet. Övervägandena finns i avsnitt 7.3.9. Med uttrycket obehörigen avses att det offentliga 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 SIN i samband med ett överklagande. Bestämmelsen omfattar alla uppgifter som det offentliga ombudet får kännedom om i angelägenhet 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.

Paragrafen beskriver förfarandet vid beslut om nationell säkerhetslagring hos Säkerhetspolisen och möjligheten för det offentliga ombudet att överklaga beslutet. Övervägandena finns i avsnitt 7.3.4.

Enligt *första stycket* ska Säkerhetspolisen, om myndigheten gör bedömningen att ett beslut om nationell säkerhetslagring ska fattas, kalla det offentliga ombudet till ett särskilt sammanträde. Företrädare för Säkerhetspolisen ska vid sammanträdet redogöra för myndighetens överväganden och för det tilltänkta beslutet. Det offentliga ombudet ska ha möjlighet att yttra sig och ställa frågor. Det ankommer på Säkerhetspolisen att närmare bestämma formerna för sammanträdet.

Ombudet ska vid sammanträdet få ta del av de omständigheter som ligger till grund för ställningstagandet och det tilltänkta beslutet. Med det avses inte att Säkerhetspolisen har skyldighet att redovisa all information som myndigheten förfogar över i ärendet. Särskilt känsliga uppgifter kan beskrivas på övergripande nivå. Exempelvis behöver normalt inte identiteten på källor eller arbetsmetoder beskrivas på ett ingående sätt. Som huvudregel ska dock redovisningen i ärendet vara tillräcklig för att ombudet ska kunna bilda sig en uppfattning kring de överväganden Säkerhetspolisen har gjort. Det är således inte tillräckligt med en mer allmän beskrivning av att Säkerhetspolisen bedömer att det finns ett allvarligt hot mot Sveriges säkerhet.

Med hänsyn till att informationen om hotet mot den nationella säkerheten ofta kan innehålla mycket känsliga uppgifter kan ett sammanträde inte ersättas av ett skriftligt förfarande. Efter det att det offentliga ombudet fått möjlighet att framföra sina synpunkter kan Säkerhetspolisen besluta om nationell säkerhetslagring. Säkerhetspolisen kan beakta de synpunkter som framförts av det offentliga ombudet och vid behov göra justeringar i det tilltänkta beslutet. Exempelvis kan justeringar göras i fråga om vilken tid beslutet ska gälla eller vilka uppgifter som ska omfattas av lagringsskyldigheten.

Enligt *andra stycket* har det offentliga ombudet rätt att överklaga ett beslut om nationell säkerhetslagring till SIN. Överklagandet ska ges in till Säkerhetspolisen senast en vecka efter beslutet. Överklagandet behöver inte innehålla någon närmare motivering.

Om beslutet inte överklagas inom en veckas tid, får Säkerhetspolisen förelägga aktuella tillhandahållare att verkställa lagringsbeslutet. Beslutet är, som följer av 10 § andra stycket, inte verkställbart dessförinnan.

Det offentliga ombudet kan också meddela att han eller hon inte kommer att överklaga beslutet. Efter ett sådant meddelande får beslutet verkställas omedelbart enligt 8 §. Ett besked att det offentliga ombudet inte avser överklaga ska vara skriftligt.

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.

Paragrafen beskriver tillsammans med 10 § förfarandet vid ett överklagande av Säkerhetspolisens beslut. Övervägandena finns i avsnitt 7.3.4 och 7.3.5.

En ny delegation inom SIN, Datalagringsdelegationen, ska överpröva Säkerhetspolisens beslut vid ett sammanträde i närvaro av företrädare för Säkerhetspolisen och det offentliga ombudet, se 8 § förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden. Företrädare för Säkerhetspolisen ska vid sammanträdet, på motsvarande sätt som vid sammanträde enligt 8 §, redogöra för myndighetens beslut liksom ett underlag som redovisar de omständigheter som ligger till grund för beslutet. Datalagringsdelegationens ledamöter och det offentliga ombudet får ställa frågor vid sammanträdet. Det ankommer på delegationen att närmare bestämma formerna för sammanträdet. I det fall endast det offentliga ombudets ersättning prövas enligt 9 § behöver Datalagringsdelegationen inte hålla sammanträde.

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.

Paragrafen beskriver tillsammans med 9 § förfarandet vid ett överklagande av Säkerhetspolisens beslut. Övervägandena finns i avsnitt 7.3.4.

Av *första stycket* framgår att SIN kan fastställa eller upphäva Säkerhetspolisens beslut. SIN kan däremot inte göra ändringar av ett beslut om nationell säkerhetslagring. SIN:s prövning omfattar om det föreligger ett hot mot den nationella säkerheten enligt 2 § och om beslutet är författningsenligt och proportionerligt. Om SIN upphäver ett beslut om nationell säkerhetslagring, ska Säkerhetspolisen underrättas om de skäl för upphävandet som SIN funnit vid sin prövning. Säkerhetspolisen är då oförhindrad att fatta ett nytt beslut om lagring avseende samma förhållanden.

SIN:s beslut får inte överklagas. Överklagandeförbudet omfattar även ersättning till det offentliga ombudet enligt 9 §.

Av *andra stycket* framgår när Säkerhetspolisens beslut får gå i verkställighet. Det får ske om beslutet inte överklagats inom överklagandefristen, om det offentliga ombudet meddelat att beslutet inte kommer att överklagas eller om beslutet har fastställts av SIN.

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.

Paragrafen reglerar tillsammans med 12 § tillgång till uppgifter som lagrats med stöd av nationell säkerhetslagring. Övervägandena finns i avsnitt 7.3.7.

För tillgång till uppgifterna krävs att två villkor är uppfyllda. I *första stycket* anges att ett villkor för tillgång till uppgifterna är att det finns ett beslut om HAK, HÖK eller inhämtning enligt inhämtningslagen. Det omfattar även hemliga tvångsmedel enligt 27 kap. rättegångsbalken då andra författningar tillämpas, i första hand preventivlagen och LSU.

I *andra stycket* anges det andra villkoret, nämligen att det i tillståndsbeslutet om hemliga tvångsmedel enligt första stycket måste

anges att tillgången får avse uppgifter som lagrats för den nationella säkerheten. Bedömningen ska således ske i samband med tillståndsgivningen för det straffprocessuella tvångsmedel som blir aktuellt i det enskilda fallet.

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, spionerі, grovt spionerі, 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. 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, 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.

Paragrafen reglerar tillsammans med 11 § tillgång till uppgifter som lagrats med stöd av nationell säkerhetslagring. Överväganden finns i avsnitt 7.3.7.

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 uppgifter får hämtas in enligt 11 §.

Punkterna 1–6 motsvarar de brott och den brottsliga verksamhet som Säkerhetspolisen har att bekämpa och för vilken inhämtning av uppgifter kan ske efter beslut enligt inhämtningslagen, eller efter tillstånd till HAK eller HÖK enligt rättegångsbalken och preventivlagen.

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 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 till slut blivit så allvarlig att den riskerar att slå ut eller försvaga viktiga funktioner i samhället. Det kan röra sig om s.k. systemhotande brottslighet med otillbörlig påverkan på rättskedjan eller andra myndigheter inom den offentliga förvaltningen.

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

14.3 Förslaget till lag (2025:000) om lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet

1 § Denna lag innehåller bestämmelser om när uppgifter om elektronisk kommunikation får lagras för att bekämpa grov brottslighet.

Paragrafen anger syftet med lagen. Övervägandena finns i avsnitt 8.2 och 8.3.4.

Med uttrycket uppgifter om elektronisk kommunikation avses i lagen uppgift om abonnemang samt trafik- och lokaliseringsuppgifter, dvs. de uppgifter som framgår av 9 kap. 31 § första stycket 1 och 3 nya LEK. Även lokaliseringsuppgifter som inte är trafikuppgifter omfattas av regleringen genom en ny fjärde punkt i 9 kap. 31 § första stycket samma lag. Med lokaliseringsuppgifter som inte är trafikuppgifter avses exempelvis satellitpositioneringsuppgifter som genererats i utrustningen. Lagen gäller såväl bekämpning av grova brott som grov

brottslighet. Med dessa uttryck avses brott och brottslighet som i dag ger rätt att använda hemliga tvångsmedel.

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.

Paragrafen reglerar geografiskt riktad lagring. Övervägandena finns i avsnitt 8.3.1.

När det gäller begreppet kommuner, se 1 kap. 7 § RF och 1 kap. 1 § kommunallagen (2017:725). I dag finns det 290 kommuner och kommunindelningen kan utläsas av regeringens tillkännagivande (2007:229) om länens indelning i kommuner.

I motsats till vad som gäller för utökad riktad lagring (se 5 § m.fl. paragrafer nedan) framgår lagringsskyldighetens omfattning vid geografiskt riktad lagring direkt av 19 kap. 19 c § nya LEK.

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.

Paragrafen reglerar inom vilka kommuner tillhandahållarna ska lagra trafik- och lokaliseringsuppgifter. Paragrafen föreskriver även beräkningsgrunder för urvalet av kommuner. Övervägandena finns i avsnitt 8.3.1.

Första stycket anger villkoren för geografiskt riktad lagring. Sådan lagring ska ske när det finns en förhöjd risk för förekomsten av grova brott eller grov brottslighet i en kommun jämfört med övriga kommuner i landet. Denna bedömning ska göras genom en relativ jämförelse av antalet brottsanmälningar där den specifika kommunen jämförs med genomsnittet för landets alla kommuner. Ett medelvärde för brottsanmälningar i kommunen ska beräknas genom en kvot, på det sätt som framgår av andra stycket. Om kvoten ligger på samma nivå eller över genomsnittet, jämfört med motsvarande kvot för samt-

liga kommuner, ska lagring ske. Med brottsanmälningar avses sådana anmälningar om brott som diarieförs i myndigheternas ärendehanteringssystem och som vidarebefordras till Brå som underlag för den officiella statistiken. Det är således inte endast anmälningar om grova brott som avses.

Andra stycket beskriver hur kvoten som ska ligga till grund för bedömningen av den förhöjda risken enligt första stycket ska räknas fram. Utgångspunkten för beräkningen är den officiella statistik som Brå sammanställer över antalet brottsanmälningar varje år enligt lagen (2001:99) och förordningen (2001:100) om den officiella statistiken. Brå publicerar statistik över antalet brottsanmälningar per kommun. Med utgångspunkt från de tre närmast föregående åren ska ett medelvärde över antalet brottsanmälningar per kommun tas fram.

Medelvärdet sätts därefter i relation till befolkningsstorleken för att få fram en kvot som ger jämförbara genomsnittsvärden mellan kommunerna.

4 § Post- och telestyrelsen ska årligen, senast den 1 juni, föreskriva vilka kommuner som omfattas av geografiskt riktad lagring enligt 3 §.

Paragrafen anger att PTS ska föreskriva inom vilka kommuner geografiskt riktad lagring ska ske. Övervägandena finns i avsnitt 8.3.1.

Eftersom statistiken sammanställs årsvis, kan PTS meddela föreskrifter först när Brå har redovisat statistiken. PTS får meddela föreskrifter även före den 1 juni om det finns underlag för det. Föreskrifterna äger giltighet från det datum som PTS bestämmer och tills de har ersatts av nya föreskrifter. När PTS anger datum för ikraftträdande ska det finnas tidsmässigt utrymme för tillhandahållarna att göra relevanta omställningar. Föreskrifterna är normbeslut som inte får överklagas (30 § myndighetsförordningen).

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.

Paragrafen reglerar förutsättningarna för utökad riktad lagring. Övervägandena finns i avsnitt 8.3.2.

Första stycket anger i vilka situationer utökad riktad lagring får användas. Utgångspunkten är att utökad riktad lagring ska vara ett komplement till geografiskt riktad lagring. Lagringsskyldigheten för tillhandahållarna följer av 19 kap. 19 d § nya LEK. Lagringstiden och lagringsskyldighetens omfattning regleras i 8 och 9 §§.

Utökad riktad lagring får avse ett *begränsat geografiskt område.* Med det menas en avgränsad yta som inte nödvändigtvis är knuten till byggnader eller andra anläggningar. Som exempel på områden kan anges stadsdelar, postområden och vägar.

För att utökad riktad lagring ska avse ett område krävs att det finns ett samband mellan området och grovt brott eller grov brottslighet. Med det avses brott i 27 kap. 19 § tredje stycket rättegångsbalken eller brottslig verksamhet som innefattar sådana brott. Ett sådant samband kan fastställas antingen då ett grovt brott har begåtts inom området eller då det är sannolikt att så kommer att ske. Det finns inga fasta kriterier för hur sannolikhetsbedömningen ska göras. Bedömningen ska baseras på konkreta omständigheter. Den kan exempelvis grundas i planerade händelser såsom ett statsbesök eller ett värdskap för ett internationellt sammanträde (se nedan om själva platsen för sådana händelser). Bedömningen kan även baseras på underrättelseuppgifter om förekomsten av grov brottslig verksamhet inom ett visst område, exempelvis att en kriminell gruppering har etablerat sig i eller bedriver verksamhet inom ett visst område.

Utökad riktad lagring får vidare avse *en skyddsvärd plats*. Med en sådan plats avses som huvudregel en yta som jämfört med ett område är mindre i storlek. Det kan i vissa situationer vara så att stora skyddsvärda anläggningar innebär en viss överlappning mellan begreppen plats och område, exempelvis i fråga om större militäranläggningar. En förutsättning för lagring är att platsen är skyddsvärd. Med skyddsvärd menas i detta sammanhang viktiga byggnader och anläggningar som är av särskild betydelse för samhället. Hur en skyddsvärd plats ska väljas ut framgår av 6 §. Avgränsningen i fråga om utökad riktad lagring avseende plats påverkas av tillhandahållarnas infrastruktur. I praktiken är det närmaste mobilmast eller motsvarande anslutning för fast telefoni eller bredband som avgör hur precist platsen kan avgränsas. Det betyder som huvudregel att utökad riktad lagring avseende en plats till ytan kommer att vara något större än den skyddsvärda platsen i sig. Det betyder dock inte att det är tillåtet att av praktiska skäl peka ut en större yta för lagring än vad som är tekniskt nödvändigt.

Utökad riktad lagring får avse *personer som är eller har varit föremål för hemliga tvångsmedel*. Hemliga tvångsmedel regleras i 27 kap. rättegångsbalken, lagen om hemlig dataavläsning och inhämtningslagen samt i preventivlagen, LIRB, EIO, och LSU.

Bestämmelsen omfattar även andra personer än de som misstänks för grova brott eller deltagande i grov brottslig verksamhet, exempelvis en målsägande.

Utökad riktad lagring får också avse *en person som blivit ålagd en påföljd för ett grovt brott.* Med påföljd avses dels straff, dvs. böter och fängelse, dels påföljder som inte utgör straff bl.a. villkorlig dom, skyddstillsyn, ungdomspåföljder och överlämnande till särskild vård. Även en s.k. konsumtionsdom enligt 34 kap. 3 § brottsbalken omfattas av bestämmelsen.

Grunden för lagring är en presumtion för att den som blivit dömd för ett grovt brott har en förhöjd risk för att återfalla i ny brottslighet. En sådan presumtion innebär dock inte att alla som dömts för grov brottslighet ska bli föremål för utökad riktad lagring. Det krävs alltjämt ett konkret behov i det enskilda fallet, exempelvis att personen på nytt misstänks för grovt brott eller grov brottslighet, eller att man bedömer att det finns en risk att personen involveras i grov brottslighet. Så kan exempelvis vara fallet när en person som är dömd för grova brott återkommer i underrättelseuppslag efter verkställig-

heten av en utdömd påföljd. En bedömning av behovet ska göras i det enskilda fallet. Ett beslut om utökad riktad lagring avseende en person får inte fattas efter att det har gått tre år sedan den utdömda påföljden till fullo verkställts. Lagringen kan dock ske upp till ett år efter den nu stadgade tiden, om beslut om lagring fattats i slutet av treårsperioden, jämför 8 § om lagringstiden.

Det finns inga formella hinder mot att utökad riktad lagring avser en person som verkställer ett straff på en kriminalvårdsanstalt. I de flesta fall saknar dock en person som är intagen i kriminalvårdsanstalt allmän tillgång till utrustning för elektronisk kommunikation (jfr 7 kap. 4 § fängelselagen och 7 kap. 10 § Kriminalvårdens föreskrifter och allmänna råd för fängelse, KVFS 2011:1).

Den omständigheten att utökad riktad lagring får avse en person som är föremål för hemliga tvångsmedel eller en person som dömts för grova brott innebär att tillhandahållarna ska bistå de behöriga myndigheterna med de uppgifter som krävs för att datalagring ska vara möjligt. Exempelvis kan tillhandahållarna genom uppgifter som de behandlar för egna ändamål, såsom fakturering, knyta en viss person till ett visst konto, abonnemang eller en viss enhet.

Utökad riktad lagring får också avse *utrustnings- och abonnemangsidentitet*. Syftet är att datalagring ska kunna ske i situationer när de brottsbekämpande myndigheterna antingen kan konstatera att viss utrustning eller visst abonnemang använts eller fortfarande används för att begå grova brott eller skäligen kan antas komma till användning vid ett grovt brott eller vid grov brottslig verksamhet. Beviskravet skäligen kan antas motsvarar den som finns i bestämmelsen om beslag i 27 kap. 1 § rättegångsbalken. För att det kravet ska vara uppfyllt krävs konkreta omständigheter som talar för att utrustningen eller abonnemanget kan antas komma till brottslig användning. Om övriga förutsättningar är uppfyllda, får datalagring ske även om viss utrustning eller visst abonnemang används av andra användare.

Lagringen tar sikte på själva utrustningsidentiteten eller abonnemangsidentiteten. En förutsättning för lagring är att utrustnings- eller abonnemangsidentiteten är känd för de behöriga myndigheterna. Lagringen kan exempelvis ske med utgångspunkt från IMEI-nummer eller en viss nummerserie för mobiltelefoner, ICCID-nummer för fysiska sim-kort och esim, IMSI-nummer för mobiltelefonabonnemang, fasta eller dynamiska ip-nummer eller ett konto hos en tillhandahållare av tjänster för kommunikation. Exemplifieringen är inte

uttömmande. Bestämmelsen är teknikneutral och kan även omfatta andra uppgifter så länge de behandlas av tillhandahållaren.

Andra stycket begränsar möjligheten till utökad riktad lagring avseende person i tiden. Ett beslut om lagring får inte grunda sig på ett tvångsmedelsbeslut, dom eller godkänt strafföreläggande som är äldre än tre år. Om en påföljd har undanröjts och ersatts av en annan påföljd, räknas tiden från det att den nya påföljden har verkställts. Om påföljden innefattar ett förordnande om konsumtionsdom enligt 34 kap. 3 § brottsbalken, räknas tiden från när påföljden i den tidigare domen 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.

Paragrafen reglerar bedömningsgrunderna för vad som är en skyddsvärd plats. Övervägandena finns i avsnitt 8.3.2 och 8.3.7.

En tydlig indikation på att en plats är skyddsvärd är om platsen har bedömts vara ett skyddsobjekt, se *första punkten*. Motsvarande gäller för platser där det bedrivs säkerhetskänslig verksamhet, se *andra punkten*. I dessa fall bör bedömningen oftast vara okomplicerad. Vid behov kan ytterligare underlag inhämtas genom samråd med den som bedriver verksamheten eller Försvarsmakten och Säkerhetspolisen i egenskap av samordnande tillsynsmyndigheter för säkerhetskänslig verksamhet. Som huvudregel bör sådan kommunikation kunna ske på övergripande nivå. Om det är nödvändigt att den som bedriver säkerhetsskyddskänslig verksamhet lämnar sekretessbelagda uppgifter till den beslutande myndigheten, bör det kunna göras med stöd av den s.k. generalklausulen i 10 kap. 27 § OSL.

Genom den *tredje punkten* ges möjlighet till beslut om utökad riktad lagring avseende platser som inte är skyddsobjekt eller där det bedrivs säkerhetskänslig verksamhet. Det får ske om platsen är av särskild betydelse för brottsbekämpningen. Så kan vara fallet när ett stort antal människor samlas på en viss plats, exempelvis knutpunkter för trafik, planerade demonstrationer, statsbesök och motsvarande

händelser. En annan situation är gränsövergångar som kan användas för smuggling.

Bestämmelsen har en motsvarighet i dansk lagstiftning. Där ges följande exempel som kan vara vägledande men inte bör uppfattas som uttömmande.

- Statschefens och statsministerns bostäder,
- ambassader,
- polishus,
- kriminalvårdsanstalter,
- bro-, tunnel- och färjeförbindelser,
- knutpunkter för trafik och större tillfartsvägar,
- gränsövergångar,
- bussterminaler,
- stationer för stads- och fjärrtrafik,
- verksamhet som bl.a. hanterar farliga kemikalier och andra hälsovådliga ämnen,
- flygplatser, och
- militäranläggningar.

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.

Paragrafen anger vilka myndigheter som får besluta om utökad riktad lagring, hur besluten ska utformas och förfarandet. Övervägandena finns i avsnitt 8.3.2.

Enligt *första stycket* är det Polismyndigheten, Säkerhetspolisen och Tullverket som är beslutande myndigheter i fråga om utökad riktad lagring. Om en annan myndighet anser att det finns ett behov av

utökad riktad lagring, får myndigheten påtala det för någon av de beslutande myndigheterna.

Ett beslut om utökad riktad lagring ska innehålla en sådan motivering att beslutet kan bli föremål för en effektiv tillsyn av SIN. Av skälen ska framgå grunden för lagringen och de överväganden som den beslutande myndigheten har gjort i fråga om beslutets längd, uppgifternas omfattning och vilka tillhandahållare som ska omfattas av beslutet. Ett beslut får inte i efterhand kompletteras med ytterligare uppgifter eller underlag. Om det blir aktuellt, kan ett nytt beslut fattas.

Som huvudregel ska ett beslut om utökad riktad lagring föregås av samråd mellan de beslutande myndigheterna i syfte att undvika parallella beslut avseende samma objekt. I två undantagssituationer får beslut fattas utan samråd, dels i brådskande fall, dels när ett samråd är olämpligt i särskilt känsliga ärenden. Med sådana ärenden avses i första hand känsligare ärenden i Säkerhetspolisens verksamhet. Det betyder dock inte att Säkerhetspolisen rent generellt är befriad från skyldigheten att samråda.

Om det är nödvändigt för ett beslut om utökad riktad lagring får samråd även ske med andra myndigheter. Det är ytterst den beslutande myndigheten som avgör behovet.

Andra stycket föreskriver en skyldighet för de beslutande myndigheterna att underrätta SIN om beslutet och skälen för detta. Beslutet får verkställas innan SIN har underrättats.

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.

Paragrafen reglerar hur länge olika typer av beslut om utökad riktad lagring får gälla. Giltighetstiden anger hur lång tid ett beslut gäller. Det är inte samma sak som hur lång tid uppgifterna ska lagras. Bestäm-

melser om hur länge trafik- och lokaliseringsuppgifter ska lagras finns i 9 kap. 22 § nya LEK. Övervägandena finns i avsnitt 8.3.2.

I *första stycket* föreskrivs en tidsbegränsning i fråga om olika typer av utökad riktad lagring. Syftet med tidsbegränsningen är att ett beslut inte ska riskera att gälla längre än vad som är absolut nödvändigt. När det gäller utökad riktad lagring avseende område, person samt utrustnings- och abonnemangsidentitet får ett beslut om utökad riktad lagring gälla i högst ett år. I fråga om skyddsvärda platser, som ofta behöver skyddas under längre perioder, får ett beslut gälla i högst tre år. Bestämmelsen reglerar den bortre gränsen för hur lång tid ett beslut om utökad riktad lagring får gälla. Den beslutande myndigheten ska i det enskilda fallet begränsa beslutet till vad som är absolut nödvändigt enligt 9 §.

I *andra stycket* regleras möjligheten att förlänga ett beslut om utökad riktad lagring. Ett beslut får förlängas, förutsatt att behovet kvarstår, med högst ett år i taget. Det gäller dock inte för beslut om utökad riktad lagring avseende person. Sådana beslut får inte fattas senare än tre år efter det att tvångsmedelsbeslutet fattades eller den ålagda påföljden till fullo har verkställts. Det gäller även möjligheten till förlängning av ett sådant beslut. Se kommentaren till 5 § angående undanröjande av påföljd och konsumtionsdom.

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.

Paragrafen anger tillsammans med 10 § grundläggande villkor som gäller för alla beslut om utökad riktad lagring. Övervägandena finns i avsnitt 8.3.2. Syftet med bestämmelsen är att begränsa det ingrepp ett beslut som utökad riktad lagring innebär. En första förutsättning är att det ska vara absolut nödvändigt att fatta ett beslut om utökad riktad lagring.

Enligt *första punkten* ska en bedömning göras avseende vilka tillhandahållare som ska omfattas av lagringsskyldigheten. I bedömningen ingår exempelvis vilken förmåga tillhandahållaren har att verkställa ett beslut om utökad riktad lagring.

Enligt *andra punkten* ska en bedömning göras avseende beslutets giltighetstid. Vid bedömningen ska beaktas att trafik- och lokaliseringsuppgifter genereras kontinuerligt under beslutets giltighetstid. Det innebär att uppgifter kan vara lagrade även efter beslutets giltighetstid.

Enligt *tredje punkten* ska en bedömning göras avseende lagringsskyldighetens omfattning av olika uppgiftstyper. Vilka uppgifter som kan omfattas av lagringsskyldigheten framgår av 9 kap. 19 d § nya LEK som hänvisar till 9 kap. 19 b § nya LEK.

Den beslutande myndigheten får vid ett beslut om utökad riktad lagring ange vilka uppgifter som ska lagras och redovisa varför myndigheten bedömer att uppgifterna är nödvändiga.

10 § Om det inte längre finns skäl för utökad riktad lagring, ska beslutet upphävas av den myndighet som har fattat beslutet.

Paragrafen anger tillsammans med 9 § grundläggande villkor som gäller för alla beslut om utökad riktad lagring. Syftet med bestämmelsen är att begränsa det ingrepp ett beslut om utökad riktad lagring innebär till vad som är absolut nödvändigt. Övervägandena finns i avsnitt 8.3.2.

Bestämmelsen innebär ett ansvar för de beslutande myndigheterna att löpande bevaka beslut om utökad riktad lagring och upphäva dem när behovet har upphört. Så kan exempelvis vara fallet om ett område som är föremål för utökad riktad lagring vid ett senare tillfälle omfattas av geografiskt riktad lagring. Ett annat exempel kan vara utökad riktad lagring avseende en person som blir frihetsberövad och begränsas i sina möjligheter att använda elektronisk kommunikation. Andra exempel kan vara överlåtelser av utrustning och abonnemang som omfattas av ett beslut om utökad riktad lagring. Även avveckling av skyddsvärda platser eller nedläggning av säkerhetskänsliga anläggningar kan vara skäl att upphäva ett beslut om utökad riktad lagring.

11 § Polismyndighetens, Säkerhetspolisens och Tullverkets beslut enligt denna lag får inte överklagas.

Paragrafen innebär ett hinder mot överklagande av beslut enligt lagen. Övervägandena finns i avsnitt 8.3.2. Bestämmelsen innebär att ett beslut om utökad riktad lagring blir verkställbart så fort beslutet har fattats.

14.4 Förslaget till lag om ändring i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet

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 *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.

I paragrafen regleras SIN:s tillsyn. Övervägandena finns i avsnitt 8.3.2.

Genom ett tillägg i tredje stycket anges att SIN:s tillsynsuppdrag utökas till att omfatta även de brottsbekämpande myndigheternas tillämpning av bestämmelserna i lagen om lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet om utökad riktad lagring.

En underrättelseskyldighet för den myndighet som har fattat ett beslut om utökad riktad lagring finns i 7 § andra stycket lagen om lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet.

SIN har ingen skyldighet att på begäran av enskild kontrollera om han eller hon har varit föremål för utökad riktad lagring och om lagringen har varit författningsenlig.

14.5 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, 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.

Paragrafen innehåller sekretessbrytande bestämmelser. Övervägandena finns i avsnitt 7.3.9.

Genom ett nytt tredje stycke införs en sekretessbrytande regel för uppgifter som lämnas till ett offentligt ombud 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 såväl Säkerhetspolisen som SIN.

18 kap.

19 §

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, hemlig dataavläsning på grund av beslut av domstol, undersökningsledare eller åklagare eller inhämtning av uppgifter 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.

I paragrafen regleras vilka tystnadsplikter enligt 18 kap. OSL som har företräde framför rätten att meddela och offentliggöra uppgifter. Övervägandena finns i avsnitt 7.3.9 och 8.3.7.

I andra stycket införs nationell säkerhetslagring och utökad riktad lagring 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 *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.

Paragrafen innehåller bestämmelser om sekretess hos en myndighet som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Övervägandena finns i avsnitt 6.6.2.

För enskilda som bedriver sådan verksamhet regleras tystnadsplikten i 9 kap. 31 § första stycket nya LEK. Paragrafen ändras endast på så sätt att begreppet *annan uppgift som angår ett särskilt elektroniskt meddelande* ersätts med begreppet *trafikuppgift*. Motsvarande ändring föreslås i nya LEK. I sak avses inte någon ändring i fråga om vilka uppgifter som skyddas av sekretess.

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,
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. 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 enligt 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 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 till skydd för enskilds personliga och ekonomiska förhållanden i viss brottsbekämpande verksamhet. Övervägandena finns i avsnitt 7.3.9 och 8.3.7.

I listan i *första stycket* införs två nya punkter, angelägenhet om nationell säkerhetslagring (punkt 10) och angelägenhet om utökad riktad lagring (punkt 11). Genom ändringarna införs sekretess för uppgift om en enskilds personliga och ekonomiska förhållanden i angelägenhet om nationell säkerhetslagring och angelägenhet om utökad riktad lagring. Av uttrycken *angelägenhet om nationell säkerhetslagring* och *angelägenhet om utökad riktad lagring* följer att det är fråga om s.k. primär sekretess. Bestämmelserna riktar sig alltså direkt till alla myndigheter som är involverade i nämnda angelägenheter.

24 §

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.

I paragrafen regleras vilka tystnadsplikter enligt 35 kap. OSL som har företräde framför rätten att meddela och offentliggöra uppgifter. Övervägandena finns i avsnitt 7.3.9 och 8.3.7.

Paragrafen innebär att även 35 kap. 1 § 10 och 11 OSL omfattas av den tystnadsplikt som inskränker rätten att meddela och offentliggöra uppgifter enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen.

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. 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, 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 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.*

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 7.3.9 och 8.3.7

Punkt 3 ändras till följd av att det införs bestämmelser om tystnadsplikt för tillhandahållarna i 9 kap. 32 § nya LEK. Tystnadsplikten gäller i angelägenhet om nationell säkerhetslagring och angelägenhet om utökad riktad lagring. Genom tillägget i punkten 3 får tystnadsplikten företräde framför meddelarfriheten. Punkten motsvarar det meddelarförbud som gäller för myndigheter enligt 18 kap. 19 § och 35 kap. 24 §§ OSL.

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 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), *och*
8. *av 7 § lagen (2025:000) om lagring av och åtkomst 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 framgår av avsnitt 7.3.9.

I uppräkningen införs en ny punkt, 8. Ändringen innebär att ett offentligt ombud enligt 10 § lagen om lagring av och åtkomst 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.

14.6 Förslaget till lag om ändring i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet

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 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.

I paragrafen anges vilka myndigheter som får bedriva sådan inhämtning av uppgifter som regleras i lagen, från vilka sådan inhämtning får ske och vilka uppgifter som får hämtas in. Övervägandena finns i avsnitt 9.6.3.

Paragrafen ändras genom att ett tidigare undantag om att uppgifter inte får hämtas in från nummeroberoende interpersonella kommunikationstjänster tas bort. Ändringen möjliggör att uppgifter inhämtas från tillhandahållare av Noik med stöd av beslut om inhämtning enligt inhämtningslagen.

Liksom vid HÖK är det inte säkert att en tillhandahållare av Noik har tillgång till uppgifter om vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område eller om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits.

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

8 kap.

5 §

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 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.

I paragrafen regleras skyldigheten för den som är lagringsskyldig enligt 9 kap. 19 § nya LEK att vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling. Övervägandena finns i avsnitt 9.6.4.

I *andra stycket* regleras skyddsåtgärder för uppgifter som bevarats med stöd av ett föreläggande enligt 27 kap. 16 § RB (bevarandeföreläggande). Tidigare utgick regleringen i andra stycket från anmälningsplikten enligt 2 kap. 1 § nya LEK. Nu knyts regleringen genom en hänvisning till första stycket i stället till den som är lagringsskyldig enligt 9 kap. 19 § nya LEK. Därigenom utvidgas paragrafens tillämpningsområde till att även omfatta tillhandahållare av Noik som har förelagts att bevara en uppgift enligt 27 kap. 16 § RB.

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 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 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 7.3.8 och 8.3.6. *Andra stycket* ändras endast på så sätt att hänvisningen till 9 kap. 19 § ändras till 9 kap. 19 b–d §§ nya LEK, eftersom lagringsskyldigheten inte längre regleras i 9 kap. 19 § nya LEK.

10 §

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, lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet får behandlas trots 7–9 §§.

Paragrafen innehåller olika undantag från 9 kap. 7–9 §§ nya LEK där det finns begränsningar för hur lokaliseringsuppgifter som inte är trafikuppgifter får behandlas av tillhandahållarna. Övervägandena finns i avsnitt 7.3.8 och 8.3.6.

I *första stycket* regleras att tillhandahållarna får lagra lokaliseringsuppgifter vid nationell säkerhetslagring enligt 19 kap. 9 b § nya LEK och utökad riktad lagring enligt 9 kap. 19 d § nya LEK.

I *andra stycket* föreskrivs undantag från de angivna bestämmelserna när sådana uppgifter omfattas av beslut om inhämtning enligt 27 kap. rättegångsbalken eller enligt lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Andra stycket är även tillämpligt vid inhämtning av uppgifter som lagrats för den nationella säkerheten enligt lagen om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte skydda Sveriges säkerhet.

Lagringsskyldiga och tjänster som omfattas av lagringsskyldighet

19 §

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 §§.*

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, eller
2. internetåtkomst.

För den som tillhandahåller en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst 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.

Paragrafen anger vilka som är skyldiga att lagra uppgift om abonnemang samt trafik- och lokaliseringsuppgifter och vilka tjänster som omfattas av lagringsskyldighet. Övervägandena finns i avsnitt 7.3.6, 7.3.8, 8.3.2 och 9.6.1.

Första stycket utvidgas så att tillhandahållare av Noik ingår i kretsen av dem som är skyldiga att lagra trafik- och lokaliseringsuppgifter. Lagringsskyldigheten träffar enbart de som tillhandahåller allmänt tillgängliga Noik i Sverige.

Med Noik avses allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster, såsom exempelvis Apple Imessage och Facetime, Discord, Google Messages och Duo, Kik Messenger, Line, Messenger from Meta, Skype, Slack, Telegram, Viber och Whatsapp. Även e-posttjänster som Gmail, Outlook och Apple Mail m.fl. omfattas av begreppet. Lagringsskyldigheten för tillhandahållare av Noik är, enligt tredje stycket, knuten till förutsättningarna att använda tjänsten i Sverige.

Hänvisningen till anmälningsplikten i 2 kap. 1 § nya LEK är oförändrad. Det innebär att de traditionella teleoperatörerna och internetleverantörerna alltjämt omfattas av kretsen som är lagringsskyldiga. Lagringsskyldighetens omfattning framgår genom en hänvisning till 19 kap. 19 a § för lagring av uppgift om abonnemang, 19 kap. 19 b § för nationell säkerhetslagring, 19 kap. 19 c § för geografiskt riktad lagring och 19 kap. 19 d för utökad riktad lagring. I stycket finns

även ett krav på att lagringen ska ske utan dröjsmål. Med uttrycket utan dröjsmål avses samma skyndsamhetskrav som föreskrivs i 9 kap. 29 b § nya LEK.

Andra stycket reglerar lagringsskyldighetens omfattning för den som bedriver anmälningspliktig verksamhet enligt 2 kap. 1 § nya LEK. Lagringsskyldigheten omfattar telefonitjänst (även videosamtal), meddelanden och internetåtkomst. Lagringsskyldigheten omfattar alla situationer där trafikuppgifter och lokaliseringsuppgifter genereras eller behandlats i tjänsterna, dvs. exempelvis även när en mobiltelefon överför lokaliseringsuppgifter till en mobilmast.

Tredje stycket reglerar lagringsskyldighetens omfattning för tillhandahållare av Noik. De ska lagra uppgifter som genereras eller behandlas vid tjänster som tillhandahåller samtal och meddelandehantering. Lagringsskyldigheten avser sådan 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. Det finns även andra sätt att lokalisera en användares kommunikationsutrustning, exempelvis genom lokaliseringsuppgifter som genereras i användarens utrustning. Om tillhandahållaren behandlar sådana uppgifter, exempelvis för felsökning eller i syfte att kunna rikta reklam, kan samma information användas för att fastställa var kommunikationen har ägt rum.

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.

Paragrafen är ny och reglerar skyldigheten att lagra uppgift om abonnemang. Övervägandena finns i avsnitt 6.6.1.

I *första stycket* regleras lagringsskyldigheten för uppgift om abonnemang. Med sådana avses uppgift om abonnemang som identifierar abonnenten eller den registrerade användaren bakom ett visst nummer eller en viss adress. Begreppet knyter an till bestämmelsen om tystnadsplikt i 9 kap. 31 § första stycket 1 nya LEK. Innebörden av

begreppet är således densamma i bägge paragraferna. Uppgift om abonnemang kan innefatta abonnentens telefonnummer, namn, titel och adress samt uppgifter om exempelvis avtal och fakturering. Vidare anses fasta ip-adresser, dynamiska ip-adresser eller ip-adresser fördelade genom NAT-teknik, IMSI-nummer och IMEI-nummer vara uppgift om abonnemang när syftet med uppgiften är att identifiera ett abonnemang eller en abonnent. Även andra uppgifter kan vara uppgift om abonnemang, exempelvis uppgift om kopplingen mellan permanenta och tillfälliga identifierare i 5G-nätet. Exemplifieringen här är inte uttömmande. Lagringsskyldigheten omfattar alla uppgifter om abonnemang som genereras och behandlas i tillhandahållarnas verksamhet. Lagringsskyldighetens närmare omfattning fastställs i förordning.

Vid en överträdelse av paragrafen kan tillsynsmyndigheten besluta om sanktionsavgift, se 12 kap. 1 §.

Andra stycket innehåller ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att få meddela föreskrifter om vilka uppgifter som ska lagras enligt paragrafen.

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.

Paragrafen är ny och reglerar lagringsskyldigheten vid nationell säkerhetslagring. Övervägandena finns i avsnitt 7.3.2. och 7.3.6.

Bestämmelsen knyter an till 2 § lagen om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

Lagringsskyldigheten avser trafik- och lokaliseringsuppgifter som framgår av 9 kap. 31 § första stycket 1 och 3 nya LEK. Även lokali-

seringsuppgifter som inte är trafikuppgifter omfattas av regleringen genom en ny fjärde punkt i 9 kap. 31 § första stycket samma lag.

Det är Säkerhetspolisen som med beaktande av proportionalitetsprincipen beslutar om lagringsskyldighetens omfattning. De uppgifter som kan omfattas av ett föreläggande om nationell säkerhetslagring beskrivs i paragrafen. Med ledning av dessa uppgifter ska det i efterhand gå att besvara följande frågor:

1. Vem kommunicerade med vem?
2. När ägde kommunikationen rum?
3. Var fanns användarnas utrustning?
4. Vilken typ av kommunikation var det fråga om?

Lagringsskyldighetens närmare omfattning preciseras i förordning.

Vid en överträdelse av paragrafen ska tillsynsmyndigheten besluta om sanktionsavgift, se 12 kap. 1 §.

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 §.

Paragrafen är ny och reglerar lagringsskyldigheten vid geografiskt riktad lagring. Övervägandena finns i avsnitt 8.3.1 och 8.3.3.

Geografiskt riktad lagring ålägger den som är lagringsskyldig enligt 9 kap. 19 § nya LEK att lagra trafik- och lokaliseringsuppgifter inom vissa kommuner. Bestämmelsen knyter an till 4 § lagen om lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet.

Lagringsskyldigheten vid geografiskt riktad lagring följer direkt av bestämmelsen. Lagringsskyldighetens omfattning fastställs således inte genom ett föreläggande eller beslut, till skillnad från vad som gäller för nationell säkerhetslagring enligt 19 b § och utökad riktad lagring enligt 9 kap. 19 d §. De uppgifter lagringsskyldigheten omfattar motsvarar uppräkningen i 9 kap. 19 b. Det görs därför en hänvisning till den bestämmelsen.

Lagringsskyldighetens närmare omfattning preciseras i förordning.

Vid en överträdelse av paragrafen kan tillsynsmyndigheten besluta om sanktionsavgift, se 12 kap. 1 §.

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 §.

Paragrafen är ny och reglerar lagringsskyldigheten för utökad riktad lagring. Övervägandena finns i avsnitt 8.3.2 och 8.3.3.

Utökad riktad lagring ålägger den som är lagringsskyldig enligt 9 kap. 19 § nya LEK att lagra trafik- och lokaliseringsuppgifter avseende begränsade geografiska områden samt avseende platser, personer och utrustnings- och abonnemangsidentitet. Bestämmelsen knyter an till 5 § lagen om lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet.

Det är Polismyndigheten, Säkerhetspolisen och Tullverket som, med beaktande av proportionalitetsprincipen, beslutar om lagringsskyldighetens omfattning. De uppgifter som kan omfattas av ett beslut om utökad riktad lagring räknas upp i 19 b §. Det görs därför en hänvisning till den bestämmelsen.

Lagringsskyldighetens närmare omfattning preciseras i förordning.

Vid en överträdelse av paragrafen kan tillsynsmyndigheten besluta om sanktionsavgift, se 12 kap. 1 §.

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 §§.

Paragrafen är ny och reglerar lagringsskyldighet vid misslyckad uppringning, dvs. uppringning som kopplas fram utan att nå en mottagare. Övervägandena finns i avsnitt 7.3.6 och 8.3.3.

Vid geografiskt riktad lagring ska lagringsskyldigheten alltid omfatta uppgifter som genereras eller behandlas vid misslyckad uppringning. Vid nationell säkerhetslagring och utökad riktad lagring får sådana uppgifter lagras om myndigheterna anser att behovet finns och anges i beslutet om lagring.

Behandling av trafik- och lokaliseringsuppgifter

21 §

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.

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.

Paragrafen anger de fall där uppgifter som har lagrats enligt 19 b–19 d §§ får behandlas. Övervägandena finns i avsnitt 7.3.8 och 8.3.6.

I *första stycket* anges att uppgifter som lagrats vid geografiskt riktad lagring och utökad riktad lagring endast får behandlas för att lämnas ut enligt 9 kap. 33 § första stycket 2 eller 5 i nya LEK, 27 kap. 19 § rättegångsbalken, eller inhämtningslagen. Utgångspunkten är annars att uppgifterna ska utplånas eller avidentifieras när de inte längre behövs för överföring av ett elektroniskt meddelande. Det finns vissa undantag från detta krav (se 9 kap. 1 § andra stycket, 2, 4 och 10 § nya LEK).

I *andra stycket* föreskrivs att uppgifter som lagrats vid nationell säkerhetslagring endast får behandlas för att lämnas ut enligt 11 § lagen om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet. Den som är lagringsskyldig enligt 19 § 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 åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet.

Lagringstider

22 §

Uppgifter som avses *i 19 a–d §§* ska lagras enligt följande:

– 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 avses i 19 c och 19 d §§ ska lagras i ett år.

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.

Paragrafen anger lagringstiden för de uppgifter som har lagrats och de åtgärder som ska vidtas vid lagringstidens slut. Övervägandena finns i avsnitt 6.6.1, 7.3.6, 8.3.3 och 9.6.1.

Första stycket anger lagringstiderna. Första strecksatsen reglerar lagringstiden för uppgift om abonnemang. I fråga om sådana uppgifter ska lagringstiden pågå fram till ett år efter det att abonnemanget upphörde. Motsvarande gäller vid avregistrering av en tjänst. I fråga om tillfälliga identifierare ska lagringstiden räknas från det att tilldelningen av identifieraren upphörde hos användaren. Med tillfälliga identifierare avses här exempelvis dynamiska ip-adresser och uppgift om kopplingen mellan permanenta och tillfälliga identifierare i 5G-nätet.

Andra strecksatsen reglerar lagringstiden för trafik- och lokaliseringsuppgifter vid nationell säkerhetslagring. Sådana uppgifter ska lagras i två år.

Tredje strecksatsen reglerar lagringstiden för trafik- och lokaliseringsuppgifter vid geografiskt riktad lagring och utökad riktad lagring. Sådana uppgifter ska lagras i ett år.

Andra stycket anger hur lagringstiden ska beräknas. Lagringstiden börjar den dag då kommunikationen avslutades. Om uppgift om när kommunikationen avslutades saknas, ska lagringstiden i stället räknas från den dag då uppgifterna genererades. Beträffande lokaliseringsuppgift som inte är trafikuppgift räknas lagringstiden från den dag då uppgiften genererades.

Tredje stycket innehåller en bestämmelse om lagringstid för meddelanden som skickas via en Noik-tjänst. För sådana räknas lagringstiden från den dag meddelandet skickades eftersom ett meddelande skickat via Noik kan tas emot vid flera olika tillfällen. Om tiden i stället knutits till mottagandet, hade det kunnat medföra att lagringstiden fortsätter löpa utan inskränkning i tid.

Fjärde stycket är oförändrad och reglerar skyldigheten att utplåna uppgifterna när lagringstiden har löpt ut. Den omständigheten att uppgift om abonnemang som lagrats med stöd av 9 kap. 19 a § ska utplånas betyder inte att tillhandahållarna ska utplåna uppgift om abonnemang som insamlats och behandlas för de egna behoven.

Upplysning om verkställighetsföreskrifter

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 b–19 d §§, och*
2. lagringstiden enligt 22 § första, *andra och tredje stycket.*

Paragrafen innehåller upplysning om verkställighetsföreskrifter enligt regeringsformen. Övervägandena finns i avsnitt 7.3.6 och 8.3.3.

29 §

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 som avses i första stycket samt får i enskilda fall besluta om undantag från kravet i första stycket.

Paragrafen innebär en skyldighet för den som är lagringsskyldig enligt 19 § att bedriva sin verksamhet så att HAK, HÖK och inhämtning enligt inhämtningslagen kan verkställas och så att verkställandet inte röjs. Här, liksom i 29 § b, regleras alltså den s.k. anpassningsskyldigheten. Övervägandena finns i avsnitt 9.6.3, 10.4.1 och 10.4.3.

Genom en ändring i *första stycket* omfattas även tillhandahållare av Noik av skyldigheten att bedriva sin verksamhet så att beslut om HAK, HÖK och inhämtning enligt inhämtningslagen kan verkställas och så att verkställandet inte röjs. Första stycket har även ändrats så att det uttryckligen framgår att anpassningsskyldigheten gäller vid beslut om inhämtning med stöd av inhämtningslagens regler.

Anpassningsskyldigheten innefattar en skyldighet för tillhandahållarna att se till att de brottsbekämpande myndigheterna kan tillgodogöra sig uppgifter om och innehållet i meddelanden oavsett ny teknik och nya tillämpningar. Det innebär bl.a. att tillhandahållare som har kommunikationstjänster som är totalsträckskrypterade måste ha förmåga att på lämpligt sätt kunna verkställa tvångsmedelbeslut. Inget hindrar att kryptering används i förhållande till externa aktörer, men krypteringen får inte vara sådan att den hindrar användningen av hemliga tvångsmedel. Vid internationell roaming kräver anpassningsskyldigheten att teleoperatörerna säkerställer att uppgifter kan levereras i läsbar form till de brottsbekämpande myndigheterna, exempelvis genom avtal med utländska teleoperatörer.

I paragrafen införs i *andra stycket* ett undantag från anpassningsskyldigheten för tillhandahållare av s.k. maskin-till-maskin-tjänster. Med maskin-till-maskin-tjänster avses tjänster som omfattar automatisk överföring av data och information mellan enheter och 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.

Undantaget innebär att den som tillhandahåller maskin-till-maskin-tjänster inte omfattas av anpassningsskyldigheten beträffande dessa tjänster.

29 a §

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.

I paragrafen finns bestämmelser om ersättning vid utlämnande av uppgifter till brottsbekämpande myndigheter. Övervägandena finns i avsnitt 10.4.4.

I paragrafen görs ett tillägg så att även tillhandahållare av Noik omfattas av rätten till ersättning vid utlämnande av uppgifter till brottsbekämpande myndigheter.

Tidigare reglerades lokaliseringsuppgifter som inte är trafikuppgifter särskilt i ett andra stycke i paragrafen. Eftersom lokaliseringsuppgifter som inte är trafikuppgifter nu omfattas av tystnadsplikten enligt en ny fjärde punkt i 9 kap. 31 § första stycket nya LEK, behövs ingen särreglering i 29 a §.

29 b §

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.

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 behandlar hur uppgifter ska lämnas ut till brottsbekämpande myndigheter. Övervägandena finns i avsnitt 10.4.3.

Genom en hänvisning till kretsen av lagringsskyldiga i 19 § i *första stycket* omfattas även tillhandahållare av Noik av bestämmelsen. Bestäm-

melsen innebär att uppgifter som gäller brottslig verksamhet eller misstanke om brott ska lämnas ut till brottsbekämpande myndigheter utan dröjsmål och på ett sådant sätt att utlämnandet inte röjs. Uppgifterna ska också ordnas och göras tillgängliga i ett format som gör att de enkelt kan tas om hand. Skyldigheten omfattar alla uppgifter som omfattas av tystnadsplikten i 9 kap. 31 § nya LEK, dvs. uppgift om abonnemang, innehållet i ett elektroniskt meddelande, trafikuppgifter (tidigare annan uppgift som angår ett särskilt elektroniskt meddelande) och lokaliseringsuppgifter som inte är trafikuppgifter.

Tidigare reglerades lokaliseringsuppgifter som inte är trafikuppgifter särskilt i ett tredje stycke i paragrafen. Eftersom lokaliseringsuppgifter som inte är trafikuppgifter nu omfattas av tystnadsplikten enligt en ny fjärde punkt i 9 kap. 31 § första stycket nya LEK, behövs ingen särreglering i 29 b §.

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 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, 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 6.6.2, 7.3.9 och 9.6.2.

Tidigare fanns ett tillägg i *första stycket* att tillhandahållare av Noik skulle undantas från paragrafens tillämpningsområde. Tystnadsplikten gäller nu för samtliga tillhandahållare av elektroniska kommu-

nikationsnät och elektroniska kommunikationstjänster med de begränsningar som framgår av andra stycket.

I första stycket 3 ersätts uttrycket annan uppgift som angår ett särskilt elektroniskt meddelande med begreppet trafikuppgift. Begreppen har samma innebörd i nya LEK. För att undvika tolkningssvårigheter utmönstras uttrycket annan uppgift som angår ett särskilt elektroniskt meddelande. I sak avses inte någon ändring i fråga om tystnadsplikten. Den tystnadsplikt som hittills gällt för annan uppgift som angår ett särskilt elektroniskt meddelande gäller således alltjämt.

Genom en ny fjärde punkt i första stycket omfattas lokaliseringsuppgifter som inte är trafikuppgifter av tystnadsplikten. Enligt 9 kap. 10 § får sådana lokaliseringsuppgifter lagras enligt 19 b–19 d §§. För den enskilde användaren kan sådana uppgifter vara integritetskänsliga. Lokaliseringsuppgifter som inte är trafikuppgifter omfattas därför av tystnadsplikten.

I andra stycket anges att tystnadsplikten för uppgift om abonnemang, innehållet i ett elektroniskt meddelande och trafikuppgift ska gälla vid kommunikation som till någon del sker i Sverige. Samma anknytning till Sverige gäller således för tystnadsplikten som lagringsskyldigheten enligt 9 kap. 19 § nya LEK.

Tredje stycket är oförändrat.

Genom att punkten fyra, som avser lokaliseringsuppgifter som inte är trafikuppgifter, läggs till i *fjärde stycket* gäller inte denna tystnadsplikt 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,

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.

Paragrafen innehåller ytterligare bestämmelser om tystnadsplikt. Övervägandena finns i avsnitt 7.3.9 och 8.3.7.

I paragrafen finns två nya punkter, angelägenhet om nationell säkerhetslagring (punkt 8) och angelägenhet om utökad riktad lagring (punkt 9). Av 44 kap. 4 § OSL 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 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 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.

Paragrafen innehåller bestämmelser om skyldighet att på begäran lämna ut vissa uppgifter som enligt 31 § första stycket omfattas av tystnadsplikt. Övervägandena finns i avsnitt 9.6.3.

Tidigare fanns ett tillägg i första stycket att tillhandahållare av Noik skulle undantas från paragrafens tillämpningsområde. Skyldigheterna att lämna ut uppgift om abonnemang m.m. med stöd av nya LEK gäller nu för samtliga tillhandahållare av elektroniska kommunikationsnät och elektroniska kommunikationstjänster.

12 kap.

1 §

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, 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 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,

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.

Paragrafen reglerar vilka överträdelser som tillsynsmyndigheten ska besluta om sanktionsavgift för. Övervägandena finns i avsnitt 10.5. Genom ändring i *punkten 12* kan sanktionsavgifter tas ut av den som inte bedriver sin verksamhet så att beslut om inhämtning enligt inhämtningslagen kan verkställas. Genom en ny *punkt 16* kan sanktionsavgifter tas ut även av den som inte lagrar uppgifter om elektronisk kommunikation på föreskrivet sätt.

14.8 Förslaget till förordning om ändring i förordningen (2022:511) om elektronisk kommunikation

9 kap.

Lagring av uppgift om abonnemang

6 §

Lagringsskyldigheten enligt 9 kap. 19 a § lagen (2022:482) om elektronisk kommunikation omfattar uppgifter som är nödvändiga för att identifiera abonnent och registrerad användare och som är uppgift om

1. abonnent och registrerad användare,

2. användares ip-adress och andra uppgifter,

3. användares abonnemangs- och utrustningsidentiteter samt

4. koppling mellan tillfälliga och permanenta identifierare för utrustning och abonnemang.

Post- och telestyrelsen får meddela ytterligare föreskrifter om vilka uppgifter som ska lagras enligt första stycket.

Paragrafen reglerar lagringsskyldigheten i fråga om uppgift om abonnemang enligt 9 kap. 19 a § nya LEK. Övervägandena finns i avsnitt 6.6.1.

Första punkten innebär att uppgifter om abonnent och registrerad användare ska lagras. Eftersom abonnent och registrerad användare kan vara olika personer ska båda uppgifterna lagras. De uppgifter som avses är t.ex. namn, adress, övriga kontaktuppgifter och person- eller organisationsnummer. Finns det flera abonnenter eller registrerade användare ska uppgifter om samtliga dessa lagras.

Andra punkten reglerar skyldigheten att lagra användares ip-adress och andra uppgifter som är nödvändiga för att identifiera abonnent och registrerad användare. Med ip-adress avses IPv4 och IPv6 (Internet Protocol version 4 och 6). Lagringsskyldigheten omfattar fasta, dynamiska eller ip-adresser styrda genom NAT-teknik (Network Address Translation) eller motsvarande teknik för adressöversättning.

Tillägget *andra uppgifter* innebär att den lagringsskyldiga förutom ip-adresser även ska lagra vissa kompletterande uppgifter, om sådana uppgifter krävs för att identifiera användaren. Vid NAT-teknik ska således uppgift om användares privata och publika ip-adress med tillhörande portnummer kopplat till ip-adresserna och spårbar tid för kopplingen lagras.

Uppgifter om kommunikation kopplad till en ip-adress ska inte lagras med stöd av denna bestämmelse. Med det avses sådant som typiskt sett förekommer i s.k. sessionsloggar och omfattar information om datapaket, spårbar tid, sändande och mottagande ip-adress, portnummer och överföringsprotokoll m.m. Lagringsskyldigheten omfattar således inte sådan information som avslöjar trafiken mellan olika ip-adresser.

Tredje punkten reglerar lagringsskyldighet för uppgifter som kan identifiera en användare av ett abonnemang eller viss utrustning. Med abonnemangs- eller utrustningsidentitet avses exempelvis IMEI-nummer för mobiltelefoner, ICCID-nummer för SIM-kort eller IMSI-nummer för mobiltelefonabonnemang, fasta eller dynamiska ip-nummer eller ett inloggningskonto hos en tillhandahållare av tjänster för elektronisk kommunikation. Uppräkningen är inte uttömmande.

Fjärde punkten reglerar lagringsskyldigheten för uppgift om kopplingen mellan permanenta och tillfälliga identifierare som är nödvändiga för att identifiera en användare och registrerad användare i exempelvis 5G-nätet.

I *andra* stycket finns genom subdelegation ett bemyndigande för PTS att meddela ytterligare föreskrifter om lagringsskyldighetens omfattning. Syftet är att PTS ska kunna undanröja eventuella framtida oklarheter vid förekomsten av ny teknik och nya kommunikationsvanor.

Nationell säkerhetslagring

6 a §

Lagringsskyldigheten i 9 kap. 19 b § lagen (2022:482) om elektronisk kommunikation får omfatta de uppgifter som anges i 6 b och 6 c §§.

Paragrafen är ny och reglerar lagringsskyldigheten vid nationell säkerhetslagring genom hänvisning till 6 b och 6 c §§.

6 b §

När det gäller telefonitjänst, samtal och meddelandehantering får följande lagras:

1. i fråga om telefonitjänst och samtal, uppringande och uppringt nummer, ip-adress eller annan meddelandeadress, abonnemangs- och utrustnings-identitet,

2. i fråga om meddelanden, avsändares och mottagares nummer, ip-adress eller annan meddelandeadress, abonnemangs-, konto- eller utrustningsidentitet,

3. nummer, ip-adress eller andra meddelandeadresser som kommunikationen styrts till vid överflyttning, vidareförmedling eller transport av 1 och 2,

4. uppgifter om abonnent och registrerad användare som uppgifterna i 1–3 kan hänföras till,

5. kopplingen mellan tillfälliga och permanenta identifierare för utrustning eller abonnemang,

6. uppgifter om den eller de tjänster som använts,

7. datum och spårbar tid för då kommunikationen påbörjades och avslutades eller ett meddelande skickades och togs emot,

8. lokaliseringsuppgifter vid kommunikationen,

9. lokaliseringsuppgifter som inte är trafikuppgifter samt lokaliseringsuppgifter som genererats i användares utrustning, och

10. uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten.

Om den som slutligt avskiljer kommunikationen till den enskilda abonnenten inte omfattas av lagringsskyldighet, ska första stycket 10 gälla för den som avskiljer kommunikationen till den som slutligt avskiljer kommunikationen till den enskilda abonnenten.

Paragrafen är ny och reglerar vilka uppgifter som ska lagras för telefonitjänst, samtal och meddelandehantering. Övervägandena finns i avsnitt 7.3.6.

I 1 kap. 7 § nya LEK finns legaldefinitioner av begreppen telefonitjänst, samtal och meddelandehantering. Med telefonitjänst avses främst traditionell telefoni dvs. en elektronisk kommunikationstjänst som innebär en möjlighet att ringa eller ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan. Såväl mobiltelefoner som telefoni med fast anslutningspunkt omfattas av lagringsskyldigheten. Genom användning av begreppet samtal omfattas även Noik-tjänster. Med samtal avses en förbindelse genom en allmänt tillgänglig interpersonell kommunikationstjänst som möjliggör talkommunikation i båda riktningarna. Med meddelandehantering avses 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- eller tv-program. Lag-

ringsskyldigheten omfattar således såväl sms som meddelanden via Noik.

Första punkten och andra punkten innebär att det nummer eller annan adress som har använts för att inleda kommunikationen och som är målet för kommunikationen ska lagras. Det spelar ingen roll om kontakt har etablerats genom abonnemangsidentitet, utrustningsidentitet eller ett annat nummer. Oftast är uppringande och uppringd adress av samma slag. Uppringt nummer eller motsvarande adress avser den adress som användaren anger för att initiera en kommunikation med motparten. För telefonitjänst är det ett telefonnummer (E.164-nummer) och för samtal via Noik och meddelandehantering kan det vara ett telefonnummer, användarnamn, en ip-adress eller en e-postadress. Lagringsskyldigheten innefattar även icke fullständiga nummer som slagits och s.k. skräppost (som hamnar direkt i mottagarens mapp för skräppost eller borttagna meddelanden).

Tredje punkten omfattar lagring för det eller de nummer som avses i punkterna 1 och 2 i de fall tilläggstjänster såsom omstyrning och överflyttning av samtal eller motsvarande tjänst har använts.

Fjärde punkten omfattar lagring av uppgifter om abonnent och registrerad användare. De uppgifter som avses är t.ex. namn, adress och person- eller organisationsnummer. Finns det flera abonnenter eller registrerade användare, ska uppgifter om samtliga dessa lagras.

Femte punkten omfattar lagring av koppling mellan tillfälliga och permanenta identifierare för utrustning eller abonnemang, exempelvis kopplingen mellan SUCI (Subscription Concealed Identifier) och SUPI (Subscription Permanent Identifier) i 5G-nätet.

Sjätte punkten omfattar lagring av tjänster som knyter an till kommunikationen, exempelvis omstyrning och överflyttning eller samtal.

Sjunde punkten omfattar vilka tidsuppgifter som ska lagras. Med spårbar tid avses tidsangivelse där förhållandet till UTC (SP) (den tillämpning av den internationella tidsskalan UTC som används i Sverige) framgår. Uppgiften ska vara så precis som möjligt.

Åttonde punkten omfattar lagring av lokaliseringsuppgifter vid kommunikation, dvs. telefonitjänst, samtal eller meddelandehantering. Vid användning av mobiltelefoni är det uppgift om kommunicerande cell tillsammans med cellens position och riktning, dvs. det geografiska område som cellen täcker som ska lagras.

Nionde punkten omfattar lagring av lokaliseringsuppgifter som inte är trafikuppgifter, dvs. sådana uppgifter som genereras när ut-

rustningen inte aktivt används för telefoni, samtal och meddelandehantering. Satellitpositioneringsuppgifter som genererats i utrustningen kan vara en sådan. Med satellitpositioneringsuppgifter avses exempelvis positioner från det amerikanska systemet Global Positioning System eller det europeiska systemet Galileo.

Lokaliseringsuppgifter som inte är trafikuppgifter kan också avse olika typer av signaleringsuppgifter som genereras i en mobiltelefon eller i ett mobiltelefoninät. Detsamma gäller även vid internetåtkomst som lagras i 6 c §. Det kan exempelvis vara fråga om periodiska uppdateringar, registrering- och bortkoppling från mobilnätet och andra uppgifter som genererats i syfte att initiera, upprätthålla och avsluta sessioner och tjänster. Motsvarande gäller även vid internetåtkomst som regleras i 6 c §.

Det ankommer på PTS att genom föreskrifter närmare precisera lagringsskyldigheten. Många gånger kommer det att vara naturligt för PTS att innan föreskrifter meddelas samråda med de brottsbekämpande myndigheterna och vid behov även med tillhandahållarna.

Tionde punkten innebär att uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten ska lagras. Den utrustning som avses är den sista utrustningen inom den lagringsskyldiges kontroll. Vid fast internetåtkomst innebär det t.ex. fibermodem eller telefonjack och vid mobil internetåtkomst utrustning i basstationen, oftast en cell, eller en router vid ett allmänt trådlöst nätverk. Uppgift som kan identifiera utrustningen kan vara ett unikt identitetsnummer, t.ex. MAC-adress, eller annan uppgift om utrustningens identitet som genereras eller behandlas av den lagringsskyldige i samband med internetåtkomsten. Vid mobil internetåtkomst motsvarar uppgifterna i princip lokaliseringsuppgifter vid telefonitjänst.

Av andra stycket framgår att om den som slutligt avskiljer kommunikationen till den enskilda abonnenten inte omfattas av lagringsskyldighet, ska första stycket 10 gälla för den som avskiljer kommunikationen till den som slutligt avskiljer kommunikationen till den enskilda abonnenten. Bestämmelsen gäller alltså punkten mellan å ena sidan det sista i kedjan av nät som ägs av någon som omfattas av lagringsskyldigheten och å andra sidan ett nät som inte omfattas av lagringsskyldigheten. På så sätt kan exempelvis kommunikation fram till ett internt företagsnätverk spåras.

6 c §

När det gäller internetåtkomst får följande lagras:

1. användares ip-adress och andra uppgifter som är nödvändiga för att identifiera abonnent och registrerad användare,

2. uppgifter om abonnent och registrerad användare,

3. användares abonnemangs- och utrustningsidentiteter,

4. koppling mellan tillfälliga och permanenta identifierare för utrustning och abonnemang,

5. den typ av kapacitet för överföring som har använts,

6. datum och spårbar tid för åtkomsten,

7. lokaliseringsuppgifter vid åtkomsten,

8. lokaliseringsuppgifter som inte är trafikuppgifter samt lokaliseringsuppgifter som genererats i användares utrustning,

9. uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten.

Om den som slutligt avskiljer kommunikationen till den enskilda abonnenten inte omfattas av lagringsskyldighet, ska första stycket 9 gälla för den som avskiljer kommunikationen till den som slutligt avskiljer kommunikationen till den enskilda abonnenten.

Paragrafen är ny och reglerar vilka uppgifter som ska lagras för internetåtkomst. Övervägandena finns i avsnitt 7.3.6.

Innehållet i kommunikation, destinations-ip (t.ex. vilka webbsidor en person besökt) eller annan information om hur användaren trafikerat internet får inte lagras med stöd av denna bestämmelse.

I huvudsak motsvarar punkterna samma som 6 a § med undantag av *femte punkten.* Av den följer att lagringen ska omfatta kapacitet för internetåtkomst. Med det avses hur den enskilde får internetåtkomst t.ex. fast fiberanslutning, xDSL (Digital Subscriber Line), UMTS (Universal Mobile Telecommunications System) LTE (Long-Term Evolution) och 5G (5th Generation Mobile Network).

Geografiskt riktad lagring

7 §

Lagringsskyldigheten i 9 kap. 19 c § lagen (2022:482) om elektronisk kommunikation ska omfatta de uppgifter som anges i 6 b och 6 c §§.

Paragrafen reglerar vilka uppgifter som ska lagras vid geografiskt riktad lagring. Övervägandena finns i avsnitt 8.3.1 och 8.3.3.

Utökad riktad lagring

8 §

Lagringsskyldigheten i 9 kap. 19 d § lagen (2022:482) om elektronisk kommunikation får omfatta de uppgifter som anges 7 §.

Paragrafen är ändrad och reglerar vilka uppgifter som kan omfattas av ett beslut om utökad riktad lagring. Övervägandena finns i 8.3.2 och 8.3.3.

Föreskriftsrätt

9 §

Post- och telestyrelsen får meddela närmare föreskrifter om vilka uppgifter som ska lagras enligt *6 b* och *6 c §§*.

Paragrafen reglerar föreskriftsrätt för PTS att meddela närmare föreskrifter om vilka uppgifter som ska lagras. Övervägandena finns i avsnitt 7.3.6 och 8.3.3.

Särskilt yttrande

Särskilt yttrande av Sofie Klahr, Johan Lengholm, Ted Murelius, Micaela Nordberg, Robert Nygren, Anna Olander Selldén, Maria Sertcanli och Christoffer Östlind

Inledning

Vid såväl utredningar om grova brott som inom underrättelseverksamhet avseende sådan brottslig verksamhet är tillgång till elektronisk kommunikation ofta av helt avgörande betydelse. En av de inledande åtgärderna vid sådana utredningar är många gånger att begära åklagarens eller rättens tillstånd till inhämtning eller hemlig övervakning av elektronisk kommunikation. För att hemliga tvångsmedel som bygger på inhämtning av lagrade uppgifter ska ge någon effekt krävs emellertid att det faktiskt finns lagrade uppgifter att ta del av. Av kommittédirektiven till denna utredning framhålls därför att uppdraget syftar till att säkerställa att de brottsbekämpande myndigheternas tillgång till information förbättras och upprätthålls över tid i takt med teknikutvecklingen och förändrade kommunikationsvanor, samtidigt som respekten för mänskliga rättigheter säkerställs.

Vi anser dock att utredarens förslag begränsar datalagringen i större utsträckning än vad som krävs för att anpassa lagstiftningen till EU-domstolens praxis. Förslagen leder i vissa delar till att de brottsbekämpande myndigheternas möjligheter att förebygga, förhindra, upptäcka och utreda grova brott, i stället för att förbättras, kommer att försämras.

Bakgrund

Våld i form av skjutningar och sprängningar har ökat tydligt i Sverige de senaste åren. Sprängningar och skjutningar har tidigare främst riktats mot individer i den kriminella miljön som en mer eller mindre förutsägbar del av en pågående konflikt. Utvecklingen på senare tid har dock medfört att helt utomstående drabbas i allt större utsträckning av uppgörelser mellan gängkriminella. Möjligheten att förutse var brotten kommer att inträffa har minskat och därmed också möjligheten att ingripa mot dessa.

Brottsligheten i de kriminella miljöerna är dock inte begränsad till skjutvapenvåld och sprängningar utan även andra allvarliga brott är vanligt förekommande, såsom narkotikabrott, vapenbrott, smugglingsbrott, cyberbrott och ekonomisk brottslighet. T.ex. har grova bedrägerier ökat kraftigt de senaste åren. Brottsligheten har en stark koppling till kriminella nätverk och brottsvinsterna, som uppgår till mångmiljardbelopp, återinvesteras i annan kriminalitet eller i legal verksamhet.

Säkerhetshoten mot Sverige har också ökat under en längre tid och händelser det senaste året har resulterat i ett allvarligt försämrat säkerhetsläge för Sverige där vi enligt Säkerhetspolisen kan förvänta oss både ökande underrättelseverksamhet och säkerhetshotande aktiviteter mot Sverige inte minst från Ryssland. Säkerhetspolisen ser vidare hur utvecklingen i omvärlden bidrar till en växande extremism och ett bredare författningshot.

Samtidigt som den allvarliga brottsligheten har blivit alltmer utbredd har den tekniska utvecklingen i samhället i det närmaste exploderat. Utbudet av olika informations- och kommunikationstjänster är i dag mycket stort och tjänsterna är lättillgängliga för alla med tillgång till internet i t.ex. en smart telefon eller en dator. Tekniska hjälpmedel används i stor utsträckning i helt legala syften, men också av kriminella aktörer för planering och kommunikation eller som direkta brottsverktyg vid t.ex. försäljning av narkotika, dataintrång och internetrelaterade sexualbrott mot barn. Teknikutvecklingen ställer helt nya krav på de brottsbekämpande myndigheterna. I stället för DNA-spår lämnar brottsligheten digitala spår som myndigheterna måste kunna komma åt för att brottsbekämpningen ska bli effektiv och verkningsfull. För att de här spåren ska kunna kommas åt är det av avgörande betydelse att de också sparas. En central del av en effek-

tiv bekämpning av nästan all grov brottslighet är nämligen tillgången till uppgifter om användning av elektronisk kommunikation. Den information som sådana uppgifter ger är unik och kan endast gå att få fram genom ett fåtal metoder. Ofta är därför uppgifterna den första och enda ingången för de brottsbekämpande myndigheterna och utgör därmed nyckeln till det fortsatta arbetet. För att säkerställa att information sparas behövs en skyldighet för tjänsteleverantörer att lagra uppgifter om elektronisk kommunikation.

Inom ramen för underrättelsearbetet har trafik- och lokaliseringsuppgifter en stor betydelse för att kunna kartlägga personers kontakt- och rörelsemönster dvs. koppla samman aktörer, platser och tidpunkter. Resultatet av ett sådant kartläggningsarbete kan sedan ligga till grund för olika åtgärder i syfte att t.ex. reducera ett hot eller lagföra begångna brott. En begränsad tillgång till historiska uppgifter av detta slag påverkar myndigheternas förmåga att utreda brott men även att bedöma t.ex. attentatshot eller förberedelse av annan grov brottslighet. I värsta fall skulle avsaknad av historiska uppgifter kunna leda till fullbordade terroristbrott eller mord, som hade kunnat förhindras.

Regeringen har i flera sammanhang betonat vikten av att teknikutvecklingen och ändrade kommunikationsvanor inte ska innebära försämrade möjligheter för de brottsbekämpande myndigheternas arbete. Det pågår även flera lagstiftningsprojekt som syftar till att stärka de brottsbekämpande myndigheternas förutsättningar att förebygga, förhindra och upptäcka samt utreda allvarliga brott genom användning av hemliga tvångsmedel. Gemensamt för dessa lagstiftningsprojekt är att riksdagen och regeringen gett uttryck för att de brottsbekämpande myndigheterna behöver effektivare verktyg i brottsbekämpningen och att hemliga tvångsmedel ofta är avgörande för att bekämpa allvarlig brottslighet och på så sätt öka tryggheten i samhället. Även i direktiven till denna utredning framhålls vikten av att de brottsbekämpande myndigheternas möjligheter att förebygga, förhindra samt utreda och lagföra brott upprätthålls och stärks.

Vi delar utredarens uppfattning att det är lämpligt att lämna förslag om riktad lagring för att bekämpa grov brottslighet. Vi anser dock att flera av utredarens förslag är mer begränsande än vad som är nödvändigt. Mot bakgrund av den extremt allvarliga brottsutvecklingen i Sverige och det faktum att tillgång till historiska uppgifter många gånger är helt avgörande för att bekämpa grov brottslighet,

anser vi att det är av yttersta vikt att ny lagstiftning på området ger de brottsbekämpande myndigheterna tillgång till lagrade uppgifter i så stor utsträckning som möjligt. EU-rättens praxis på området innebär en begränsning i förhållande till rådande svenska regler. För att säkerställa en så effektiv och ändamålsenlig datalagring som möjligt anser vi det påkallat att utnyttja hela det område som EU-domstolens praxis erbjuder. Vi anser inte att utredaren i sitt förslag till fullo har utnyttjat detta område.

Synpunkter på förslagen i utredningen

Nationell säkerhetslagring

Vi delar utredarens bedömning att det finns behov av att införa en särskild möjlighet till lagring av trafik- och lokaliseringsuppgifter i syfte att skydda nationell säkerhet. Vi anser dock att utredaren inte utnyttjat det utrymme som finns när det gäller datalagring i syfte att skydda nationell säkerhet. I kapitel 6 finns en utförlig redogörelse över relevant praxis från EU-domstolen. Av den redogörelsen framgår att EU-domstolens praxis medger att behöriga myndigheter under en begränsad tid ålägger tjänsteleverantörer en generell och odifferentierad lagringsskyldighet avseende trafik- och lokaliseringsuppgifter, om målet är att skydda nationell säkerhet. Såsom vi tolkar EU-domstolens avgöranden är det endast i förhållande till tidsaspekten som EU-domstolen har ställt som krav att lagringsskyldigheten ska vara begränsad till vad som är strängt nödvändigt. Enligt utredarens förslag uppställs emellertid ett sådant krav även beträffande vilka tillhandahållare och uppgifter som ska omfattas av lagringsskyldigheten.

Detta innebär att datalagring i syfte att skydda Sveriges säkerhet, i vissa delar kan komma att bli mer begränsad än datalagring enligt bestämmelserna om geografiskt riktad lagring. När det gäller geografiskt riktad lagring så träffar lagringsskyldigheten i en kommun som omfattas av sådan lagring nämligen samtliga tjänsteleverantörer och uppgiftstyper. Som skäl för utformningen av förslaget anför utredaren att det anses mest ändamålsenligt att låta samtliga tjänsteleverantörer omfattas av lagringsskyldigheten och att det vidare framstår som angeläget att de brottsbekämpande myndigheterna får tillgång till trafik- och lokaliseringsuppgifter oberoende av vilka tjänster som den enskilde

har använt sig av. I utredarens motivering saknas det argument för varför detta inte bör gälla även vid lagring för ändamålet nationell säkerhet.

Som ovan angetts finns det enligt vår uppfattning inte några hinder mot en lagstiftning som – under förutsättning att Sverige står inför ett allvarligt hot mot nationell säkerhet som har visat sig vara verkligt och aktuellt eller förutsägbart – medger att alla tjänsteleverantörer åläggs en skyldighet att lagra samtliga uppgifter som får lagras för syftet att skydda nationell säkerhet. Enligt vår mening bör lagstiftningen därför utformas på detta sätt, dvs. utan krav på att Säkerhetspolisen pekar ut vilka tjänsteleverantörer och vilka uppgifter som ska omfattas av lagringsskyldigheten. Det hindrar förstås inte en reglering som innebär en möjlighet för Säkerhetspolisen att avgränsa lagringsskyldighetens omfattning. Ett sådant förslag skulle bättre och mer ändamålsenligt utnyttja det utrymme som EU-domstolen medgett och resultera i en generell och odifferentierad lagringsskyldighet i syfte att skydda den nationella säkerheten.

Geografisk riktad lagring

Utredarens förslag om geografiskt riktad lagring

EU-domstolen har, i bl.a. SpaceNet-domen, slagit fast att nationell lagstiftning som föreskriver att det ska ske en generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter inte är tillåten. Däremot är det tillåtet med lagstiftning som föreskriver en riktad lagring av trafik- och lokaliseringsuppgifter om den, på grundval av objektiva och icke-diskriminerande faktorer, är avgränsad genom de kategorier av personer som berörs eller genom ett geografiskt kriterium, för en period som är tidsmässigt begränsad till vad som är strängt nödvändigt men som kan förlängas. Domstolen har inte lämnat närmare förklaringar till vad den avser med ett geografiskt kriterium.

Utredaren har i sitt förslag utgått från att geografiskt riktad lagring bör ske i områden där det utifrån objektiva kriterier går att konstatera att det jämförelsevis finns större sannolikhet för förekomst av grov brottslighet. För att bedöma risken för brottslighet på en viss geografisk plats föreslår utredaren att geografiskt riktad lagring ska grunda sig på den officiella statistiken över anmälda brott som redovisas av Brå och med kommunerna som geografiska enheter. Sannolikheten för att en viss kommun är mer brottsutsatt än en annan ska

bedömas utifrån ett genomsnitt av anmälda brott delat med befolkningsmängden under en treårsperiod som föregår lagringsskyldigheten.

Vi instämmer i utredarens bedömning att det – mot bakgrund av EU-domstolens uttalanden – finns anledning att lämna förslag på hur en geografiskt riktad lagring kan utformas. Om sådan lagring införs, delar vi även utredarens bedömning att kommuner, under vissa förutsättningar, är en lämplig geografisk avgränsning. Vi anser dock att den av utredaren föreslagna modellen inte bör läggas till grund för geografiskt riktad lagring i Sverige. Den valda modellen kommer enligt vår mening inte leda till en behovsanpassad lagring av elektronisk kommunikation. En behovsanpassad lagring skulle enligt vår mening i stället innebära att lagring sker i större utsträckning under tider då många grova brott begås i landet och i lägre utsträckning när den allvarliga brottsligheten ligger på lägre nivåer. Den av utredaren föreslagna modellen ger vidare den effekten att datalagring inte kommer att ske i alla de kommuner där flest brott begås och där behovet av datalagring således är störst. Vi anser vidare att utfallet av den föreslagna modellen, som det presenteras genom ögonblicksbilden i kapitel 8, innebär en lagringsskyldighet som kraftigt kommer att försämra de brottsbekämpande myndigheternas möjligheter att bekämpa grova brott.

Förslaget ger dålig träffsäkerhet

Utredaren har slagit fast att syftet med den geografiskt riktade lagringen är att identifiera områden där det finns en jämförelsevis större sannolikhet att det kommer att begås grova brott och där det därmed kan sägas finnas ett behov av lagring. Någon exakthet är det enligt utredaren svårt att uppnå med utgångspunkt från ett statistiskt underlag. Utredaren utgår i den föreslagna modellen från samtliga brottsanmälningar i kommunen, dvs. inte endast från anmälningar om grova brott.

Utredaren har därefter konstaterat att utgångspunkten för den geografiskt riktade lagringen är att de kommuner som har genomsnittligt högre sannolikhet för grova brott än andra kommuner ska lagra uppgifter. Beräkningarna ska grunda sig på årsvisa statistiska uppgifter och genomsnittet ska beräknas genom att det tas fram medelvärden av antalet anmälda brott över tre på varandra följande

år i kommunerna. Mot bakgrund av att det förekommer mycket stora variationer i kommunernas invånarantal föreslår utredaren vidare att det framräknade antalet anmälda brott i kommunerna, dvs. medelvärdet över tre år, relateras till befolkningsstorleken, genom en beräkning av antalet anmälda brott per 1 000 invånare.

Av den ögonblicksbild som presenteras framgår att gränsvärdet för geografiskt riktad lagring utifrån den föreslagna modellen motsvarar 92,1 anmälda brott per 1 000 invånare, räknat utifrån brottsanmälningar per kommun för åren 2020–2022. Av de tabeller som presenteras i kapitel 8 framgår att det i Jönköpings kommun under åren 2020–2022 anmäldes 39 086 brott. I Umeå kommun anmäldes det under samma år 34 091 brott. Mot bakgrund av medelvärdet relaterat till befolkningsstorleken (90,7 för Jönköpings kommun respektive 86,7 för Umeå kommun) leder den valda modellen till att dessa kommuner inte skulle omfattas av lagringsskyldigheten. Detta kan jämföras med Dorotea kommun där det under åren 2020–2022 anmäldes 734 brott och Arjeplog kommun där det anmäldes 810 brott under samma period. Efter att medelvärdet relaterats till befolkningsstorleken (99,5 för Dorotea kommun respektive 99,7 för Arjeplogs kommun) skulle den föreslagna modellen innebära att båda dessa kommuner skulle omfattas av lagringsskyldighet enligt den föreslagna modellen. Exemplet visar tydligt på den bristande träffsäkerhet som den valda modellen leder till.

Sammanfattningsvis anser vi att den föreslagna modellen för geografiskt riktad lagring leder till att datalagringsskyldigheten inte kommer att omfatta alla de kommuner där det finns störst behov av en sådan. För att datalagringen ska bli så effektiv som möjligt bör den som ovan angetts riktas mot de kommuner där flest allvarliga brott behöver utredas, dvs. där behovet av tillgång till lagrade uppgifter är som högst.

Omfattningen av lagringsskyldigheten

Som utredaren konstaterar innebär den valda modellen att lagringsskyldigheten skulle bestå även om brottsligheten närmast skulle upphöra i hela eller delar av landet. Utredaren konstaterar att en sådan utveckling inte verkar särskilt sannolik i dag. Motsatsvis, konstaterar utredaren, skulle lagringen inte öka om brottsligheten tilltog kraftigt

men jämnt fördelat över landet. Utredaren lyfter i det sammanhanget fram att det i vissa situationer då kan finnas möjlighet att besluta om nationell säkerhetslagring samt att den geografiska lagringen, i sådana situationer, även kan kompletteras med andra möjligheter till lagring för att motverka de negativa effekterna.

Vi delar inte utredarens bedömning i dessa delar. Även om det inte är sannolikt att brottsligheten närmast skulle upphöra i delar av eller hela landet bör en modell för riktad lagring ändå konstrueras på så sätt att en minskning av den grova brottsligheten också leder till att datalagringen minskar i omfattning. På motsvarande sätt bör enligt vår mening en mycket hög brottslighet i landet leda till att uppgifter lagras i en större omfattning. Den modell som utredaren har valt innebär i stället att lagringsskyldigheten relativt sett kommer att vara lika omfattande oavsett om brottsligheten i landet ökar eller minskar.

Som framgår av kartan i kapitel 8 skulle det valda förslaget, om det tillämpades i dag, innebära att över hälften av landets kommuner och en betydande del av Sveriges geografiska yta inte skulle omfattas av någon geografiskt riktad lagring. Vi återkommer till vilka konsekvenser detta skulle innebära för brottsbekämpningen i landet och möjligheten för brottsoffer att få upprättelse.

Vi delar inte heller utredarens uppfattning om möjligheten till nationell säkerhetslagring som en kompensatorisk åtgärd vid mycket hög brottslighet i landet. Lagring för ändamålet nationell säkerhet utgör endast ett ändamålsenligt alternativ till geografiskt riktad lagring när det gäller viss brottslighet, eftersom tillgång till sådana uppgifter, enligt EU-rätten och utredarens förslag, endast kan ges för att bekämpa brottslighet och brott som kan innebära ett hot mot Sveriges säkerhet.

Bristerna med den föreslagna geografiska lagringen kan inte läkas med hjälp av utökad riktad lagring

Den valda modellen leder till att stora delar av Sverige inte kommer omfattas av någon lagringsskyldighet. Om ett brott begås inom ett sådant område kommer de brottsbekämpande myndigheternas förutsättningar att utreda det brottet vara betydligt sämre än då ett brott begås inom ett område som omfattas av lagringsskyldighet. Utredaren menar emellertid att möjligheten till utökad riktad lagring delvis

skulle kunna läka denna brist. Vi delar inte denna bedömning. Vi ställer oss i och för sig positiva till utökad riktad lagring, inte minst med tanke på de grundläggande brister vi ser med den valda modellen för geografiskt riktad lagring. Vi vill emellertid framhålla att möjligheten att besluta om utökad riktad lagring, särskilt i den omfattning som föreslås, endast i viss mån kan läka den brist som utredarens förslag om geografiskt riktad lagring skulle innebära för möjligheten att bekämpa allvarliga brott.

Utredarens förslag om utökad riktad lagring innebär att geografiskt riktad lagring får kompletteras med beslut om utökad lagring avseende ett visst område, en skyddsvärd plats, en person eller viss teknisk utrustning. Visserligen finns det förstås en stor kunskap inom de brottsbekämpande myndigheternas underrättelseverksamheter när det gäller aktörer, geografiska platser, brottsfenomen etc. Som utredaren framför är det emellertid ofta mycket svårt att i förväg veta när, var eller av vem ett allvarligt brott kommer att begås. Även om de brottsbekämpande myndigheterna har möjlighet att besluta om utökad riktad lagring kommer det därför vara närmast omöjligt att fatta sådana beslut med tillräcklig träffsäkerhet och i sådan omfattning att förmågan att bekämpa grov brottslighet upprätthålls. Utökad riktad lagring kommer enligt vår bedömning därför endast i begränsad omfattning kunna läka de allvarliga brister vi ser med förslaget om riktad geografisk lagring.

Ett alternativt förslag

Den alternativa modell som utredaren har övervägt bygger på utgångspunkten att det är antalet grova brott i ett område som styr om datalagring ska ske. Utredaren konstaterar att en sådan modell kräver att man tar ställning till hur stort antal grova brott det ska vara fråga om för att datalagring ska påbörjas i det aktuella området. Utredaren menar också att det är problematiskt ur det perspektivet att om antalet grova brott sätts för lågt blir följden att den geografiskt riktade lagringen kan komma att omfatta hela landet. Om antalet grova brott å andra sidan sätts för högt, går själva syftet med datalagringen förlorat.

Ett av utredarens argument mot den alternativa modellen är att det finns en risk för att ett beslut om att lagringsskyldighet ska inträffa

vid ett visst antal grova brott uppfattas som godtyckligt. Vi anser emellertid att samma argument kan göras gällande i förhållande till den av utredaren föreslagna modellen. Även om det i botten finns en beräkningsgrund som leder fram till vilka kommuner som ska omfattas av lagringsskyldighet kan det konstateras att det för allmänheten torde framstå som godtyckligt att elektroniska uppgifter avseende personer i Gotlands kommun, som har ett medelvärde på 92,2 anmälda brott, ska lagras medan inga sådana uppgifter ska lagras avseende personer som bor i Ljungby kommun, där medelvärdet är 92,1 anmälda brott. Vidare saknas det i utredningen en motivering till varför det är kommuner som ligger över medelvärdet som ska omfattas av lagringsskyldigheten. Den bedömningen är således också i viss mån godtycklig. Det hade i stället varit möjligt att välja en annan gräns, t.ex. över medianvärdet eller över en viss percentil.

Vi har ovan redogjort för att vi anser att lagringsskyldigheten i så stor utsträckning som möjligt bör sättas i relation till behovet av lagrade uppgifter. Det bör med andra ord lagras fler uppgifter under tider och i områden då det begås många allvarliga brott och behovet av sådana uppgifter därmed är som högst. Vi anser därför att den alternativa modell som utredaren har övervägt skulle ge en bättre anpassad lagringsskyldighet än den nu föreslagna. Vi delar utredarens uppfattning att det kan vara förenat med svårigheter att komma fram till vilket antal allvarliga brott som ska sättas som gräns för när en lagringsskyldighet ska inträda. Detta kan dock inte utgöra det enda argumentet mot en lagringsmodell som i övrigt får anses ha klart starkare fördelar än den modell som utredaren har valt. Det bör vara möjligt att utifrån ett väl underbyggt statistiskt underlag kunna ta fram vilket antal grova brott som kan utgöra en rimlig nivå att utgå från. Exempelvis skulle man kunna överväga att vid beräkningarna utgå från brottsanmälningar under en betydligt längre period än tre år eller att endast utgå från anmälningar om grova brott. Det kan också övervägas om inte antalet brottsanmälningar ska vara styrande för lagringsskyldigheten, snarare än att relateras till befolkningsmängden i en kommun. Vi anser därför att det i den fortsatta beredningen bör övervägas ytterligare alternativ för hur ett gränsvärde för lagringsskyldighet skulle kunna utformas. För att kunna föreslå en beräkningsmodell som bättre speglar behoven behövs enligt vår uppfattning ytterligare underlag, vilket förslagsvis Brå skulle kunna få i uppdrag att ta fram.

Särskilt om Noik-leverantörer

Av direktiven till utredningen framgår att regeringen anser att det finns behov av att modernisera lagstiftningen i syfte att även s.k. Noik-leverantörer ska omfattas av skyldigheterna att lagra och lämna ut uppgifter om elektronisk kommunikation. Utredaren har fått till uppgift att analysera förutsättningarna, även ur ett tekniskt perspektiv. En sådan modernisering skulle enligt regeringen innebära att brottsbekämpande myndigheter skulle kunna förbättra möjligheterna att komma åt uppgifter om elektronisk kommunikation som de på grund av teknikutvecklingen och ändrade kommunikationsvanor har förlorat. Särskilt värt att notera här är att regeringen har velat förbättra de brottsbekämpande myndigheternas tillgång till uppgifter.

Ett generellt problem med den geografiskt riktade lagringen, oavsett om den sker på kommunnivå eller utifrån andra avgränsade geografiska kriterier, är att Noik-leverantörerna i många fall inte har tillgång till någon annan uppgift om var användaren befinner sig än vilken ip-adress som denne för tillfället nyttjar. Utifrån ip-adress kan användarens position ofta bestämmas relativt säkert på landnivå, men sällan med högre precision än så. Detta innebär att det är långt ifrån säkert att användarens beräknade position på kommunnivå, baserat på ip-adress, överensstämmer med den kommun där användaren fysiskt befinner sig. Av detta skäl finns det en betydande risk för att Noik-leverantörerna kommer anse att de inte har tillräckligt med data för att kunna omfattas av den geografiskt riktade lagringen. Eftersom den absoluta merparten av alla textmeddelanden i dag sänds via Noik riskerar därför den önskade effekten, att även uppgifter som avser sådana textmeddelanden ska omfattas av lagringsskyldighet, till stor del att utebli.

Vilken data en Noik-leverantör väljer att samla in om sin användares geografiska position är emellertid en fråga som enbart Noik-leverantören förfogar över. För att förslaget inte helt ska förlora sin effekt vore det bättre med en ordning där det av lagen framgår att trafik- och lokaliseringsuppgifter ska lagras om det inte står klart att uppgifterna inte omfattas av ett beslut om geografisk lagring.

Utökad riktad lagring

För att minimera de negativa konsekvenser som kommer bli följden av en anpassning till EU-domstolens praxis är det nödvändigt att de brottsbekämpande myndigheterna får goda möjligheter att rikta lagringen med andra parametrar än geografiska. Vi anser dock att utredaren, även när det kommer till utökad riktad lagring, inte fullt ut har utnyttjat de möjligheter till lagring som EU-domstolens praxis ger utrymme för.

Personbaserad riktad lagring

Enligt EU-domstolen finns det en möjlighet för medlemsstaterna att vidta lagringsåtgärder avseende vissa personer, om dessa personer direkt eller indirekt kan sättas i samband med brott eller brottslig verksamhet, under förutsättning att bedömningen sker på objektiva och icke-diskriminerande grunder. Som utredaren har tolkat detta kan personbaserad riktad lagring avse en person som förekommer i utredningar om allvarliga brott och i underrättelseverksamhet avseende allvarlig brottslighet. Utredaren har emellertid valt att endast föreslå personbaserad riktad lagring när det gäller dels personer som genom en lagakraftvunnen dom eller godkänt strafföreläggande ålagts påföljd för brott som ger rätt att använda hemlig övervakning av kommunikation enligt rättegångsbalken, dels personer som är eller har varit föremål för hemliga tvångsmedel.

Utredaren konstaterar att integritetsintrånget framstår som särskilt allvarligt om lagring kan ske beträffande personer utan att det föreligger någon konkret brottsmisstanke mot personen. Det handlar enligt utredaren dels om risk för stort intrång genom att uppgifter lämnas till tillhandahållarna, dels om risk för att de enskilda personerna blir utpekade såsom misstänkta för brott. Utredaren har vidare framfört att det finns svårigheter med att föreskriva ett beviskrav i fråga om den enskildes anknytning till grova brott eller grov brottslig verksamhet. Vi menar att det naturligtvis är viktigt att säkerställa att uppgifter om att enskilda omfattas av ett beslut om riktad lagring hanteras på ett säkert sätt så att obehöriga inte får ta del av uppgifterna. Man kan i detta avseende tänka sig flera lösningar när det kommer till hur trafiken leds eller hur man i övrigt kan säkerställa att uppgifterna finns tillgängliga efter att beslut om personbaserad lagring

har fattats. Mot bakgrund av, dels att EU-domstolens praxis ger utrymme för en mer omfattad personbaserad lagring än vad utredaren föreslår, dels det stora behov som de brottsbekämpande myndigheterna har av datalagrade uppgifter, anser vi att förslaget om personbaserad lagring är för begränsat. Att rikta lagring enbart mot personer som tidigare är lagförda för allvarliga brott eller annars varit föremål för hemliga tvångsmedel, kommer inte på ett effektivt sätt ge förutsättningar för att förebygga, förhindra och upptäcka nya brott. Historiska uppgifter används inte sällan för att kunna avfärda eller bekräfta misstankar mot en person liksom för att bedöma dennes avsikt och förmåga att begå brott. Vi anser därför att de brottsbekämpande myndigheterna bör kunna få fatta beslut om utökad riktad lagring även beträffande en person som förekommer i utredningar om allvarliga brott och underrättelseverksamhet avseende allvarlig brottslighet. T.ex. skulle en sådan lagring kunna avgränsas till personer som kan antas bli föremål för beslut om hemliga tvångsmedel. I sammanhanget är det värt att påminna om att även icke misstänkta personer kan bli föremål för hemliga tvångsmedel, t.ex. vid hemliga tvångsmedel utanför förundersökning eller då det inom ramen för en förundersökning finns synnerlig anledning att anta att en person kommer vara i kontakt med den misstänkte.

Vi vill även tydliggöra att personbaserad riktad lagring innebär att alla uppgifter hänförliga till en viss person ska omfattas av lagringsskyldigheten. Det innebär att om en person, som omfattas av ett beslut om riktad lagring, efter beslutet byter tjänsteleverantör så ska även den nya tjänsteleverantören lagra personens uppgifter, under förutsättning att leverantören omfattas av beslutet.

Tekniskt riktad lagring

Vi ställer oss mycket positiva till förslaget om utökad riktad lagring när det gäller sådan utrustnings- eller abonnemangsidentitet som använts vid eller skäligen kan antas komma till användning vid ett grovt brott eller vid grov brottslig verksamhet. Vi anser dock att det saknas en möjlighet att besluta att tillhandahållaren ska lagra sådana uppgifter om datapaket som är nödvändiga för att kartlägga trafikflöden. Det kan exempelvis handla om avsändande och mottagande ip-adress, avsändande och mottagande portnummer samt tidpunkt. Beslut om

sådan tekniskt riktad lagring skulle typiskt komma att riktas med hög precision mot specifika servrar, i syfte att säkra tillgång till information som är nödvändig för att förebygga, förhindra och upptäcka samt utreda exempelvis pågående allvarlig cyberbrottslighet. Precis som utredaren anger skulle en generell och odifferentierad lagring av uppgifter om datapaket vara att betrakta som oproportionerlig, men det förefaller högst rimligt att sådan lagring skulle kunna ske inom ramen för beslut om tekniskt riktad lagring. De uppgiftstyper som kommer i fråga för beslut om tekniskt riktad lagring behöver därför kompletteras med en möjlighet att besluta om lagring av sådana uppgifter om datapaket som är nödvändiga för att kartlägga trafikflöden.

Konsekvenser av förslagen

Konsekvenser för brottsbekämpningen

Lagringsskyldigheten syftar bl.a. till att säkerställa att de brottsbekämpande myndigheterna kan få tillgång till uppgifter om elektronisk kommunikation. Som flera gånger nämnts är tillgång till sådan information ofta av avgörande betydelse i utredningar och underrättelseverksamhet avseende grov brottslighet. I takt med en ökad brottslighet, ett försämrat säkerhetsläge, förändrad teknik och förändrade kommunikationsvanor blir de brottsbekämpande myndigheternas behov av verkningsfulla verktyg än viktigare.

En uppenbar konsekvens av att införa geografisk lagring, oavsett i vilken form det görs, är att möjligheterna att utreda brott, i de delar av landet som inte omfattas av lagringsskyldigheten, kraftigt kommer att försämras. De senaste åren har det, under förundersökning, meddelats omkring 13 000 beslut om hemlig övervakning av elektronisk kommunikation per år. Därtill kommer beslut som fattas i underrättelseverksamhet med stöd av bland annat inhämtningslagen. I sammanhanget bör också framhållas att antalet beslut om hemlig övervakning av elektronisk kommunikation i princip har fördubblats jämfört med de nivåer som gällde för fem år sedan. Av det sagda bör den slutsatsen kunna dras att hemlig övervakning av elektronisk kommunikation är ett viktigt verktyg i de brottsbekämpande myndigheternas uppdrag att utreda och även förhindra allvarlig brottslighet.

Vid utredningar om grova brott är ofta en av de inledande åtgärderna att begära rättens tillstånd till hemlig övervakning av elektronisk

kommunikation. Saknas det skäligen misstänkt person inleds det oftast med att det begärs tillstånd att få information om vilka elektroniska kommunikationsutrustningar som funnits i anslutning till brottsplatsen vid tiden för gärningen. Den informationen kan sedan jämföras med annan information i utredningen. På det sättet är det många gånger möjligt att identifiera en eller flera personer som kan vara intressanta för utredningen att titta närmare på. Exempel på hur information kan användas är t.ex. för att se vilka personer som befunnit sig på en plats för ett terrorattentat, för att se vilka nummer som kontaktat en äldre person utsatt för bedrägeri, för att se hur en telefon rört sig efter dess att målsägande rånats på den eller för att se vilka nummer som kontaktat ett barn som tvingats posera och skicka avklädda bilder under hot.

Även i underrättelseverksamheten är tillgång till elektronisk kommunikation av väsentlig betydelse. Tillgång till uppgifter om elektronisk kommunikation redan i underrättelsestadiet är avgörande för att aktörer, platser och tidpunkter ska kunna kopplas samman och ligga till grund för olika åtgärder som t.ex. reducera hot, upptäcka brott och inleda förundersökning. Resultatet av analyserade uppgifter om elektronisk kommunikation är också väsentliga för en effektiv planering av den yttre fysiska spaning som är resurskrävande och därför viktig att använda på rätt plats och vid rätt tillfälle. Analys av inhämtade uppgifter redan i underrättelseskedet kan bidra även till kortare förundersökningstider och ett effektivare utredningsarbete. Det är även relativt vanligt förekommande att befarade förestående mord, terroristbrott och andra grova brott förhindras till följd av bland annat analys av inhämtade uppgifter om elektronisk kommunikation.

En annan uppenbar konsekvens av förslaget är att avsaknad av lagringsskyldighet i delar av Sverige kommer kunna utnyttjas av personer som planerar att begå brott. Eftersom det kommer vara känt på förhand i vilka kommuner lagring inte sker, kommer exempelvis personer som avser att begå bedrägerier med telefonen som brottsverktyg kunna rikta in sig på personer boendes i dessa kommuner. Ett vanligt förekommande modus under de senaste åren har varit att bedragare ringt upp äldre personer under förespegling att de är polismän eller annan myndighetsperson. De har därigenom fått målsägandenas förtroende och sedan kunnat bli insläppta i deras bostäder och lurat till sig pengar och andra värdesaker. I dessa utredningar är möjligheten att kunna begära ut telefonlistor och positioneringsuppgifter i

det närmsta en nödvändig förutsättning för att ens kunna börja utreda brotten.

Även när det gäller andra grova brott skulle det kunna antas ske en förflyttning av brottsligheten. En geografiskt riktad lagring riskerar t.ex. att motivera kriminella att genomföra grova brott och våldsbrott i områden som kan antas vara undantagna den geografiska lagringen.

Den föreslagna geografiska lagringen skulle ha särskilt negativa konsekvenser för utredningen av dödligt våld mot kvinnor i de kommuner som inte omfattas av lagringen. Kvinnor mördas i 80 procent av fallen i det egna, förövarens, eller det gemensamma hemmet. Det dödliga våldet mot kvinnor är alltså inte kopplat till miljöer och områden där annan grov brottslighet nödvändigtvis förekommer utan kan lika gärna inträffa i en kommun där ingen geografisk lagring anses motiverad.

När det gäller konsekvenser av den personbaserade lagringen finns en risk för att detta skulle tjäna som ytterligare incitament för kriminella att rekrytera och använda yngre personer i deras närhet för att genomföra skjutningar och andra grova brott. Ungdomar utan belastningsregister eller som inte tidigare varit föremål för hemliga tvångsmedel skulle kunna användas som skyttar eller på andra sätt delta vid våldsbrott och riskfritt kunna kommunicera med varandra över mobilnätet. Det finns även en risk för att unga och personer som är ostraffade skulle användas som målvakter vid inköp av telefoner, abonnemang och kontantkort.

Konsekvenser för brottsoffer

Var och en som vistas i Sverige har rätt att göra anspråk på att staten vidtar effektiva åtgärder för att skydda hans eller hennes säkerhet. Staten har alltså en skyldighet att skydda enskildas privatliv och personliga integritet mot intrång som begås av andra enskilda och, om intrång görs, se till att brotten utreds (jfr prop. 2015/16:167 s. 26). Att ge de brottsbekämpande myndigheterna möjlighet att effektivt utreda brott i den elektroniska miljön faller in under detta ansvar.

Geografiskt riktad lagring kommer att leda till att brottsoffer kommer ha olika chans till att brottet de utsatts för klaras upp beroende på var i landet de bor. Förslaget om geografiskt riktad lagring innebär

att möjligheten att inhämta en områdesförfrågan helt kan saknas när en person mördas eller våldtas i en kommun där uppgifter inte lagras. I förhållande till en kommun där möjligheter till inhämtning av lagrad information kan finnas tillgänglig kommer möjligheten till upprättelse och skadestånd därmed väsentligt variera i olika delar av landet.

Slutsats

Sammanfattningsvis anser vi att vissa delar av utredarens förslag skulle leda till allvarliga konsekvenser för möjligheterna att bekämpa brott i Sverige. Som vi har framhållit till utredaren kan förslaget även komma att leda till stötande effekter för brottsoffer. Särskilt mot bakgrund av det allvarliga läge Sverige befinner sig i är det av avgörande vikt att de brottsbekämpande myndigheternas möjligheter att bekämpa brott upprätthålls och stärks. Med utredarens förslag om riktad lagring riskerar resultatet bli det motsatta.

Källförteckning

Offentligt tryck

Direktiv

Dir. 2020:66 *Effektivare möjligheter att ta brottsvinster från kriminella – en översyn av lagstiftningen om förverkande.*

Dir. 2020:104 *Utökade möjligheter att använda hemliga tvångsmedel.*

Dir. 2021:102 *Preventiva tvångsmedel för att förhindra allvarlig brottslighet.*

Dir. 2022:32 Tilläggsdirektiv till Utredningen om preventiva tvångsmedel.

Utredningsbetänkanden och promemorior

SOU 1979:6 *Polisen.*

SOU 1984:54 *Tvångsmedel – Anonymitet – Integritet.*

SOU 2002:60 *Lag om elektronisk kommunikation.*

SOU 2003:99 *Ny sekretesslag.*

SOU 2005:38 *Tillgång till elektronisk kommunikation i brottsutredningar m.m.*

SOU 2009:1 *En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen.*

SOU 2010:103 *Särskilda spaningsmetoder.*

SOU 2013:39 *Europarådets konvention om it-relaterad brottslighet.*

SOU 2015:31 *Datalagring och integritet.*

SOU 2016:65 *Ett samlat ansvar för tillsyn över den personliga integriteten.*

SOU 2017:75 *Datalagring – brottsbekämpning och integritet.*

SOU 2017:89 *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet.*

SOU 2017:100 *Beslag och husrannsakan – ett regelverk för dagens behov.*

SOU 2018:61 *Rättssäkerhetsgarantier och hemliga tvångsmedel.*

SOU 2022:50 *Bättre möjligheter att verkställa frihetsberövanden.*

SOU 2021:91 *En ny rymdlag.*

Ds 2005:6 s. 282 *Brott och brottsutredning i IT-miljö. Europarådets konvention om IT-relaterad brottslighet med tilläggsprotokoll.*

Ds 2017:53 *Rätten till offentlig försvarare – Genomförande av EU:s rättshjälpsdirektiv.*

Ds 2020:12 *Registrering av kontantkort, m.m.*

Propositioner och regeringens skrivelser

Prop. 1971:30 del 2 *Förslag till lag om allmänna förvaltningsdomstolar, m.m.*

Prop. 1979/80:2 del A *Förslag till sekretesslag m.m.*

Prop. 1992/93:200 *Om en telelag och en förändrad verksamhetsform för Televerket, m.m.*

Prop. 1994/95:227 *Hemlig teleavlyssning och hemlig teleövervakning.*

Prop. 1995/96:180 *Teleoperatörernas skyldigheter vid hemlig teleavlyssning och hemlig teleövervakning.*

Prop. 2002/03:74 *Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering.*

Prop. 2002/03:110 *Lag om elektronisk kommunikation, m.m.*

Prop. 2005/06:178 *Hemlig rumsavlyssning.*

Prop. 2008/09:201 *Förstärkt integritetsskydd vid signalspaning.*

Prop. 2009/10:80 *En reformerad grundlag.*

Prop. 2008/09:150 *Offentlighets- och sekretesslag.*

Prop. 2009/10:87 *Skyddslagen.*

Prop. 2010/11:46 *Lagring av trafikuppgifter för brottsbekämpande ändamål - genomförande av direktiv 2006/24/EG.*

Prop. 2011/12:55 *De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation.*

Prop. 2012/13:132 *Tolkning och översättning i brottmål.*

Prop. 2016/17:180 *En modern och rättssäker förvaltning – ny förvaltningslag.*

Prop. 2016/17:218 *Nya regler om bevisinhämtning inom EU.*

Prop. 2018/19:71 *Genomförandet av barnrättsdirektivet och några andra straffprocessuella frågor.*

Prop. 2018/19:86 *Datalagring vid brottsbekämpning – anpassningar till EU-rätten.*

Prop. 2018/19:163 *Ny lag om Säkerhetspolisens behandling av personuppgifter.*

Prop. 2019/20:15 *Skydd av Sveriges säkerhet vid radioanvändning.*

Prop. 2019/20:64 *Hemlig dataavläsning.*

Prop. 2020/21:72 *Sveriges tillträde till Europarådets konvention om it-relaterad brottslighet.*

Prop. 2021/22:183 *Registrering av kontantkort – förbättrad tillgång till uppgifter för brottsbekämpande myndigheter.*

Prop. 2021/22:131 *Nytt regelverk för kvalificerade säkerhetsärenden.*

Prop. 2021/22:119 *Modernare regler för användningen av tvångsmedel.*

Prop. 2021/22:136 *Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation.*

Prop. 2021/22:183 *Registrering av kontantkort – förbättrad tillgång till uppgifter för brottsbekämpande myndigheter.*

Skr. 2020/21:59 *Redovisning av användningen av hemliga tvångsmedel under 2019.*

Utskottsbetänkanden

Bet. 2018/19: JuU2 *Datalagring vid brottsbekämpning – anpassningar till EU-rätten.*

Bet. 2020/21:JuU16 *Sveriges tillträde till Europarådets konvention om it-relaterad brottslighet.*

Bet. 2021/22:JuU24 *Processrättsliga frågor.*

Bet. 2021/22: JuU34 *Registrering av kontantkort – förbättrad tillgång till uppgifter för brottsbekämpande myndigheter.*

Rättsfall och myndighetspraxis

EU-domstolen

UPC Nederland, mål C-518/11, 7 november 2013.

UPC DTH, mål C-475/12, 30 april 2014.

Åkerberg Fransson, mål C-617/10, 26 februari 2013.

Tele2 Sverige AB, mål C-203/15, och *Tom Watson m.fl.* mål C-698/15, 21 december 2016.

Digital Rights Ireland Ltd, mål C-293/12, och Kärntner Landesregierung m.fl., mål C-594/12, 8 april 2014.

Ministerio Fiscal, mål C-207/16, 2 oktober 2018.

La Quadrature du Net m.fl. mål C-511/18 och C-512/18 och *Ordre des barreaux francophones et germanophone* m.fl. mål C-520/18, 6 oktober 2020.

Privacy International, C-623/17, 6 oktober 2020.

Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), mål C-746/18, 2 mars 2021.

M.I.C.M. mål C-597/19, 17 juni 2021.

Commissioner of An Garda Síochána, mål C-140/20, 5 april 2022.

SpaceNet, mål C-793/19 och *Telekom Deutschland GmbH* C-794/19, 20 september 2022.

Europadomstolen

K.U. mot Finland, mål 2872/02, 2 december 2008.

Roman Zakharov mot Ryssland, mål 47143/06, 4 december 2015.

Big Brother Watch m.fl. mot Förenade Kungariket, mål 58170/13, 62322/14 och 24960/15, 13 september 2018.

Centrum för Rättvisa mot Sverige, mål 35252/08, 25 maj 2021.

Högsta domstolen

Högsta domstolens beslut i mål Ö 5686.22.

Högsta förvaltningsdomstolen

HFD 2021 ref. 23.

Övriga domstolar

The SS Lotus (France v. Turkey), Series A, No. 9/10, Permanent Court of International Justice, PCIJ, 1927.

Yahoo! Inc [2015] Court of Cassation of Belgium, Nr. P.13.2082.N.

United States v. Kreuger, 809 F3d 316 (1st Cir. 2017).

Myndigheter

PTS:s beslut den 17 mars 2021 i ärende dnr 20-3144.

Litteratur

Linderfalk, Ulf (2012), *Folkrätten i ett nötskal*, 2:e uppl., Studentlitteratur.

Danelius, Hans (2015) *Mänskliga rättigheter i europeisk praxis*,

5:e uppl., Norstedts juridik.

Ove Bring m.fl. (2020) *Sverige och folkrätten*, JUNO version 6.

Lenberg Eva, Tansjö Anna och Geijer Ulrika (2022), *Offentlighets- och sekretesslagen*, JUNO version 26.

Lindberg, Gunnel (2022) *Straffprocessuella tvångsmedel*, JUNO version 5.

Peter Fitger m.fl. (2022), *Rättegångsbalken*, JUNO version 93.

Övrigt

Directorate-General for Internal Policies: *Over-the-Top players [OTTs]*, Study for the IMCO Committee, 2015.

Europeiska unionens råd: *Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace*, 2016.

Brå: *It-inslag i brottsligheten och rättsväsendets förmåga att hantera dem*, 2016:17.

Regeringskansliet: *Nationell säkerhetsstrategi*, 2017.

Journal of Information Technology and Control (ITC 3/46), *Location Accuracy of Commercial IP Address Geolocation Databases*, 2017.

Rådet för de europeiska advokatsamfunden (CCBE): *Recommendations on the protection of fundamental rights in the context of 'national security'*, 2019.

Polismyndigheten: Myndighetsgemensam lägesbild om organiserad brottslighet 2019, A457.772/2019.

Integritetsskyddsmyndigheten: Integritetsrapport 2020, 2021:1.

PTS: *Koppla upp till internet med framtidssäkra IPv6-adresser*, PTS-ER-2021:11.

Internetstiftelsen, *Svenskarna och internet 2021*, oktober 2021.

PTS: *Tillhandahållande av IPv6 i fasta allmänna kommunikationsnät i Sverige 2022*, PTS-ER-2022:21.

Internetstiftelsen, *Svenskarna och internet 2022*, oktober 2022.

Regeringskansliet*: Förordning för att bekämpa sexuella övergrepp mot barn*, Faktapromemoria 2021/22:FPM99.

Åklagarmyndigheten: *Åklagarmyndighetens rättsliga vägledning Territorialitetsprincipen vid HDA*, 2022:13.

Kommittédirektiv 2021:58

Datalagring vid brottsbekämpning – ytterligare åtgärder för en modern och ändamålsenlig reglering

Beslut vid regeringssammanträde den 5 augusti 2021

Sammanfattning

En särskild utredare ska 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. Uppdraget syftar till att säkerställa att de brottsbekämpande myndigheternas tillgång till information förbättras och upprätthålls över tid i takt med teknikutvecklingen och förändrade kommunikationsvanor, samtidigt som respekten för mänskliga rättigheter säkerställs.

Utredaren ska bl.a.

- analysera förutsättningarna för att leverantörer av s.k. OTT-tjänster ska kunna omfattas av skyldigheten att lagra och ge tillgång till uppgifter om elektronisk kommunikation samt ta ställning till om en sådan skyldighet bör införas,
- analysera och föreslå moderniseringar av regleringen när det gäller tjänsteleverantörers skyldighet att anpassa sin verksamhet så att hemliga tvångsmedel kan verkställas på ett effektivt sätt,
- analysera och utvärdera nuvarande reglering om lagring av och tillgång till uppgifter om elektronisk kommunikation i förhållande till bl.a. ny praxis från EU-domstolen och ta ställning till om regelverket behöver förändras, och

- analysera vissa frågor om jurisdiktion, inklusive folkrättsliga överväganden, i förhållande till elektronisk information som finns eller kan finnas utanför Sverige och ta ställning till om det bör införas en särskild lagreglering för exekutiv jurisdiktion.

Utredaren ska föreslå de författningsändringar och andra åtgärder som behövs.

Uppdraget ska redovisas senast den 6 februari 2023.

Behovet av åtgärder

Teknikutvecklingen och nya kommunikationsvanor leder till en förändrad spelplan

De brottsbekämpande myndigheterna behöver ha tillgång till ändamålsenliga och verkningsfulla verktyg för att kunna förhindra, upptäcka, utreda och lagföra brott. Brottsligheten är i förändring, liksom kriminellas handlingssätt och hur de kommunicerar. Detta har medfört att de brottsbekämpande myndigheternas behov av att kunna använda hemliga tvångsmedel har ökat. Brott som begås inom ramen för kriminella nätverk är ofta svåra att utreda eftersom brottsoffer och vittnen av olika anledningar kan vara obenägna att lämna information till de brottsbekämpande myndigheterna. Tillgång till information och bevisning från elektroniska kommunikationer är ofta av stor betydelse i utredningar av allvarlig brottslighet. Också brottslighet som begås över internet är till sin natur sådan att uppgifter om elektroniska kommunikationer i regel är avgörande för utredningens framgång.

Den tekniska utvecklingen och nya kommunikationsmönster har gjort att mycket av den information som tidigare varit tillgänglig för brottsbekämpande myndigheter inte längre går att komma åt. Det blir allt vanligare att kommunikation sker genom tjänster som inte omfattas av någon rättslig skyldighet att lagra och tillhandahålla uppgifter, nämligen via tjänster som tillhandahålls av andra än de traditionella teleoperatörerna. Sådana tjänster kallas OTT-tjänster (over the top) eller nummeroberoende interpersonella kommunikationstjänster. Exempel på OTT-tjänster är Apple Imessage och Facetime, Facebook Messenger och Whatsapp.

Användningen av de tjänster som direkt tillhandahålls av teleoperatörerna – främst telefonsamtal och sms – har minskat till förmån för kommunikation genom tjänster som tillhandahålls av andra än operatörerna, men vars information överförs genom bland annat teleoperatörernas nät. Enligt statistik från Post- och telestyrelsen ökade användningen av sms till och med 2010, då det genomsnittliga antalet sms som skickades från mobiltelefon per samtalsabonnemang och månad var 139, för att därefter minska. År 2020 uppgick det genomsnittliga antalet till 44. Enligt en rapport från en arbetsgrupp vid Europaparlamentet förväntades OTT-tjänster stå för närmare 90 procent av alla elektroniska kommunikationsmeddelanden 2020 (Directorate-General for Internal Policies, Over-the-Top players [OTTs], Study for the IMCO Committee, 2015, s. 43).

Det pågår även en utveckling av de tjänster som tillhandahålls av teleoperatörerna, som kan komma att påverka de brottsbekämpande myndigheternas verktyg. Införandet av 5G kan till exempel medföra tillämpning av krypterings- och autentiseringsprocesser som riskerar att väsentligt försvåra möjligheterna att verkställa hemliga tvångsmedel. Den standard för roaming som kan bli aktuell riskerar också att försvåra eller omöjliggöra verkställande av hemlig avlyssning och hemlig övervakning av utländska abonnemang i Sverige.

Information lagras allt oftare på andra platser än hos användaren och inte sällan utomlands. Informationen kan ständigt förflyttas eller finnas på flera platser samtidigt, vilket gör det omöjligt att bestämma en specifik plats där informationen finns. Den traditionella tolkningen av territorialitetsprincipen har inneburit att informationens fysiska belägenhet är avgörande för om brottsbekämpande myndigheter har jurisdiktion att hämta in den. Tolkningen gjordes innan informationssamhället antog sin nuvarande form och är alltså inte anpassad för dagens tekniska verklighet. Internationellt går fler länder mot att andra anknytningsmoment får betydelse för jurisdiktionen, såsom den misstänktes hemvist, platsen där brottet begåtts eller hemvistet för den som förfogar över användarkontot. 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 det är okänt var den finns. Det finns därför skäl att överväga om det, med beaktande av folkrättsliga aspekter, bör lagstiftas

om exekutiv jurisdiktion som baseras på andra anknytningsfaktorer än den plats där informationen lagras.

Regleringen behöver anpassas efter de brottsbekämpande myndigheternas behov i den nya tekniska verkligheten

De hemliga tvångsmedlen utgörs bl.a. av hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. De båda tvångsmedlen får användas såväl under en förundersökning som innan en förundersökning har inletts, dvs. i underrättelseverksamhet. Dessa tvångsmedel regleras i rättegångsbalken (RB), lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen) och lagen (1991:572) om särskild utlänningskontroll (LSU). Även lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) har regler om inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet. Hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan också aktualiseras inom ramen för Sveriges internationella samarbete enligt lagen (2017:1000) om en europeisk utredningsorder och lagen (2000:562) om internationell rättslig hjälp i brottmål.

Bestämmelserna om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation i rättegångsbalken är i sig teknikneutrala och således inte begränsade till en viss typ av teknik för att befordra meddelanden. Enligt reglerna får meddelanden avlyssnas eller övervakas om de överförs eller har överförts i ett elektroniskt kommunikationsnät till eller från ett telefonnummer eller annan adress. Huruvida det är fråga om fast telefoni, mobiltelefoni eller kommunikation över internet har alltså ingen betydelse för frågan om meddelandet som sådant faller under tvångsmedelsregleringen.

Det svenska regelverket för elektronisk kommunikation finns huvudsakligen i lagen (2003:389) om elektronisk kommunikation (LEK). De tjänsteleverantörer som i dag omfattas av regelverket är framför allt traditionella teleoperatörer. I lagen om elektronisk kommunikation finns bl.a. bestämmelser om hur tjänsteleverantörerna ska lagra viss information samt anpassa sin verksamhet så att hemliga tvångsmedel kan verkställas. Tjänsteleverantörerna har också en skyl-

dighet att lämna ut vissa s.k. abonnemangsuppgifter till olika myndigheter för vissa ändamål, t.ex. till brottsbekämpande myndigheter vid misstanke om brott.

Genom propositionen Datalagring vid brottsbekämpning – anpassningar till EU-rätten (prop. 2018/19:86) trädde den 1 oktober 2019 nya regler om datalagring i kraft. Ändringarna innebär bl.a. att lagringens omfattning har begränsats och att lagringstiderna har differentierats. I förarbetena uttalade regeringen att det senast inom fyra år efter ikraftträdandet kunde finnas anledning att se över de föreslagna ändringarna, bl.a. mot bakgrund av den tekniska utvecklingen, ändrade kommunikationsvanor och nya mål om datalagring i EU-domstolen (samma prop. s. 38 och 108). Som beskrivits inledningsvis har teknikutvecklingen och kommunikationsvanorna förändrat de brottsbekämpande myndigheternas förutsättningar påtagligt. I oktober 2020 kom också EU-domstolen med nya avgöranden på området. Mot denna bakgrund finns det skäl att redan nu inleda den aviserade översynen av regelverket.

Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (e-kodexdirektivet) ska genomföras i Sverige. Genom e-kodexdirektivet inrättas ett harmoniserat ramverk för bl.a. elektroniska kommunikationsnät och tjänster. En nyhet är att definitionen av elektroniska kommunikationstjänster utvidgas till att även omfatta OTT-tjänster. För att genomföra direktivet pågår ett arbete med att ta fram ett förslag till en ny lag som ska ersätta den nuvarande lagen om elektronisk kommunikation. Promemorian Genomförande av direktivet om inrättande av en kodex för elektronisk kommunikation har tagits fram inom Regeringskansliet och remitterats. Promemorians lagförslag omfattar, liksom e-kodexdirektivet, i vissa delar OTT-tjänster. Frågorna om lagringsskyldighet, anpassningsskyldighet och skyldighet att lämna ut uppgifter behandlas dock inte i e-kodexdirektivet. Lagförslaget innebär därför inte någon skyldighet för de som tillhandahåller OTT-tjänster att lagra eller ge tillgång till uppgifter om elektronisk kommunikation för brottsbekämpande syften. Det finns därför anledning att se över regelverket för att förbättra de brottsbekämpande myndigheternas möjligheter att utföra sina uppdrag. Med hänsyn till den snabba tekniska utvecklingen är det angeläget att regleringen, så långt det är möjligt, är teknikneutral för att kunna stå sig över tid.

Utredaren bör överväga hur brottsbekämpningens behov kan mötas på ett sätt som säkerställer mänskliga rättigheter och rättssäkerheten

Regleringen av hemliga tvångsmedel har utformats efter en avvägning mellan å ena sidan samhällets behov av en effektiv brottsbekämpning till skydd för medborgarna och å andra sidan den enskildes rätt till privatliv och rättssäkerhet i förhållande till staten.

Regeringsformen (RF) garanterar den enskilde ett skydd i förhållande till det allmänna mot bl.a. husrannsakan och liknande intrång, hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Skyddet omfattar även betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden (2 kap. 6 § RF). Dessa grundläggande fri- och rättigheter får begränsas endast genom lag och endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningarna får aldrig gå utöver vad som är nödvändigt eller utgöra ett hot mot den fria åsiktsbildningen (2 kap. 20 och 21 §§ RF).

Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) är inkorporerad i svensk lag. Enligt artikel 8.1 i Europakonventionen har var och en rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens, vilket bl.a. omfattar skydd mot övervakning i olika former. Tvångsmedel som innefattar ingrepp i området som artikel 8 skyddar kan enligt konventionen endast godtas om de har stöd i lag och omfattas av de undantag som anges i artikel 8.2. Undantagen avser t.ex. åtgärder som i ett demokratiskt samhälle är nödvändiga för att upprätthålla den allmänna säkerheten och för att förebygga brott. Artikel 8 innebär också att staten har ett ansvar för att skydda enskildas privatliv och personliga integritet mot intrång som begås av andra enskilda. En förutsättning för att staten ska kunna leva upp till kravet på att upprätthålla rättstryggheten för enskilda är att det finns en väl fungerande och effektiv brottsbekämpning.

EU:s stadga om de grundläggande rättigheterna gäller när unionsrätten utformas och tillämpas. Enligt artikel 7 i stadgan har var och en rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Vidare anges i artikel 8 att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. I det sam-

manhanget kan tekniska skyddslösningar såsom kryptering vara en viktig faktor för att säkerställa skyddet av mänskliga rättigheter.

FN:s konvention om barnets rättigheter (barnkonventionen) är inkorporerad i svensk lag. Enligt artikel 16 får inget barn utsättas för godtyckliga eller olagliga ingripanden i sitt privat- och familjeliv, sitt hem eller sin korrespondens och inte heller för olagliga angrepp på sin heder och sitt anseende. Vidare framgår av artikel 3 i barnkonventionen att vid samtliga åtgärder och beslut som rör barn ska i första hand beaktas vad som bedöms vara barnets bästa. Enligt artikel 19 ska barn skyddas från alla former av fysiskt eller psykiskt våld, inklusive misshandel, utnyttjande och sexuella övergrepp. Det ska finnas effektiva medel för bl.a. förebyggande, identifiering, undersökning och uppföljning samt förfaranden för rättsligt ingripande om barn farit illa.

För all tvångsmedelsanvändning gäller ändamålsprincipen, behovsprincipen och proportionalitetsprincipen. Ändamålsprincipen innebär att en myndighets befogenhet att använda ett tvångsmedel ska vara bundet till det ändamål för vilket tvångsmedlet har beslutats. Enligt behovsprincipen får en myndighet använda ett tvångsmedel bara när det finns ett påtagligt behov av det och en mindre ingripande åtgärd inte är tillräcklig. Proportionalitetsprincipen innebär att ett tvångsmedel får användas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller något annat motstående intresse.

Regelverket om hemliga tvångsmedel innehåller även flera rättssäkerhetsgarantier. Förhandsprövning av domstol är en sådan. Huvudregeln är att domstol prövar frågor om hemliga tvångsmedel innan de får användas och domstolen har dessutom möjlighet att ange närmare villkor för tvångsmedelsanvändningen i syfte att säkerställa att enskildas personliga integritet inte kränks utöver vad som är nödvändigt. Förutom den föregående prövningen av domstol finns olika former av tillsyn som genomförs av Säkerhets- och integritetsskyddsnämnden, Justitiekanslern, Riksdagens ombudsmän och Integritetsskyddsmyndigheten.

De brottsbekämpande myndigheternas befogenheter att med stöd av hemliga tvångsmedel bereda sig tillgång till information om en enskild innebär ett ingrepp i den enskildes personliga integritet.

Utredaren ska därför

- noga väga behovet av en effektiv brottsbekämpning mot den enskildes rätt till skydd för sin personliga integritet,
- analysera förslagens påverkan på skyddet för mänskliga rättigheter, inklusive rätten till respekt för privatlivet,
- ta ställning till om skyddet för privat- och familjelivet respektive den personliga integriteten bör stärkas, och
- se till att de förslag som lämnas uppfyller högt ställda krav på rättssäkerhet.

Uppdraget att modernisera förutsättningarna för datalagring och åtkomst till data från OTT-tjänster

Hemlig övervakning av elektronisk kommunikation och datalagringens praktiska betydelse

Med stöd av bl.a. 27 kap. 19 § RB kan hemlig övervakning av elektronisk kommunikation tillåtas under vissa förutsättningar. Genom hemlig övervakning av elektronisk kommunikation kan brottsbekämpande myndigheter inom ramen för en förundersökning få tillgång till bl.a. information om meddelanden (annat än innehållet), vilka elektroniska kommunikationsutrustningar som varit i ett visst område vid ett visst tillfälle och i vilket område en viss elektronisk kommunikationsutrustning finns eller har funnits. Också lagen om särskild utlänningskontroll och preventivlagen medger användning av hemlig övervakning av elektronisk kommunikation genom hänvisningar till rättegångsbalkens bestämmelser.

Utöver tvångsmedelsregleringen i rättegångsbalken finns det i inhämtningslagen bestämmelser som ger Polismyndigheten, Säkerhetspolisen eller Tullverket möjlighet att i underrättelseverksamhet hämta in uppgifter från den som enligt lagen om elektronisk kommunikation tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Det gäller bl.a. uppgifter om meddelanden som i ett elektroniskt kommunikationsnät har överförts till eller från ett telefonnummer eller annan adress.

Myndigheternas faktiska möjligheter att komma framåt med sitt arbete för att förhindra, upptäcka, utreda och lagföra brottslighet

med hjälp av bl.a. hemlig övervakning av elektronisk kommunikation är beroende av att uppgifterna som behövs finns lagrade hos en aktör som går att nå med hjälp av tvångsmedlet. Av denna anledning finns det regler som innebär en skyldighet för teleoperatörer att lagra uppgifter om elektronisk kommunikation, s.k. datalagring.

Enligt 6 kap. 16 a § LEK ska den som bedriver ett allmänt kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning eller en allmänt tillgänglig elektronisk kommunikationstjänst lagra uppgifter som behövs för brottsbekämpande verksamhet. Skyldigheten omfattar uppgifter 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. Någon skyldighet att lagra innehållet i en kommunikation finns inte.

OTT-tjänster omfattas för närvarande inte av begreppet elektronisk kommunikationstjänst och att tillhandahålla en OTT-tjänst är inte heller att betrakta som bedrivande av ett allmänt kommunikationsnät. Sådana tjänsteleverantörer har således inte någon lagringsskyldighet enligt gällande rätt.

I 6 kap. 20 § första stycket 1 LEK föreskrivs tystnadsplikt för den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har fått del av eller tillgång till s.k. abonnemangsuppgifter. Med abonnemangsuppgifter avses t.ex. uppgifter om abonnentens nummer, namn, titel och adress (prop. 1992/93:200 s. 164). Vidare har det ansetts innefatta ip-adresser och IMSI-nummer, vilket är ett nummer som är kopplat till abonnentens simkort och därmed telefonnummer (se t.ex. prop. 2011/12:55 s. 101 och Kammarrätten i Stockholms dom den 19 januari 2010 i RK 2010:1). Post- och telestyrelsen har inom ramen för sin tillsyn av skyldigheten att lämna ut uppgifter om IMEI-nummer till brottsbekämpande myndigheter bedömt att uppgifter om IMEI-nummer är att anse som uppgift om abonnemang, när det tydligt framgår av begäran att syftet är att identifiera ett abonnemang eller en abonnent. I 6 kap. 22 § LEK finns bestämmelser som anger under vilka förutsättningar som abonnemangsuppgifter ska lämnas ut till vissa myndigheter och regionala alarmeringscentraler. Utlämnande av abonnemangsuppgifter får exempelvis ske i brottsbekämpande syfte, för att kunna delge personer som håller sig undan eller för att leta

efter försvunna personer vars liv eller hälsa är i fara. I det sistnämnda syftet kan även annan uppgift som angår ett särskilt elektroniskt meddelande lämnas ut.

Skyldigheten att lämna ut abonnemangsuppgifter m.m. gäller den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Eftersom OTT-tjänster i dag inte omfattas av begreppet elektronisk kommunikationstjänst i lagen om elektronisk kommunikation kan myndigheterna inte, med stöd av den bestämmelsen, få ut information om t.ex. vem som är avsändare av ett meddelande från en sådan tjänsteleverantör.

Utredaren bör se över regelverket i förhållande till OTT-tjänster

Det är angeläget att teknikutvecklingen och ändrade kommunikationsvanor inte innebär försämrade möjligheter för de brottsbekämpande myndigheternas arbete. Som framgått ovan ska, med anledning av genomförandet av e-kodexdirektivet, definitionen av elektronisk kommunikationstjänst enligt det remitterade förslaget till ny lag om elektronisk kommunikation vara vidare än i dag och kommer att omfatta de s.k. OTT-tjänsterna. När det gäller lagringsskyldigheten och skyldigheten att lämna ut abonnemangsuppgifter och annan uppgift som angår ett särskilt elektroniskt meddelande föreslås, på grund av e-kodexdirektivets omfattning, att bestämmelserna ska föras över till den nya lagen utan ändring i sak. Detta innebär att något ställningstagande till frågan om lagring och utlämnande av uppgifter från OTT-tjänsteleverantörer inte görs inom ramen för det lagstiftningsprojektet. Även vad gäller inhämtningslagen föreslås att bestämmelserna ska ha samma tillämpningsområde som hittills. Det innebär att också förutsättningarna att hämta in uppgifter enligt inhämtningslagen kvarstår oförändrade i förhållande till OTT-tjänster. Polismyndigheten, Säkerhetspolisen och Åklagarmyndigheten har, i sina remissvar med anledning av förslaget till ny lag om elektronisk kommunikation, uppgett att den tekniska utvecklingen och ändrade kommunikationsvanor medför att det är mycket angeläget att frågan utreds och att OTT-tjänster bör omfattas av regleringen. Ekobrottsmyndigheten har framfört liknande synpunkter. Det finns således behov av att modernisera lagstiftningen i syfte att även OTT-tjänsteleverantörer ska omfattas av skyldigheterna att lagra och lämna ut upp-

gifter om elektroniska kommunikationer. En sådan modernisering skulle innebära att brottsbekämpande myndigheter kan förbättra möjligheterna att komma åt uppgifter om elektronisk kommunikation som de på grund av teknikutvecklingen och ändrade kommunikationsvanor har förlorat.

Utöver ovannämnda skyldigheter att lagra och lämna ut uppgifter finns flera bestämmelser i lagen om elektronisk kommunikation som kan vara av betydelse för att OTT-tjänster ska omfattas av regelverket på ett konsekvent sätt, såsom krav på säkerhet (6 kap. 3–4 b §§ LEK), tystnadsplikt (6 kap. 20–23 §§), villkor för behandling (6 kap. 5–10 a §§) och föreläggande att bevara elektronisk information (6 kap. 16 g §). I lagen (2020:62) om hemlig dataavläsning finns också bestämmelser om medverkansskyldighet och tystnadsplikt (24 och 32 §§). Utredaren bör även se över hur dessa bestämmelser ska förhålla sig till OTT-tjänsteleverantörer.

Hur vissa EU-rättsliga termer förhåller sig till nationella termer kan även behöva klarläggas. Ett exempel på detta är hur det EU-rättsliga begreppet ”trafikuppgift” förhåller sig till begreppet ”annan uppgift som angår ett särskilt elektroniskt meddelande” som finns i 6 kap. 20 § LEK (som flera andra bestämmelser hänvisar till), samt den närmare omfattningen av begreppet abonnemangsuppgifter i förhållande till exempelvis s.k. NAT-teknik, där många användare kan dela på samma ip-adress.

I kommissionens förslag till en förordning om tillgång till e-bevisning (COM(2018) 225) finns också vissa förslag som har koppling till frågan om tillgång till uppgifter från bl.a. OTT-tjänsteleverantörer. I förordningen föreslås införande av s.k. europeiska utlämnandeordrar som kommer att medföra en möjlighet för en rättslig myndighet i en medlemsstat att utfärda en order om utlämnande av elektronisk bevisning mot en tjänsteleverantör i en annan medlemsstat. I förordningen föreslås ingen skyldighet för tjänsteleverantörer att lagra data. Däremot finns förslag till s.k. europeiska bevarandeordrar. De innebär att en rättslig myndighet i en medlemsstat kan beordra en tjänsteleverantör i en annan medlemsstat att under en viss tid bevara vissa uppgifter medan en framställan om utlämnande av de aktuella uppgifterna tas fram. Även om förordningen som sådan kommer att vara direkt tillämplig i Sverige kan den medföra behov av en översyn av svensk rätt, innefattande de regler som nu blir föremål för utredning. Det är därför viktigt att utredaren bevakar utveck-

lingen i dessa förhandlingar och eventuellt kommande lagstiftningsprojekt.

Utredaren ska därför

- analysera förutsättningarna, även ur ett tekniskt perspektiv, för att OTT-tjänsteleverantörer ska kunna omfattas av skyldigheterna att lagra och lämna ut uppgifter om elektroniska kommunikationer, och
- lämna förslag på de författningsändringar och andra åtgärder som bedöms nödvändiga.

Uppdraget att modernisera anpassningsskyldigheten

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 sådan. För att underlätta för de brottsbekämpande myndigheterna har tjänsteleverantörerna ålagts vissa skyldigheter. I 6 kap. 19 § LEK föreskrivs den s.k. anpassningsskyldigheten. Enligt denna bestämmelse ska verksamheten bedrivas så att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas och att det kan ske på ett sådant sätt att verkställandet inte röjs. Innehållet i och uppgifter om avlyssnade eller övervakade meddelanden ska göras tillgängliga så att informationen enkelt kan tas om hand. Bestämmelserna om anpassningsskyldighet är i praktiken ofta en förutsättning för att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation över huvud taget ska kunna verkställas och att verkställandet kan ske i nära anslutning till tvångsmedelsbeslutet.

Anpassningsskyldigheten gäller i fråga om uppgifter som hämtas in efter beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation med stöd av rättegångsbalken, inhämtningslagen, preventivlagen eller lagen om särskild utlänningskontroll.

Det finns också särskilda regler om anpassning för utlämnande för den som är skyldig att lagra uppgifter enligt 6 kap. 16 a § LEK. Även här gäller att uppgifterna ska göras tillgängliga på ett sådant sätt att

informationen enkelt kan tas om hand (se 6 kap. 16 f §). Anpassningsskyldigheten enligt 6 kap. 16 f och 19 §§ gäller emellertid endast för vissa särskilt angivna verksamheter och träffar i huvudsak traditionella telekomleverantörer. De omfattar inte t.ex. OTT-tjänsteleverantörer. Det inbördes förhållandet mellan lagrings- och anpassningsskyldigheten kan också leda till tolkningsproblem. Lagringsskyldigheten omfattar i dag fler tjänsteleverantörer än de som är anpassningsskyldiga enligt 6 kap. 19 § LEK. Detta eftersom lagringsskyldigheten inte, såsom anpassningsskyldigheten, är begränsad vad gäller telefonitjänster till att avse samtal inom en nationell eller internationell nummerplan. Lagringsskyldigheten innehåller inte heller några begränsningar vad gäller tjänster för datakommunikation. Det kan t.ex. innebära att internetleverantörer som inte tillhandahåller telefonitjänster kan omfattas av lagringsskyldigheten enligt 6 kap. 16 a § utan att omfattas av anpassningsskyldigheten i 6 kap. 19 §.

I juni 2020 överlämnades departementspromemorian Registrering av kontantkort, m.m. (Ds 2020:12). I promemorian föreslås, utöver registrering av kontantkort, bl.a. en omarbetning av anpassningsskyldigheten i 6 kap. 19 § andra stycket LEK på så sätt att uppgifter som lämnas ut till brottsbekämpande myndigheter ska ordnas och göras tillgängliga i ett format som gör det möjligt att enkelt ta hand om dem. När det gäller bestämmelserna om anpassningsskyldighetens omfattning i 6 kap. 19 § första stycket LEK konstaterar utredaren att den teknikutveckling som pågått länge och som fortfarande pågår innebär att bestämmelsen blivit oklar och ålderdomlig samt att det vore önskvärt att bestämmelsen förtydligades och formulerades på ett så teknikneutralt sätt som möjligt. Utredaren anser också att det vore lämpligt att utforma bestämmelserna om anpassningsskyldighet i 6 kap. 19 § första stycket och lagringsskyldighet enligt 6 kap. 16 a § så att de träffar samma aktörer, men lämnar inget förslag i denna del. I sina remissvar med anledning av promemorian har Polismyndigheten, Säkerhetspolisen, Tullverket och Post- och telestyrelsen uttalat att det är angeläget att frågan blir föremål för utredning. Promemorian bereds inom Regeringskansliet.

Som framgår ovan ska definitionen av elektronisk kommunikationstjänst enligt det remitterade förslaget till ny lag om elektronisk kommunikation vara vidare än i dag och även omfatta OTT-tjänster. När det gäller anpassningsskyldigheten föreslås att dessa bestämmelser ska föras över till den nya lagen utan ändring i sak. Därför kvar-

står de oklarheter som påpekas i promemorian Registrering av kontantkort, m.m. Det är angeläget att anpassningsskyldighetens omfattning är tydlig, modern och anpassad efter brottsbekämpningens behov. Det bör därför utredas hur anpassningsskyldighetens utformning bör se ut framöver och om OTT-tjänster kan omfattas av denna skyldighet.

Därtill behöver det utredas om introduktionen av 5G medför behov av förändringar av anpassningsskyldigheten. 5G kan exempelvis medföra tillämpningar av flera krypterings- och autentiseringsprocesser som riskerar att väsentligt försvåra möjligheten att verkställa hemliga tvångsmedel. Bland annat har 5G en inbyggd möjlighet till så kallad totalsträckskryptering (eng. end-to-end encryption, E2EE). Totalsträckskryptering skulle väsentligt försvåra för brottsbekämpande myndigheter att få tillgång till elektronisk kommunikation trots domstolsbeslut om tillstånd till hemlig övervakning av elektronisk kommunikation eller hemlig avlyssning av elektronisk kommunikation. Det kommer också vara möjligt att kryptera IMSI-nummer i 5G-nätet. Detta skulle göra det närmast omöjligt för brottsbekämpande myndigheter att identifiera enskilda enheter eller var vissa personer, såsom misstänkta gärningsmän, befinner sig. Kringinformation (metadata) som normalt är tillgänglig via hemlig övervakning av elektronisk kommunikation – såsom plats, datum, tid, samtalslängd, samtal och motpart – skulle därmed kunna gå förlorad för brottsbekämpande myndigheter.

Ytterligare en fråga som kan ha betydelse för anpassningsskyldigheten är hur internationell roaming sker. Internationell roaming kan i såväl 5G-mobilnätet som befintliga mobilnät ske enligt flera olika standarder. Antingen kan informationen hanteras av operatören i landet som simkortet är uppkopplat mot, eller så kan informationen omedelbart vidarebefordras till simkortets operatör i hemlandet. I det senare fallet, s.k. S8 Home Routing som redan är standard i 4G-näten, behandlas en mycket begränsad mängd information av operatören i det land som simkortet, och därmed användaren, befinner sig i. Beroende på vilken lösning som tillämpas kan information som härrör från utländska simkort som finns i Sverige bli otillgänglig eller svår att få tillgång till för de brottsbekämpande myndigheterna. Frågan har lyfts i internationella sammanhang men hittills har någon lösning inte föreslagits.

Sammanfattningsvis är det angeläget att anpassningsskyldighetens omfattning är tydlig, modern och tillgodoser brottsbekämpningens

behov. Samtidigt behöver regleringen vara välavvägd så att teknikutvecklingen främjas, nätsäkerheten bibehålls och företagen inte påförs orimliga bördor. Kryptering är centralt för säkerheten i ett läge där allt större delar av industri, samhälle och stat är sammanlänkade genom elektronisk kommunikation. Föreslagna åtgärder får inte innebära att generella sårbarheter införs i kryptering eller att systematiska bakdörrar introduceras.

Utredaren ska därför

- analysera anpassningsskyldighetens omfattning och ta ställning till hur en reglering kan utformas på ett så tydligt, enhetligt, säkert och teknikneutralt sätt som möjligt,
- analysera behovet av lagstiftning eller andra åtgärder i fråga om anpassningsskyldigheten så att hemliga tvångsmedel kan verkställas på ett effektivt sätt även i framtiden, och
- lämna förslag på de författningsändringar och andra åtgärder som bedöms nödvändiga.

Uppdraget att se över datalagringsregleringen utifrån bl.a. ny domstolspraxis

Ändrad svensk datalagringslagstiftning och behovet av en uppföljande översyn

EU-rätten sätter upp ramarna för nationell lagstiftning om datalagring för brottsbekämpande ändamål. Europaparlamentets och rådets direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv 2002/58) 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. brottsbekämpande verksamhet. Direktivet är genomfört i svensk rätt främst genom bestämmelser i lagen om elektronisk kommunikation. Kommissionen lämnade i januari 2017 ett förslag på en förordning om integritet och elektronisk kommunikation (COM(2017) 10) (eDataskyddsförordning) som ska ersätta direktiv 2002/58. Förslaget förhandlas fortfarande.

I samband med att EU-domstolen i Digital Rights-domen den 8 april 2014 (förenade målen C-293/12 och C-594/12) ogiltigförklarade det s.k. datalagringsdirektivet (Europaparlamentets och rådets direktiv 2006/24/EG om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG) ifrågasattes de svenska datalagringsreglerna. Kammarrätten i Stockholm begärde därför ett förhandsavgörande från EU-domstolen (Kammarrättens mål nr 7380-14). EU-domstolen besvarade begäran genom en dom den 21 december 2016 (förenade målen C-203/15 och C-698/15), den s.k. Tele2-domen. EU-domstolens slutsats var bl.a. att en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter, avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel, inte var förenlig med EU-rätten. Domstolen gjorde även vissa uttalanden om förutsättningarna för de brottsbekämpande myndigheternas åtkomst till lagrade uppgifter och om säkerheten för uppgifterna.

Med anledning av Tele2-domen sågs den svenska lagstiftningen över och den 1 oktober 2019 trädde nya regler om datalagring i kraft (prop. 2018/19:86). Som framgått ovan innebär ändringarna bl.a. att lagringens omfattning har begränsats och att lagringstiderna har differentierats (6 kap. 16 a och d §§ LEK samt 39 och 40 §§ förordningen [2003:396] om elektronisk kommunikation). I förarbetena uttalade regeringen att det senast inom fyra år efter ikraftträdandet kunde finnas anledning att se över regleringen, bl.a. mot bakgrund av den tekniska utvecklingen, ändrade kommunikationsvanor och nya mål om datalagring i EU-domstolen (samma prop. s. 38 och 108). Som förutsågs har den tekniska utvecklingen fortsatt i snabb takt och kommunikationsvanorna har förändrats. EU-domstolen har nu även meddelat domar i flera av de mål som nämndes i förarbetena (se vidare nedan). Riksdagen har också tillkännagett för regeringen att den skyndsamt ska återkomma med förslag som dels innebär en mer omfattande skyldighet att lagra uppgifter med koppling till nationell säkerhet, dels innebär en mer omfattande lagringsskyldighet generellt (bet. 2018/19:JuU27 punkt 6, rskr. 2018/19:296). Det finns således flera skäl att se över regleringen och redan nu göra den aviserade översynen av regelverket.

Bör lagstiftningen förändras med anledning av ny domstolspraxis?

Den 6 oktober 2020 meddelade EU-domstolen ytterligare domar om lagring och tillgång till uppgifter om elektronisk kommunikation (målet C-623/17 och förenade målen C-511/18, C-512/18 och C-520/18). I domarna konstaterade domstolen att direktiv 2002/58 är tillämpligt också när det gäller lagring av eller tillgång till uppgifter i elektroniska kommunikationer som syftar till att skydda den nationella säkerheten. Samtidigt konstaterade domstolen att EU-rätten, under vissa förutsättningar, inte hindrar en lagstiftning till skydd för nationell säkerhet som ålägger tjänsteleverantörer en generell och odifferentierad lagringsskyldighet avseende trafik- och lokaliseringsuppgifter i situationer där den berörda medlemsstaten står inför ett allvarligt hot mot nationell säkerhet som visar sig vara verkligt, aktuellt eller förutsägbart. En sådan lagring kan tillåtas under förutsättning att beslutet kan bli föremål för en effektiv kontroll av en domstol eller av en oberoende myndighet och att den sker under en period som måste vara tidsmässigt begränsad till vad som är strängt nödvändigt, men som kan förlängas om hotet består.

När det gäller datalagring för bekämpning av grov brottslighet och för att förebygga allvarliga hot mot den allmänna säkerheten stod domstolen fast vid sina uttalanden i Tele2-domen om att en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter om samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel inte är förenlig med EU-rätten. Samtidigt uttalade domstolen att en generell och odifferentierad lagring av uppgifter om den fysiska identiteten (eng. civil identity) för användare av elektroniska kommunikationsmedel är tillåten utan någon specifik tidsbegränsning. Domstolen öppnade också upp för en generell och odifferentierad lagring av ip-adresser som har tilldelats källan för en internetanslutning i syfte att skydda den nationella säkerheten, bekämpa grov brottslighet och för att förebygga allvarliga hot mot den allmänna säkerheten, om lagringen är tidsmässigt begränsad till vad som är strängt nödvändigt. Domstolen stod vidare fast vid sina tidigare uttalanden om att medlemsstaterna är oförhindrade att föreskriva om en tidsbegränsad riktad lagring vilken, på grundval av objektiva och icke-diskriminerande faktorer, är avgränsad genom de kategorier av personer som berörs eller genom ett geografiskt kriterium. Domstolen uttalade sig också om möjlig-

heterna att genom beslut från en behörig myndighet ålägga tjänsteleverantörer att skyndsamt säkra de trafik- och lokaliseringsuppgifter som de har tillgång till. Domstolen uttalade sig inte specifikt om den begränsade och differentierade lagring som införts i Sverige efter Tele2-domen.

Också vad gäller villkoren och formerna för tillgång till lagrad information har ny praxis kommit från EU-domstolen (se EU-domstolens dom den 2 mars 2021 i mål C-746/18).

Vid EU-domstolen finns ytterligare mål, som ännu inte avgjorts, som gäller datalagring för brottsbekämpande ändamål (bl.a. förenade målen C-793/19 och C-794/19 samt målet C-140/20). Den 25 maj 2021 meddelade den Europeiska domstolen för de mänskliga rättigheterna en dom i ett mål som rör en rad olika frågor om bl.a. avlyssning och inhämtning av s.k. mängddata (eng. bulk interception) i underrättelseverksamhet (Europadomstolens dom den 25 maj 2021 i Big Brother Watch m.fl. mot Förenade Kungariket, mål nr 58170/13, 62322/14 och 24960/15). Målet prövades i stor sammansättning (eng. Grand Chamber).

Mot bakgrund av de nya och kommande domarna finns det skäl att analysera om de ger anledning till anpassningar av den svenska lagstiftningen. Det är angeläget att de brottsbekämpande myndigheternas möjligheter att förhindra, upptäcka, utreda och lagföra brott upprätthålls och stärks, samtidigt som ett starkt skydd för de grundläggande rättigheterna säkerställs. Som framgått ovan har EU-domstolen i sina avgöranden den 6 oktober 2020 lämnat flera öppningar för datalagring under förutsättning att effektiva skyddsmekanismer finns på plats. Särskilt när det gäller åtgärder till skydd för nationell säkerhet, lagring av ip-adresser och för att ta reda på en användares fysiska identitet anser domstolen att det finns större utrymme för datalagring.

Utredaren ska därför

- analysera hur dagens regler om lagring och tillgång till uppgifter om elektronisk kommunikation förhåller sig till ny praxis på området,
- överväga och ta ställning till vilka möjligheter som finns till förändringar av reglerna om lagring och tillgång till uppgifter om elektronisk kommunikation i syfte att tillgodose de brottsbekämpande myndigheternas möjligheter att upprätthålla och stärka sin

förmåga, samtidigt som skyddet för de mänskliga rättigheterna säkerställs, och

- lämna förslag på de författningsändringar och andra åtgärder som bedöms nödvändiga.

Utredaren ska hålla sig informerad om och beakta de pågående EU-förhandlingarna om eDataskyddsförordningen samt eventuella lagstiftningsprojekt som kan följa av förhandlingarna.

Uppdraget att se över vissa frågor om exekutiv jurisdiktion

Rätten för en stat att vidta åtgärder och verkställa beslut som har fattats inom ramen för lagstiftning och rättsskipning kallas exekutiv jurisdiktion. Utgångspunkten i folkrätten är att det råder ett förbud för stater att vidta verkställighetsåtgärder inom andra staters territorier, t.ex. att använda hemliga tvångsmedel där. 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 stater. I många fall är det inte ens för den som tillhandahåller tjänsten möjligt att klargöra var uppgifterna finns i varje givet ögonblick. När detta trots allt är möjligt kan förhållandena ändras på bråkdelen av en sekund. I Sverige har territorialitetsprincipen traditionellt sett tolkats så att svenska brottsbekämpande myndigheter saknar jurisdiktion om uppgifter lagras elektroniskt på annan plats än i Sverige eller om det är okänt var uppgifterna lagras. I det första fallet, dvs. när det är känt att informationen lagras i ett annat land, är det många gånger möjligt att få biträde med att få åtgärden verkställd av myndigheterna i det land där uppgifterna finns. Detta kan ske genom internationell rättslig hjälp eller en europeisk utredningsorder. En sådan process kan dock ta lång tid, särskilt när det rör sig om en framställan till en stat utanför EU. I det andra fallet, när det råder ovisshet om var informationen finns – s.k. loss of location – kan det inte klarläggas till vilket eller vilka länder ansökan om rättslig hjälp ska skickas. När det framför allt gäller loss of location-fall gör många andra stater en annan tolkning av territorialitetsprincipen än som traditionellt gjorts i Sverige och anser tvärtom att myndigheterna har befogenhet att vidta åtgärder.

Utredningen om hemlig dataavläsning och Beslagsutredningen har i sina betänkanden uppmärksammat frågan och bedömt att det finns skäl att ändra tolkningen av territorialitetsprincipen (SOU 2017:89 s. 479–485 och SOU 2017:100 s. 374–375). De båda utredningarna uttalade att frågan borde prövas i rättstillämpningen. I remissyttranden med anledning av Utredningen om hemlig dataavläsning anförde Svea hovrätt, Göteborgs tingsrätt, Polismyndigheten och Skatteverket att frågan borde lösas genom lagstiftning. Uppsala universitet (juridiska fakultetsnämnden) ansåg att det framstår som mindre lämpligt att utan vidare överlämna frågan åt rättstillämpningen. Säkerhets- och integritetsskyddsnämnden anförde att ett överlämnande till rättstillämpningen inte kan godtas. Det framkom även i remissyttrandena med anledning av Beslagsutredningen att flera remissinstanser ansåg att frågan borde lösas genom lagstiftning. Polismyndigheten uttalade i sitt yttrande att det var önskvärt att regeringen i varje fall uttalade vilka omständigheter som bör iakttas vid bedömningen.

I propositionen Hemlig dataavläsning konstaterade regeringen att det inte inom ramen för det lagstiftningsprojektet var möjligt att omhänderta denna fråga samt att frågan bäst tas om hand inom ramen för det internationella samarbetet eller på annat lämpligt sätt (prop. 2019/20:64 s. 203). Beslagsutredningen bereds för närvarande inom Regeringskansliet.

Den fortsatta teknikutvecklingen gör att frågan blir av allt större betydelse för de brottsbekämpande myndigheterna. Frågan om tillgång till elektroniska uppgifter ses för närvarande över i olika internationella forum. Som nämnts ovan pågår det inom EU förhandlingar om förslag till en förordning om tillgång till e-bevisning och ett direktiv om utseende av företrädare för insamling av e-bevisning (COM(2018) 225 och COM(2018) 226). Kommissionen har föreslagit att en myndighet i en medlemsstat ska kunna beordra en tjänsteleverantör i en annan medlemsstat att bevara eller lämna ut uppgifter. Om tjänsteleverantören inte skulle följa en sådan order får den utfärdande myndigheten begära hjälp från myndigheterna i den verkställande staten. Kommissionen har också fått mandat att förhandla fram ett avtal med USA som rör tillgång till elektronisk bevisning. Inom Europarådet pågår förhandlingar om ett andra tilläggsprotokoll till Europarådets konvention om it-relaterad brottslighet, den s.k. Budapestkonventionen. Beroende på utfallet från de pågående förhandlingarna skulle vissa delar av jurisdiktionsproblematiken

kunna lösas. Det står dock klart att frågan om s.k. loss of location inte kommer att få en lösning i förhandlingarna.

Någon lösning inom ramen för det internationella samarbetet har ännu inte kommit till stånd. Det har hittills inte heller kommit någon vägledande praxis från de inhemska prejudikatsinstanserna som löser jurisdiktionsfrågan för svensk del. 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. Det finns därför skäl att se över förutsättningarna, inklusive de folkrättsliga aspekterna, för att införa en särskild lagreglering för territorialitetsprincipen vid exekutiv jurisdiktion i förhållande till elektronisk information som finns utanför Sverige.

Utredaren ska därför

- analysera de folkrättsliga frågorna om exekutiv jurisdiktion i förhållande till elektroniska uppgifter utanför Sverige, och i denna analys även göra en jämförelse med rättsläget i andra relevanta länder,
- ta ställning till om det bör införas en särskild lagreglering för territorialitetsprincipen vid exekutiv jurisdiktion som också tar hänsyn till andra anknytningsfaktorer än var data lagras, och
- vid behov lämna förslag på de författningsändringar och andra åtgärder som bedöms nödvändiga.

Utredaren ska hålla sig informerad om och beakta det arbete som pågår inom ramen för ovan nämnda EU-förhandlingar, pågående förhandlingar med USA samt inom Europarådet. Utredaren ska också hålla sig informerad om eventuella lagstiftningsprojekt som kan följa av de ovan nämnda förhandlingarna.

Konsekvensbeskrivningar

Utredaren ska bedöma och redogöra för förslagens ekonomiska konsekvenser och konsekvenser i övrigt för enskilda, företag och det allmänna samt redogöra för förslagens samhällsekonomiska effekter. Utredaren ska särskilt beskriva vilka konsekvenser de förslag som lämnas har för det nationella och internationella skyddet för mänsk-

liga rättigheter, inklusive den personliga integriteten, och för möjligheterna att kommunicera på ett säkert sätt. De offentligfinansiella effekterna av förslagen ska beräknas, och om förslagen kan förväntas leda till offentligfinansiella kostnader ska utredaren föreslå hur dessa ska finansieras.

Kontakter, genomförande och redovisning av uppdraget

Utredaren ska föra dialog med och inhämta upplysningar från Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Säkerhets- och integritetsskyddsnämnden, Integritetsskyddsmyndigheten, Post- och telestyrelsen, It- och telekomföretagen, teleoperatörer, ISOC-SE och OTT-tjänsteleverantörer, men även med andra myndigheter och berörda aktörer, såsom civilsamhället, i den utsträckning som utredaren finner det lämpligt.

Utredaren ska också hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet och inom utredningsväsendet. Utredaren ska beakta utvecklingen vid såväl EU:s lagstiftande institutioner som EU-domstolen, Europadomstolen och Europarådet.

Utredaren ska säkerställa att en välfungerande systematik i regelverket kring hemliga tvångsmedel upprätthålls. Det innebär att utredaren även ska bedöma behovet av följdändringar i rättegångsbalken, inhämtningslagen, preventivlagen, lagen om särskild utlänningskontroll, lagen om hemlig dataavläsning och lagen om elektronisk kommunikation. Utredaren ska även bedöma behovet av följdändringar i lagen om internationell rättslig hjälp i brottmål och lagen om en europeisk utredningsorder. När det finns behov av det ska utredaren lämna förslag på författningsändringar. Utredaren har även möjlighet att ta upp andra frågor som har samband med de frågeställningar som ska utredas under förutsättning att uppdraget kan redovisas i tid.

Uppdraget ska redovisas senast den 6 februari 2023.

(Justitiedepartementet)

Kommittédirektiv 2023:2

Tilläggsdirektiv till 2021 års datalagringsutredning (Ju 2021:09)

Beslut vid regeringssammanträde den 19 januari 2023

Förlängd tid för uppdraget

Regeringen beslutade den 5 augusti 2021 kommittédirektiv om datalagring vid brottsbekämpning – ytterligare åtgärder för en modern och ändamålsenlig reglering (dir. 2021:58). Uppdraget skulle enligt direktiven redovisas senast den 6 februari 2023.

Utredningstiden förlängs. Uppdraget ska i stället redovisas senast den 1 juni 2023.

(Justitiedepartementet)

Jämförelsetabell

Vi vill genom en jämförelsetabell underlätta överblicken av vilka uppgifter som tidigare lagrades för brottsbekämpande ändamål jämfört med gällande regler och våra förslag om lagring. I tabellen markerar vi lagringsskyldighet med grön färg. Röd färg betyder att någon lagringsskyldighet inte föreligger.

Utgångspunkten för tabellens utformning har varit 39–43 §§ gamla FEK i dess lydelse mellan 2012 och 2019 (se SFS 2012:128). Skälet till detta är att det i dag finns en samlad bestämmelse om lagring av uppgifter för telefoni och meddelanden (se 9 kap. 7 och 8 §§ nya FEK). Genom uppdelningen tydliggörs skillnader mellan lagringsskyldighetens omfattning i dag i förhållande till den tidigare regleringen.

Det bör dock uppmärksammas att vi har föreslagit att fler uppgifter ska kunna lagras än tidigare. Vissa av uppgifterna saknar motsvarighet i äldre lagstiftning. Till detta kommer att tillhandahållare av allmänt tillgängliga Noik ska omfattas av lagringsskyldigheten enligt våra förslag. Vi föreslår också en samlad bestämmelse för samtal, telefonitjänst och meddelandehantering. Vi redovisar inte abonnemangsuppgifter i tabellen och man bör hålla i minnet att den närmare omfattningen av lagringsskyldigheten vid nationell säkerhetslagring beror på Säkerhetspolisens beslut i det enskilda fallet. Sammanfattningsvis ger alltså jämförelsetabellen inte en exakt bild av lagringsskyldigheten. Syftet med den är som sagt att ge överblick över regleringen. För en fullständig redovisning hänvisas till avsnitt 7.3.6, 8.3.3 och 9.6.1 och 9 kap. 6–8 §§ nya FEK.

Tabell 1 Datalagring vid fast telefoni[1]

Typ av uppgift	Datalagring 2012–2019	Gällande regler	Datalagring enligt våra förslag
Uppringande nummer			
Uppringt nummer och nummer som samtalet styrts till			
Uppgifter om uppringande och uppringd abonnent och, i förekommande fall, registrerad användare			
Datum och spårbar tid när kommunikationen påbörjades och avslutades			
Uppgifter om den eller de tjänster som använts			

Tabell 2 Datalagring vid telefonitjänst via en mobil nätanslutningspunkt

Typ av uppgift	Datalagring 2012–2019	Gällande regler	Datalagring enligt våra förslag
Uppringande nummer			
Uppringt nummer och nummer som samtalet styrts till			
Uppgifter om uppringande och uppringd abonnent och, i förekommande fall, registrerad användare			
Datum och spårbar tid när kommunikationen påbörjades och avslutades			
Uppgifter om den eller de tjänster som använts			
Uppringandes och uppringds abonnemangsidentitet och utrustningsidentitet			
Lokaliseringsuppgifter för kommunikationens början och slut			

[1] Våra förslag utgår från en samlad bestämmelse för telefonitjänst, samtal och meddelandehantering. Även tillhandahållare av allmänt tillgängliga Noik omfattas av våra förslag. Jämförelsen är därför inte heltäckande.

Typ av uppgift	Datalagring 2012–2019	Gällande regler	Datalagring enligt våra förslag
Lokaliseringsuppgifter vid kommunikationen			
Lokaliseringsuppgifter som inte är trafikuppgifter samt lokaliseringsuppgifter som genererats i användares utrustning			
Datum, spårbar tid och lokaliseringsuppgifter för den första aktiveringen av en förbetald anonym tjänst			
Koppling mellan tillfälliga och permanenta identifierare			
Uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten			

Tabell 3 Datalagring vid telefonitjänst som använder ip-paket

Typ av uppgift	Datalagring 2012–2019	Gällande regler	Datalagring enligt våra förslag
Uppringande nummer			
Uppringt nummer och nummer som samtalet styrts till			
Uppgifter om uppringande och uppringd abonnent och, i förekommande fall, registrerad användare			
Datum och spårbar tid när kommunikationen påbörjades och avslutades			
Uppgifter om den eller de tjänster som använts			
Uppringandes och uppringds abonnemangsidentitet och utrustningsidentitet			

Typ av uppgift	Datalagring 2012–2019	Gällande regler	Datalagring enligt våra förslag
Lokaliseringsuppgifter för kommunikationens början och slut			
Lokaliseringsuppgifter vid kommunikationen			
Lokaliseringsuppgifter som inte är trafikuppgifter samt lokaliseringsuppgifter som genererats i användares utrustning			
Datum, spårbar tid och lokaliseringsuppgifter för den första aktiveringen av en förbetald anonym tjänst			
Koppling mellan tillfälliga och permanenta identifierare			
Uppringandes och uppringds ip-adresser			
Datum och spårbar tid för på- och avloggning i den eller de tjänster som använts			
Uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten.			

Tabell 4 Datalagring vid meddelandehantering[2]

Typ av uppgift	Datalagring 2012–2019	Gällande regler	Datalagring enligt våra förslag
Avsändares och mottagares nummer, ip-adress eller annan meddelandeadress			
Uppgifter om avsändande och mottagande abonnent och, i förekommande fall, registrerad användare			
Datum och spårbar tid för på- och avloggning i den eller de tjänster som använts			
Datum och spårbar tid för avsändande och mottagande av meddelande			
Uppgifter om den eller de tjänster som har använts			
Avsändares och mottagares abonnemangsidentitet och utrustningsidentitet			
Lokaliseringsuppgifter vid kommunikationen			
Lokaliseringsuppgifter som inte är trafikuppgifter samt lokaliseringsuppgifter som genererats i användares utrustning			
Kopplingen mellan tillfälliga och permanenta identifierare för utrustning eller abonnemang			
Uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten			

[2] Våra förslag utgår från en samlad bestämmelse för telefonitjänst, samtal och meddelandehantering. Även tillhandahållare av allmänt tillgängliga Noik omfattas av våra förslag. Jämförelsen är därför inte heltäckande.

Tabell 5 Datalagring vid internetåtkomst

Typ av uppgift	Datalagring 2012–2019	Gällande regler	Datalagring enligt våra förslag
Användares ip-adress			
Uppgifter om abonnent och, i förekommande fall, registrerad användare			
Datum och spårbar tid för på- och avloggning i tjänsten som ger internetåtkomst			
Den typ av kapacitet för överföring som har använts			
Användares abonnemangs- och utrustningsidentiteter			
Koppling mellan tillfälliga och permanenta identifierare för utrustning och abonnemang			
Lokaliseringsuppgifter vid åtkomsten			
Lokaliseringsuppgifter som inte är trafikuppgifter samt lokaliseringsuppgifter som genererats i användares utrustning			
Uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten.			

Statens offentliga utredningar 2023

Kronologisk förteckning

1. Skärpta straff för flerfaldig brottslighet. Ju.
2. En inre marknad för digitala tjänster – ansvarsfördelning mellan myndigheter. Fi.
3. Nya regler om nödlidande kreditavtal och inkassoverksamhet. Ju.
4. Posttjänst för hela slanten. Finansieringsmodeller för framtidens samhällsomfattande posttjänst. Fi.
5. Från delar till helhet. Tvångsvården som en del av en sammanhållen och personcentrerad vårdkedja. S.
6. En lag om tilläggsskatt för företag i stora koncerner. Fi.
7. På egna ben. Utvecklad samverkan för individers etablering på arbetsmarknaden. A.
8. Arbetslivskriminalitet – arbetet i Sverige, en bedömning av omfattningen, lärdomar från Danmark och Finland. A.
9. Ett statligt huvudmannaskap för personlig assistans. Ökad likvärdighet, långsiktighet och kvalitet. S.
10. Tandvårdens stöd till våldsutsatta patienter. S.
11. Tillfälligt miljötillstånd för samhällsviktig verksamhet – för ökad försörjningsberedskap. KN.
12. Förstärkt skydd för demokratin och domstolarnas oberoende. Ju.
13. Patientöversikter inom EES och Sverige. S.
14. Organisera för hållbar utveckling. KN.
15. Förnybart i tanken. Ett styrmedelsförslag för en stärkt bioekonomi. LI.
16. Staten och betalningarna. Del 1 och 2. Fi.
17. En tydligare bestämmelse om hets mot folkgrupp. Ju.
18. Värdet av vinden. Kompensation, incitament och planering för en hållbar fortsatt utbyggnad av vindkraften. Del 1 och 2. KN.
19. Statlig forskningsfinansiering. Underlagsrapporter. U.
20. Förbud mot bottentrålning i marina skyddade områden. LI.
21. Informationsförsörjning på skolområdet. Skolverkets ansvar. U.
22. Datalagring och åtkomst till elektronisk information. Ju.

Statens offentliga utredningar 2023

Systematisk förteckning