Registrering av kontantkort, m.m.

Ds 2020:12

Regeringskansliet
Justitiedepartementet

SOU och Ds kan köpas från Norstedts Juridiks kundservice.
Beställningsadress: Norstedts Juridik, Kundservice, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: kundservice@nj.se
Webbadress: www.nj.se/offentligapublikationer

För remissutsändningar av SOU och Ds svarar Norstedts Juridik AB
på uppdrag av Regeringskansliets förvaltningsavdelning.
Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
En kort handledning för dem som ska svara på remiss.
Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remisser

Omslag: Regeringskansliets standard
Tryck: Elanders Sverige AB, Stockholm 2020

ISBN 978-91-38-25054-9
ISSN 0284-6012

Förord

Genom beslut den 27 augusti 2019 uppdrog statsrådet Mikael Damberg åt f.d. lagmannen Sigurd Heuman att biträda Justitiedepartementet med att lämna förslag om en registreringsskyldighet för kontantkort och att se över vissa frågor om verkställighet (Ju 2019:E). Samma dag anställdes hovrättsassessorn Anna-Karin Leo för att arbeta som sekreterare inom ramen för uppdraget.

Härmed överlämnas promemorian *Registrering av kontantkort, m.m.* (Ds 2020:12). Med detta är uppdraget slutfört.

Ängelholm i juni 2020

Sigurd Heuman

/Anna-Karin Leo

Innehåll

Sammanfattning

Uppdraget

Utredningsuppdraget avser de brottsbekämpande myndigheternas tillgång till uppgifter på området för elektronisk kommunikation. Uppdraget består av två separata delar. Den första gäller frågan om det bör införas en registreringsskyldighet som omfattar kontantkort till mobiltelefoner. Enligt uppdragsbeskrivningen ska vi ta ställning till om det bör införas en skyldighet att registrera uppgifter om abonnemang för kontantkort i syfte att säkerställa att uppgifterna finns tillgängliga för brottsbekämpande ändamål. I uppdraget ingår att lämna förslag till regler om en sådan skyldighet, även om vi skulle komma till slutsatsen att någon reglering inte bör införas.

Utredningens andra del avser vissa verkställighetsfrågor kopplade till de brottsbekämpande myndigheternas inhämtning av uppgifter på området för elektronisk kommunikation. En av dessa frågor handlar om att förtydliga reglerna om leverantörers skyldighet att medverka och verksamhetsanpassa för att möjliggöra att uppgifter som lämnas ut till de brottsbekämpande myndigheterna enkelt kan tas om hand. I denna del ingår att överväga om regler bör införas som möjliggör att de utlämnade uppgifterna följer en gemensam standard. De övriga verkställighetsfrågorna avser tydligare krav på skyndsamhet vid utlämnandena samt rätten till ersättning för kostnader som uppstår vid utlämnanden.

Registrering av kontantkort

Vi har funnit att de brottsbekämpande myndigheterna har ett påtagligt behov av uppgifter om vem som innehar kontantkort. Det är vidare vår bedömning att det i och för sig kommer att finnas vägar att kringgå en registreringsskyldighet som omfattar kontantkort och

att fortsatt kommunicera anonymt. En skyldighet att registrera uppgifter om abonnemang rörande kontantkort kommer dock att innebära ett försvårande för de kriminella och ett effektivare arbete för de brottsbekämpande myndigheterna. En skyldighet att registrera uppgifter om abonnemang rörande kontantkort skulle därmed innebära fördelar i förhållande till dagens system. Således skulle en registreringsskyldighet också vara till nytta för brottsbekämpningen.

Vi har även konstaterat att en registreringsskyldighet kommer att få konsekvenser för bl.a. enskilda som av helt legitima skäl i dag kommunicerar via oregistrerade kontantkort. Vid en avvägning mellan de positiva effekter som en registreringsskyldighet kan förväntas få genom att försvåra de kriminellas verksamhet och de negativa effekter som registreringsskyldigheten kan ha för enskilda framstår det dock som en proportionerlig åtgärd att innehavaren av ett telefonabonnemang registrerar sina identitetsuppgifter. Det är således vår bedömning att en skyldighet att registrera abonnemangsuppgifter för kontantkort bör införas.

Enligt vårt förslag ska registreringsskyldigheten regleras i lagen (2003:389) om elektronisk kommunikation (LEK). Regleringen ska omfatta de som tillhandahåller förbetalda allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster eller internetanslutningstjänster. Registreringsskyldigheten träffar dock inte de tillhandahållare som endast erbjuder s.k. maskin till maskin-tjänster (M2M). De kontantkort som ska registreras är sådana kort som ger tillgång telefonitjänster eller internetanslutningstjänster och som därmed kan användas för att ringa, sända textmeddelanden eller surfa på internet. De uppgifter som ska registreras är abonnentens namn, adress, personnummer eller motsvarande och nummer för tjänsten. Den som tillhandahåller en förbetald tjänst ska inte få ge tillgång till tjänsten, om inte denne först har genomfört en registrering. De registrerade uppgifterna ska finnas tillgängliga från registreringen och i ett år efter att tillhandahållandet av tjänsten har upphört. I samband med registreringen ska abonnentens identitet kontrolleras genom en giltig identitetshandling med fotografi eller en tillförlitlig elektronisk identifiering. Saknar abonnenten en identitetshandling ska identiteten göras sannolik på annat sätt. Identitetskontrollen ska dokumenteras.

Registreringsplikten ska omfatta även förbetalda tjänster som har tagits i bruk innan lagen trädde i kraft. Dessa ska dock vara möjliga

att använda i sex månader efter lagens ikraftträdande utan att en registrering har skett. Om en registrering av en sådan tjänst inte har skett inom denna tid ska tillhandahållandet av tjänsten avbrytas.

Om en förbetald och registrerad tjänst har överlåtits till någon annan, fysisk eller juridisk person, utan att en ny registrering har skett, ska tillhandahållandet av tjänsten avbrytas. Detta ska dock inte gälla om tjänsten har överlåtits till en närstående, om tjänsten har införskaffats av en juridisk person och används på dennes uppdrag eller om tjänsten har införskaffats på uppdrag av Försvarsmakten, Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som har till uppgift att ingripa mot brott.

Vi har funnit att det inte bör införas någon begränsning i det antal kontantkort eller förbetalda tjänster som en enskild ska få registrera eller inneha. Vi har inte heller funnit att det bör införas någon reglering som begränsar möjligheten att använda utländska kontantkort i Sverige.

Post- och telestyrelsen är tillsynsmyndighet enligt lagen om elektronisk kommunikation och har ett samlat ansvar inom området för elektronisk kommunikation. Myndighetens tillsyn kommer att omfatta efterlevnaden av den föreslagna registreringsskyldigheten. Vi har funnit att regleringen om tillsyn i lagen om elektronisk kommunikation är tillräcklig för att säkerställa att en registreringsskyldighet efterlevs. För det fall lagen om elektronisk kommunikation framöver kommer att innehålla en möjlighet för Post- och telestyrelsen att meddela sanktionsavgift, kan det övervägas om denna möjlighet även bör omfatta efterlevnaden av skyldigheten att registrera abonnemangsuppgifter avseende förbetalda tjänster och i samband därmed genomföra en identitetskontroll.

Verkställighetsfrågor

I syfte att uppgifter om elektronisk kommunikation ska lämnas ut från leverantörer till brottsbekämpande myndigheter i gemensamma format föreslår vi att det i 6 kap. 19 § andra stycket LEK ska föreskrivas att när uppgifter som avses i 20 § första stycket lämnas ut för brottsbekämpning till Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som har till uppgift att ingripa mot brott, ska

uppgifterna ordnas och göras tillgängliga i ett format som gör det möjligt att enkelt ta hand om dem. Vidare föreslår vi att det i förordningen (2003:396) om elektronisk kommunikation ska föreskrivas att leverantörerna och de brottsbekämpande myndigheterna gemensamt ska verka för att informationsöverföringen sker i gemensamma format på ett enhetligt sätt.

Vi föreslår även att uppgifter om elektronisk kommunikation ska lämnas ut till de brottsbekämpande myndigheterna utan dröjsmål. Även detta ska regleras i 6 kap. 19 § andra stycket LEK. I promemorian föreslås också att Post- och telestyrelsen ska ges mandat att genom föreskrifter fastställa ersättningen vid utlämnande av uppgifter om elektronisk kommunikation från leverantörer till brottsbekämpande myndigheter.

Ikraftträdande- och övergångsbestämmelser

Författningsförslagen föreslås träda i kraft den 1 januari 2022. En förbetald tjänst knuten till ett kontantkort som har tillhandahållits innan regleringen trädde i kraft ska dock vara möjlig att använda till den 1 juli 2022 utan att en registrering har skett. Om inte en registrering har skett senast vid denna tidpunkt ska tillhandahållandet av tjänsten avbrytas.

Konsekvenser

Förslagen kommer i viss utsträckning medföra ökade kostnader för berörda myndigheter. Dessa kostnader bedöms dock rymmas inom befintliga anslag. Förslagen kan vidare medföra konsekvenser för företag som tillhandahåller kontantkort, i form av försäljningsminskning och framför allt ökad administrativ börda. Förslagen bedöms också innebära en begränsad inskränkning i enskildas rätt till personlig integritet.

1 Författningsförslag

1.1 Förslag till lag om ändring i lagen (2003:389) om elektronisk kommunikation

Härigenom föreskrivs i fråga om lagen (2003:389) om elektronisk kommunikation[1]

dels att 6 kap. 16 e och 16 f §§ ska upphöra att gälla,

dels att 6 kap. 5, 19 och 22 §§ och rubriken närmast före 6 kap. 19 § ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 6 kap. 23 a och 23 b §§, och närmast före 6 kap. 23 a § en ny rubrik av följande lydelse,

dels att det närmast före 6 kap. 19 a § ska införas en ny rubrik som ska lyda ”Signalspaning”.

Nuvarande lydelse	*Föreslagen lydelse*
	6 kap.
	5 §[2]
Den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § ska utplåna eller avidentifiera lagrade eller på annat sätt behandlade trafikuppgifter som avser användare som är fysiska personer eller som avser abonnenter, när uppgifterna inte längre behövs för att	Den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § ska utplåna eller avidentifiera lagrade eller på annat sätt behandlade trafikuppgifter som avser användare som är fysiska personer eller som avser abonnenter, när uppgifterna inte längre behövs för att

[1] Senaste lydelse av
6 kap. 16 e § 2012:127
6 kap. 16 f § 2012:127
6 kap. 19 a § 2008:719.

[2] Senaste lydelse 2012:127.

överföra ett elektroniskt meddelande. Det gäller dock inte om uppgifterna sparas för sådan behandling som anges i 6, 13, 16 a *eller* 16 c §.	överföra ett elektroniskt meddelande. Det gäller dock inte om uppgifterna sparas för sådan behandling som anges i 6, 13, 16 a, 16 c *eller 23 a §*.
Hemlig avlyssning av elektronisk kommunikation m.m.[3]	***Anpassning m.m.***
19 §[4]	
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 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 kommunikationsnät vilka består av	
a) en allmänt tillgänglig telefonitjänst till 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.	
Innehållet i och uppgifter om avlyssnade eller övervakade meddelanden ska göras tillgängliga så att informationen enkelt kan tas om hand.	*När uppgifter som avses i 20 § första stycket lämnas ut för brottsbekämpning till Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som har till uppgift att ingripa mot brott, ska uppgifterna ordnas och göras tillgängliga i ett format som gör det möjligt att enkelt ta hand om dem. Uppgifterna ska lämnas ut utan dröjsmål.*

[3] Senaste lydelse 2012:285.
[4] Senaste lydelse 2018:1917.

Den som lämnar ut uppgifter som avses i 20 § första stycket till Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som har till uppgift att ingripa mot brott, har rätt till ersättning för kostnader som uppstår när uppgifter lämnas ut. Ersättningen ska betalas av den myndighet som har begärt uppgifterna.

Vad som föreskrivs om uppgifter i andra och tredje styckena gäller även lokaliseringsuppgifter som inte är trafikuppgifter.

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

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

22 §[5]

Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och därvid har fått del av eller tillgång till uppgift som avses i 20 § första stycket ska på begäran lämna

1. uppgift som avses i 20 § första stycket 1 till en myndighet som i ett särskilt fall behöver en sådan uppgift för delgivning enligt delgivningslagen (2010:1932), om myndigheten finner att det kan antas att den som söks för delgivning håller sig undan eller att det annars finns synnerliga skäl,

2. uppgift som avses i 20 § första stycket 1 och som gäller

2. uppgift som avses i 20 § första stycket 1 och som gäller

[5] Senaste lydelse 2016:1311.

misstanke om brott till *en åklagarmyndighet*, Polismyndigheten, Säkerhetspolisen eller någon annan myndighet som ska ingripa mot brottet,	misstanke om brott *eller brottslig verksamhet* till *Åklagarmyndigheten*, *Ekobrottsmyndigheten*, Polismyndigheten, Säkerhetspolisen eller någon annan myndighet som ska ingripa mot brottet *eller den brottsliga verksamheten*,

3. uppgift som avses i 20 § första stycket 1 och 3 samt uppgift om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits till Polismyndigheten, om myndigheten finner att uppgiften behövs i samband med efterforskning av personer som har försvunnit under sådana omständigheter att det kan befaras att det finns fara för deras liv eller allvarlig risk för deras hälsa,

4. uppgift som avses i 20 § första stycket 1 till Kronofogdemyndigheten om myndigheten behöver uppgiften i exekutiv verksamhet och myndigheten finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende,

5. uppgift som avses i 20 § första stycket 1 till Skatteverket, om verket finner 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),

6. uppgift som avses i 20 § första stycket 1 till Polismyndigheten, om myndigheten finner 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),

7. uppgift som avses i 20 § första stycket 1 till Polismyndigheten eller en åklagarmyndighet, om myndigheten finner att uppgiften behövs i ett särskilt fall för att myndigheten ska kunna fullgöra underrättelseskyldighet enligt 33 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare,

8. uppgift som avses i 20 § första stycket 1 och 3 till regional alarmeringscentral som avses i lagen (1981:1104) om verksamheten hos vissa regionala alarmeringscentraler, och

9. uppgift som avses i 20 § första stycket 1 till Finansinspektionen, om inspektionen finner 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 mark-

nadsmissbruk (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.

Ersättning för att lämna ut andra uppgifter enligt första stycket 8 än lokaliseringsuppgifter ska vara skälig med hänsyn till kostnaderna för utlämnandet.

Förbetalda tjänster

23 a §

Den som tillhandahåller en förbetald allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst eller en förbetald internetanslutningstjänst får inte ge tillgång till tjänsten, om inte denne har registrerat abonnentens namn, adress, personnummer eller motsvarande och nummer för tjänsten. Uppgifterna ska finnas tillgängliga hos tillhandahållaren från registreringen och i ett år efter att tillhandahållandet har upphört.

I samband med registreringen ska abonnentens identitet kontrolleras genom en giltig identitetshandling med fotografi eller en tillförlitlig elektronisk identifiering. Saknar abonnenten en identitetshandling ska identiteten göras sannolik på annat sätt. Identitetskontrollen ska dokumenteras.

Regeringen eller den myndighet som regeringen bestämmer får med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om identitetskontrollen enligt andra stycket.

23 b §

Om en förbetald tjänst som har registrerats enligt 23 a § har överlåtits till någon annan utan att en ny registrering har skett, ska tillhandahållandet av tjänsten avbrytas.

Vad som sägs i första stycket gäller inte om tjänsten

1. har överlåtits till en närstående,

2. har införskaffats av en juridisk person och används på dennes uppdrag, eller

3. har införskaffats på uppdrag av Försvarsmakten, Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som har till uppgift att ingripa mot brott.

---

1. Denna lag träder i kraft den 1 januari 2022.

2. En förbetald allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst eller en förbetald internetanslutningstjänst som har tillhandahållits innan lagen trädde i kraft får tillhandahållas till och med den 1 juli 2022 trots att en registrering inte skett i enlighet med 6 kap. 23 a §.

1.2 Förslag till förordning om ändring i förordningen (2003:396) om elektronisk kommunikation

Härigenom föreskrivs i fråga om förordningen (2003:396) om elektronisk kommunikation[6]

dels att nuvarande 36 a § ska betecknas 36 b §,

dels att 36 och 46 §§ ska ha följande lydelse,

dels att det ska införas en ny paragraf, 36 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	36 §[7]
Post- och telestyrelsen får efter samråd med Åklagarmyndigheten, Polismyndigheten *och* Säkerhetspolisen	Post- och telestyrelsen får, efter samråd med Åklagarmyndigheten, *Ekobrottsmyndigheten*, Polismyndigheten, Säkerhetspolisen *och Tullverket, meddela föreskrifter om*
1. *meddela de verkställighetsföreskrifter som behövs för hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation enligt 6 kap. 19 § lagen (2003:389) om elektronisk kommunikation, och*	1. *kravet på format och utlämnande av uppgifter utan dröjsmål enligt 6 kap. 19 § andra stycket lagen (2003:389) om elektronisk kommunikation, och*
2. *i enskilda fall medge undantag från krav enligt 6 kap. 19 § första stycket samma lag.*	2. *ersättning enligt 6 kap. 19 § tredje stycket samma lag.*
	Post- och telestyrelsen får i enskilda fall medge undantag från krav enligt 6 kap. 19 § första stycket samma lag.

[6] Senaste lydelse av 36 a § 2008:928.
[7] Senaste lydelse 2014:1270.

	36 a §
	Den som lämnar ut uppgifter som avses i 6 kap. 20 § första stycket lagen (2003:389) om elektronisk kommunikation till Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som har till uppgift att ingripa mot brott ska gemensamt med de myndigheterna verka för att informationsöverföringen sker i gemensamma format på ett enhetligt sätt.
	Vad som föreskrivs om uppgifter i första stycket gäller även lokaliseringsuppgifter som inte är trafikuppgifter.
	46 §[8]
Post- och telestyrelsen får, efter *att ha hört* Polismyndigheten, Säkerhetspolisen och Tullverket, meddela föreskrifter om *ersättningen enligt 6 kap. 16 e § lagen (2003:389) om elektronisk kommunikation.*	Post- och telestyrelsen får, efter *samråd med Åklagarmyndigheten, Ekobrottsmyndigheten*, Polismyndigheten, Säkerhetspolisen och Tullverket, meddela föreskrifter om *identitetskontrollen enligt 6 kap. 23 a § andra stycket lagen (2003:389) om elektronisk kommunikation.*

Denna förordning träder i kraft den 1 januari 2022.

---

[8] Senaste lydelse 2014:1270.

2 Uppdrag och arbete

2.1 Uppdraget

Utredningsuppdraget avser de brottsbekämpande myndigheternas tillgång till uppgifter på området för elektronisk kommunikation. Uppdraget består av två separata delar. Den första gäller frågan om det bör införas en registreringsskyldighet som omfattar kontantkort till mobiltelefoner. Enligt uppdragsbeskrivningen ska vi ta ställning till om det bör införas en skyldighet att registrera uppgifter om abonnemang för kontantkort i syfte att säkerställa att uppgifterna finns tillgängliga för brottsbekämpande ändamål. I uppdraget ingår att lämna förslag till regler om en sådan skyldighet, även om vi skulle komma till slutsatsen att någon reglering inte bör införas. Det ingår också i uppdraget att överväga om nuvarande regler om tillsyn och sanktioner är tillräckliga för att säkerställa att en registreringsskyldighet efterlevs.

Utredningens andra del avser vissa verkställighetsfrågor kopplade till de brottsbekämpande myndigheternas inhämtning av uppgifter på området för elektronisk kommunikation. En av dessa frågor handlar om att förtydliga reglerna om leverantörers skyldighet att medverka och verksamhetsanpassa för att möjliggöra att uppgifter som lämnas ut till de brottsbekämpande myndigheterna enkelt kan tas om hand. I denna del ingår att överväga om regler bör införas som möjliggör att de utlämnade uppgifterna följer en gemensam standard. De övriga verkställighetsfrågorna avser tydligare krav på skyndsamhet vid utlämnandena samt rätten till ersättning för kostnader som uppstår vid utlämnanden. I detta sammanhang behandlar vi också behovet av ett förtydligande när det gäller utlämnande av abonnemangsuppgifter i underrättelseverksamhet.

Uppdragsbeskrivningen i sin helhet finns i bilaga 1.

2.2 Tillvägagångssätt

Arbetet påbörjades i augusti 2019. Under utredningens gång har vi haft ett flertal kontakter med berörda aktörer. I syfte att bereda de brottsbekämpande myndigheterna möjlighet att framföra sina behov av förändrad lagstiftning har vi besökt Polismyndigheten, Säkerhetspolisen och Tullverket. Vi har också besökt en av Polismyndighetens teknikgrupper. Synpunkter har därefter inhämtats från de aktuella myndigheterna under arbetets gång. Synpunkter har också hämtats in från Ekobrottsmyndigheten. Vi har även haft kontakter med företrädare för Åklagarmyndigheten och Försvarsmakten.

Enskilda möten har hållits med var och en av de fyra stora mobiloperatörerna, dvs. Hi3G, Tele2, Telenor och Telia. Vi har även sammanträffat med branschorganisationen IT&Telekomföretagen. Synpunkter från mobiloperatörerna har också hämtats in under arbetets gång.

Post- och telestyrelsen har lämnat värdefulla synpunkter under utredningsarbetet. Ett möte har hållits med representanter för Post- och telestyrelsen. Vi har därefter haft ett flertal kontakter med företrädare för myndigheten.

I syfte att utreda vilken påverkan en skyldighet att registrera kontantkort kan komma att få för mediernas arbete har vi sammanträffat med representanter för Sveriges Radio. Vi har även haft kontakter med Föreningen Grävande journalister och Journalistförbundet.

En del av utredningstiden har gått åt till att från olika källor hämta in uppgifter om hur en skyldighet att registrera kontantkort har utformats i andra länder. Vi har i detta arbete bl.a. haft kontakter med företrädare för Kommunal- og moderniseringsdepartementet i Norge och den nationella kommunikationsmyndigheten i Norge, som har lämnat uppgifter angående utformningen och erfarenheterna av den norska lagstiftningen.

Denna promemoria är resultatet av ett gemensamt arbete av mig och Anna-Karin Leo. Den är därför skriven i vi-form. Jag är dock ensam ansvarig för förslagen.

3 Grundläggande rättigheter

3.1 Integritetsbegreppet

Svensk rätt innehåller ingen allmängiltig definition av begreppet personlig integritet. Någon enhetlig definition finns inte heller i internationell rätt (se SOU 2016:65 s. 34). Begreppet personlig integritet har dock 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 angetts att det inte är 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 (se t.ex. prop. 2009/10:80 s. 175). Utformningen av integritetsskyddet i svensk rätt har således inte tagit sin utgångspunkt i en viss definition av begreppet, utan skyddet har i stället kommit att bestämmas av summan av ett stort antal skyddsregler av varierande slag (se bl.a. SOU 2015:31 s. 51).

3.2 Reglering av skyddet för privatlivet

3.2.1 FN:s konventioner

Förenta nationernas allmänna förklaring om de mänskliga rättigheterna antogs 1948. I artikel 12 i förklaringen slås fast att ingen får utsättas för godtyckligt ingripande i fråga om privatliv, familj, hem eller korrespondens. Av artikel 29 framgår att en person endast får 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. Mot-

svarande skydd för den personliga integriteten finns i FN:s konvention om medborgerliga och politiska rättigheter, som antogs 1966.

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 (se lagen [1994:1219] om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna). Enligt 2 kap. 19 § regeringsformen 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. Enligt artikel 8 i Europakonventionen har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. 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 (se Hans Danelius, Mänskliga rättigheter i europeisk praxis, 5 uppl. 2015, s. 369 f.). Konventionsstaterna har ett visst handlingsutrymme att själva avgöra om begränsningarna är nödvändiga för ett givet syfte (eng. margin of appreciation). Europadomstolen förbehåller sig dock rätten att överpröva denna bedömning inom ramen för prövningen av någons enskilda klagomål hos domstolen.

Artikel 8 i Europakonventionen ger enligt sin praxis upphov inte bara 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 (se t.ex. SOU 2015:31 s. 52 f. och SOU 2017:75 s. 60 f.).

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 har 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 vika för brottsbekämpande ändamål (se Europadomstolens dom den 2 december 2008 i mål K.U. mot Finland, mål nr 2872/02).

Europadomstolen har prövat om den registreringsskyldighet för kontantkort som har införts i Tyskland strider mot rätten till respekt för privat- och familjelivet (se Europadomstolens dom den 30 januari 2020 i mål Breyer mot Tyskland, mål nr 50001/12). Domstolen fann att skyldigheten att registrera abonnemangsuppgifter som namn, adress, födelsedatum och telefonnummer innebär en begränsad inskränkning i rätten till privatliv. Det ansågs således inte vara fråga om något betydande ingrepp i den enskildes sfär. Den nationella lagen ansågs vidare innehålla tillräckliga skyddsåtgärder för de behandlade personuppgifterna. När det gällde nödvändigheten av en registreringsskyldighet anförde domstolen att moderna kommunikationsvägar och förändrade kommunikationsmönster kräver att de brottsbekämpande myndigheternas verktyg anpassas. Domstolen angav även att en registreringsplikt kraftigt förenklar och påskyndar det brottsutredande arbetet. Enligt domstolen hade inskränkningarna i rätten till privatliv varit proportionella och nödvändiga i ett

demokratiskt samhälle med hänsyn till intresset av att skydda den allmänna säkerheten och bekämpa brott. Någon kränkning av artikel 8 i Europakonventionen hade därför inte förekommit.

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 (se t.ex. Åkerberg Fransson, mål C-617/10).

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 målsättningsstadgandet i 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

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 (se 2 kap. 20 och 21 §§). För utländska medborgare som är bofasta i riket gäller att särskilda begränsningar i dessa rättigheter får göras genom lag (se 2 kap. 25 §).

3.3 Reglering av 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 tillhörde de första konventionsstaterna att underteckna protokollet. Processen för att ändringsprotokollet ska träda i kraft har därmed inletts.

3.3.2 EU-rättslig reglering

Bestämmelser om behandling av personuppgifter finns i unionsrättens primärrätt och sekundärrätt. I artikel 8 i rättighetsstadgan före-

skrivs 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).

EU har antagit ett nytt regelverk för behandling av personuppgifter. Det huvudsakliga syftet med de nya EU-rättsliga bestämmelserna är att ytterligare harmonisera och effektivisera skyddet för personuppgifter för att förbättra den inre marknadens funktion och öka enskildas kontroll över sina personuppgifter. 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 dataskyddsförordningen. Dataskyddsförordningen är tillämplig i medlemsstaterna sedan den 25 maj 2018. Den utgör numera den generella regleringen för personuppgiftsbehandling inom EU.

Dataskyddsförordningen 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 (nedan dataskyddsdirektivet). Dataskyddsdirektivet ska vara genomfört i medlemsstaterna genom nationell lagstiftning.

Viss behandling av personuppgifter undantas från både dataskyddsförordningens och dataskyddsdirektivets tillämpnings-

områden. Det gäller personuppgiftsbehandling i verksamhet som inte omfattas av unionsrätten, däribland området nationell säkerhet.

3.3.3 Nationell lagstiftning

EU:s dataskyddsförordning började alltså tillämpas den 25 maj 2018. Samma dag trädde lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, (nedan kallad dataskyddslagen) i kraft. I lagen finns kompletterande bestämmelser till dataskyddsförordningen. Den innehåller bl.a. bestämmelser om att dataskyddsförordningen med vissa undantag ska gälla utanför sitt egentliga tillämpningsområde, exempelvis i verksamhet som rör nationell säkerhet. 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 andra 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.

De brottsbekämpande myndigheterna har även egna registerförfattningar som gäller utöver brottsdatalagen och som innehåller bestämmelser som innebär preciseringar, undantag eller avvikelser från bestämmelserna i den lagen. Som exempel kan nämnas lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område och lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område. För Säkerhetspolisen gäller även 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 t.ex. i 6 kap. lagen (2003:389) om elektronisk kommunikation.

3.4 Meddelarskyddet

Rätten att meddela och offentliggöra uppgifter följer av grundlagarna tryckfrihetsförordningen (TF) och yttrandefrihetsgrundlagen (YGL). Enligt 1 kap. 7 § TF och 1 kap. 10 § YGL står det var och en fritt att meddela uppgifter i vilket ämne som helst till bl.a. utgivare, redaktioner och nyhetsbyråer i syfte att göra uppgifterna offentliga i de medier som grundlagarna omfattar (*meddelarfrihet*). Uppgifterna som får lämnas med stöd av meddelarfriheten kan röra i princip vilka förhållanden som helst, så länge syftet är att uppgifterna ska meddelas i något av de medier som grundlagarna skyddar. Det spelar ingen roll om något offentliggörande verkligen kommer till stånd. I vissa undantagsfall kan dock en meddelare straffas för sitt uppgiftslämnande. Det rör sig om fall där utlämnandet av uppgifter omfattar vissa grövre brott mot rikets säkerhet, oriktigt utlämnande av hemlig handling eller ett uppsåtligt åsidosättande av s.k. kvalificerad sekretess, dvs. sådan sekretess som enligt offentlighets- och sekretesslagen (2009:400) bryter meddelarfriheten. Exempel på kvalificerad sekretess är uppgifter om enskildas personliga eller ekonomiska förhållanden inom viss vård- och omsorgsverksamhet.

Meddelarfriheten kan sägas vara en beståndsdel i det s.k. meddelarskyddet enligt grundlagarna. Andra beståndsdelar i detta skydd är rätten till anonymitet, efterforskningsförbud och repressalieförbud. Meddelarskyddet gäller i förhållande till myndigheter och andra allmänna organ, men kan också gälla för dem som arbetar i vissa enskilda verksamheter (se lagen [2017:151] om meddelarskydd i vissa enskilda verksamheter).

Rätten till anonymitet innebär att en författare, en upphovsman eller en meddelare inte är skyldig att avslöja sin identitet. Vidare

finns det också ett förbud för den som har tagit befattning med utgivning eller motsvarande att avslöja vem som är författare eller står bakom ett meddelande, det s.k. källskyddet (se 3 kap. 1 och 3 §§ TF och 2 kap. 1 och 3 §§ YGL). Det betyder att en journalist inte får avslöja identiteten på en uppgiftslämnare som inte vill framträda öppet. Denna tystnadsplikt är straffsanktionerad. Förbudet är dock inte absolut utan kan frångås i vissa undantagsfall, bl.a. om författaren eller meddelaren har samtyckt till att identiteten avslöjas eller om det finns misstanke om vissa brott.

Efterforskningsförbudet innebär att en myndighet eller annat allmänt organ inte får efterforska identiteten hos bl.a. en meddelare som omfattas av anonymitetsskyddet annat än i den begränsade utsträckning som följer av 3 kap. 5 § TF och 2 kap. 5 § YGL. Det är endast Justitiekanslern som är behörig att under vissa förutsättningar besluta om sådana åtgärder. Uttrycket efterforska har en vidsträckt innebörd och innefattar alla former av förfrågningar och åtgärder som syftar till att få fram vem som har lämnat en uppgift eller offentliggjort sådan. Överträdelser av förbudet är straffbelagda.

Repressalieförbudet betyder att en myndighet eller allmänt organ inte får ingripa mot någon för att denne har utnyttjat sin tryck- och yttrandefrihet (se 3 kap. 6 § TF och 2 kap. 6 § YGL). Förbudet avser alla åtgärder som medför negativa konsekvenser för den enskilde.

4 Uppgifter om elektronisk kommunikation i brottsbekämpande verksamhet

4.1 Elektronisk kommunikation

4.1.1 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 växer samman.

Uppgifter om elektronisk kommunikation har i svensk rätt delats in i tre olika grupper. Med *uppgift om abonnemang* avses främst uppgifter om abonnentens nummer, namn, titel och adress. Vidare innefattas uppgift om vem som har använt en fast eller dynamisk ip-adress (ett nummer som används som adress på internet) eller ett IMSI-nummer (International Mobile Subscriber Identity, ett nummer som är kopplat till abonnentens simkort och telefonnummer). Med *trafikuppgifter* avses i detta sammanhang uppgifter som behandlas i syfte att förmedla ett elektroniskt meddelande i ett elektroniskt kommunikationsnät eller för att fakturera ett sådant meddelande. Med *lokaliseringsuppgifter* avses uppgifter som visar den geografiska positionen för terminalutrustningen för en användare. Det kan t.ex. vara fråga om vilken cell (antenn på basstation) som utrustningen kopplat upp sig mot. De olika uppgiftskategorierna är delvis överlappande.

4.1.2 EU-direktiv om elektronisk kommunikation

På området för elektronisk kommunikation finns ett flertal EU-direktiv. För att säkerställa rätten till respekt för privatlivet och rätten till skydd för personuppgifter inom sektorn för elektronisk kommunikation har EU antagit Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), även kallat e-dataskyddsdirektivet. Direktivet definierar trafikuppgifter och lokaliseringsuppgifter, men inte uppgifter om abonnemang. Direktivet föreskriver bl.a. att medlemsstaterna ska säkerställa konfidentialitet vid elektronisk kommunikation och därmed förbundna trafikuppgifter. Uppgifter som inte längre behövs ska utplånas eller avidentifieras. Medlemsstaterna får dock göra undantag från dessa åligganden om det behövs för bl.a. brottsbekämpande verksamhet. Direktivet har genomförts i svensk rätt främst genom bestämmelser som tagits in i lagen (2003:389) om elektronisk kommunikation (LEK).

Europeiska kommissionen har lämnat ett förslag till en ny förordning om respekt för privatlivet och skydd för personuppgifter i samband med elektronisk kommunikation. Förordningen ska ersätta e-dataskyddsdirektivet och utgöra en specialreglering i förhållande till den allmänna dataskyddsförordningen. Förslaget bereds för närvarande inom EU.

Den 11 december 2018 antogs Europaparlamentets och rådets direktiv (EU) 2018/1972 om inrättande av en europeisk kodex för elektronisk kommunikation. Direktivet trädde i kraft den 21 december 2018. Det utgör en omarbetning av och ersätter vissa tidigare gällande EU-direktiv på området för elektronisk kommunikation. Direktivet innehåller inga förändringar när det gäller det nationella utrymmet att anta bestämmelser som gäller för brottsbekämpande ändamål. Medlemsstaterna ska senast den 21 december 2020 anta och offentliggöra de lagar och andra författningar som är nödvändiga för att genomföra direktivet. Dessa bestämmelser ska tillämpas från och med samma dag.

4.1.3 Lagen om elektronisk kommunikation m.m.

Lagen om elektronisk kommunikation trädde i kraft år 2003. Genom lagen genomförs i huvudsak den EU-rättsliga regleringen på området för elektronisk kommunikation.

Lagen om elektronisk kommunikation är i huvudsak en näringsrättslig lagstiftning som syftar till att enskilda och myndigheter ska få tillgång till säkra och effektiva elektroniska kommunikationer och största möjliga utbyte vad gäller urvalet av elektroniska kommunikationstjänster samt deras pris och kvalitet.

Vid lagens tillämpning ska särskilt beaktas elektroniska kommunikationers betydelse för yttrandefrihet och informationsfrihet (1 kap. 1 §). Åtgärder som vidtas med stöd av lagen får inte vara mer ingripande än som framstår rimligt och ska vara proportionella med hänsyn till bl.a. lagens syften (1 kap. 2 §).

Lagen gäller elektroniska kommunikationsnät och kommunikationstjänster med tillhörande installationer och tjänster samt annan radioanvändning (1 kap. 4 § första stycket). Elektroniskt kommunikationsnät definieras i lagen som 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 elektronisk kommunikationstjänst avses i lagen en tjänst som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät (1 kap. 7 §).

Bestämmelser om säkerhet vid tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster finns i 6 kap. 3–4 b §§. Här anges bl.a. att lämpliga tekniska och organisatoriska åtgärder ska vidtas för att säkerställa att behandlade uppgifter skyddas. Lagen innehåller vidare bestämmelser om under vilka förutsättningar trafikuppgifter får behandlas (6 kap. 5–8 §§). 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.

För att säkerställa tillgången till vissa uppgifter för brottsbekämpande ändamål föreskrivs i 6 kap. 16 a § en skyldighet för vissa leverantörer att lagra vissa närmare angivna uppgifter. Omfattningen av lagringen är begränsad till uppgifter som genereras eller behandlas vid telefonitjänst, meddelandehantering, internetåtkomst och tillhandahållande av kapacitet för att få internetåtkomst (anslutningsform). Lagringsskyldighetens längd regleras i 6 kap. 16 d § och varierar från två månader upp till tio månader beroende på uppgiftsslag. När lagringstiden har löpt ut ska uppgifterna omedelbart utplånas, om inte en begäran om utlämnande dessförinnan har kommit in. I sådana fall ska uppgifterna i stället utplånas så snart de har lämnats ut. Den som är skyldig att lagra uppgifter har rätt till ersättning för kostnader som uppstår när lagrade uppgifter lämnas ut. Ersättningen ska betalas av den myndighet som har begärt uppgifterna (6 kap. 16 e §).

Vissa bestämmelser i lagen om elektronisk kommunikation knyter an till rättegångsbalkens regler om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. I 6 kap. 19 § LEK regleras anpassningsskyldigheten för leverantörerna. 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 sådana former att verkställandet inte röjs. Innehållet i och uppgifter om avlyssnade eller övervakade meddelanden ska göras tillgängliga så att informationen enkelt kan tas om hand. En liknande bestämmelse finns i 16 f § samma kapitel. Enligt den ska verksamheten bedrivas så att uppgifterna som omfattas av lagringsskyldigheten utan dröjsmål kan lämnas ut och så att verkställandet av utlämnandet inte röjs. Uppgifterna ska göras tillgängliga på ett sådant sätt att informationen enkelt kan tas om hand.

I 6 kap. 20 § föreskrivs att den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst 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. Enligt lagen har leverantörerna dessutom tystnadsplikt för uppgift som hänför sig till användning av vissa hemliga tvångs-

medel, nämligen hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, kvarhållande av försändelser samt inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen). Tystnadsplikt gäller även för uppgift som hänför sig till en begäran om utlämnande av abonnemangsuppgifter till brottsbekämpande myndigheter vid misstanke om brott (6 kap. 21 § 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 ger såväl de brottsbekämpande som andra myndigheter möjligheter att utan domstolsprövning få tillgång till vissa uppgifter (6 kap. 22 § LEK). Reglerna innebär bl.a. att leverantörerna i vissa fall är skyldiga att på begäran lämna ut uppgifter om abonnemang, dvs. uppgifter som identifierar en abonnent eller ett abonnemang, framför allt namn, titel, adress och nummer (se nedan).

Post- och telestyrelsen är tillsynsmyndighet enligt lagen om elektronisk kommunikation (se 2 § förordningen [2003:396] om elektronisk kommunikation).

I promemorian Genomförande av direktivet om inrättande av en kodex för elektronisk kommunikation, som har upprättats inom Regeringskansliet, föreslås en ny lag som ersätter den nuvarande lagen om elektronisk kommunikation. Den nya lagen genomför bl.a. EU:s direktiv om inrättande av en kodex för elektronisk kommunikation. Bestämmelserna om integritetsskydd och lagring av trafikuppgifter m.m. för brottsbekämpande ändamål i den nuvarande lagen förs enligt förslaget över till den nya lagen. Enligt förslaget ska tillsynsmyndigheten ha möjlighet att ta ut en sanktionsavgift av den som inte uppfyller kraven i lagen på att bl.a. bedriva sin verksamhet så att beslut om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation kan verkställas och att uppgifter om abonnemang lämnas ut (se 11 kap. 1 § i lagförslaget). Lagändringarna föreslås träda i kraft den 21 december 2020.

4.2 Brottsbekämpande verksamhet

Brottsbekämpande verksamhet innefattar främst åtgärder för att dels förebygga, förhindra och upptäcka brottslig verksamhet, dels för att utreda och beivra brott. Polisen (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 i rättegångsbalken (RB) 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. Verksamheten omfattar bl.a. underrättelseverksamhet. Både Polismyndigheten och Säkerhetspolisen bedriver underrättelseverksamhet. Sådan verksamhet bedrivs också vid vissa andra myndigheter, såsom Ekobrottsmyndigheten och Tullverket. Underrättelseverksamheten är i huvudsak inriktad på att avslöja om en viss, inte närmare specificerad brottslighet har ägt rum, pågår eller kan antas komma att begås. Ett övergripande mål är att förse de brottsutredande myndigheterna med kunskap som kan omsättas i operativ verksamhet.

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, se nedan. 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. (Se SOU 2017:75 s. 84 f., Ds 2018:35 s. 34 och prop. 2018/19:96 s. 14.)

4.3 Brottsbekämpande myndigheters tillgång till elektronisk kommunikation

4.3.1 Tillgång till uppgifterna inom en förundersökning

Tillgången till uppgifter från elektronisk kommunikation är ofta avgörande för att utredningar om allvarlig brottslighet ska kunna föras framåt. Bestämmelser som ger de brottsbekämpande myndigheterna tillgång till sådana uppgifter inom en förundersökning finns i 27 kap. RB som reglerar vissa straffprocessuella tvångsmedel.

Straffprocessuella åtgärder företas i myndighetsutövning och innebär intrång i en persons rättssfär utan att personen lämnat sitt samtycke. Reglerna bygger på en avvägning mellan samhällets krav på en effektiv brottsbekämpning och den enskildes krav på integritet och rättssäkerhet. Bland de straffprocessuella tvångsmedlen intar de hemliga tvångsmedlen en särställning. Den berörde är inte medveten om dessa åtgärder, men det antas att de äger rum mot hans eller hennes vilja. Till de hemliga tvångsmedlen räknas främst hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig

rumsavlyssning. Den 1 april 2020 infördes ytterligare ett hemligt tvångsmedel, hemlig dataavläsning.

För all användning av tvångsmedel gäller – vid sidan av kravet på uttryckligt lagstöd (legalitetsprincipen) – tre allmänna principer. Dessa principer är 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. Ett tvångsmedel får alltså endast användas för det ändamål som framgår av lagstiftningen. Reglerna om hemliga tvångsmedel innehåller dock inte några ändamålsbestämmelser (se t.ex. SOU 2018:61 s. 42). *Behovsprincipen* innebär att en myndighet får använda ett tvångsmedel bara när det finns ett påtagligt behov av det och en mindre ingripande åtgärd inte är tillräcklig. När det inte längre föreligger skäl för åtgärden ska den upphävas. Åtgärder som huvudsakligen har till syfte att underlätta för myndigheten anses strida mot principen. Enligt *proportionalitetsprincipen*, som är lagfäst i bl.a. 27 kap. 1 § tredje stycket RB, ska en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet stå i rimlig proportion till vad som står att vinna med åtgärden. 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 rättsliga skyddade intressen. Proportionalitetsavvägningar kan därför få till följd att en myndighet exempelvis underlåter en tvångsåtgärd mot en advokatbyrå, ett sjukhus, en tidningsredaktion eller någon annan inrättning där särskilt känsliga uppgifter bevaras eller yppas (se SOU 2017:75 s. 91).

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 kallas att 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 efter-

hand underrätta vissa personer om att hemliga tvångsmedel har använts samt Säkerhets- och integritetsskyddsnämndens tillsyn över de brottsbekämpande myndigheternas användning av tvångsmedlen.

Hemlig avlyssning av elektronisk kommunikation

Hemlig avlyssning av elektronisk kommunikation 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.

Hemlig avlyssning av elektronisk kommunikation får användas vid förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år. Därutöver får tvångsmedlet användas vid förundersökning om vissa samhällsfarliga brott som bekämpas av Säkerhetspolisen, t.ex. sabotage, spionerі och vissa former av terroristbrottslighet. Tvångsmedlet får också användas vid förundersökning om försök, förberedelse eller stämpling till nu nämnd brottslighet i den mån sådana förstadier till brott är straffbelagda. Avlyssning 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 (27 kap. 18 § andra stycket RB).

En förutsättning för att hemlig avlyssning av elektronisk kommunikation 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 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 (t.ex. en ip-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 ger inte tillgång till innehållet i utväxlade meddelanden. Det som kan hämtas in är i stället trafikuppgifter och lokaliseringsuppgifter. Hemlig övervakning av elektronisk kommunikation omfattar såväl inhämtning av uppgifter från telefoni- och internetleverantörer som inhämtning genom egna tekniska medel som de brottsbekämpande myndigheterna förfogar över. Tvångsmedlet kan även användas för att hindra meddelanden som överförs i ett elektroniskt kommunikationsnät från att nå fram.

Hemlig övervakning av elektronisk kommunikation 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, spioneri och vissa former av terroristbrottslighet. Tvångsmedlet 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).

Hemlig övervakning av elektronisk kommunikation får användas när någon är skäligen misstänkt för brottet eller, med vissa begränsningar, för att utreda vem som skäligen kan misstänkas för brottet. Åtgärden ska vara av synnerlig vikt för utredningen (27 kap. 20 § RB).

4.3.2 Tillgång till uppgifterna utanför en förundersökning

En grundläggande förutsättning för att straffprocessuella tvångsmedel ska få användas är normalt att en förundersökning har inletts. Användningen ska då ytterst ha till syfte att utreda och lagföra ett visst brott. Regleringen ger dock stöd även för att i vissa fall använda hemliga tvångsmedel för att förebygga, avslöja eller förhindra brottslig verksamhet utan att en förundersökning har inletts, dvs. i underrättelseverksamhet. Lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott och lagen (1991:572) om särskild utlänningskontroll utökar möjligheterna att under särskilda omständigheter ge Polismyndigheten och Säkerhetspolisen tillstånd att använda vissa hemliga tvångsmedel enligt 27 kap. RB. Även inhämtning av uppgifter enligt den ovan nämnda inhämtningslagen utgör ett hemligt tvångsmedel. De allmänna principerna för all användning av tvångsmedel gäller även i dessa fall. Vidare finns det krav på kontrollmekanismer och rättssäkerhetsgarantier knutna till var och en av de här angivna lagarna.

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. hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation 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.

Hemlig avlyssning och övervakning av elektronisk kommunikation 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. Det sker dock mycket sällan.

Frågan om tillstånd till tvångsmedel enligt lagen prövas av domstol (Stockholms tingsrätt) efter ansökan av åklagare. Tillstånd får meddelas endast om åtgärden är proportionerlig och av synnerlig vikt för att förhindra brottslig verksamhet.

Lagen om särskild utlänningskontroll

Enligt lagen om särskild utlänningskontroll (LSU) får en utlänning utvisas ur landet bl.a. om det med hänsyn till vad som är känt om utlänningens tidigare verksamhet och övriga omständigheter kan befaras att han eller hon kommer att begå eller medverka till terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott eller försök, förberedelse eller stämpling till sådant brott (1 § LSU). Om ett beslut om sådan utvisning tills vidare inte ska verkställas på grund av inhibition eller ett tidsbegränsat uppehållstillstånd, får Migrationsverket eller regeringen besluta att vissa tvångsmedelsregler som finns i lagens 19–22 §§ ska tillämpas på utlänningen. Detsamma gäller om det utvisningsbeslut som inte ska verkställas har fattats enligt 8 kap. utlänningslagen (2005:716) och det finns sådana omständigheter avseende utlänningen som nämnts ovan (11 och 11 a §§ LSU).

Lagens tvångsmedelsregler innebär bl.a. att rätten under vissa förutsättningar kan meddela tillstånd enligt 27 kap. RB till hemlig avlyssning av elektronisk kommunikation eller, om det är tillräckligt, hemlig övervakning av elektronisk kommunikation. Sådant tillstånd får meddelas om det är av betydelse för att utreda om utlänningen eller en organisation eller grupp som han eller hon tillhör eller verkar för planlägger eller förbereder terroristbrott enligt 2 § lagen om straff för terroristbrott och det finns synnerliga skäl (19 och 20 §§ LSU).

Frågan om tillstånd till tvångsmedel enligt lagen prövas av Stockholms tingsrätt på begäran av Säkerhetspolisen eller Polismyndigheten.

Inhämtningslagen

Enligt lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet får Polismyndigheten, Säkerhetspolisen 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 (1 §). Lagen reglerar enbart inhämtning från den som enligt lagen om elektronisk kommunikation tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och 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 spionerі (2 §). Genom rekvisitet ”brottslig verksamhet” framgår att det inte ställs krav på

att det ska finnas en misstanke om ett specifikt brott (se prop. 2011/12:55 s. 121). Det föreligger därför en principiell skillnad i förhållande till tillämpningsområdet för straffprocessuella tvångsmedel enligt rättegångsbalken.

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

4.3.3 Särskilt om hemlig dataavläsning

Genom lagen (2020:62) om hemlig dataavläsning har ett nytt hemligt tvångsmedel införts. Hemlig dataavläsning 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 §). Tvångsmedlet ger Polismyndigheten, Säkerhetspolisen, Tullverket och Ekobrottsmyndigheten möjligheter att avlyssna och övervaka personer som är misstänkta för eller förväntas begå allvarliga brott. Hemlig dataavläsning 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 läsa av innehållet. 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. Om hårdvara behöver installeras i till exempel 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 innehåller ett flertal bestämmelser som innebär krav på kontrollmekanismer och rättssäkerhetsgarantier. Tvångsmedlet får till exempel inte användas mot vissa yrkesgrupper, såsom läkare, journalister och advokater.

4.3.4 Abonnemangsuppgifter

Någon definition av begreppet abonnemangsuppgift saknas såväl i EU-rätten som i nationell rätt. Som tidigare anförts avses dock med uppgift om abonnemang vanligtvis uppgifter om abonnentens nummer, namn, titel och adress. Till abonnemangsuppgifter brukar även räknas uppgifter om exempelvis avtal och fakturering. Vidare har begreppet ansetts omfatta såväl fasta som dynamiska ip-adresser och IMSI-nummer (ett nummer som är kopplat till abonnentens simkort och därmed telefonnummer). 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 (se prop. 2018/19:86 s. 93).

Som tidigare framkommit har en leverantör som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst tystnadsplikt för bl.a. uppgifter om abonnemang (6 kap. 20 § första stycket 1 LEK). Trots tystnadsplikten har en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen eller någon annan myndighet som ska ingripa mot brottet (Tullverket, Kustbevakningen och Skatteverket) rätt att få tillgång till abonnemangsuppgifter, om uppgiften gäller misstanke om brott som myndigheten ska ingripa mot (6 kap. 22 § första stycket 2). 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. Inhämtning av sådana uppgifter får även göras i underrättelseverksamhet (se SOU 2015:31 s. 198 f. och SOU 2017:75 s. 101). 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.

Uppgifter om abonnemang anses typiskt sett vara mindre integritetskänsliga än t.ex. trafik- och lokaliseringsuppgifter. Tillgången till abonnemangsuppgifter har inte heller bedömts utgöra ett hemligt tvångsmedel och regleras därför direkt i lagen om elektronisk kommunikation. När bestämmelserna år 2012 utökades till att avse

utlämnande för alla slags brott gjordes övervägandena bl.a. utifrån att det skett en betydande teknisk utveckling och förändring av i vilken omfattning enskilda använder bl.a. datorer och mobiltelefoner. Trakasserier över internet och vuxnas kontakter med barn i sexuellt syfte bedömdes ha blivit ett allt vanligare fenomen. Regeringen fann att intresset av att lämna ut abonnemangsuppgifter för att bekämpa brott vägde tyngre än det motstående intresset av att skydda enskildas integritet (se prop. 2011/12:55 s. 102 f.).

Abonnemangsuppgifter kan på begäran lämnas ut till brottsbekämpande myndigheter även med stöd av andra bestämmelser i 6 kap. 22 § första stycket LEK. Bestämmelserna omfattar utlämnande för bl.a. delgivning i vissa fall, efterforskning av försvunna personer, identifiering vid olyckor och dödsfall samt underrättelse av vårdnadshavare till en underårig som misstänks för brott (punkterna 1, 3, 6 och 7). Tystnadsplikten genombryts i dessa fall, med ett undantag, enbart i fråga om just uppgifter om abonnemang. För ändamålet att eftersöka försvunna personer ska dock även andra uppgifter som angår ett elektroniskt meddelande, t.ex. lokaliseringsuppgifter, på begäran lämnas ut. I lagparagrafen finns också bestämmelser som under vissa närmare angivna omständigheter bryter tystnadsplikten vid utlämnande av abonnemangsuppgifter till andra än brottsbekämpande myndigheter, såsom Kronofogdemyndigheten, regionala alarmeringscentraler och Finansinspektionen.

Uppgifter om abonnemang finns tillgängliga för leverantören i elektronisk form. För att uppgifter om en fysisk person ska tas in i en abonnentförteckning som görs allmänt tillgänglig krävs att den enskilde har samtyckt till det (6 kap. 16 § 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 (se prop. 2018/19:86 s. 94).

5 Registrering av kontantkort

5.1 Inledning

Den första delen av utredningsuppdraget avser frågan om det bör införas en registreringsskyldighet avseende kontantkort till mobiltelefoner. Enligt uppdragsbeskrivningen ska vi ta ställning till om det bör införas en skyldighet att registrera uppgifter om abonnemang för kontantkort i syfte att säkerställa att uppgifterna finns tillgängliga för brottsbekämpande ändamål. I uppdraget ingår att lämna förslag till regler om en sådan skyldighet, även om vi skulle komma till slutsatsen att någon reglering inte bör införas. Det ingår också i uppdraget att överväga om nuvarande regler om tillsyn och sanktioner är tillräckliga för att säkerställa att en registreringsskyldighet efterlevs.

5.2 Kontantkort för mobiltelefoner

En mobiltelefon skickar och tar emot information med hjälp av radiovågor. När en mobiltelefon används för att ringa skickas radiosignaler till en basstation i närheten. Radiosignalerna skickas från basstationen till en annan trådlös enhet eller vidare via ett trådbundet stamnät till en annan basstation. Här kopplas samtalet till en annan mobiltelefon, till en stationär telefon eller någon annan terminal som kommunikationen sker med. För att kunna använda mobiltelefonen för att ringa behövs ett abonnemang, antingen ett kontraktsabonnemang eller ett kontantkortsabonnemang.

Vid tecknande av ett kontraktsabonnemang ingås ett avtal med en mobiloperatör om att kunna använda operatörens tjänst för en viss tid eller tillsvidare. Ett kontantkort för mobiltelefoner ger däremot en möjlighet för den enskilde att i förskott betala kostnaden för användandet av telefonen. Kostnaden för användandet dras av

från beloppet på kortet och den enskilde får därför inga räkningar. Kontantkortet togs ursprungligen fram under 1990-talet i syfte att ge nya kundgrupper möjlighet att ringa. Kontantkortet riktade sig till människor som av olika skäl inte kunde skaffa sig fast mobilabonnemang, t.ex. eftersom de saknade fast inkomst, var minderåriga eller saknade identitetshandlingar. Kontantkortsabonnemangen har visat sig vara populära av flera skäl. De kan bl.a. innebära en större flexibilitet än kontraktsabonnemang och ger en kostnadskontroll för abonnenten som skapar trygghet.

Den 30 juni 2019 fanns det totalt 14,3 miljoner mobilabonnemang i Sverige. Ett mobilabonnemang kan avse enbart samtal, både samtal och data eller endast data (mobilt bredband). Vanligast är att ett mobilabonnemang avser såväl samtal som data. Den 30 juni 2019 fanns det 11 miljoner sådana mobilabonnemang i Sverige. Antalet mobilabonnemang avseende enbart data eller enbart samtal uppgick vid samma mätning till vardera 1,6 miljoner. Av det totala antalet mobilabonnemang i Sverige är 78 procent kontraktsabonnemang. Övriga 22 procent utgörs av kontantkortsabonnemang, dvs. drygt 3,1 miljoner. Användningen av kontantkort har sjunkit kontinuerligt under senare tid. För tio år sedan var motsvarande andel av marknaden 40 procent. (Se Post- och telestyrelsens rapport Svensk telemarknad Första halvåret 2019, s. 6).

En och samma person kan inneha flera kontantkort. Det finns alltså ingen begränsning när det gäller innehavet av kontantkort. Det är stor omsättning på kontantkorten och en stor andel används endast under en kortare period.

Ett kontantkort kan köpas via mobiloperatörens hemsida. Det finns också möjlighet att köpa kontantkort i operatörernas egna butiker eller i andra affärer. Det är t.ex. möjligt att köpa kontantkort i vanliga mataffärer, på bensinmackar och i kiosker. Det förekommer också att kontantkort, som den enskilde sedan själv får ladda, delas ut gratis på stan.

Ett kontantkort för mobiltelefoni fungerar genom ett simkort som sätts in i mobiltelefonen och som sedan fylls på med en önskad summa pengar. Det är ofta möjligt att välja mellan att få ett nytt telefonnummer eller att behålla ett gammalt mobilnummer. Kontantkort har oftast en viss giltighetstid. Vidare behöver kontantkortet normalt fyllas på med pengar en gång per år för att det ska fungera.

Den som vill ladda sitt kontantkort kan använda en s.k. voucher eller laddningscheck som kan köpas där kontantkort säljs. På checken finns angivet en kod som kan knappas in direkt i mobiltelefonen. När koden har knappats in är kontantkortet laddat. Ett kontantkort kan också laddas via en internettjänst eller app.

Kontantkort kan även användas i surfplattor just för att surfa, men inte för att ringa eller skicka sms. Det kontantkort som används kan gälla för endast datakommunikation (s.k. mobilt bredband kontant) men även ett kontantkort som avser både samtal och data kan användas. Ett simkort som ger tillgång till data kan också sättas in t.ex. i ett USB-modem eller i en router. Således kan kontantkort användas även för att surfa med datorer.

Simkort kan även användas för trådlös kommunikation mellan olika maskiner. Tekniken kallas för M2M (maskin till maskin) och används för t.ex. övervakning, mätning, styrning, transport och logistik. Simkorten kan på detta sätt användas t.ex. i bilar, tåg, elmätare, hemlarm och gräsklippare. Den 30 juni 2019 fanns det 14,3 miljoner svenska simkort för M2M som använder sig av mobilnummer och marknaden växer snabbt. Svenska simkort för M2M används inte nödvändigtvis bara i Sverige utan också av kunder i utlandet. Av de 14,3 miljonerna svenska simkort för M2M används 3,6 miljoner i Sverige (se Post- och telestyrelsens rapport, s. 10). Simkort för M2M används normalt med ett kontraktsabonnemang.

Det finns numera inbyggda simkort som kallas e-sim. E-sim står för embedded sim (och alltså inte elektroniskt sim). Ett e-sim fungerar genom att den information som normalt sparats på ett fysiskt litet plastkort i stället lagras direkt i en mobiltelefon eller annan teknisk utrustning. Således programmeras information om abonnemanget och inställningar som behövs för att kunna surfa, ringa och skicka sms direkt i den tekniska produkten. För att kunna använda e-sim behövs en produkt som stöder e-sim samt en operatör som erbjuder tjänsten för denna produkt. De största operatörerna i Sverige erbjuder alla e-sim.

Den som beställer ett kontantkort på en mobiloperatörs hemsida måste uppge sitt personnummer. Detta sker för att operatören ska kunna hämta den enskildes adress och skicka hem simkortet till denne. Av säkerhetsskäl skickar nämligen operatörerna endast korten till den enskildes folkbokföringsadress Det förekommer

också att kontantkort kan beställas på nätet och därefter hämtas ut i butik.

Hos en av de större operatörerna registreras alltid uppgifter om den som köper kontantkort i operatörens egna butiker eller via hemsidan. Registreringen sker för att operatören ska kunna nå kunden i marknadsföringssyfte. Även hos operatörens större återförsäljare kan en registrering ske. Huvuddelen av kontantkorten säljs dock i mindre kiosker, där någon registrering inte sker. Hos en annan mobiloperatör är det nödvändigt att en kund registrerar sitt kontantkort för att få tillgång till mobilsvar och andra tilläggstjänster. En registrering kan också vara nödvändig för att kontantkortet ska vara möjligt att använda utomlands. En registrering av kontantkort kan ske på mobiloperatörens hemsida, i mobiloperatörens egna butiker eller hos vissa större återförsäljare. Det skiljer sig dock mellan mobiloperatörerna när det gäller i vilken grad de arbetar för att kunderna ska registrera sig. Huvuddelen av de kunder som köper kontantkort är inte registrerade.

För att registrera ett kontantkort kan det krävas att den enskilde har uppnått en viss ålder. Denna ålder skiljer sig mellan operatörerna och varierar mellan 12, 16 och 18 år. I många fall sker registreringen av barnets vårdnadshavare, som ofta är den som betalar för tjänsten. För att köpa själva kontantkortet kan det också finnas en åldersgräns enligt operatörernas villkor. Någon ålderskontroll sker dock normalt inte vid inköp i butik.

Av lagen (2010:751) om betaltjänster framgår att mobiloperatörer ska ha kontroll över vem som gör betalningar med sin mobiltelefon och mobiloperatörerna får därför inte låta sina kunder använda sådana tjänster anonymt. Reglerna syftar bl.a. till att förhindra ekonomisk brottslighet. De tjänster som berörs är till exempel inköp av bussbiljetter och betalning av parkeringsavgifter via mobiltelefonen. Den som utnyttjar dessa tjänster och betalar med sitt kontantkort måste därför registrera sitt kontantkort hos sin mobiloperatör. Detta sätt att betala har dock blivit allt mer ovanligt i takt med att andra möjligheter till mobila betalningar, t.ex. Swish, har växt sig starkare.

Ett oregistrerat kontantkort behöver alltså registreras innan det kan användas för vissa typer av betalning. Ett kontantkort kan också kopplas till den som har laddat kortet om betalningen har skett via en internettjänst. Mobiloperatörerna kan således ha tillgång till upp-

gifter om vem som innehar ett kontantkort, om kunderna själva har lämnat sådana uppgifter. Personer som köper kontantkort kontant i butik eller använder sig av kontantkort som delats ut gratis och laddar dem via en voucher som också inhandlats kontant kan dock förbli anonyma.

Det är inte alltid möjligt att använda ett kontantkort för att ringa, surfa och skicka sms utomlands. Det går dock att köpa särskilda utlandspaket till kontantkort som gör att det går att använda telefonen utomlands. Vissa mobiloperatörer kräver i stället att ett kontantkort registreras innan det kan användas utomlands.

För att det ska vara möjligt att använda ett svenskt kontantkort utomlands måste den svenska mobiloperatören ha ett avtal med minst en operatör i det land man befinner sig i (ett s.k. internationellt roamingavtal). På motsvarande sätt krävs att en utländsk operatör har avtal med minst en svensk operatör för att ett utländskt kontantkort ska kunna användas i Sverige. Roaming innebär alltså att man kopplar upp sig mot en utländsk operatörs nät när man använder sin mobiltelefon utomlands. Roaming inom EU/EES regleras genom ett antal förordningar, bl.a. i den så kallade roamingförordningen (Europaparlamentets och Rådets förordning (EU) 531/2012). Denna förordning ändrades genom införande av den s.k. TSM-förordningen (Europaparlamentets och Rådets förordning (EU) 2015/2120). Det finns också en genomförandeförordning som ska garantera en enhetlig tillämpning av roamingreglerna (se Kommissionens genomförandeförordning [EU] 2016/2286).

De fyra största mobiloperatörerna i Sverige är Telia, Tele2, Telenor och Hi3G (Tre). De har också egna telenät i landet. Det finns därtill en rad mobiloperatörer som inte äger sitt nät och som köper kapacitet från operatörerna som äger nät. Mobiloperatörer utan eget nät kallas virtuella operatörer eller MVNO (Mobile Virtual Network Operator). Totalt finns det ett 60-tal mobiloperatörer i Sverige, men endast sex av dessa säljer kontantkort. Enligt Post- och telestyrelsens senaste mätning den 9 december 2019 innehade de fyra största mobiloperatörerna, via olika varumärken, sammanlagt 94 procent av marknaden för kontantkort. Kontantkort säljs även av Lycamobile och Wifog.

5.3 Behovet och nyttan av uppgifter om kontantkortsabonnemang i brottsbekämpande verksamhet

Uppgifter om elektronisk kommunikation i brottsbekämpningen

För att de brottsbekämpande myndigheterna ska kunna fullgöra sina uppgifter att förebygga, förhindra och utreda brott har myndigheterna behov av information. Detta behov kan vara olika stort beroende på vilken brottslighet och vilka aktörer det är fråga om. Brottsbekämparna 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 från 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 (se t.ex. SOU 2017:75 s. 120 f.).

Uppgifter om elektronisk kommunikation kan svara på frågor om vilka nummer som har haft kontakt med varandra, hur intensiv kommunikationen har varit och var användare av t.ex. mobiltelefoner har befunnit sig. Genom tillgången till historiska trafik- och lokaliseringsuppgifter kan de brottsbekämpande myndigheterna klarlägga händelser som anknyter såväl till själva brottstillfället som till planläggning och flykt. Inhämtade uppgifter kan i många fall också få till följd att personer avförs från en utredning eftersom misstankarna mot dem visar sig sakna substans. Det är inte möjligt att ersätta den här inhämtningen med t.ex. fysisk spaning eftersom inhämtningen avser historiska uppgifter. Trafikuppgifternas betydelse i brottsutredningar hänger också samman med att den information som kommer fram vid hemlig övervakning och hemlig avlyssning av elektronisk kommunikation ofta bedöms ha ett

betydande bevisvärde i rättegångar som rör grov och organiserad brottslighet. (Se a.a. s. 121 f.)

Som framgått i avsnitt 4 finns bestämmelser som ger de brottsbekämpande myndigheterna möjlighet att under en förundersökning hämta in uppgifter om elektronisk kommunikation främst i 27 kap. RB, där bl.a. tillgången till de hemliga tvångsmedlen hemlig avlyssning av elektronisk kommunikation (HAK) och hemlig övervakning av elektroniska kommunikation (HÖK) regleras.

Uppgifter om elektronisk kommunikation kan även vara av största vikt för att i underrättelseverksamhet upptäcka, förebygga och förhindra 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 yttre fysisk spaning, som är resurskrävande och därför viktig att använda på rätt plats och vid rätt tillfälle (se skr. 2018/19:19 s. 34). Som framgått ovan regleras förutsättningarna för att få tillgång till uppgifter om elektronisk kommunikation utanför en förundersökning främst i 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) och lagen (1991:572) om särskild utlänningskontroll.

Tillgången till abonnemangsuppgifter

Med uppgift om abonnemang avses främst uppgifter om abonnentens nummer, namn, titel och adress. Fler uppgifter kan dock inrymmas i begreppet och viss osäkerhet råder kring hur begreppet närmare bör tolkas (se t.ex. prop. 2018/19:86 s. 93). De brottsbekämpande myndigheterna har möjlighet att få tillgång till abonnemangsuppgifter på samma sätt som enskilda personer, dvs. via de tjänster för abonnentupplysning som finns. Sådana tjänster finns vanligtvis på internet, på hemsidor som t.ex. Eniro och hitta.se. För uppgifter som finns öppet på internet är det oftast enklast för de brottsbekämpande myndigheterna att använda sig av abonnentupplysningstjänsterna. När det gäller abonnenter som inte har

samtyckt till att deras uppgifter publiceras i en abonnentförteckning kan de brottsbekämpande myndigheterna vända sig direkt till operatörerna. Trots operatörernas tystnadsplikt har nämligen de brottsbekämpande myndigheterna rätt att få tillgång till abonnemangsuppgifter, om uppgifterna gäller misstanke om brott som myndigheten ska ingripa mot (6 kap. 22 § första stycket 2 LEK). Regleringen innebär att de brottsbekämpande myndigheterna i princip har rätt att från operatörerna hämta in abonnemangsuppgifter för att beivra alla typer av brott utom sådana som åtalas enbart av målsäganden. Inhämtning av abonnemangsuppgifter får även göras i underrättelseverksamhet. Uppgifter om abonnemang får också lämnas ut till brottsbekämpande myndigheter i vissa andra situationer, som omfattar delgivning, efterforskning av försvunna personer, identifiering vid olyckor och dödsfall samt underrättelse av vårdnadshavare till en underårig som misstänks för brott (se 6 kap. 22 § första stycket 1, 3, 6 och 7 LEK).

För att säkerställa tillgången till vissa uppgifter om elektronisk kommunikation för brottsbekämpande ändamål är bl.a. mobiloperatörer skyldiga att lagra vissa uppgifter, däribland sådana uppgifter om abonnemang som är nödvändiga för att spåra och identifiera kommunikationskällan (6 kap. 16 a § LEK). Lagringsskyldigheten omfattar uppgifter om vem som har ringt vem (t.ex. det uppringande numret och abonnentens namn liksom de nummer som slagits och den abonnentens namn), vid vilken tidpunkt och varaktigheten av kommunikationen (t.ex. datum och tid för ett telefonsamtals påbörjande och avslutande). De lagrade uppgifterna får behandlas endast för vissa särskilt angivna ändamål, däribland för att lämnas ut enligt 6 kap. 22 § första stycket 2 LEK (se 6 kap. 16 c §). Lagringsskyldigheten förutsätter dock att den enskilde operatören har genererat eller behandlat uppgifterna. Uppgifterna behöver inte ha varit föremål för en mer konkret hantering eller användning, men lagringsskyldigheten förutsätter att uppgifterna någon gång har funnits hos operatören. Operatörerna har däremot varken någon rätt eller skyldighet att samla in abonnemangsuppgifter som de inte behöver för egna ändamål även om uppgifterna omfattas av lagringsskyldigheten (se prop. 2010/11:46 s. 77). Det kan dock noteras att lagring i och för sig krävs av uppgifter om första aktiveringen av en förbetald anonym tjänst, dvs. oregistrerade

kontantkort (se 39 § 6 förordningen [2003:396] om elektronisk kommunikation, FEK).

Huruvida de brottsbekämpande myndigheterna har möjlighet att få tillgång till abonnemangsuppgifter från mobiloperatörerna beror därmed på vilka uppgifter som dessa behandlar. Detta är i sin tur avhängigt vilka uppgifter som operatörerna behöver för sina egna ändamål. Trafikuppgifter som krävs för abonnentfakturering och avräkning av samtrafik får enligt 6 kap. 6 § LEK behandlas till dess att fordran är betald eller preskription inträtt och det inte längre lagligen går att göra invändningar mot faktureringen eller avgiften. Uppgifterna får även, med den enskildes samtycke, behandlas av den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst för att marknadsföra elektroniska kommunikationstjänster eller för att tillhandahålla andra tjänster där uppgifterna behövs. Operatörer har också rätt att fortsätta behandla trafikuppgifter för att avslöja obehörig användning av elektroniska kommunikationsnät- och tjänster (6 kap. 8 §). Sammantaget ger dessa regler ett relativt stort utrymme för tillhandahållare att behandla trafikuppgifter för eget behov. Lagrade och på annat sätt behandlade trafikuppgifter ska dock utplånas eller avidentifieras så snart de inte längre behövs (6 kap. 5 §).

Mobiloperatörerna har behov av att hålla register med uppgifter över sina kontraktsabonnenter, kanske främst för att kunna sköta sin fakturering. Eftersom identiteten hos den som har ett kontantkortsabonnemang sällan behövs för fakturering förblir sådana abonnenter i regel anonyma för operatörerna. Som framgått ovan kan en registrering av en kontantkortskund ske hos en operatör av andra orsaker, t.ex. för att kunden ska få tillgång till vissa tjänster. Registreringen sker dock endast om kunden själv väljer detta. Det stora flertalet kontantkortskunder förblir oregistrerade och därmed anonyma för operatörerna. Detta innebär att de brottsbekämpande myndigheterna inte har möjlighet att genom operatörernas försorg få tillgång till direkta uppgifter om vem som innehar dessa kontantkortsabonnemang.

Behovet av en skyldighet att registrera uppgifter om kontantkortsabonnemang

Möjligheten att använda hemlig avlyssning av elektronisk kommunikation förutsätter att åtgärden kan hänföras till antingen en adress, t.ex. ett telefonnummer, eller en elektronisk kommunikationsutrustning, t.ex. en viss mobiltelefon. Som huvudregel gäller detsamma vid hemlig övervakning av elektronisk kommunikation. Det beslut som läggs till grund för åtgärden ska vidare innehålla uppgift om adressen eller kommunikationsutrustningen, dvs. uppgifter om abonnemanget eller den fysiska utrustningen. Att åtgärden konkretiseras med avseende på adress eller kommunikationsutrustning är en förutsättning såväl för tillstånd som för att beslutet ska vara praktiskt verkställbart. (Se tex. 27 kap. 20 och 21 §§ RB och 2 och 8 §§ preventivlagen.)

En grundläggande tanke bakom regleringen om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation är att åtgärderna endast får avse den som är skäligen misstänkt för brott (se prop. 1994/95:227 s. 20). En förutsättning för tillstånd att avlyssna eller övervaka ett telefonnummer är i normalfallet att numret har en viss närmare anknytning till den misstänkte. Kopplingen kan vara hänförlig till antingen ett innehav eller ett användande. Kravet innebär, förutom att åtgärden måste avse en adress (t.ex. ett telefonnummer) eller en viss elektronisk kommunikationsutrustning, att adressen eller kommunikationsutrustningen 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. Om en sådan koppling saknas krävs i stället att det finns synnerlig anledning att anta att den misstänkte har kontaktat eller kommer att kontakta numret under den tid som tillståndet avser. Det finns därutöver en möjlighet för brottsbekämpande myndigheter att vid förundersökning använda hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brott (27 kap. 20 § andra stycket RB). För att så ska få ske krävs att det är av synnerlig vikt för utredningen. Övervakningen får dessutom endast användas vid särskilt grov brottslighet och får, såvitt avser uppgifter om meddelanden, endast avse förfluten tid. Tvångsmedlet kan på detta sätt användas för att t.ex. i samband med ett grovt brott hämta in

uppgifter om vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område eller för att övervaka en målsägandes telefon.

I normalfallet är det dock alltså så att det krävs att ett nummer kan knytas till en misstänkt för att en brottsbekämpande myndighet ska erhålla tillstånd att avlyssna eller övervaka ett telefonnummer. Något krav på att personen ska vara identifierad med t.ex. namn torde inte finnas. Däremot får inte den misstänkte vara helt okänd utan ska kunna identifieras så att förväxlingsrisk praktiskt tagen är utesluten (se JO 2006/07 s. 30).

Tillgång till uppgift om innehavaren av ett telefonnummer är nödvändig för att det ska vara möjligt att utröna om det finns en koppling mellan numret och den skäligen misstänkte. Kunskap om den personens identitet krävs oavsett om det är den misstänkte som är innehavare av det telefonnummer som åtgärden avser eller om det är någon annan som innehar den adress som man vill avlyssna eller övervaka, t.ex. någon som det finns synnerlig anledning att anta att den misstänkte kommer att kontakta. Med hjälp av registrerade abonnemangsuppgifter kan brottsbekämpande myndigheter på ett effektivt sätt knyta en viss person till ett visst nummer. Denna koppling kan visserligen gå att få fram på andra sätt än genom att hämta in direkta abonnemangsuppgifter från operatörerna. Uppgifterna kan t.ex. hämtas in via fysisk spaning eller avlyssning och övervakning av andra personers telefoner. Även andra metoder kan användas. Av sekretesshänsyn redovisas inte dessa metoder här. De olika sätten att hämta in de relevanta uppgifterna är dock ofta mycket ineffektiva och långt ifrån alltid tillförlitliga. Utan tillgång till registrerade abonnemangsuppgifter har därför de brottsbekämpande myndigheterna ofta stora svårigheter att knyta en viss person till ett visst kontantkort och därmed att få tillstånd att övervaka eller avlyssna elektronisk kommunikation. Detta gäller både i underrättelseverksamhet och i förundersökningsverksamhet.

Som framgått ovan är brottsbekämpande myndigheters möjligheter att få tillgång till elektronisk kommunikation ofta avgörande för om en brottsutredning ska bli framgångsrik. Det förhållandet att brottsbekämpande myndigheter inte genom operatörernas försorg direkt kan få tillgång till uppgifter om vem som är registrerad innehavare av ett kontantkort, medför alltså att det blir svårare för myndigheterna att få till stånd beslut om hemlig avlyssning eller

övervakning. Möjligheterna att få tillgång till uppgifter om vem som har varit i kontakt med vem, när detta skett och var blir därmed kraftigt begränsade. Enligt vad vi har tagit del av känner många personer involverade i organiserad brottslighet till detta. I dagsläget är det mycket vanligt att mobiltelefoner på olika sätt används vid brottslig verksamhet. Det finns en tydlig tendens bland kriminella att använda anonyma kontantkort för sådan kommunikation som gäller brottslig verksamhet. Enligt den information vi har tagit del av är det också vanligt att kriminella personer köper, byter och slänger mobiltelefoner och/eller anonyma kontantkort mycket frekvent. I samband med husrannsakan hos misstänkt kriminella personer påträffas ofta oanvända och oregistrerade kontantkort i stora mängder. Ett vanligt förfaringssätt är att ha många telefoner och oregistrerade kontantkort. I samband med grov brottslighet är det också vanligt förekommande att kontantkort aktiveras kort tid före brottet och därefter slängs. Polismyndigheten har angett att det t.ex. i utredningar om narkotikarelaterad brottslighet endast i undantagsfall förekommer mobiltelefoner med kontraktsabonnemang. Förfaringssättet är inte nytt utan har förekommit under flera år. Det har i olika sammanhang under senare år konstaterats att användningen av oregistrerade kontantkort är vanligt förekommande bland personer med koppling till den organiserade brottsligheten. (se t.ex. SOU 2012:44 s. 221, SOU 2015:31 s. 165, SOU 2017 :75 s. 236, SOU 2017:89 s. 185, SOU 2018 :30 s. 53 f. och prop. 2019/20:145).

Det är ofta ett problem för de brottsbekämpande myndigheterna att kriminella personer har fullt klart för sig vilka gränser som finns för myndigheternas operativa möjligheter och utnyttjar den kunskapen i sin brottsliga verksamhet. Den anonymitet som kontantkorten ger och fördelarna med anonymiteten är enligt uppgifter från polisen helt känd i kriminella kretsar ”ner på lägsta nivå” och utnyttjas av personer vid all typ av brottslighet i syfte att försvåra eller omöjliggöra de brottsbekämpande myndigheternas arbete. Detta sker givetvis mot bakgrund av att det ofta ligger ett högt bevisvärde i den information hemlig avlyssning och övervakning av elektronisk kommunikation kan ge.

Oregistrerade kontantkort används även av brottsaktiva inom Säkerhetspolisens verksamhetsområde, t.ex. av personer inom extremistmiljöer. Efter terrordådet på Drottninggatan i Stockholm 2017 framkom att den dömde Rakhmat Akilov hade tillgång till 53 olika

oregistrerade kontantkort. Svenska oregistrerade kontantkort användes även av några av hans kontakter utomlands. Enligt Säkerhetspolisen är det i dagsläget mer sannolikt att ett svenskt telefonnummer i konfliktområdet Syrien och Irak inte tillhör en svensk person – ett fenomen som är unikt för just Sverige (se Säkerhetspolisens årsbok 2018 s. 55).

Uppgifter om abonnemang kan också ligga till grund för sådana utredningsåtgärder som inte kräver att hemliga tvångsmedel används. Tillgången till abonnemangsuppgifter har självständig betydelse för möjligheten att utreda och beivra brott som begås med hjälp av elektronisk kommunikation. Abonnemangsuppgifter kan t.ex. behövas för att utreda brott som innefattar hot, bedrägerier och trakasserier över telefon. Uppgifterna kan också användas för att utreda vuxnas kontakter med barn i sexuellt syfte. Behovet av abonnemangsuppgifter är uppenbart i de fall ett visst telefonnummer har använts i samband med brott och en uppgift om telefonnumrets innehavare skulle kunna leda utredningen framåt. Med hjälp av en uppgift om vem som står bakom ett abonnemang kan man många gånger fastställa vem som är skäligen misstänkt för brottet, vilket normalt är en förutsättning för andra utredningsåtgärder, t.ex. för att förhör ska kunna hållas med den misstänkte.

Den anonymitet som följer med oregistrerade kontantkort kan i sig också missbrukas och inbjuda till brottslighet där användningen av telefon utgör en del av brottet, t.ex. hot per telefon. Det har t.ex. påpekats att samtal från oregistrerade kontantkort kan användas av män för att trakassera en tidigare partner eller av ungdomar som ett medel för mobbning eller trakasserier.

Företrädare för Säkerhetspolisen, Polismyndigheten och Tullverket har alla uttryckt att anonyma kontantkort utgör ett stort effektivitetshinder vid utredning av grova brott. När det saknas registrerade uppgifter om vem står för ett abonnemang måste myndigheterna förlita sig på andra metoder för att fastställa vem som innehar ett visst telefonnummer. Dessa metoder bedöms dock, som berörts ovan, vara långt mindre effektiva och dessutom mindre tillförlitliga. Det anges från de brottsbekämpande myndigheterna att det läggs ner mycket stora resurser på att på olika sätt försöka identifiera vilka telefonnummer som används i samband med brottslig verksamhet och vilka personer som använder numren. Arbetet med att identifiera brukaren av ett visst telefonnummer kan

engagera en mängd personer under flera veckors tid, vilket kostar mycket pengar och resurser samtidigt som brottsutredningsarbetet tappar markant i effektivitet. Det finns dessutom en uppenbar risk för att arbetet med att identifiera vem som innehar ett visst telefonnummer blir resultatlöst, vilket innebär att hemlig avlyssning eller övervakning över huvud taget inte kan användas i det brottsbekämpande arbetet. Mycket tid och arbete behöver också läggas ned på att sortera bort de kontantkortsnummer som används av personer som inte alls är intressanta för den aktuella brottsutredningen. Problemen anges vara desamma i både underrättelse- och förundersökningsarbetet.

Säkerhetspolisen har därutöver under de senaste åren kunnat se ett nytt användningsområde för svenska oregistrerade kontantkort. Med hjälp av oregistrerade svenska kontantkort skapas konton för webbaserade tjänster som därefter används för krypterad och anonym kommunikation. De aktuella kontantkorten, som beställs i Sverige eller plockas upp här gratis på stan, används alltså inte för att ringa eller skicka meddelanden utan endast för att skapa konton i olika chattapplikationer. Information om chattkonton kopplade till svenska mobilnummer skickas därefter till länder som Syrien, Irak, Libyen och Somalia. Syftet är att dessa chattkonton ska kunna användas för krypterad och anonym kommunikation. Svenska kontantkort bidrar på detta sätt till att skapa möjligheter att anonymt diskutera brottsplaner och sprida propaganda. Säkerhetspolisen har uppmärksammat flera fall av vad som benämns som massdistribution av telefonnummer i form av inloggningsuppgifter till terrorkopplade utländska aktörer utomlands. Enligt Säkerhetspolisen skulle ett förbud mot oregistrerade kontantkort försvåra för de här aktörerna. (Se Säkerhetspolisens årsbok 2018 s. 55 f.)

Enligt de brottsbekämpande myndigheterna finns det alltså ett klart behov av att uppgifter om abonnemang registreras även för de personer som innehar kontantkortsabonnemang. Det är en gemensam uppfattning att en registreringsskyldighet för kontantkort skulle innebära besparingar för både förundersöknings- och underrättelsearbetet. Det kan visserligen ifrågasättas hur pass effektiv en registreringsskyldighet skulle vara och därmed vilka nytta det finns av en registreringsskyldighet för den brottsbekämpande verksamheten. Vi återkommer till dessa frågor nedan. Det kan dock redan här konstateras att det är en gemensam uppfattning bland de

brottsbekämpande myndigheterna att en skyldighet att registrera uppgifter om kontantkortsinnehav även skulle vara av nytta för brottsbekämpningen.

5.4 Tidigare behandling av frågan

Frågan om det borde införas en skyldighet att registrera uppgifter om abonnemang för kontantkort har övervägts i ett tidigare lagstiftningsärende. Frågan behandlades av Beredningen för rättsväsendets utveckling i delbetänkandet Tillgång till elektronisk kommunikation i brottsutredningar m.m. (SOU 2005:38). Dåvarande Rikspolisstyrelsen hade i en skrivelse till beredningen påtalat behovet av att mobiloperatörerna åläggs en skyldighet att registrera uppgifter om vem som innehar ett kontantkort samt uppgifter om var och när kortet köpts. Rikspolisstyrelsen hade också redovisat att Norge, Schweiz och Tyskland infört lagstiftning som innebär en skyldighet att registrera abonnenten bakom kontantkort. Beredningen anförde bl.a. att när mobiltelefoner förekommer vid brottslig verksamhet är det i princip uteslutande anonyma kontantkort som utnyttjas för att undgå upptäckt och försvåra det brottsutredande arbetet. Det angavs att det i beredningen fanns en mycket stor förståelse för de brottsutredande myndigheternas påtagliga behov av att i olika sammanhang få tillgång till uppgifter om abonnemang rörande kontantkort. Vid en avvägning mot andra intressen bedömde dock beredningen att någon registreringsskyldighet inte borde införas. Det främsta skälet härför var den tveksamhet som ansågs finnas rörande hur effektiv den föreslagna ordningen skulle bli för den brottsutredande verksamheten. Beredningen bedömde dock att frågan skulle få allt större betydelse framöver och förespråkade att den drevs i internationella sammanhang eller utifrån de erfarenheter som finns i andra länder av nationell lagstiftning på området. (Se SOU 2005:38 s. 239 ff.)

Den dåvarande regeringen delade bedömningen att en registreringsskyldighet för kontantkort inte borde införas (prop. 2011/12:55). Regeringen uttalade visserligen att de brottsutredande myndigheterna hade ett påtagligt behov av att få tillgång till uppgifter om abonnemang avseende kontantkort, men bedömde samtidigt att det fanns stora problem förknippade med ett system för registrering av

abonnemangsuppgifter till kontantkort. Regeringen konstaterade att en registreringsskyldighet skulle innebära dels ett åliggande för leverantörer med kostnader som följd, dels en skyldighet för den som köper ett kontantkort att ge upp sin anonymitet. Regeringen konstaterade också att det var osäkert hur effektiv en registreringsskyldighet skulle bli från brottsbekämpningssynpunkt. Tvivlen på effektiviteten grundades bl.a. på att man inte heller med en registreringsskyldighet skulle kunna säkerställa att den som har eller använder ett visst telefonnummer också alltid är den som finns registrerad. En registreringsskyldighet skulle inte heller förhindra att anonyma kontantkort köps utomlands och utnyttjas i Sverige i brottsliga sammanhang. (Se prop. 2011/12:55 s. 104 f.)

5.5 Registreringsskyldighet i andra länder

Som tidigare framgått består 22 procent av alla mobilabonnemang i Sverige av kontantkortsabonnemang. Resten utgörs av kontraktsabonnemang. Världen över sker dock majoriteten, 73 procent, av mobilanvändandet via kontantkortsabonnemang. Av dessa abonnemang är flertalet aktiva i länder där det krävs någon form av identifiering för att registrera och använda ett simkort för mobilanvändning i eget namn. I januari 2020 hade någon form av registreringsskyldighet som omfattar kontantkort införts i 155 länder över hela världen och övervägdes därtill i flera länder (se GSMA, Access to Mobile Services and Proof of Identity 2020: The Undisputed Linkages, s. 6 f.). En registreringsskyldighet som omfattar kontantkort har således införts i en majoritet av världens länder. I världsdelar som Afrika, Asien och Sydamerika förekommer en registreringsskyldighet i så gott som samtliga länder. Även i Australien finns en registreringsskyldighet, men inte i Nordamerika.

I Europa förekommer en registreringsskyldighet för kontantkort i något mer än hälften av länderna. Någon EU-gemensam lagstiftning har inte införts på området vilket har medfört att registreringsskyldigheten är utformad på olika sätt i de länder där den införts. En registreringsskyldighet som omfattar kontantkort infördes i Norge, Tyskland och Schweiz redan 2004. Även Frankrike, Spanien, Italien, Ungern och Slovakien införde tidigt en registreringsskyldighet som omfattar kontantkort till mobiltelefoner. Under senare år har en

registreringsskyldighet införts i allt fler länder. I Belgien och Polen infördes en sådan skyldighet 2016, i Luxemburg 2017 och i Österrike 2019. En registreringsskyldighet som omfattar kontantkort finns också i Bulgarien, Grekland, Nordmakedonien, Ukraina, Turkiet, Vitryssland, Albanien, Kosovo, Montenegro, Andorra, San Marino och Monaco (se a.a. s. 26 f.).

Det främsta skälet till att en registreringsskyldighet har införts har varit att bekämpa terrorism och organiserad brottslighet. Registrering av simkort har också setts som en möjlighet att reducera mängden skräppost, verifiera användarnas ålder och motverka bedrägerier (se GSMA, Mandatory registration of prepaid SIM cards. Adressing challenges through best practice, 2016, s. 4). Enligt en enkät som utfördes bland medlemsländerna i Eurojust 2019 har, i de fall en registreringsskyldighet införts i dessa länder, detta skett i syfte att motverka kriminalitet och terrorism. Majoriteten av de stater inom EU där det finns en registreringsskyldighet har infört regleringar om detta i sin lagstiftning angående elektronisk kommunikation. Det varierar mellan länderna när det gäller t.ex. vilka uppgifter som ska registreras, under hur lång tid dessa får sparas och för vilka syften uppgifterna får användas.

Bland de länder som inte har infört någon registreringsskyldighet för kontantkort märks t.ex. USA, Danmark, Finland, Storbritannien, Portugal, Tjeckien och de baltiska staterna. Frågan om en registreringsskyldighet utreddes i Nederländerna 2017, men ledde inte till någon lagstiftning. De främsta skälen härför var att det skulle finnas vägar att kringgå registreringsskyldigheten och att det finns andra sätt att kommunicera anonymt (se bilaga 804702 till den parlamentariska handlingen 29754 nr 419). Frågan har utretts också i andra länder, däribland Litauen, utan att någon registreringsskyldighet har införts.

Registreringsskyldigheten är alltså utformad på olika sätt i olika länder. Det kan sägas finnas tre olika modeller för hur en registreringsskyldighet kan utformas. Enligt den första modellen är mobiloperatörerna skyldiga att samla in och föra ett register med viss personlig information om sina användare. Vilken information som krävs varierar mellan länderna. I januari 2020 följde 81 procent av länderna i världen som har krav på en registreringsskyldighet denna modell. Enligt den andra modellen är mobiloperatörerna skyldiga att samla in data om sina användare och föra denna information vidare

till ett centralt register vid någon form av myndighet. I januari 2020 använde sig endast sex procent av aktuella länder av denna modell. Enligt den sista modellen är operatörerna skyldiga att validera sina kunders identitetsuppgifter mot en central myndighetsdatabas. Den här modellen användes i januari 2020 i tolv procent av de länder som har någon form av registreringsskyldighet. (Se GSMA, Access to Mobile Services and Proof of Identity 2020: The Undisputed Linkages, s. 8.)

Nedan följer en kortare beskrivning av lagstiftningen i några europeiska länder.

Norge

Som framgått ovan infördes en registreringsskyldighet i Norge redan 2004. Regleringen infördes bl.a. i syfte att reducera risken för förväxling och missbruk av andras identitet. Polisens behov av tillgång till information i det brottsbekämpande arbetet var ett centralt element i sammanhanget (se Høring om endringer i ekomloven og ekomforskriften med forslag om lovhjemmel for leveringsplikt for bredbånd og tydeligere krav till entydig identifisering av sluttbrukere, september 2019, s. 20).

Regleringen, som återfinns i den norska ekomloven med tillhörande föreskrifter, innebär att den som tillhandahåller offentliga telefonitjänster ska tillse att den s.k. slutbrukaren av tjänsten är entydigt identifierad. Detta ska ske såväl vid ingående av nya avtal som vid ändring eller upphörande av befintliga avtal. Tillhandahållaren ska dokumentera identitetskontrollen och föra ett register över varje slutbrukares namn, adress och nummer eller adress för tjänsten (se ekomloven § 2-4 och ekomforskriften § 6-2).

Skyldigheten att registrera slutbrukaren avser samtliga användare av telefonitjänster, alltså även de som använder fasta telefoner eller kontraktsabonnemang till mobiltelefoner. När regleringen infördes kom den att gälla även för befintliga abonnemang. Dessa skulle registreras inom sex månader. De kontantkortsabonnemang som inte registrerades inom denna tid deaktiverades.

Vad som menas med entydig identifiering är inte reglerat i lagen. Regelverket förutsätter att tillhandahållarna själva ska avgöra vilken identifieringsmetod som är lämplig beroende på vilken fas avtalen är

i och risken för missbruk. Den nationella kommunikationsmyndigheten har utarbetat en vägledning i frågan. Det har dock framkommit att operatörerna har hanterat identifieringskravet på olika sätt och att rutiner inte alltid har följts. Det har bl.a. förekommit fall då portering av telefonnummer (flytt av mobilnummer från en operatör till en annan) har skett utan att någon identifieringskontroll har gjorts. Den norska regeringen har av dessa skäl föreslagit vissa ändringar i ekomforskriften. Syftet med ändringarna är att tydliggöra och konkretisera kravet på tillhandahållare av offentliga telefonitjänster att entydigt identifiera slutbrukarna. De föreslagna ändringarna innebär att det införs krav på hur en entydig identifiering ska gå till och att det uttryckligen anges vilka identifikationshandlingar som får godtas (se a.a. s. 20 ff.). Förslagen bereds för närvarande inom det norska Regeringskansliet.

Tyskland

Tyskland har också haft en registreringsskyldighet sedan 2004. Lagstiftningen, som återfinns i den nationella lagen om telekommunikation, innebär att telefonoperatörerna är skyldiga att samla in och lagra uppgifter om alla kunder som innehar telefonabonnemang. Regleringen träffar därmed även de kunder som innehar kontantkortsabonnemang. Enligt regleringen ska operatörerna samla in och spara uppgifter om bl.a. abonnentens telefonnummer, namn, folkbokföringsadress och födelsedatum där abonnenten är en fysisk person. Insamlingen av uppgifter ska ske innan abonnemanget aktiveras. Om en operatör får kännedom om ändringar i de uppgivna uppgifterna ska dessa ändras. Operatörerna är även skyldiga att retroaktivt försöka få tillgång till saknade uppgifter om sina kunder om detta är möjligt utan särskild ansträngning. Det är möjligt för en operatör att använda sig av en tredje part för att samla in uppgifterna. Det är dock operatören som är ansvarig för att skyldigheterna enligt regleringen uppfylls. Om tredje part blir medveten om förändringar i uppgifterna som en del av sin normala affärsverksamhet, måste denne omedelbart överföra dessa till operatören. De insamlade uppgifterna ska raderas i slutet av kalenderåret året efter det att avtalet har upphört.

Den tyska lagstiftningen skärptes 2017 vad gäller kontantkort för mobiltelefoner. Lagändringen var ett led i arbetet mot internationell terrorism och annan organiserad brottslighet såsom människosmuggling. Den innebar att riktigheten i de uppgifter som samlas in måste kontrolleras före aktivering av ett kontantkort. Lagstiftningen innehåller numera utförliga regler om vilka identitetshandlingar som godtas för denna kontroll. Identifieringen kan ske t.ex. i en operatörs butik, hos vissa större återförsäljare, online via video där en giltig identitetshandling visas upp eller genom att en kopia av identitetshandlingen skicka till operatören. Lagändringen gäller endast för försäljningen av nya kontantkort efter juli 2017.

Schweiz

En registreringsskyldighet för kontantkort till mobiltelefoner infördes i Schweiz 2004 i syfte är att förhindra terrorism och droghandel. Regleringen initierades sedan det blivit känt att schweiziska oregistrerade kontantkort använts i samband med planering av terrorism. Regleringen innebär att alla kontantkort köpta efter den 1 november 2002 ska registreras. De kontantkort som inte registrerades inom tre månader från lagens införande blev avaktiverade till dess att en registrering skett.

Enligt den schweiziska regleringen är leverantörer av telekommunikationstjänster skyldiga att bl.a. registrera uppgifter om kundernas namn, adress och födelsedatum. För förbetalda tjänster, dvs. kontantkort, ska även leveransplats och namn på den person som tillhandahöll de nödvändiga medlen för åtkomst till telekommunikationstjänsten anges. En identitetskontroll ska genomföras och dokumenteras innan ett kontantkort får aktiveras. Uppgifterna ska registreras när kundrelationen upprättas och kunna tillhandahållas under kundrelationens varaktighet och i sex månader efter att den har upphört.

Belgien

En skyldighet att registrera användare av kontantkort infördes i Belgien 2016 som en del i arbetet mot terrorism. Regleringen innebär att en operatör endast är tillåten att aktivera ett kontantkort efter att

ha fastställt brukarens identitet. Regleringen gäller för såväl befintliga kontantkort som för nya kontantkort som ger tillgång till mobila elektroniska kommunikationstjänster, såsom att ringa, surfa på internet, sända textmeddelanden m.m. Regleringen gäller dock inte för kontantkort som endast användas för trådlös kommunikation mellan olika maskiner, s.k. M2M-applikationer. Vid införandet av den nya lagstiftningen gavs kunder en möjlighet att inom sex månader registrera existerande kontantkort. De kort som inte registrerades inom denna tid blev avaktiverade.

Den belgiska lagstiftningen föreskriver en skyldighet att registrera abonnemangsuppgifter som för- och efternamn, nationalitet och adress. Därutöver ska uppgifter om det dokument som använts för identifiering vid köpet anges. Om detta inte är ett belgiskt id-kort ska även ett foto av köparen sparas. Identifieringen kan ske vid köpet eller via operatörens hemsida.

Den som registrerat ett kontantkort i Belgien får inte överlåta ett aktivt kort till en tredje part förutom i vissa fall. Det är t.ex. tillåtet att köpa kontantkort till familjemedlemmar och till anställda. Det är också tillåtet att lämna ett förbetalt kort vidare om det har köpts på uppdrag av en underrättelse- eller säkerhetstjänst, av polisen eller vissa andra myndigheter. I övriga fall får kontantkort endast överlåtas till någon annan om denne har identifierat sig hos operatören. För det fall inköp av kontantkort sker av en juridisk person ska den fysiska person som kräver aktiveringen registreras. En juridisk person ska också föra en uppdaterad lista över vilka personer som innehar vilka kontantkort. För det fall regleringen inte följs kan sanktioner utgå.

Österrike

En registreringsskyldighet för kontantkort infördes i Österrike 2019. Enligt regleringen måste en leverantör registrera vissa basuppgifter om innehavaren innan en aktivering av ett kontantkortsabonnemang får ske. De uppgifter som ska registreras omfattar namn, titel och födelsedatum. Registreringen ska ske med hjälp av vissa lämpliga identifieringsförfaranden. Bland de metoder som godtas återfinns officiella id-kort med foto och en form av elektronisk identifiering.

Registreringen kan ske i operatörernas butiker, hos vissa återförsäljare, i postkontor och online.

Registreringsskyldigheten gäller för såväl nya abonnemang som gamla. Vid införandet av regleringen gavs en möjlighet att inom åtta månader registrera existerande kontantkort. De kort som inte blev registrerade inom denna period avaktiverades till dess en registrering skett.

De registrerade uppgifterna ska raderas av operatören inom två veckor efter avslutat avtalsförhållande om inte uppgifterna behövs för andra lagstadgade ändamål. Uppgifterna kan dock behandlas under en längre tid om den enskilde har lämnat sitt samtycke till det.

Luxemburg

I Luxemburg gäller sedan 2017 en registreringsskyldighet för förskottsbetalningstjänster, dvs. för elektroniska kommunikationstjänster som är tillgängliga för allmänheten genom att använda Luxemburgs numreringsresurser och för vilka tjänsterna betalas innan tjänsten tillhandahålls. Alla företag som tillhandahåller sådana förbetalda tjänster är skyldiga att ange identiteten på den person till vilken tjänsten tillhandahålls. Innan tjänsten tillhandahålls ska företaget därför samla in uppgifter om namn, adress och födelsedatum för den fysiska person som vill köpa en förskottsbetalningstjänst. En identitetskontroll ska göras. Uppgifter om vilken typ av identitetsdokument som har använts ska registreras och en kopia av dokumentet sparas. Om inköpet görs av en juridisk person ska samma uppgifter lämnas om den fysiska person som företräder den juridiska personen. Uppgifterna ska sparas under hela perioden för tillhandahållandet av tjänsten, och under en period på tre år från dagen för inaktiveringen av samtalsnumret. Därefter ska informationen raderas utan dröjsmål. Om uppgifterna samlas in av en återförsäljare ska denne radera uppgifterna så snart de har överförts till operatören.

5.6 Överväganden och förslag

5.6.1 Bör det införas en skyldighet att registrera kontantkort?

Bedömning: De brottsbekämpande myndigheternas behov och nytta av en registreringsskyldighet väger tyngre än de motstående intressen som talar mot en sådan skyldighet. Det bör därför införas en skyldighet att registrera uppgifter om abonnemang för kontantkort.

För att besvara frågan om det bör införas en skyldighet att registrera uppgifter om abonnemang för kontantkort bör behovet och nyttan av en sådan registreringsskyldighet övervägas. Uttrycket behov syftar här på den straffprocessuella behovsprincipen som i detta sammanhang innebär att det ska föreligga ett påtagligt behov av en registreringsskyldighet och att en mindre ingripande åtgärd inte är tillräcklig för att tillgodose behovet. Med nytta avses registreringsskyldighetens förväntade värde i det brottsbekämpande arbetet. I det sammanhanget bör övervägas hur pass effektiv en registreringsskyldighet kan förväntas vara för det brottsbekämpande arbetet. Effektiviteten i en registreringsskyldighet har ju tidigare ifrågasatts och har varit ett skäl till att en sådan skyldighet inte har införts.

Behovet och nyttan av en registreringsskyldighet bör också vägas mot andra berörda intressen. En skyldighet att registrera abonnemangsuppgifter avseende kontantkortskunder skulle t.ex. innebära olägenheter för enskilda som av helt legitima skäl vill ha möjlighet att kommunicera anonymt. En registreringsskyldighet skulle även medföra ökad administration och kostnader för dem som tillhandahåller kontantkortsabonnemang. Även andra intressen kan komma att påverkas. För att komma till en slutsats i frågan om en registreringsskyldighet bör införas måste därmed en proportionalitetsavvägning göras mellan registreringsskyldighetens betydelse för det eftersträvade målet å ena sidan och motstående intressen å andra sidan.

Behovet och nyttan av en registreringsskyldighet

Det är viktigt att samhället kan ingripa på ett effektivt sätt mot brott. Därför är det nödvändigt att de brottsbekämpande myndigheterna har tillgång till verkningsfulla och ändamålsenliga verktyg. Inte minst behöver myndigheterna kunna samla in information för att fullgöra sina uppgifter. Hemlig övervakning av elektronisk kommunikation och hemlig avlyssning av elektronisk kommunikation är betydelsefulla tvångsmedel, särskilt i kampen mot den allvarligaste brottsligheten. Med hjälp av dessa tvångsmedel kan myndigheterna få tillgång till innehållet i meddelanden och uppgifter om elektronisk kommunikation.

Som redogjorts för i avsnitt 5.3 ovan krävs i normalfallet att ett nummer kan knytas till en misstänkt för att tillstånd att avlyssna eller övervaka ett telefonnummer ska kunna erhållas. För att det ska gå att säkerställa vem som är brukare av ett telefonnummer och som därmed bör omfattas av ett beslut om hemlig avlyssning eller övervakning är det många gånger nödvändigt med tillgång till abonnemangsuppgifter. Användningen av anonyma kontantkort innebär i detta hänseende ett allvarligt effektivitetsproblem för de brottsbekämpande myndigheterna. När mobiltelefoner förekommer i samband med brottslig verksamhet är det i princip uteslutande oregistrerade och anonyma kontantkort som används. Det förhållandet att brottsbekämpande myndigheter inte genom operatörernas försorg kan få direkt tillgång till uppgifter om vem som innehar dessa telefonnummer medför att det i många fall är svårt att knyta en misstänkt till ett visst nummer. Därmed blir det också svårt för myndigheterna att få till stånd beslut om avlyssning eller övervakning. Möjligheterna att få tillgång till uppgifter om vem som har varit i kontakt med vem, när detta skett och var blir på detta sätt kraftigt begränsade. Det är problematiskt att tillgången till betydelsefulla verktyg i brottsbekämpningen är kringskuren för att grundläggande uppgifter om vem som innehar ett abonnemang inte finns att tillgå.

Som angetts ovan är det visserligen möjligt för de brottsbekämpande myndigheterna att få fram en koppling mellan ett kontantkortsnummer och en person på andra sätt än genom att hämta in registrerade abonnemangsuppgifter från operatörerna. Dessa andra sätt är dock ofta mycket ineffektiva och långt ifrån alltid tillförlitliga.

Det finns också en viss möjlighet att använda hemlig övervakning av elektronisk kommunikation utan att ett nummer kan knytas till en misstänkt. Tvångsmedlet kan t.ex. användas i syfte att hämta in uppgifter om vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område där ett allvarligt brott har begåtts i syfte att utreda vem som skäligen kan misstänkas för brottet (27 kap. 19 § första stycket 2 och 20 § andra stycket RB). Möjligheterna att använda tvångsmedlet i detta syfte är dock begränsade. När en sådan s.k. basstationstömning har gjorts medför vidare avsaknaden av grundläggande abonnemangsuppgifter att det är svårt att ur det inhämtade materialet sålla fram de uppgifter som är intressanta att arbeta vidare med. För det fall samtliga kontantkortskunder hade varit registrerade hade det dock varit möjligt att snabbt utesluta de personer som inte är intressanta för det vidare arbetet.

Förutom de svårigheter som användningen av oregistrerade kontantkort innebär för möjligheterna att via hemliga tvångsmedel hämta in information om elektronisk kommunikation och analysera denna, föreligger också andra problem kopplade till användningen av oregistrerade kontantkort. Behovet av abonnemangsuppgifter är t.ex. uppenbart i de fall ett visst telefonnummer använts i samband med brott men det ännu inte finns någon misstänkt för brottet. Således kan uppgifter om vem som är innehavare av ett kontantkort vara nödvändiga för att utreda och beivra hot, bedrägerier och trakasserier över telefon. Även i underrättelsearbetet innebär användningen av oregistrerade kontantkort svårigheter, t.ex. när det gäller att följa intressanta personer. Ett ytterligare problem är att oregistrerade kontantkort kan användas som mobilt bredband och därmed kan användas för att koppla ihop enheter för anonym konversation. Vidare har det framkommit att telefonnummer kopplade till svenska oregistrerade kontantkort används av terrorkopplade utländska aktörer utomlands.

Förekomsten av kontantkort till mobiltelefoner som inte kan kopplas till någon innehavare medför således att de brottsbekämpande myndigheterna går miste om viktig och ibland avgörande information för att upptäcka, förhindra, utreda och beivra många gånger allvarlig brottslighet.

De brottsbekämpande myndigheterna lägger i dag stora resurser på att på olika sätt försöka identifiera vilka telefonnummer som

används i samband med brottslig verksamhet och vilka personer som använder numren. När det saknas abonnemangsuppgifter som direkt pekar ut vem som kan knytas till ett visst nummer måste myndigheterna alltså förlita sig på andra metoder för att fastställa vem som innehar telefonnumret. Arbetet med att på olika sätt fastställa vem som innehar ett visst telefonnummer tar mycket tid och resurser i anspråk för de brottsbekämpande myndigheterna. Det är dessutom långt ifrån säkert att uppgifterna verkligen leder till att en viss person kan pekas ut som innehavare av ett kontantkort. En registrerad uppgift om vem som är innehavaren skulle vara betydligt mer tillförlitlig och medföra ett klart effektivare brottsbekämpande arbete.

Regeringen bedömde redan 2011 att de brottsbekämpande myndigheterna har ett påtagligt behov av att i olika sammanhang få tillgång till uppgifter om vem som innehar kontantkort. Sedan dess har intresset av att använda kontantkort visserligen minskat. Som framgått ovan finns det dock alltjämt mer än tre miljoner aktiva svenska kontantkort (M2M inte inräknade). Vidare är det fortfarande så att kriminella regelmässigt använder sig av oregistrerade kontantkort för sådan kommunikation som rör brottslig verksamhet. Användningen av oregistrerade kontantkort medför stora negativa konsekvenser för de brottsbekämpande myndigheterna. Den kan innebära att utredningar läggs ned eller väljs bort eftersom befintliga utredningsåtgärder inte är en framkomlig väg. Det är vår bedömning att de brottsbekämpande myndigheternas fortfarande har ett påtagligt behov av tillgång till uppgifter om vem som har införskaffat ett kontantkort. Någon mindre ingripande åtgärd än en skyldighet att registrera abonnemangsuppgifterna synes inte vara tillräcklig för att tillgodose behovet.

Frågan är härefter om en skyldighet att registrera abonnemangsuppgifter för kontantkort kan förväntas bidra till en lösning av de redovisade problemen. Som tidigare konstaterats kan effektiviteten i en registreringsskyldighet ifrågasättas. Detta eftersom det kommer att finnas vägar att kringgå en sådan skyldighet. Man kan t.ex. tänka sig att en registreringsskyldighet kommer att leda till att oregistrerade utländska kontantkort kommer att köpas och användas i Sverige i brottsliga sammanhang. De möjligheter till fri roaming som numera finns inom EU medför att det i dag är enklare att använda utländska oregistrerade kontantkort här än när frågan utreddes senast. Dock kan det även för utländska kontantkort finnas krav på

registrering för att korten ska få användas utomlands. I takt med att allt fler länder i Europa och övriga världen inför en generell skyldighet att registrera uppgifter om abonnemang rörande kontantkort kommer rimligen risken för att oregistrerade utländska kontantkort används i brottsliga sammanhang att minska. Samtidigt är det så att flera av våra närmaste grannländer inte har infört någon registreringsskyldighet som omfattar kontantkort och att det därför alltjämt är ganska enkelt att komma över utländska oregistrerade kontantkort.

Ett argument som tidigare har lyfts fram är att registreringen kan komma att utföras av andra personer än de verkliga innehavarna, dvs. av en sorts målvakter. Vi bedömer att denna risk alltjämt föreligger. En registreringsplikt kommer inte att innebära en garanti för att den registrerade uppgiften om vem som innehar ett kontantkort överensstämmer med den faktiska användaren av kontantkortet. För det fall ett kontantkort skulle vara registrerat på en målvakt har de brottsbekämpande myndigheterna dock i vart fall en fysisk koppling till kortet och en ingång att börja nysta i. En registreringsskyldighet kommer därför med stor sannolikhet att ge de brottsbekämpande myndigheterna påtagligt bättre förutsättningar att fastställa vem som har ett visst telefonnummer eller vilket telefonnummer en viss person har. Sålunda kan en registreringsskyldighet medföra att tillstånd att avlyssna och övervaka elektronisk kommunikation kan användas i fler fall. Det medför att brott kan förebyggas, förhindras, utredas och beivras effektivare och i fler fall. Vidare kan de kontantkortskunder som inte alls är intressanta snabbt sållas bort. Som de brottsbekämpande myndigheterna har påpekat skulle därför en registreringsskyldighet innebära fördelar i förhållande till dagens system, även om en viss registrering skulle utföras av målvakter. Vi återkommer nedan till frågan om det bör införas en begränsning av hur många kontantkort som det ska vara tillåtet att registrera.

Sedan frågan om en registreringsskyldighet utreddes förra gången har det skett en avsevärd teknisk utveckling på området för elektronisk kommunikation. Numera ersätts ofta traditionell taltelefoni, sms och e-posttjänster med funktionsmässigt likvärdiga onlinetjänster som ip-telefoni, meddelandetjänster och webbaserade e-posttjänster. Användningen av traditionella kommunikationstjänster har minskat till förmån för nya nummeroberoende interpersonella kommunikationstjänster som t.ex. meddelandetjänster i internet-

baserade appar. Kommunikationen i dessa appar är ofta krypterad och därmed inte möjlig att läsa i klartext av den som har tillstånd till hemlig avlyssning. Leverantörer av meddelandetjänster såsom Facebook Messenger, Whatsapp och Instagram har inbyggda funktioner i programvaran som utför kryptering i syfte att hindra utomstående från att ta del av kommunikationen. Det finns också olika slags tjänster som gör det möjligt för enskilda att kommunicera anonymt utan att det är möjligt att ta reda på vem som står bakom kommunikationen. Ett exempel på enkel anonymiserad internetkommunikation, eller i vart fall sådan som blir svårare att spåra, är då en telefon ansluter till ett wifi-nätverk på ett café eller en flygplats. De olika krypterings- och anonymiseringstjänsterna har ofta ett legitimt syfte och möjliggör för användare att kunna bevara sin integritet på internet. Tjänsterna används dock även av individer och grupperingar för att dölja kriminell verksamhet. Den 1 april 2020 infördes därför ett nytt hemligt tvångsmedel, hemlig dataavläsning, som ger de brottsbekämpande myndigheterna möjlighet att under vissa förutsättningar ta del av krypterad och anonymiserad kommunikation (se prop. 2019/20:64). Genom tvångsmedlet blir det möjligt att med någon form av tekniskt hjälpmedel i hemlighet bereda sig tillgång till viss teknisk utrustning, t.ex. en mobiltelefon, och därigenom få besked om hur utrustningen används eller har använts och vilken information som finns i den. Tvångsmedlet skiljer sig därmed från hemlig avlyssning eller övervakning av elektronisk kommunikation där uppgifterna hämtas in på väg till eller från någons tekniska utrustning.

En registreringsplikt för kontantkort kommer inte att förhindra att kommunikation sker via internetbaserade appar eller andra onlinetjänster. För det fall det går att koppla en enhet till en viss person kan det dock vara möjligt att genom hemlig övervakning av elektronisk kommunikation få tillgång till lokaliseringsuppgifter som talar om var en persons kommunikationsutrustning har befunnit sig. En registreringsskyldighet för abonnemangsuppgifter rörande kontantkort kan på så sätt medföra att det går att t.ex. positionera en person i närheten av en brottsplats.

Det kommer alltid att finnas svårigheter för de brottsbekämpande myndigheterna när det gäller att följa de kriminella som har planerat sina brott noggrant. En stor del av de grova brotten föregås dock inte av noggrann planering och begås inte alltid av personer

med hög säkerhetsförmåga. En skyldighet att registrera abonnemangsuppgifter rörande kontantkort skulle i vart fall försvåra för den som avser att använda ett kontantkort för att försöka dölja spår i anledning av ett brott. En sådan skyldighet skulle också innebära att tid och resurser hos de brottsbekämpande myndigheterna skulle kunna läggas på annat än att utreda vem som är innehavare av ett visst telefonnummer. På så sätt kan det brottsbekämpande arbetet effektiviseras. Härmed skapas förbättrade förutsättningar att bekämpa allvarlig brottslighet.

En registreringsskyldighet för kontantkort kan komma att innebära att fler kriminella kommer att kommunicera via internetbaserade appar och andra onlinetjänster som möjliggör kommunikation i krypterad och anonymiserad form. För att de brottsbekämpande myndigheterna ska kunna få tillgång till information som kommuniceras på detta sätt har det alltså nyligen införts ett nytt hemligt tvångsmedel, hemlig dataavläsning. Det har dessutom uppmärksammats att ytterligare frågor som berör användningen av nummeroberoende interpersonella kommunikationstjänster och regleringen om hemliga tvångsmedel behöver övervägas (se promemorian Genomförande av direktivet om inrättande av en kodex för elektronisk kommunikation, s. 332).

Sammanfattningsvis är det vår bedömning att de brottsbekämpande myndigheterna har ett påtagligt behov av uppgifter om vem som innehar kontantkort. Det är vidare vår bedömning att det i och för sig kommer att finnas vägar att kringgå en registreringsskyldighet och fortsatt kommunicera anonymt. En skyldighet att registrera uppgifter om abonnemang rörande kontantkort kommer dock att innebära ett försvårande för de kriminella och ett effektivare arbete för de brottsbekämpande myndigheterna. En skyldighet att registrera uppgifter om abonnemang rörande kontantkort skulle därmed innebära fördelar i förhållande till dagens system. Således skulle en registreringsskyldighet också vara till nytta för brottsbekämpningen, särskilt i fråga om möjligheten att förebygga, förhindra, utreda och beivra allvarligare brottslighet.

En registreringsskyldighets betydelse för andra berörda intressen

En skyldighet att registrera abonnemangsuppgifter för kontantkort skulle få följder för alla enskilda som använder kontantkort för sin kommunikation. En lagstadgad registreringsplikt skulle innebära att en enskild måste ge upp en möjlighet som för närvarande finns att kommunicera ofta utan några större risker för att hans eller hennes identitet ofrivilligt ska röjas. För den som inte har möjlighet att skaffa kontraktsabonnemang exempelvis på grund av en betalningsanmärkning, innebär en lagstadgad registreringsskyldighet i praktiken en skyldighet att uppge sin identitet för att erhålla ett telefonabonnemang.

Det finns enligt svensk grundlag inte någon *allmän rätt att vara anonym*. Visserligen finns det enligt tryckfrihetsförordningen en sådan rätt i vissa närmare angivna situationer, men den gäller alltså inte generellt. Det finns inte heller någon allmän rätt att vara anonym enligt Europakonventionen eller EU:s rättighetsstadga. Individens rätt att själv förfoga över och ta ställning till det allmännas tillgång till sådan information som rör hans eller hennes privata förhållanden är dock av vikt i en demokrati. En rätt att inte i alla sammanhang behöva uppge vem man är kan därmed anses vara en del av *skyddet för den personliga integriteten*. I 2 kap. 6 § andra stycket RF anges att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Begränsningar i detta skydd får endast ske genom lag och endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningarna får inte heller gå utöver vad som är nödvändigt eller utgöra ett hot mot den fria åsiktsbildningen (se 2 kap. 20 och 21 §§). I förarbetena framhålls att det är naturligt att det läggs stor vikt vid uppgifternas karaktär vid bedömningen av hur ingripande ett intrång kan anses vara i samband med bl.a. insamling och lagring av uppgifter om enskildas personliga förhållanden. Ju känsligare uppgifterna är, desto mer ingripande anses hanteringen av uppgifterna normalt vara. Vid bedömningen av vilka åtgärder som kan anses utgöra ett betydande intrång ska både åtgärdens omfattning och arten av det intrång åtgärden innebär beaktas. Bestämmelsen i 2 kap. 6 § andra stycket RF omfattar endast sådana intrång som på grund av åtgärdens intensitet eller omfattning,

eller av hänsyn till uppgifternas integritetskänsliga natur eller andra omständigheter, innebär ett betydande ingrepp i den enskildes privata sfär (se prop. 2009/10:80 s. 171 ff.) Bestämmelsen, som alltså endast gäller i förhållande till det allmänna, innebär att åtgärder som är av sådant slag som anges i bestämmelsen får vidtas bara om det finns lagstöd för detta.

I artikel 8 i Europakonventionen anges att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. 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 bl.a. statens säkerhet, den allmänna säkerheten, till förebyggande av oordning och brott eller till skydd 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. En bestämmelse om rätt till respekt för bl.a. privatlivet finns också i artikel 7 i EU:s rättighetsstadga.

Europadomstolen har prövat om den registreringsskyldighet för kontantkort som har införts i Tyskland strider mot rätten till respekt för privat- och familjelivet (se Europadomstolens dom den 30 januari 2020 i målet Breyer mot Tyskland, mål nr 50001/12). Domstolen fann att skyldigheten att registrera abonnemangsuppgifter som namn, adress, födelsedatum och telefonnummer innebär en begränsad inskränkning i rätten till privatliv. Det ansågs således inte vara fråga om något betydande ingrepp i den enskildes sfär.

Även om abonnemangsuppgifterna naturligtvis är skyddsvärda avser de inte uppgifter om innehållet i den kommunikation som har ägt rum eller uppgifter som skapas med anledning av en viss kommunikation (trafikuppgifter). Sistnämnda uppgifter kan många gånger vara mycket känsliga. För att få fram trafikuppgifter krävs därför att de brottsbekämpande myndigheterna får tillstånd att avlyssna elektronisk kommunikation eller att hämta in uppgifter om elektronisk kommunikation, t.ex. om vilken telefon som har varit i kontakt med en annan telefon. Abonnemangsuppgifter däremot möjliggör i princip enbart att telefonnummer kan hänföras till sin respektive innehavare och att en indikation kan erhållas om vem som använder numret. Abonnemangsuppgifterna ger alltså inte i sig besked om vem som har ringt till vem eller vad som har framkommit

vid telefonsamtalen. Uppgifterna om abonnemang kan således inte användas för att dra några mer precisa slutsatser om berörda personers privatliv (se t.ex. Kammarrätten i Stockholms dom den 14 december 2018 i mål 2471-18 med hänvisning till EU-domstolens avgörande Ministerio Fiscal, dom den 2 oktober 2018 i mål C 207/16, se även Europadomstolens ovannämnda dom i målet Breyer mot Tyskland). De uppgifter som normalt uppfattas som abonnemangsuppgifter omfattar inte heller några känsliga personuppgifter (s.k. särskilda kategorier av personuppgifter) enligt artikel 9 i dataskyddsförordningen.

Mot den bakgrunden menar vi att en registrering av abonnemangsuppgifter inte skulle innebära något betydande intrång i enskildas rätt till privatliv eller i enskilda personers yttrandefrihet.

Men enskilda kan ändå ha ett behov av att kunna teckna ett abonnemang utan att avslöja sin identitet. Det kan nämligen ha betydelse för enskildas berättigade intresse av att kunna kommunicera anonymt. Frågan är om och i så fall på vilket sätt som en registreringsskyldighet har betydelse för enskildas intresse av att kunna kommunicera utan att avslöja sin identitet.

Som exempel på ett berättigat behov av att kunna kommunicera utan att avslöja sin identitet kan nämnas enskilda som vill utnyttja den grundlagsskyddade meddelarfriheten för att lämna uppgifter till medier i syfte att dessa ska göras offentliga (se 1 kap. 7 § TF och 1 kap. 10 § YGL). Det har vid våra kontakter med medierna framförts att oregistrerade kontantkort i stor utsträckning används i dag av de som kontaktar journalister. Flera stora journalistiska avslöjanden som skett under senare år har inletts genom att enskilda kontaktat medierna på detta sätt. Avslöjandena har, sägs det, avsett bl.a. misstänkt terrorism och misstänkta oegentligheter inom svenska myndigheter. Det förekommer också att journalister förser källor med oregistrerade kontantkort för fortsatt kontakt. Fysiska möten mellan journalister och källor undviks helst av säkerhetsskäl. Anledningen till att kontakterna sker via oregistrerade kontantkort är att man vill undvika risken för att enskilda, myndigheter eller främmande makt kommer över uppgifter om källan. Risken för att obehöriga kommer över uppgifterna anses öka om uppgifter om abonnenten finns registrerade. Det har vid våra kontakter med medierna hävdats att det alltid finns en risk, eller i vart fall en upplevd risk, för att lagrade uppgifter kan hackas, hanteras ovarsamt eller

tillgängliggöras medvetet eller omedvetet. Det har vidare framförts att en registreringsskyldighet för kontantkort skulle kunna medföra att personer framöver avstår från att ta kontakt med medierna av rädsla för att bli spårade eller upptäckta.

Det förekommer också att journalister själva använder sig av oregistrerade kontantkort i sitt arbete i fall då det inte är lämpligt att uppge sin egen identitet. Skälen härför är desamma som angetts ovan. Som exempel har nämnts fall när en journalist tar anställning där misstänkta oegentligheter förekommer och där behöver uppge ett telefonnummer. Vidare krävs för uppkoppling på vissa från journalistisk synpunkt intressanta mediesajter att användaren registrerar sig med telefonnummer. För att kartlägga individer som använder sig av sådana sajter förekommer också att journalister använder sig av telefonnummer som härrör från oregistrerade kontantkort.

Även andra personer kan ha behov av tillgång till anonym kommunikation. Som exempel kan nämnas källdrivare hos de brottsbekämpande myndigheterna och informatörer av olika slag. Även förföljda personer som lever gömda från t.ex. en tidigare partner eller familjemedlemmar kan i dag använda sig av oregistrerade kontantkort för sin kommunikation för att inte bli röjda. Det finns vidare betalteletjänster där telefonnummer används för betalning via operatörernas telefonfakturor. Sådana tjänster omfattar t.ex. dejtingtjänster och webb-communities. Oregistrerade kontantkort möjliggör här för användare att nyttja dessa tjänster utan att användningen går att knyta till den enskilde. För t.ex. HBTQ-personer och andra grupper kan den anonymitet som ett kontantkort kan innebära vara avgörande för att de här tjänsterna ska vara intressanta att använda för att möta likasinnade.

För skyddet av den enskildes integritet är det viktigt att det även framöver kommer att finnas möjlighet att kommunicera utan att avslöja sin identitet. En registreringsskyldighet för kontantkort kommer dock inte att innebära att enskildas abonnemangsuppgifter blir allmänt kända. Uppgifterna kommer hos operatörerna att omfattas av en straffsanktionerad tystnadsplikt och får således endast röjas om den enskilde har samtyckt till det eller det annars är tillåtet enligt lag. Således innebär inte en registreringsskyldighet i sig att den enskilde kontantkortsinnehavarens identitet röjs.

Det råder vidare ett grundlagsskyddat förbud för det allmänna att efterforska vem som har lämnat uppgifter till en journalist i publi-

ceringssyfte. Varken abonnemangsuppgifter eller hemliga tvångsmedel får således användas av brottsbekämpande myndigheter för att ta reda på vem som har lämnat uppgifter till en journalist. I sammanhanget kan påpekas att hemlig avlyssning inte heller får avse samtal eller andra meddelanden där den som yttrar sig har tystnadsplikt på grund av källskyddet (se 27 kap. 22 § RB och 11 § preventivlagen).

Som konstaterats ovan finns det andra sätt att kommunicera anonymt än genom oregistrerade kontantkort. Sådan kommunikation kan t.ex. ske via olika internetbaserade appar och onlinetjänster. De flesta medier har i dag krypterade tjänster där tips kan lämnas och kontakt med s.k. meddelare kan inledas. Vidare kan ett abonnemang registrerad på någon annan användas för vissa kontakter.

Det är sammantaget vår bedömning att enskildas intresse av anonym kommunikation kommer att vara möjligt att skydda även om en registreringsskyldighet för kontantkort införs.

En registreringsskyldighet skulle innebära att mobiloperatörerna skulle ha tillgång till fler uppgifter än i dag gällande vem som är innehavare av abonnemang. Uppgifterna skulle omfatta ett stort antal personer, varav de flesta inte alls skulle vara av intresse för de brottsbekämpande myndigheterna. Denna omständighet ger anledning till att något fundera kring skyddet för uppgifterna hos operatörerna. Till en början kan konstateras, vilket framgått ovan, att abonnemangsuppgifter hos operatörerna omfattas av tystnadsplikt. Uppgifterna får alltså endast röjas när detta är tillåtet enligt lag. Operatörerna har därmed ett ansvar för att abonnemangsuppgifterna inte läcker ut. Hanteringen av dem hos operatörerna är således viktig.

Det kan vidare konstateras att en registreringsskyldighet inte förändrar de grundläggande förutsättningarna som gäller för att de brottsbekämpande myndigheterna ska få hämta in uppgifter om elektronisk kommunikation från operatörerna. Rätten för brottsbekämpande myndigheter att få tillgång till abonnemangsuppgifter gäller som framgått vid misstanke om brott som myndigheten ska ingripa mot (6 kap. 22 § första stycket 2 LEK). Som också framgått är möjligheten att avlyssna eller övervaka elektronisk kommunikation omgärdad 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.

Operatörerna behandlar redan i dag abonnemangsuppgifter avseende de kunder som innehar kontraktsabonnemang, dvs. flertalet mobilanvändare. Det förekommer också redan i dag att abonnemangsuppgifter registreras avseende kontantkortskunder på frivillig väg. En registreringsskyldighet kommer visserligen innebära att det införs en rättslig förpliktelse och därmed en ny rättslig grund för personuppgiftsbehandlingen (enligt artikel 6.1 c i dataskyddsförordningen). En registreringsskyldighet kommer dock inte i sig leda till någon ny form av personuppgiftsbehandling. Den dataskyddsreglering som gäller enligt den allmänna dataskyddsförordningen och lagen om elektronisk kommunikation kommer att vara tillämplig även för de abonnemangsuppgifter som skulle behandlas på grund av en registreringsskyldighet.

Det är av stor vikt att de krav som ställs på hur en registrering ska gå till inte innebär att enskilda utesluts från möjligheten att köpa kontantkort. Enligt vår bedömning bör ett system för registrering av kontantkortskunder i stora delar kunna utformas på samma sätt som gäller för den registrering som sker i dag. Själva registreringsförfarandet behöver därför inte bli särskilt betungande för enskilda.

En registreringsskyldighet skulle medföra ökad administration och kostnader för mobiloperatörerna. Det finns dock verksamhetsområden där samhället som en förutsättning för att tillåta ett företag att driva näringsverksamhet kräver att vissa samhälleliga intressen beaktas. Den som tillhandahåller kontantkort för mobiltelefoner är verksam inom ett sådant område och måste ibland anpassa sin verksamhet till vissa centrala intressen, däribland samhällets berättigade intresse att bekämpa brott. Regeringen har i tidigare sammanhang bedömt att operatörer kan vara skyldiga att vidta åtgärder för att underlätta den brottsutredande verksamheten och i viss utsträckning bära kostnaderna för detta (se prop. 2010/11:46 s. 67 och prop. 1995/96:180 s. 29 ff.). Här kan tilläggas att en registreringsskyldighet för kontantkort sannolikt skulle innebära en viss fördel för mobiloperatörerna genom att de lättare kan nå kontantkortskunderna för marknadsföring.

Kontantkort säljs dock inte endast av mobiloperatörer utan även av återförsäljare. Flera av återförsäljarna är företag av sådan storlek att de bör kunna administrera en registrering av kontantkort. Kontantkort säljs dock även av fristående handlare, såsom kioskägare och liknande, som inte bedöms ha de tekniska och praktiska

möjligheterna att kunna genomföra en registrering. Enligt en uppskattning säljer så många som 7 000 fristående handlare kontantkort. Vid införandet av en registreringsskyldighet bör hänsyn tas till dessa aktörer och utformningen av systemen ske på ett sätt som innebär så liten påverkan som möjligt för dem. Vi återkommer till denna fråga nedan.

Det har framförts att en registreringsskyldighet för kontantkort skulle kunna leda till att mobiltelefoner blir mer stöldbegärliga, eftersom kriminella skulle vilja hitta nya former för att kommunicera utan att kunna spåras. En stulen mobiltelefon kan dock relativt enkelt spärras, vilket borde minska intresset för sådan brottslighet. Hos de flesta mobiloperatörer är det också möjligt att på ett enkelt sätt spärra ett stulet simkort. Vi återkommer nedan till frågan om när en registrering av kontantkort bör ske för att minska risken för att ännu inte registrerade kort blir stöldbegärliga.

Det är proportionerligt att nu införa en registreringsskyldighet

En förutsättning för att införa bestämmelser om en registreringsskyldighet som omfattar kontantkort är att detta är proportionerligt vid en avvägning mellan å ena sidan behovet och nyttan av en sådan skyldighet och å andra sidan det intrång eller men i övrigt som skyldigheten kan förväntas innebära för motstående intressen. Vi har ovan konstaterat att det finns ett påtagligt behov av en registreringsskyldighet och att en sådan också kan vara av nytta för det brottsbekämpande arbetet. Vi har även konstaterat att en registreringsskyldighet kommer att få konsekvenser för bl.a. enskilda som i dag kommunicerar via oregistrerade kontantkort. Frågan är om behovet och nyttan av en registreringsskyldighet väger tyngre än de motstående intressen som talar emot en sådan skyldighet.

För bekämpningen av allvarlig brottslighet är det avgörande att de brottsbekämpande myndigheterna under vissa förutsättningar har tillgång till uppgifter som kan erhållas med användning av hemliga tvångsmedel. Möjligheten att använda hemliga tvångsmedel på området för elektronisk kommunikation är många gånger beroende av att abonnemangsuppgifter finns tillgängliga. Det är ytterst otillfredsställande att personer som sysslar med grov brottslighet genom så relativt enkla åtgärder som det är fråga om kan förbli

anonyma och därmed bl.a. kan undvika att hemliga tvångsmedel används. Detta leder till att brottslighet i många fall inte kan avslöjas, utredas och beivras. I andra fall kommer avslöjandet av vem som döljer sig bakom ett anonymt kontantkort inte att kunna ske utan att betydande resurser förbrukas.

Som konstaterats ovan kommer det att finnas vägar att kringgå en registreringsskyldighet för kontantkort. Det finns också andra sätt att kommunicera där det föreligger andra svårigheter för de brottsbekämpande myndigheterna när det gäller att följa kommunikationen. Införandet av en registreringsskyldighet kommer sannolikt att öka användningen av internetbaserade appar och andra onlinetjänster som möjliggör kommunikation i krypterad och anonymiserad form. En registreringsskyldighet för kontantkort är således inte en åtgärd som ensamt kan antas bidra till att minska brottsligheten. Däremot kan en registreringsskyldighet vara en bit i ett större pussel i arbetet med att försvåra för kriminella aktörer som vill lägga hinder i vägen för de brottsbekämpande myndigheternas arbete. En registreringsskyldighet skulle leda till en säkrare tillgång till abonnemangsuppgifter och kan därmed bidra till att uppgifter från elektronisk kommunikation oftare kan göras åtkomliga för brottsbekämpande ändamål. På så sätt kan det brottsbekämpande arbetet effektiviseras och resurser läggas på annat. Härmed skapas förbättrade förutsättningar att bekämpa allvarlig brottslighet.

Sedan frågan om en skyldighet att registrera abonnemangsuppgifter för kontantkort utreddes förra gången har ett stort antal länder i världen infört en sådan skyldighet. I dag har minst 155 länder infört någon form av registreringsskyldighet som omfattar kontantkort. I Europa har nu mer än hälften av länderna infört någon form av registreringsplikt som omfattar kontantkort. Frågan utreds också på fler håll. Möjligheterna att köpa oregistrerade utländska kontantkort har således begränsats samtidigt som intresset från kriminella i andra länder av att använda svenska oregistrerade kontantkort har ökat. Det har framkommit att telefonnummer som tillhör svenska oregistrerade kontantkort i stor omfattning används av terrorkopplade utländska aktörer utomlands. Svenska kontantkort bidrar på detta sätt till att skapa möjligheter att anonymt diskutera brottsplaner och sprida propaganda (se Säkerhetspolisens årsbok 2018 s. 55 f.). Sverige bör inte vara ett land som underlättar för kriminella i andra länder att planera sin verksamhet.

Det är ofta en svår uppgift att avväga integritetsintresset mot nödvändigheten av att myndigheterna har effektiva metoder för brottsbekämpning. Det ligger i sakens natur att sådana metoder ofta innefattar ett integritetsintrång. Samtidigt måste beaktas att detta intrång ofta är blygsamt i jämförelse med den kränkning som offren för allvarlig brottslighet måste utstå. I det sammanhanget bör beaktas att de abonnemangsuppgifter som skulle behandlas till följd av en registreringsplikt i sig inte kan anses vara särskilt känsliga och att det inte är fråga om mer än en begränsad inskränkning av den enskildes rätt till personlig integritet. Abonnemangsuppgifter registreras dessutom redan i dag avseende de kunder som innehar kontraktsabonnemang eller som har valt att lämna sådana uppgifter för sitt kontantkortsabonnemang. Som har framgått innebär en registreringsskyldighet inte något avgörande hinder för den som i ett legitimt syfte vill kunna kommunicera utan att avslöja sin identitet. En registreringsskyldighet skulle således endast innebära en utvidgning av förevarande system och de registrerade uppgifterna skulle skyddas av befintlig reglering om dataskydd och sekretess.

Vid en avvägning mellan de positiva effekter som en registreringsskyldighet kan förväntas få genom att försvåra de kriminellas verksamhet och de negativa effekter som registreringsskyldigheten kan ha för enskilda framstår det som en proportionerlig åtgärd att innehavaren av ett telefonabonnemang registrerar sina identitetsuppgifter. Det är således vår bedömning att en skyldighet att registrera abonnemangsuppgifter för kontantkort bör införas.

5.6.2 Hur bör en registreringsskyldighet utformas?

Var bör registreringsskyldigheten regleras?

Förslag: Registreringsskyldigheten ska regleras i lagen om elektronisk kommunikation.

En författningsreglerad registreringsplikt innebär ett krav på att uppgifter om enskilda ska samlas in och behandlas under viss tid. Med hänsyn till enskildas rätt till privatliv enligt artikel 8 i Europakonventionen ska en sådan registreringsplikt regleras i lag. Även det förhållandet att registreringsskyldigheten kommer att innebära

åligganden för mobiloperatörerna medför att regleringen ska införas i lag (se 8 kap. 2 § RF). Bestämmelserna bör lämpligen föras in i lagen om elektronisk kommunikation, där frågor om mobiloperatörernas lagring och övriga behandling av personuppgifter regleras. Att bestämmelserna förs in i den lagen är också lämpligt med hänsyn till att andra frågor om abonnenter regleras här liksom operatörernas tystnadsplikt.

Det bör dock vara möjligt för regeringen eller den myndighet som regeringen bestämmer att meddela närmare föreskrifter i frågor som är av för enskilda mindre ingripande karaktär. En sådan möjlighet bör, som vi återkommer till nedan, finnas i fråga om den identitetskontroll som ska göras i samband med registreringen.

Vilka aktörer bör omfattas av ett registringskrav?

Förslag: Regleringen ska omfatta de som tillhandahåller förbetalda allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster eller internetanslutningstjänster.

Som framgått ovan finns det i andra länder olika modeller för hur en registreringsskyldighet kan utformas. Enligt den vanligaste modellen är operatörerna skyldiga att samla in och föra ett register över sina kunder. I januari 2020 följde 81 procent av länderna i världen som har krav på en registrering av kontantkort denna modell. Modellen används också av andra europeiska länder. Även en svensk registreringsplikt bör enligt vår mening utformas på detta sätt, dvs. som ett krav på att de som tillhandahåller kontantkort ska registrera och under viss tid bevara uppgifter om sina kunders abonnemang. Den uppenbara fördelen med en sådan ordning är att uppgifterna därmed kommer att föras vidare till brottsbekämpande myndigheter endast i de fall där detta begärs och befintlig lagstiftning tillåter det.

I ett flertal länder, däribland Norge och Tyskland, träffar registreringsplikten alla aktörer som tillhandahåller telefonitjänster, dvs. även de som tillhandahåller fasta telefonabonnemang och kontraktsabonnemang för mobiltelefoner. Enligt vår uppdragsbeskrivning ingår i uppdraget att lämna förslag till regler om en skyldighet att registrera uppgifter om abonnemang avseende kontantkort. Uppdraget får således anses omfatta endast de som tillhandahåller

förbetalda tjänster och inte andra former av abonnemang. Det kan konstateras att uppgifter om övriga abonnemangsformer registreras ändå. Således bör den föreslagna regleringen endast omfatta de som tillhandahåller kontantkort, alltså förbetalda tjänster.

Som tidigare framgått kan ett kontantkort avse enbart samtalstjänster, både samtalstjänster och datatjänster eller endast datatjänster (mobilt bredband). Vanligast är att ett mobilabonnemang ger tillgång till såväl samtalstjänster som datatjänster (ofta benämnt surf). Det finns även simkort som använder telefonnummer och som endast ger tillgång till kommunikation mellan maskiner, s.k. M2M. Vid M2M används simkort för t.ex. övervakning, mätning, styrning, transport och logistik. Simkorten kan på detta sätt användas t.ex. i bilar, tåg, elmätare, hemlarm och gräsklippare. Även M2M-tjänster kan vara förbetalda, även om det är ovanligt.

Eftersom det numera finns inbyggda simkort, s.k. e-sim, bör regleringen inte knytas till ett simkort såsom en fysisk bärare av en tjänst, utan till de förbetalda elektroniska kommunikationstjänster som kan erhållas via ett fysiskt simkort eller ett e-sim. De aktörer som tillhandahåller sådana tjänster ska omfattas av registreringskravet. Frågan är då om detta ska gälla för alla tjänster.

Europaparlamentets och rådets direktiv (EU) 2018/1972 om inrättande av en europeisk kodex för elektronisk kommunikation, trädde i kraft den 21 december 2018. Enligt kodexen kan elektroniska kommunikationstjänster vara av tre slag; internetanslutningstjänster, interpersonella kommunikationstjänster eller tjänster som helt eller huvudsakligen utgörs av överföring av signaler (t.ex. M2M). Med en *internetanslutningstjänst* avses en tjänst som erbjuder anslutning till internet. Med en *interpersonell kommunikationstjänst* menas en tjänst som vanligen tillhandahålls mot ersättning och som möjliggör 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. De interpersonella kommunikationstjänsterna kan vara antingen nummerbaserade eller nummeroberoende. En nummerbaserad interpersonell kommunikationstjänst använder nummer i nationella eller internationella nummerplaner eller möjliggör kommunikation med nummer i nationella eller internationella nummerplaner (se artikel 2).

I förslaget till ny lag om elektronisk kommunikation används begreppet allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst för att beskriva de telefonitjänster som tillhandahålls via bl.a. kontantkort. För att beskriva de datatjänster som kan nås via kontantkorten används begreppet internetanslutningstjänst (se tex. 7 kap. 31 § i lagförslaget). Vi har valt att använda oss av samma begrepp.

Det står klart att regleringen bör omfatta de kontantkort som ger tillgång till traditionella telefonitjänster. Detta bör komma till uttryck på det sättet att regleringen ska omfatta tillhandahållande av förbetalda allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster.

Merparten av de kontantkort som används i dag ger tillgång till såväl samtalstjänster som datatjänster. En registreringsskyldighet som endast omfattar allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster skulle medföra att en registrering skulle behöva ske för användning av de korten. Det har dock under utredningens gång framförts från brottsbekämpande myndigheter att regleringen bör omfatta samtliga förbetalda tjänster som kan knytas till ett kontantkort. På så sätt skulle regleringen bli mer teknikneutral.

När det för det första gäller de internetanslutningstjänster som kan nås via kontantkort har det från brottsbekämpande myndigheter framförts att dessa tjänster används alltmer i kriminella sammanhang. Enligt myndigheterna skulle en reglering som inte omfattar internetanslutningstjänster kunna medföra att enskilda i större utsträckning kommer att använda sig av dessa tjänster för att få åtkomst till appar som gör det möjligt att kommunicera krypterat. Kommunikationen sker då med hjälp av internet utan användning av något nummer som ingår i en nationell eller internationell nummerplan. I förlängningen kan det innebära att fler använder sig av krypterade internetbaserade tjänster för sin kommunikation. Vi delar bedömningen av vilken utveckling som kan komma att ske. Visserligen krävs det inte ens ett simkort utan endast tillgång till en internetuppkoppling, såsom ett wifi-nätverk, för att det ska vara möjligt att via exempelvis en mobiltelefon få tillgång till internet och därmed till olika former av kommunikationstjänster som inte kräver användning av nummer i nationella eller internationella nummerplaner. Således kommer det att finnas möjligheter att kommunicera

anonymt oavsett hur regleringen utformas i denna del. Det är dock inte lämpligt om den föreslagna regleringen får till effekt att det blir svårare för de brottsbekämpande myndigheterna att följa de kriminellas aktiviteter på grund av den förväntade utvecklingen.

Som vi redovisat i avsnitt 4.3 innebär hemlig övervakning av elektronisk kommunikation att man kan få fram uppgifter om vilka elektroniska kommunikationsutrustningar, exempelvis mobiltelefoner, som har funnits inom ett visst geografiskt område (s.k. basstationstömning). Detta gäller även om mobiltelefonen är försedd med ett kontantkort som bara ger tillgång till internetanslutning. Det är således möjligt för de brottsbekämpande myndigheterna att genom hemlig övervakning av elektronisk kommunikation få tillgång till uppgifter om på vilken geografisk plats ett sådant kontantkort har funnits vid en viss tidpunkt. För de brottsbekämpande myndigheterna är det naturligtvis av stort värde att få tillgång till registrerade uppgifter om vem som innehar även de här korten. De aktuella uppgifterna blir också allt viktigare i takt med att de kriminella väljer att kommunicera över internet i stället för via traditionell telefoni.

Ett annat argument som har framförts för att regleringen bör omfatta internetanslutningstjänster är att kontantkort som endast ger tillgång till dessa tjänster kan användas för att motta den kod som krävs för att aktivera ett konto i en internetbaserad kommunikationstjänst. Således kan, som berörts ovan, de kontantkort som ger tillgång till internet användas för att skapa appar som i sin tur kan användas för krypterad och anonym kommunikation. Det finns visserligen andra sätt att motta den kod som behövs för att aktivera ett konto i en internetbaserad app. Dock skulle ett registreringskrav som omfattar även de kontantkort som ger tillgång till internetanslutningstjänster försvåra för de kriminella som har satt i system att via kontantkort starta konton i internetbaserade appar och som därefter vidarebefordrar uppgifter om dessa till andra för krypterad och anonym kommunikation.

Det anförda har lett oss till slutsatsen att även de operatörer som tillhandahåller förbetalda internetanslutningstjänster bör omfattas av registreringsskyldigheten.

När det därefter gäller de överföringstjänster som endast används för tillhandahållande av M2M-tjänster kan det konstateras att de vanligtvis innehas via kontraktsabonnemang. Således är det normalt

möjligt att spåra ett nummer som tillhör ett simkort som endast används för M2M i vart fall till det företag som har köpt kortet och eventuellt har placerat det i en viss utrustning. Av de 14,3 miljoner svenska simkort för M2M som använder sig av mobilnummer finns den större delen av korten inplacerade i maskiner som används utanför Sverige. För det fall registreringsskyldigheten skulle omfatta även sådana kort uppkommer frågor kring när, hur och av vem registreringen bör ske för att den över huvud taget ska vara av värde för brottsbekämpningen. Det kan vidare konstateras att en registrering av redan befintliga kontantkort som är avsedda för M2M skulle vara mycket svår att genomföra i praktiken. Här ska också erinras om att de aktuella simkorten endast är avsedda för kommunikation mellan maskiner och inte för kommunikation mellan människor. De ger därmed som utgångspunkt inte tillgång till några större datamängder. Det ovanstående har medfört att vi sammantaget inte har identifierat något tydligt behov av att det införs en registreringsskyldighet för de som tillhandahåller M2M-tjänster.

Den föreslagna regleringen omfattar därmed de aktörer som tillhandahåller förbetalda allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster eller internetanslutningstjänster, men inte de som tillhandahåller förbetalda tjänster som endast kan användas för kommunikation mellan maskiner. Således är det kontantkort som ger tillgång till förbetalda telefonitjänster eller internetanslutningstjänster som ska registreras.

Det är tillgången till de förbetalda tjänsterna som avgör om det föreligger en registreringsplikt. För det fall kontantkort som ger tillgång till telefonitjänster eller internetanslutningstjänster används för kommunikation mellan maskiner omfattas de därför av registreringskravet.

Vilka uppgifter bör registreras?

Förslag: De uppgifter som ska registreras är abonnentens namn, adress, personnummer eller motsvarande och nummer för tjänsten.

En registreringsskyldighet bör omfatta uppgifter om den som genom att köpa ett kontantkort eller på annat sätt ingår avtal med en mobiloperatör om att denne ska tillhandahålla en förbetald tjänst.

Registreringen bör således avse abonnenten och dennes abonnemangsuppgifter.

Med abonnemangsuppgifter avses främst uppgifter om abonnentens nummer, namn, titel och adress (se t.ex. prop. 2018/19:86 s. 93). De uppgifter som i sammanhanget torde vara mest intressanta för en registrering avser uppgifter om abonnentens nummer, namn och adress. Med hänsyn till vikten av en säker identifiering bör en registreringsskyldighet därutöver omfatta personnummer eller motsvarande, såsom ett samordningsnummer eller organisationsnummer för det fall abonnenten är en juridisk person. Personnummer anges i dag av de kunder som frivilligt registrerar sitt kontantkort och innebär att kundens adress automatiskt hämtas från folkbokföringen.

I spellagen (2018:1138) finns krav på registrering av de som deltar i spel. Syftet med registreringen är att licenshavaren ska kunna identifiera och registrera spelare för att kunna upprätthålla kravet på att personer som inte uppnått gällande åldersgräns inte deltar i spel. Registreringen krävs också för att licenshavaren ska kunna övervaka spelen i syfte att motverka och förhindra fusk, bedrägeri och annan brottslig verksamhet. Vid registreringen ska spelaren uppge namn, adress och personnummer eller motsvarande (se 12 kap. 2 §). Med begreppet motsvarande avses här t.ex. samordningsnummer eller uppgift om när personen är född (se prop. 2017/18:220 s. 139 f.).

Det följer av 6 kap. 2 § LEK att dataskyddsförordningen och dataskyddslagen är tillämpliga även vid behandling av personuppgifter enligt lagen om elektronisk kommunikation. För behandling av personnummer och samordningsnummer gäller särskilda krav enligt dataskyddsregleringen. Personnummer och samordningsnummer anses inte som känsliga personuppgifter i dataskyddsförordningens mening, men har ändå en särställning genom att medlemsstaterna ges möjlighet att införa särskilda villkor för behandlingen av sådana uppgifter (se artikel 87). I 3 kap. 10 § dataskyddslagen har det tagits in en generell bestämmelse om behandling av personnummer och samordningsnummer. Av bestämmelsen framgår att sådana personuppgifter får behandlas om de registrerade har gett sitt samtycke. Finns det inget samtycke får personnummer och samordningsnummer behandlas bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Bestämmelsen

innebär att en intresseavvägning mellan behovet av behandlingen och de integritetsrisker som den innebär ska göras (se prop. 2017/18:105 s. 199).

För att undvika att en registreringsskyldighet blir tandlös bör det säkerställas att de uppgifter som lämnas om enskilda är korrekta. Behovet av en säker identifiering överväger de integritetsrisker som en behandling av uppgifter om personnummer eller samordningsnummer innebär för den enskilde. Det får därför anses vara klart motiverat att registreringsskyldigheten omfattar uppgifter om enskildas personnummer, samordningsnummer eller motsvarande. För juridiska personer bör registreringen omfatta ett organisationsnummer.

De uppgifter som ska registreras motsvarar sådana abonnemangsuppgifter som operatörerna behandlar redan i dag avseende de kunder som har kontraktsabonnemang. Uppgifterna kommer hos operatörerna att omfattas av tystnadsplikten för abonnemangsuppgifter enligt 6 kap. 20 § första stycket 1 LEK och av de integritetsskyddsbestämmelser som i övrigt följer av 6 kap. LEK och den allmänna dataskyddsregleringen. Utlämnande av abonnemangsuppgifterna till den som bedriver abonnentupplysning (5 kap. 7 § första stycket 3 LEK) kommer endast att få ske om den enskilde har samtyckt till det. Utlämnande till myndigheter kommer endast att få ske i de fall så begärs och tillämplig lagstiftning tillåter det.

När bör registreringen ske?

Förslag: Den som tillhandahåller en förbetald tjänst ska inte få ge tillgång till tjänsten, om inte denne först har genomfört en registrering.

Förbetalda tjänster bör inte vara möjliga att använda innan en registrering har skett. I annat fall riskerar regleringen att bli mindre effektiv. För det fall tjänsterna skulle kunna användas utan att en registrering har skett finns det också en risk för att osålda kontantkort skulle kunna bli stöldbegärliga. En förbetald tjänst som omfattas av regleringen bör därför inte på något sätt vara möjlig att ta i bruk om inte en registrering har skett. Det bör t.ex. inte vara möjligt att motta samtal eller sms innan en registrering har skett. Inte heller

bör internetanslutningstjänster vara möjliga att utnyttja före registreringen. Således bör det av regleringen framgå att den som tillhandahåller en förbetald tjänst inte ska få ge tillgång till tjänsten förrän denne har genomfört en registrering.

Den föreslagna regleringen hindrar inte att kontantkort säljs utan att en registrering har skett. Det bör alltså vara möjligt att köpa kontantkort även av fristående handlare som inte har möjlighet att genomföra en registrering. Registreringen kan därefter utföras t.ex. i en butik som tillhör den aktuelle mobiloperatören eller hos större återförsäljare. Man kan också tänka sig att registreringen kan utföras via internet eller vid kontakt med kundtjänst. Först när en registrering har skett kommer det dock att vara möjligt att utnyttja de tjänster som omfattas av regleringen.

Under vilken tid bör uppgifterna lagras?

Förslag: De registrerade uppgifterna ska finnas tillgängliga från registreringen och i ett år efter att tillhandahållandet har upphört.

Lagen om elektronisk kommunikation innehåller vissa bestämmelser om lagring som även omfattar abonnemangsuppgifter. Huvudregeln är att en uppgift ska utplånas eller avidentifieras när den inte längre behövs för att överföra ett elektroniskt meddelande (6 kap. 5 §). Från denna huvudregel finns flera undantag. En operatör kan exempelvis, med den enskildes samtycke, lagra abonnemangsuppgifter viss tid för marknadsföring (6 kap. 6 §). Den lagringsskyldighet för brottsbekämpande ändamål som följer av 6 kap. 16 a § LEK utgör ett annat undantag från huvudregeln. Lagringsskyldigheten omfattar sådana uppgifter om abonnemang som är nödvändiga för att spåra och identifiera kommunikationskällan och slutmålet för kommunikationen. Bland de uppgifter som ska lagras ingår uppgifter om abonnent och registrerad användare liksom uppgifter om den uppringda abonnenten (39 § FEK). Skyldigheten att lagra uppgifter omfattar uppgifter som genereras eller behandlas vid telefonitjänst och meddelandehantering via mobil nätanslutningspunkt. Dessa uppgifter ska lagras i sex månader. Lagringstiden räknas från den dag kommunikationen avslutades (6 kap. 16 d § LEK).

Lagringsskyldigheten enligt 6 kap. 16 a § LEK gäller alltså från den dag en viss kommunikation avslutas. Det förekommer dock att telefonnummer kopplade till kontantkort endast används för att starta konton i vissa mobilapplikationer. I sådant fall sker ingen sådan kommunikation som gör att lagringsskyldigheten påbörjas. Det kan också vara så att brottsbekämpande myndigheter vill få kännedom om vem som är innehavare av ett visst kontantkort eller vilka kontantkort som innehas av en viss person även om ett kort ännu inte har använts för kommunikation. Man kan också tänka sig att enskilda inte lämnar samtycke till behandling i marknadsföringssyfte. För att säkerställa att de abonnemangsuppgifter som avser kontantkort lagras är det därför nödvändigt med särskilda bestämmelser om lagring.

En särskild lagringsregel för här aktuella abonnemangsuppgifter skulle alltså endast avse uppgifter om de som innehar kontantkortsabonnemang. Syftet är att uppgifterna ska finnas tillgängliga för brottsbekämpande ändamål, vilket är ett godtagbart syfte enligt såväl EU-rätten som Europakonventionen. EU-domstolens förhandsavgörande den 21 december 2016 i de förenade målen C-203/15 och C-698/15, den s.k. Tele2-domen, avser inte specifikt uppgifter om abonnemang (se prop. 2018/19:86 s. 91 f.). EU-domstolen har dock förklarat att uppgifter om abonnemang, till skillnad från trafikuppgifter och lokaliseringsuppgifter, inte gör det möjligt att dra några mer precisa slutsatser om berörda personers privatliv (se det ovannämnda avgörandet Ministerio Fiscal). I likhet med Europadomstolen i målet Breyer mot Tyskland anser vi att en skyldighet att lagra abonnemangsuppgifter inte utgör något betydande ingrepp i enskildas skyddade sfär. Som framgår ovan kan de brottsbekämpande myndigheternas tillgång till uppgifterna förväntas leda till ett effektivare arbete för de brottsbekämpande myndigheterna och är sålunda motiverat för att brott ska kunna avslöjas, utredas och beivras. Det ingrepp i enskildas grundläggande rättigheter som en skyldighet att lagra uppgifter utgör står enligt vår mening i rimlig proportion till det behov och den nytta som de brottsbekämpande myndigheternas tillgång till uppgifterna medför. Tele2-domen innebär således inte något hinder mot att en särskild reglering om lagring införs för abonnemangsuppgifter. Visserligen kommer det i viss mån bli fråga om en dubbelreglering i förhållande till lagringsskyldigheten enligt 6 kap. 16 a §. Vi ser dock inte det som

något problem eftersom regleringarna har olika syften. Därtill kan en särskild reglering för abonnemangsuppgifter avseende förbetalda tjänster bidra till att skapa tydlighet.

Hur länge abonnemangsuppgifter gällande kontantkortskunder bevaras varierar stort mellan olika europeiska länder. I något fall ska uppgifterna raderas direkt efter att ett avtal har upphört och i något fall bevaras i tre år. I Tyskland ska de insamlade uppgifterna raderas i slutet av kalenderåret året efter det att avtalet har upphört. Europadomstolen fann i målet Breyer mot Tyskland att den tyska lagringstiden inte framstod som olämplig med hänsyn till att en brottsutredning kan ta viss tid och pågå längre än ett kontantkort är aktivt.

Abonnemangsuppgifterna bör lagras i vart fall under den tid tjänsten är i bruk. Med hänsyn till att en brottsutredning kan pågå en längre tid än en förbetald tjänst är aktiv bör uppgifterna också lagras en viss tid därutöver. Det förekommer t.ex. att telefonnummer som tillhör kontantkort används för att aktivera konton i olika internetbaserade appar. Kommunikationen i dessa appar kan pågå lång tid efter det att kontantkorten har tagits ur bruk. För att få tillgång till information om vem som har skapat apparna kan således de brottsbekämpande myndigheterna ha behov av att få tillgång till abonnemangsuppgifterna efter en längre tid. Samtidigt är det så att en lagring av de abonnemangsuppgifter som avser kontantkortskunder kommer att medföra att operatörerna har tillgång till uppgifter om ett stort antal enskilda, varav de flesta inte alls är av intresse för de brottsbekämpande myndigheterna. Med hänsyn till enskildas behov av ett rimligt skydd för sin personliga integritet kan uppgifterna inte lagras under hur lång tid som helst. Enligt vår mening får ett år anses utgöra en rimlig lagringstid enligt den föreslagna regleringen. Eftersom lagring av abonnemangsuppgifter kan grunda sig på fler bestämmelser i lagen om elektronisk kommunikation, kan dock de aktuella uppgifterna komma att bevaras en längre tid än vad som föreslås av oss. En längre lagring kan t.ex. bli aktuell i marknadsföringssyfte, om den enskilde har lämnat sitt samtycke till det.

Av 39 § 6 FEK framgår att mobiloperatörerna, för att fullgöra lagringsskyldigheten enligt 6 kap. 16 a § LEK, ska lagra uppgifter om datum, spårbar tid och lokaliseringsuppgifter för den första aktiveringen av en förbetald anonym tjänst. Enligt vår uppdragsbeskrivning ingår det inte i uppdraget att lämna förslag som innebär att

lagringsskyldighetens omfattning ändras. Den av oss föreslagna registreringsskyldigheten medför dock att det inte kommer att finnas förbetalda anonyma och allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster eller internetanslutningstjänster. Det kan därför finnas anledning att senare se över den aktuella regleringen.

Hur bör identitetskontrollen gå till?

Förslag: Abonnentens identitet ska kontrolleras genom en giltig identitetshandling med fotografi eller en tillförlitlig elektronisk identifiering. Saknar abonnenten en identitetshandling ska identiteten göras sannolik på annat sätt. Identitetskontrollen ska dokumenteras.

Regeringen eller den myndighet regeringen bestämmer ska få meddela närmare föreskrifter om identitetskontrollen. Post- och telestyrelsen ska i förordning bemyndigas att meddela föreskrifter om identitetskontrollen.

Allmänt om identitetshandlingar

En kontroll av en persons identitet syftar till att utreda om personen är den han eller hon utger sig för att vara. En identitetshandling används för att personen ska kunna identifiera sig eller styrka sin identitet. Som utgångspunkt gäller att det är den som en identitetshandling visas upp för som måste ta ställning till om den aktuella handlingen kan godtas som bevis om en persons identitet. Det brukar dock sägas att det finns fem svenska identitetshandlingar som allmänt accepteras som bevis på innehavarens identitet (se t.ex. SOU 2019:14 s. 107). De fem handlingarna är pass, nationellt identitetskort, identitetskort för folkbokförda i Sverige, körkort och SIS-märkt id-kort (SIS står för Swedish Standards Institute).

Pass är först och främst en resehandling. Passet är dock det dokument som internationellt sett i störst utsträckning accepteras som identitetshandling. *Det nationella identitetskortet* infördes 2005 delvis i syfte att underlätta resandet inom Schengenområdet där det råder passfrihet. Kortet utfärdas enligt 1 § förordningen (2005:661)

om nationellt identitetskort endast till svenska medborgare. Till skillnad från vissa andra länder finns det här inte något krav på att alla ska ha ett nationellt identitetskort. *Identitetskort för folkbokförda i Sverige* utfärdas sedan 2009 av Skatteverket. Införandet av kortet innebär att det i dag finns en handling som enbart har som funktion att styrka identitet och som staten har ansvar för att tillhandahålla. Id-kortet utfärdas till personer som har fyllt 13 år och är folkbokförda i landet enligt folkbokföringslagen (1991:481). Det krävs inte att sökanden är svensk medborgare. Ett *körkort* har till primärt syfte är att utvisa behörigheten att köra vissa körkortspliktiga fordon. Körkortet är dock sedan länge en allmänt accepterad identitetshandling i Sverige. Det s.k. *SIS-märkta id-kortet* är en identitetshandling som tillverkas av en licensierad tillverkare och utfärdas av en godkänd utfärdare enligt vissa standarder. SIS-märkta id-kort utfärdas av privata aktörer och utfärdandet är inte till någon del författningsreglerat. Vanliga utfärdare av SIS-märkta id-kort är bankerna som utfärdar korten som en tjänst till sina kunder. Större företag, organisationer eller myndigheter kan också ha tillstånd att utfärda SIS-märkta id-kort till sina anställda.

Utöver de fem allmänt accepterade fysiska identitetshandlingarna finns det en mängd olika handlingar av skiftande kvalitet som ibland kan användas för att identifiera sig. Dessa handlingar godtas allmänt inte som identitetshandlingar, men kan i vissa sammanhang anses som tillräckligt identitetsbevis. Bland sådana handlingar finns det tillfälliga LMA-kortet för utlänning i Sverige, det s.k. LMA-kortet. LMA-kortet utfärdas av Migrationsverket till utlänningar som har rätt till bistånd enligt lagen (1994:137) om mottagande av asylsökande m.fl. LMA-kortet innehåller ett fotografi av innehavaren och de uppgifter som finns om personen i den centrala utlänningsdatabasen. LMA-kortet är inte en identitetshandling utan ett bevis på att innehavaren är asylsökande och får vara i Sverige i avvaktan på beslut. Kortet godtas dock som identitetsbevis i vissa myndighetskontakter. Det kan i vissa fall användas för att hämta ut postpaket från utlandet eller rekommenderad post från Migrationsverket. Det kan också användas i kontakter med hälso- och sjukvård och apotek samt kan under vissa förutsättningar accepteras vid öppnande av bankkonto. LMA-kortet ska som huvudregel återlämnas när uppehållstillstånd beviljas och personen folkbokförs.

Det finns även tjänstekort som utfärdas av myndighet, men som inte är SIS-märkta. De regleras i förordningen (1958:272) om tjänstekort. Tjänstekort utfärdade av myndigheter godtas ibland som identitetsbevis, t.ex. vid utfärdande av identitetskort för folkbokförda i Sverige.

Till de handlingar som generellt sett inte godtas som bevis om identitet räknas medborgarskapsbevis, studentlegitimation och uppehållstillståndskort (se SOU 2019:14 s. 127).

Utländska identitetshandlingar accepteras i vissa fall i Sverige som bevis om någons identitet. Exempelvis godtas pass utfärdade av andra EU-länder samt Island, Liechtenstein, Norge och Schweiz som identitetshandling vid utfärdande av identitetskort för folkbokförda och körkort. Pass utfärdade av länder utanför EU godtas som identitetshandling vid utlämnade av paket, rekommenderad post eller postförskott. Vid sådan utlämning godtas också nationellt identitetskort utfärdat av länder inom Schengenområdet. Bankerna godtar också vissa utländska identitetshandlingar.

Förutom fysiska handlingar finns det elektroniska identitetshandlingar (e-legitimationer). En e-legitimation innehåller liksom en fysisk identitetshandling uppgifter som entydigt kan kopplas till en viss person. Med hjälp av en e-legitimation kan innehavaren identifiera sig och myndigheter eller andra aktörer som har e-tjänster få en bekräftelse om vem personen är. E-legitimation används framför allt vid identifiering i samband med att en person vill använda en e-tjänst. E-legitimation kan också användas vid telefonkontakt med en kundtjänst. Den e-legitimation som dominerar på den svenska marknaden är BankID. Alla privatpersoner som har svenskt personnummer kan skaffa BankID genom sin bank. Över åtta miljoner svenskar använder sig i dag av BankID. En annan utfärdare av e-legitimationer är Verisec.

Användningen av e-legitimationer inom EU regleras i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (eIDAS-förordningen). Syftet med förordningen är att säkerställa en väl fungerande inre marknad och uppnå en lämplig säkerhetsnivå för e-legitimationer och betrodda tjänster. I Sverige gäller även lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering, och en

tillhörande förordning. Det finns dock inte någon reglering av vad som krävs för att få en e-legitimation utfärdad eller om vilka krav en sådan handling ska uppfylla. I stället har det tagits fram ett tillitsramverk för svensk e-legitimation. Svensk e-legitimation är ett kvalitetsmärke som är baserat på internationella standarder. Myndigheten för digital förvaltning granskar och godkänner svenska e-legitimationer för kvalitetsmärket.

Krav på identifiering i annan lagstiftning

Det finns, inom andra områden, lagstadgade skyldigheter om registrering av identitetsuppgifter som har likheter med kravet på registrering av identitetsuppgifter vid tillhandahållande av här aktuella förbetalda tjänster. Som exempel kan nämnas lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism. Lagen riktas mot den som utövar finansiell verksamhet och viss annan näringsverksamhet och ställer upp regler för att dessa aktörer ska försvåra och förhindra att verksamheten utnyttjas för penningtvätt eller finansiering av terrorism. Enligt lagen ska en verksamhetsutövare vidta s.k. kundkännedomsåtgärder i vissa särskilda situationer, t.ex. när en affärsförbindelse ingås. Åtgärder för kundkännedom omfattar kontroll av kundens identitet. I lagens 3 kap. 7 § anges att en verksamhetsutövare ska identifiera kunden och kontrollera kundens identitet genom identitetshandlingar eller registerutdrag eller genom andra uppgifter och handlingar från en oberoende och tillförlitlig källa. Bestämmelsen innebär att verksamhetsutövare som en åtgärd för kundkännedom ska identifiera kunden och kontrollera kundens identitet. Identifikation av kunden innebär inhämtande av uppgifter, normalt direkt från kunden, om kundens namn och andra relevanta uppgifter såsom adress och i förekommande fall personnummer, organisationsnummer, födelsedatum, samordningsnummer eller liknande uppgifter. Kontroll av identiteten ska bestå i åtgärder som syftar till att verifiera att de uppgifter om identiteten som inhämtats är korrekta. Om kunden är en juridisk person ska uppgifter om namn, organisationsnummer m.m. kontrolleras gentemot registerutdrag eller andra tillförlitliga uppgifter. Om kundens rättskapacitet inte följer av registrering av behörig registreringsmyndighet, bör verksamhetsutövaren kontrol-

lera och bedöma kundens rättskapacitet på annat sätt. Omfattningen av kontrollåtgärderna ska bestämmas av den risk som kan förknippas med kundrelationen (se prop. 2016/17:173 s. 523). Om risken för penningtvätt eller finansiering av terrorism som kan förknippas med kundrelationen bedöms som låg, får verksamhetsutövaren enligt 3 kap. 15 § tillämpa förenklade åtgärder för kundkännedom. Det innebär bl.a. att identitetskontrollen kan vara av mer begränsad omfattning och vidtas på annat sätt.

Finansinspektionen har meddelat särskilda föreskrifter om identitetskontrollen som ska tillämpas utöver bestämmelserna i lagen. Enligt 3 kap. 2 § Finansinspektionens föreskrifter om åtgärder mot penningtvätt och finansiering av terrorism (FFFS 2017:11) ska en verksamhetsutövare kontrollera identiteten hos en fysisk person genom svenskt körkort, svenskt pass eller identitetskort utfärdat av en svensk myndighet eller ett svenskt certifierat identitetskort. Om en fysisk person saknar svensk identitetshandling, ska identiteten kontrolleras mot pass eller en annan identitetshandling. Passet eller identitetshandlingen ska innehålla ett fotografi av personen, uppgift om medborgarskap och vara utfärdat av en myndighet eller en annan behörig utfärdare. En kopia ska tas av det utländska passet eller den utländska identitetshandlingen. Om en fysisk person helt saknar identitetshandling ska identiteten kontrolleras genom andra tillförlitliga dokument och andra kontroller enligt de riskbaserade rutiner verksamhetsutövaren ska ha. När förenklade åtgärder för kundkännedom tillämpas ska verksamhetsutövaren identifiera och kontrollera den fysiska personens identitet genom att inhämta uppgifter om kundens namn, adress och personnummer eller motsvarande, och kontrollera dessa uppgifter mot externa register, intyg, annan dokumentation eller motsvarande (se 3 kap. 9 §). Finansinspektionen har gjort särskilda uttalanden om kundkännedomsåtgärder för kunder som är asylsökande. Enligt Finansinspektionen kan finansiella aktörer acceptera identifiering genom Migrationsverkets LMA-kort, i kombination med annan kontroll. En sådan annan kontroll kan vara att banken ringer till Migrationsverket eller att en nära anhörig, med en godkänd svensk id-handling, intygar identiteten. Vidare kan den asylsökande uppvisa en vidimerad kopia på sitt utländska identitetskort som ett sätt att verifiera sin identitet.

I den tidigare nämnda spellagen anges att en licenshavare ska registrera vissa uppgifter om den som vill delta i spel, nämligen namn, adress och personnummer eller motsvarande. I 12 kap. 2 § nämnda lag anges att licenshavaren ska kontrollera spelarens identitet på ett betryggande sätt genom en tillförlitlig elektronisk identifiering eller motsvarande. I förarbetena anges att en kontroll kan ske genom att spelaren befinner sig på samma plats som licenshavaren eller dess spelombud och spelarens identitet där kontrolleras genom uppvisande av identitetshandlingar. Kontroll kan även ske genom en tillförlitlig elektronisk identifiering eller motsvarande, i första hand genom e-legitimation, t.ex. BankID. Skyldigheten anses omfatta även den situationen då spelaren vill ändra sina registrerade uppgifter (se prop. 2017/18:220 s. 318).

Regler om skyldighet att registrera identitetsuppgifter finns också på området för fartygssäkerhet. Av 7 kap. 2 § 2 fartygssäkerhetslagen (2003:364) framgår att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om skyldighet att registrera uppgifter om ombordvarande på passagerarfartyg. Transportstyrelsen får enligt 2 kap. 3 § fartygssäkerhetsförordningen (2003:438) meddela sådana föreskrifter. I 2 kap. 3 a § fartygssäkerhetsförordningen anges att en skyldighet att registrera uppgifter om ombordvarande ska ske efter kontroll av giltig identitetshandling med fotografi. Kontrollskyldigheten gäller dock inte för registrering av personer under 18 år som reser i sällskap med förälder som kan uppvisa en giltig identitetshandling med fotografi. Kontrollskyldigheten gäller dessutom bara om det för passagerarfartygets resa finns skäl att anta att uppgifter som lämnas utan att styrkas med identitetshandling kan vara oriktiga. Regleringen infördes i november 2015. Av den promemoria som låg till grund för införandet framgår att med giltig identitetshandling med fotografi avses t.ex. passhandling, legitimation, körkort eller liknade handling. Det framhålls att även kombinationer av handlingar som bekräftar att de uppgivna uppgifterna är riktiga kan godtas (se promemorian Registrering av ombordvarande på passagerarfartyg, s. 12).

Även i utlänningsförordningen (2006:97) finns bestämmelser om registreringsplikt. Enligt 6 kap. 13 § ska den som driver hotell, pensionat eller annan yrkesmässig uthyrningsverksamhet för övernattning se till att utlänningar på ett egenhändigt undertecknat registreringskort lämnar uppgifter om sig. Utlänningen ska styrka

sin identitet med en giltig legitimationshandling. I Polismyndighetens föreskrifter och allmänna råd om registreringskort för hotellgäster m.m.; (PMFS 2015:6) finns närmare föreskrifter om vilka uppgifter som ska lämnas. Här anges att registreringskortet ska innehålla uppgifter om utlänningens efternamn, förnamn, födelsetid, hemortsadress, ankomstdag och avresedag. Vidare ska det på kortet finnas uppgift om vilken legitimationshandling som uppvisats, handlingens nummer samt utlänningens underskrift och datum för denna (3 §). Den registreringsansvarige ska kontrollera att den utlänning som lämnar uppgifterna styrker sin identitet med en giltig legitimationshandling och att namn och födelsetid stämmer överens med uppgifterna i den uppvisade legitimationshandlingen (4 §). Registreringskorten ska sparas hos den registreringsansvarige i tre månader räknat från den dag utlänningen registrerades (6 §).

Våra överväganden

Det bör säkerställas att de uppgifter som lämnas om enskilda abonnenter av förbetalda tjänster är korrekta. De identitetsuppgifter som lämnas bör därför kontrolleras. Detta bör i första hand ske gentemot en identitetshandling. Som framgått ovan finns det ett flertal olika identitetshandlingar som normalt godtas för identifiering i Sverige. Därtill finns det flera motsvarande handlingar som godtas för identifiering i vissa fall. Det är av stor vikt att enskilda inte utesluts från möjligheten att använda kontantkort på grund av att de inte har tillgång till en godkänd identitetshandling. För enskilda som inte har möjlighet att teckna kontraktsabonnemang, t.ex. på grund av en betalningsanmärkning, saknas i många fall andra möjligheter att ringa än via ett kontantkort. För att få registrera sig som abonnent av en förbetald tjänst bör det därför vara tillräckligt att en enskild uppvisar någon form av identitetshandling med fotografi. Härmed avses t.ex. passhandling, id-kort, körkort eller liknade handling. Även ett LMA-kort eller ett sådant tjänstekort som regleras i förordningen om tjänstekort bör kunna godtas. För att inte utländska turister ska utestängas från möjligheten att använda svenska kontantkort bör även utländska identitetshandlingar med fotografi godtas.

En identifiering bör inte bara kunna ske i samband med besök i en fysisk butik. Identifieringen bör även kunna ske i samband med registrering via internet eller vid kontakt med kundtjänst. En identitetskontroll som sker genom en tillförlitlig elektronisk identifiering, i första hand genom en e-legitimation såsom BankID, bör därför godtas.

För det fall en abonnent saknar identitetshandling bör identiteten kunna göras sannolik på annat sätt. Om kunden är ett barn som saknar identitetshandlingar bör en nära anhörig, med en godkänd svensk id-handling, kunna intyga identiteten. För det fall kunden är en juridisk person bör lämnade uppgifter kunna kontrolleras gentemot registerutdrag eller andra tillförlitliga uppgifter. Den som företräder den juridiska personen bör således kunna styrka detta. Omfattningen av kontrollåtgärderna bör baseras på den risk för felaktig registrering som kan anses föreligga i det enskilda fallet.

Regleringen bör innehålla ett krav på att identitetskontrollen ska dokumenteras. På så sätt införs en kontrollmekanism för att identitetskontrollen utförs på ett korrekt sätt. Dokumentationen kan t.ex. avse en anteckning om vilken identitetshandling som har använts.

Det kan komma att visa sig nödvändigt med närmare regler om den identitetskontroll som ska utföras efter att systemet har varit igång en tid. Det kan exempelvis visa sig erforderligt att närmare reglera vad som utgör en tillförlitlig elektronisk identifiering eller hur en identitetskontroll ska dokumenteras, t.ex. genom att en kopia tas av vissa id-handlingar. Det kan också finnas anledning att närmare reglera hur identiteten avseende en juridisk person bör kontrolleras. Det bör därför finnas en möjlighet för regeringen eller den myndighet som regeringen bestämmer att meddela närmare föreskrifter om identitetskontrollen. Post- och telestyrelsen är tillsynsmyndighet enligt lagen om elektronisk kommunikation och har ett samlat ansvar inom området för elektronisk kommunikation. Myndigheten kan därför säkerställa att hänsyn tas till såväl mobiloperatörernas som de brottsbekämpande myndigheternas intressen vid utformningen av föreskrifterna. Post- och telestyrelsen har också goda förutsättningar att utreda effekterna på integritet för användare och kostnader för leverantörerna beroende på vilka krav som kan ställas. Det är därmed lämpligt att föreskriftsrätten anförtros Post- och telestyrelsen. Ett bemyndigande för Post- och telestyrelsen att

meddela föreskrifter om identitetskontrollen bör föras in i förordningen om elektronisk kommunikation.

Bör registreringsplikten även avse befintliga förbetalda tjänster?

Förslag: Registreringsplikten ska omfatta även förbetalda tjänster som har tagits i bruk innan lagen trädde i kraft. Dessa ska dock vara möjliga att använda i sex månader efter lagens ikraftträdande utan att en registrering har skett. Om en registrering inte har skett inom denna tid ska tillhandahållandet av tjänsterna avbrytas.

Det finns i dag miljontals kontantkort i Sverige. För det fall befintliga kontantkort inte skulle omfattas av den föreslagna regleringen skulle det vara möjligt att fortsätta använda dessa kort anonymt. En andrahandsmarknad för befintliga kontantkort skulle därmed kunna skapas i syfte att undgå en registrering. För att undvika en sådan situation krävs att även de tjänster som tillhör befintliga kontantkort registreras.

Om den som tillhandahåller en elektronisk kommunikationstjänst till en abonnent vill ändra avtalet ska abonnenten enligt 5 kap. 16 § LEK underrättas om ändringen minst en månad innan den träder i kraft. En abonnent som inte godtar de nya villkoren får säga upp avtalet utan att därvid drabbas av någon kostnad, avgift eller annan förpliktelse. I underrättelsen ska abonnenten upplysas om sin rätt att säga upp avtalet. Bestämmelsen, som grundar sig i EU-rätten, gäller för det fall det är operatören som vill ändra befintliga avtal. Bestämmelsen kan inte anses vara tillämplig när en ändring påfordras i lag. Den utgör därmed inte något hinder mot en lagstadgad registreringsskyldighet för de tjänster som nås via befintliga kontantkort. Det kan därtill konstateras att det bör vara möjligt att använda det värde som har laddats på ett kontantkort även efter att en registrering har skett.

Andra europeiska länder som har infört en registreringsskyldighet som omfattar kontantkort har låtit denna gälla även för befintliga kontantkort eller förbetalda tjänster och har lagstiftat om en övergångsperiod inom vilken registrering av dessa ska ske. De

kort eller tjänster som inte har registrerats inom denna tid har tagits ur bruk.

En registreringsskyldighet även för befintliga förbetalda tjänster kommer visserligen att innebära ytterligare administrativ börda för operatörerna. Det får dock anses rimligt att de krav som gäller i andra europeiska länder ska gälla även här. Således bör även den svenska regleringen omfatta de förbetalda tjänster som har tillhandahållits innan registreringsskyldigheten trädde i kraft.

För att regleringen i så liten mån som möjligt ska innebära besvär för enskilda och för mobiloperatörerna bör det, liksom i andra europeiska länder, införas en övergångsperiod inom vilken enskilda kan låta registrera sina befintliga förbetalda tjänster. Detta sker lämpligen genom att det i en övergångsbestämmelse införs en dispens med innebörden att förbetalda tjänster som har tillhandahållits innan registreringsskyldigheten trädde i kraft får användas viss tid därefter utan att en registrering har skett. Sex månader bör utgöra en tillräckligt lång tid för att de som vill fortsätta använda befintliga tjänster ska beredas möjlighet att registrera dem. För det fall en förbetald tjänst inte har registrerats inom denna tid ska tillhandahållandet av tjänsten upphöra. Beslutet om upphörande ska fattas av operatören. Det är således inte fråga om något förvaltningsbeslut av en myndighet.

Bör det finnas möjlighet till undantag från registreringsplikten?

Bedömning: Någon möjlighet till undantag från registreringsplikten bör inte införas.

En fråga i sammanhanget är om registreringsskyldigheten bör omfatta uppgifter om samtliga enskilda som innehar en förbetald tjänst, eller om regleringen bör innehålla en möjlighet att undanta t.ex. barn eller enskilda som kan ha särskilda behov av att använda förbetalda tjänster anonymt.

För barn gäller särskilda regler om att ingå avtal. Den som är under 18 år och därmed omyndig får inte själv åta sig förbindelser (9 kap. 1 § föräldrabalken). Ett barn kan alltså inte ingå avtal som innebär skuldsättning utan förmyndarens samtycke. Med skuldsättning jämförs att ingå avtal som innebär att användandet av en

tjänst ska betalas i efterhand (se prop. 2007/08:150 s. 66). Avtal som ett barn ingår utanför sin behörighet och utan förmyndares samtycke är normalt ogiltigt. Ett avtal blir dock bindande för båda parter när det har fullgjorts, t.ex. genom att en skuld har betalats (9 kap. 6 § FB). Inte heller förmyndare får dock som utgångspunkt företa rättshandlingar som innebär att barn skuldsätts (13 kap. 12 § FB). Det anförda innebär att barn normalt inte får skaffa kontraktsabonnemang till mobiltelefoner. Ett förbud mot registrering av barn som köper kontantkort skulle därmed kunna innebära att barn inte har någon möjlighet att skaffa mobilabonnemang. Ett förbud mot att registrera barn som abonnenter av kontantkort skulle därmed kunna ses som ett ingrepp i barns rätt till korrespondens enligt artikel 8 i Europakonventionen och artikel 16 i Barnkonventionen. Vidare ser vi en större risk för att barn skulle utnyttjas i syfte att införskaffa kontantkort för annans räkning om de inte skulle omfattas av registreringsplikten. Något undantag från registreringsskyldigheten när det gäller barn verkar inte heller finnas i andra länder. Vi föreslår inte heller något sådant undantag.

Som det tidigare redogjorts för kan det finnas enskilda som har legitima skäl för att inte vilja registrera uppgifter om sitt telefoninnehav. Så kan vara fallet för poliser eller journalister som arbetar undercover. Även enskilda som t.ex. fungerar som källor till journalister eller brottsbekämpare eller som lever under hot kan ha legitima skäl för att vilja undgå en registrering av sitt kontantkort. Med hänsyn härtill har vi övervägt om regleringen bör innehålla en möjlighet till undantag från registreringsplikten i vissa sådana situationer. Enligt vår bedömning är det dock inte säkert att ett undantag från registreringskravet skulle medföra något ökat skydd för den enskilde. Man kan nämligen inte bortse från risken att den omständigheten att någon inte behöver registrera sig kan peka ut just den personen som särskilt skyddsvärd av någon anledning. En sådan effekt skulle i sämsta fall kunna leda till ett sämre skydd för den enskilde. För de aktuella grupperna är det därför lämpligare att frågan om anonymitet löses på annat sätt (se avsnitt 5.6.1 ovan). Vi föreslår mot den bakgrunden att det inte införs något undantag från registreringsplikten.

Bör regleringen innehålla ett uttryckligt krav på att de registrerade uppgifterna är uppdaterade?

Bedömning: Tillämplig dataskyddsreglering är tillräcklig för att säkerställa att de registrerade uppgifterna är uppdaterade.

Registreringen av abonnemangsuppgifter ska enligt förslaget ske innan tillhandahållaren får ge tillgång till en förbetald tjänst. De uppgifter som har registrerats kan efter registreringen komma att ändras. Regleringen skulle med hänsyn härtill kunna innehålla ett krav på att abonnemangsuppgifterna ska vara uppdaterade eller att en ny registrering ska ske i samband med ändring av ett avtal. En sådan reglering skulle ha till syfte att säkerställa att de lämnade uppgifterna kontrolleras och eventuellt ändras t.ex. i samband med att ett kontantkort fylls på. Det följer dock redan av artikel 5.1 i dataskyddsförordningen att personuppgifter som behandlas ska vara riktiga och om nödvändigt uppdaterade. Operatörerna har således redan krav på sig att se till att deras kundregister är uppdaterade. Med hänsyn härtill är det vår bedömning att den nu föreslagna regleringen inte bör innehålla ett uttryckligt krav på att de registrerade uppgifterna ska vara uppdaterade eller att ny registrering ska göras i samband med ändring av ett avtal. För att operatörerna ska leva upp till dataskyddsförordningens krav på att hålla sina kundregister uppdaterade kan de dock ha anledning att regelbundet kontrollera att lämnade uppgifter alltjämt är korrekta. Detta kan ske t.ex. i samband med att kunden fyller på sitt kontantkort.

Bör överlåtelser av förbetalda tjänster regleras?

Förslag: Om en förbetald och registrerad tjänst har överlåtits till någon annan, fysisk eller juridisk person, utan att en ny registrering har skett, ska tillhandahållandet av tjänsten avbrytas. Detta ska dock inte gälla om tjänsten har överlåtits till en närstående, om tjänsten har införskaffats av en juridisk person och används på dennes uppdrag eller om tjänsten har införskaffats på uppdrag av Försvarsmakten, Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som har till uppgift att ingripa mot brott.

En registrering ska enligt förslaget avse uppgifter om den som har ingått ett avtal med en mobiloperatör om tillhandahållande av en förbetald tjänst. Man kan dock tänka sig att den registrerade personen därefter väljer att låta någon annan använda tjänsten. Exempelvis kan en enskild köpa och registrera sig som abonnent för tjänster som är knutna till ett kontantkort som senare överlåts på hans eller hennes barn eller andra anhöriga. Det finns i de flesta fall ingen anledning att ha synpunkter på sådana överlåtelser. Men det kan också vara så att kriminella personer kommer att låta en s.k. målvakt köpa och registrera sig som abonnent för tjänster som är knutna till ett kontantkort som senare kommer att överlåtas på någon annan. Huruvida det rent civilrättsligt är möjligt för en abonnent att överlåta ett kontantkortsabonnemang skiljer sig åt mellan mobiloperatörerna. Hos en operatör är en överlåtelse av kontantkort inte alls möjlig. Hos andra operatörer är detta möjligt men kräver operatörens medgivande. Oavsett hur frågan har reglerats civilrättsligt kan dock överlåtelser komma att ske utan att operatören informeras om detta. Ett sådant förfarande väcker frågan om det bör införas något lagkrav gällande överlåtelser av registrerade förbetalda tjänster.

I den belgiska regleringen föreskrivs att den som har registrerat ett kontantkort inte får överlåta ett aktivt kort till en tredje part utan att en ny registrering har skett, förutom i vissa fall. Det är t.ex. tillåtet att köpa kontantkort till familjemedlemmar och till anställda. Det är också tillåtet att lämna ett förbetalt kort vidare om det har köpts på uppdrag av underrättelse- eller säkerhetstjänsten, av polisen eller vissa andra myndigheter. I övriga fall får kontantkort endast överlåtas till någon annan om denne har identifierat sig hos operatören. Vid överträdelser av regleringen kan sanktioner utgå.

Någon reglering motsvarande den belgiska har vi inte hittat i något annat land. I Norge har det nyligen utretts om registreringsskyldigheten för en slutbrukare bör kompletteras med ett krav på att den faktiske brukaren av en telefonitjänst ska vara registrerad. I samband härmed har konstaterats att det i vissa sammanhang kan vara ändamålsenligt med ett krav på att registrera en faktisk brukare, när denne är någon annan än den slutbrukare som har ingått avtal med tillhandahållaren. Rättigheter som att säga upp eller ändra ett avtal tillkommer dock tillhandahållarens avtalspart, dvs. slutbrukaren. För operatörens del är det därför inte nödvändigt att någon annan är slutbrukaren är registrerad. Det har vidare angetts att det

skulle vara oproportionerligt krävande för såväl operatörerna som tillsynsmyndigheten att säkra att ett krav på registrering av en faktisk användare efterlevs. Ett krav på registrering av en faktisk brukare har därför inte ansetts ändamålsenligt eller proportionerligt och något förslag härom har inte lämnats (se Høring om endringer i ekomloven og ekomforskriften med forslag om lovhjemmel for leveringsplikt for bredbånd og tydeligere krav till entydig identifisering av sluttbrukere, september 2019, s. 28). Frågan bereds för närvarande inom det norska Regeringskansliet.

En lagreglering som innebär att det är den som använder en förbetald tjänst som också ska vara registrerad som abonnent av tjänsten skulle vara av stor nytta för brottsbekämpningen. Genom en sådan reglering skulle det i högre grad vara möjligt att säkerställa att de abonnemangsuppgifter som har registrerats kan kopplas till den verklige brukaren av en förbetald tjänst. På så sätt skulle de registrerade uppgifterna i större utsträckning kunna komma till nytta i det brottsbekämpande arbetet, vilket ju är det bakomliggande syftet till att en registreringsskyldighet alls föreslås. Visserligen lär det vara svårt för tillsynsmyndigheten, dvs. Post- och telestyrelsen, och mobiloperatörerna att kunna kontrollera om den registrerade abonnenten också är den som använder tjänsten. Enligt vår bedömning skulle dock en reglering i frågan ändå vara av värde. En regel som innebär att en ny registrering ska göras om en förbetald tjänst överlåts till någon annan skulle rimligen efterföljas av de allra flesta. För de kriminella skulle regleringen i vart fall innebära ett försvårande och skulle rimligen medföra att man känner sig kringskuren i sina möjligheter att överlåta kontantkort och tillhörande tjänster till någon annan. För det fall regleringen innehåller ett krav på att tillhandahållaren ska stänga av en förbetald tjänst som har överlåtits utan att någon ny registrering har gjorts, skulle denna effekt sannolikt bli större. Med en sådan reglering skulle det dessutom vara möjligt för en brottsbekämpande myndighet att vända sig till en operatör i de fall det t.ex. i en förundersökning har framkommit att en förbetald tjänst används av någon annan än den registrerade abonnenten, och med stöd av dessa uppgifter få tjänsten avstängd. Med hjälp av en sådan reglering skulle också förbetalda tjänster som har registrerats på en person i Sverige men används av okända i krigsområden utomlands, kunna tas ur bruk. Trots de svårigheter som det kommer att finnas med att kontrollera efter-

levnaden av en sådan reglering, har vi därför kommit till slutsatsen att det bör införas någon form av bestämmelser som innebär att en ny registrering ska ske om en förbetald och registrerad tjänst överlåts till någon annan.

Vid en överlåtelse ligger det närmast till hands att det är den nye innehavaren som bör se till att en ny registrering sker. Utgångspunkten är ju att det är den som använder den förbetalda tjänsten som ska vara registrerad. Men det bör också ligga i den registrerade abonnentens intresse att se till att en ny registrering äger rum vid en överlåtelse. Om det inte längre finns en koppling mellan tjänsten och den registrerade abonnenten, bör denne rimligen inte längre vilja stå som registrerad innehavare. Frågan är då om det bör införas någon form av reglering, rimligen straffsanktionerad, som ålägger nämnda personer någon anmälningsskyldighet då ett kontantkort överlåts. Vi tror inte att det är lämpligt. Det främsta skälet mot en sådan reglering är att den knappast kan bli särskild effektiv. Rent generellt är det också bra om lagstiftaren är restriktiv med straffbestämmelser för gärningar som närmast har karaktären av förseelser.

Om ingen ny registrering sker vid en överlåtelse av en förbetald tjänst, bör dock tillhandahållandet av tjänsten avbrytas. I 5 kap. 19 § LEK finns intaget bestämmelser som behandlar åtgärder vid utebliven betalning av bl.a. allmänt tillgängliga telefonitjänster. Enligt huvudregeln får ett tillhandahållande av en tjänst avbrytas först efter att abonnenten har uppmanats att betala inom viss skälig tid, med upplysning om att tillhandahållandet av tjänsten annars kan komma att avbrytas. Om en abonnent vid upprepade tillfällen har betalat för sent får tillhandahållandet avbrytas omedelbart. Den som tillhandahåller tjänsten ska i sådant fall genast underrätta abonnenten om avbrytandet och under en tid av lägst tio dagar från avbrytandet ge abonnenten möjlighet att ringa nödsamtal och andra avgiftsfria samtal. Regleringen i 5 kap. 19 §, som har sin grund i EU-rätten, är av konsumenträttslig karaktär och har till syfte att skydda konsumenten från att stå utan telefonitjänst vid en utebliven betalning. Den av oss föreslagna regleringen har dock ett annat syfte, nämligen att försvåra ett kringgående av den föreslagna registreringsskyldigheten. Regleringen har således ett brottsbekämpande syfte. Vi ser därför inte skäl att föreslå några bestämmelser liknande de som finns intagna i 5 kap. 19 §. Det kan i sammanhanget konstateras att den som har överlåtit sin förbetalda tjänst inte synes ha något behov av

att själv fortsätta använda den för sin telefoni. Regleringen bör således innebära att tillhandahållandet av en förbetald tjänst ska avbrytas om det framkommer att en överlåtelse av tjänsten har skett utan att en ny registrering gjorts. Som framgått ovan torde detta främst bli aktuellt när en brottsbekämpande myndighet har uppmärksammat operatören om att en överlåtelse torde ha ägt rum.

Regleringen bör dock innehålla vissa undantag. Det bör för det första vara möjligt att överlåta förbetalda tjänster till närstående utan att en ny abonnent behöver registreras. Således bör det vara möjligt för en abonnent att lämna vidare kontantkort till barn och andra familjemedlemmar utan att en ny registrering har skett. Det bör också vara möjligt för en juridisk person att låta personal och andra uppdragstagare använda förbetalda tjänster som har registrerats på den juridiska personen. En ny registrering ska inte heller behöva ske när en förbetald tjänst som har införskaffats på uppdrag av vissa myndigheter lämnas vidare till annan. Således bör kontantkort som har införskaffats på uppdrag av Försvarsmakten, Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som har till uppgift att ingripa mot brott, kunna lämnas vidare till informatörer och källdrivare utan att en ny registrering behöver ske. En ny registrering bör i övrigt ske i de fall ett kontantkort säljs vidare eller överlåts till annan på ett beständigt sätt. Regleringen bör dock inte hindra att förbetalda tjänster utnyttjas av någon annan än den registrerade abonnenten under ett kortare tag, t.ex. för att ringa något samtal. Således bör en journalist kunna låna ut ett kontantkort till en källa under ett kortare tag om det finns behov av det. I sådana fall handlar det i formell mening inte om någon överlåtelse.

Det finns i dag olika tjänster som en enskild enkelt kan använda för att spärra ett kontantkort som har förkommit. Vi har övervägt om det därutöver bör införas ett krav på att en enskild som har tappat bort eller på annat sätt blivit av med sitt kontantkort ska anmäla detta till operatören så att denne kan stänga av aktuella tjänster. Det finns fördelar med en sådan reglering. Vi har dock inte funnit att behovet är tillräckligt stort för att motivera ett sådant förslag.

Bör det införas något tak för hur många förbetalda tjänster det är tillåtet att registrera?

Bedömning: Det bör inte införas någon begränsning i det antal kontantkort eller förbetalda tjänster som en enskild får registrera.

Det har under utredningsarbetet framförts att det skulle kunna införas en begränsning i det antal kontantkort som får innehas eller registreras av en enskild. Syftet med en sådan reglering skulle vara att minska risken för att målvakter används för registreringen. En begränsning gällande hur många kontantkort som får innehas finns i Ungern och Turkiet. En liknande begränsning finns däremot inte i andra europeiska länder.

Det finns alltså i dag inte någon begränsning i Sverige av hur många kontantkort en fysisk eller juridisk person får köpa eller inneha. Ytterst är denna ordning ett uttryck för rätten att fritt ingå avtal och principen om äganderätt; att fritt äga och förfoga över sin egendom. En bestämmelse som innebär att en registrering av ett kontantkort ska vägras för det fall en person redan har ett visst antal kontantkort registrerade på sig, skulle medföra att en registrering inte kan ske trots att det skett ett civilrättsligt förvärv. Det innebär i sin tur en inskränkning i nyttjanderätten för köparen eftersom en registrering enligt vårt förslag är en förutsättning för att de tjänster som är kopplade till kontantkortet ska få användas. En begränsning av antalet kontantkort som en person får registrera aktualiserar därför frågor om det s.k. egendomsskyddet.

Skyddet för egendom är en grundlagsskyddad rättighet som finns intagen i 2 kap. 15 § RF, artikel 17 i EU:s rättighetsstadga och i artikel 1 i första tilläggsprotokollet till Europakonventionen. I den senare artikeln stadgas att varje fysisk eller juridisk person ska ha rätt till respekt för sin egendom. Ingen får berövas sin egendom annat än i det allmännas intresse och under de förutsättningar som anges i lag och i folkrättens allmänna grundsatser. En stat har dock rätt att genomföra sådan lagstiftning som staten finner nödvändig för att reglera nyttjandet av egendom i överensstämmelse med det allmännas intresse.

För att en inskränkning i nyttjanderätten ska få göras krävs alltså att det utförs en proportionalitetsbedömning där en avvägning ska ske mellan det allmännas intresse och det men som den enskilde kan

tänkas lida. En inskränkning måste dock anges i inhemsk lag, vara tillräckligt tydlig för att säkerställa rättssäkerhetskrav och göra äganderättsingrepp förutsebara. Ytterst är det Europadomstolen som avgör om ett intrång i äganderätten är försvarligt. När det gäller rätten att använda egendom har Europadomstolen funnit att även större inskränkningar i äganderätten kan accepteras i det allmännas intresse. Staten har med andra ord tillerkänts ett ganska stort utrymme för att bedöma vilka inskränkningar som ter sig rimliga med hänsyn till övergripande intressen (se Hans Danelius, Mänskliga rättigheter i europeisk praxis, 2015, s. 595 f.).

Enligt vår bedömning skulle en begränsning av det antal kontantkort eller förbetalda tjänster som får registreras av en enskild troligen inte innebära en kränkning av äganderätten. Det finns dock andra skäl som talar mot att en sådan begränsning bör införas. Ett tak för hur många kontantkort eller tjänster som får registreras av en viss fysisk eller juridisk person skulle t.ex. innebära att operatörerna var tvungna göra kontroller sinsemellan inför varje registrering. Visserligen skulle man kunna tänka sig en ordning där varje operatör endast får registrera ett visst antal förbetalda tjänster på en viss person och att en kontroll mot andra operatörer därmed inte skulle behöva göras. Ett system med en begränsning av antalet tjänster som får registreras skulle dock innebära ytterligare åligganden för mobiloperatörerna. Operatörernas arbete i denna fråga skulle också behöva kontrolleras. Det kan därutöver konstateras att det antal kontantkort eller förbetalda tjänster som en enskild skulle få rätt att registrera skulle behöva sättas ganska högt. En person kan nämligen ha behov av flera olika simkort till olika utrustningar och kanske också till sina barn. Det förekommer också att företag köper in en stor mängd kontantkort åt gången till sina anställda och därmed har behov av att ha ett stort antal förbetalda tjänster registrerade på sig. Det främsta argumentet mot ett tak för hur många kontantkort som får registreras är dock att en sådan ordning skulle kunna få motsatt effekt och i stället öka användningen av målvakter. Eftersom en målvakt skulle vara ”förbrukad” så snart denne registrerats för ett visst antal tjänster skulle de kriminella behöva sprida ut kontantkorten på fler personer. En sådan spridning skulle försvåra arbetet för de brottsbekämpande myndigheterna. En reglering som innebär att företag har rätt att registrera ett större antal tjänster än enskilda skulle troligen få till följd att företag används som målvakter i stället

för enskilda. En begränsning av det antal kontantkort eller förbetalda tjänster som en fysisk eller juridisk person får registrera behöver således inte innebära en fördel för det brottsbekämpande arbetet. Sammantaget är det vår uppfattning att det inte bör införas någon begränsning av antalet kontantkort eller förbetalda tjänster som en enskild får registrera.

Möjligheten att begränsa användandet av utländska kontantkort

Bedömning: Det bör inte införas någon reglering som begränsar möjligheten att använda utländska kontantkort.

I uppdraget ingår att undersöka möjligheten att begränsa användandet av oregistrerade kontantkort köpta utomlands. För att ett simkort som är knutet till en utländsk operatör ska kunna användas i Sverige krävs, som tidigare konstaterats, att den utländska operatören har ett roamingavtal med minst en svensk operatör. Med roaming menas alltså att en användare kopplar upp sig mot en utländsk operatörs nät vid användning av sin enhet utomlands. Som framgått ovan regleras roaming genom ett antal EU-förordningar, bl.a. den s.k. TSM-förordningen.

Huvudprincipen är att slutanvändare ska få roama i utländska operatörers mobilnät. Operatörerna skiljer därmed inte mellan slutanvändare som har ett registrerat eller oregistrerat simkort. Det är troligen inte heller möjligt för operatörerna att avgöra om någon som roamar i deras nät är kontantkortskund eller har ett kontraktsabonnemang i sitt hemland. En lagstiftning som begränsar möjligheterna för EU-medborgare från andra länder att utnyttja mobilnäten i Sverige skulle troligen innebära en sådan diskriminerande behandling som står i strid med EU-rätten. Någon motsvarande lagstiftning har inte heller införts i någon annan medlemsstat. Det synes därmed inte vara en framkomlig väg att i Sverige införa en reglering som begränsar roaming från utländska oregistrerade kontantkort. Vi föreslår inte någon sådan reglering.

Tillsyn och sanktioner

Bedömning: Regleringen om tillsyn i lagen om elektronisk kommunikation kan användas och är tillräcklig för att säkerställa att en registreringsskyldighet efterlevs.

Post- och telestyrelsen är tillsynsmyndighet enligt lagen om elektronisk kommunikation och har ett samlat ansvar inom området för elektronisk kommunikation. Myndighetens tillsyn omfattar efterlevnaden av lagen och de beslut om skyldigheter eller villkor samt de föreskrifter som har meddelats med stöd av lagen (7 kap. 1 § första stycket LEK).

För att kunna utöva en effektiv tillsyn har Post- och telestyrelsen en rad befogenheter. Enligt 7 kap. 2 § LEK har myndigheten rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, där verksamhet som omfattas av lagen om elektronisk kommunikation bedrivs. Myndigheten får också förelägga den som bedriver verksamhet som omfattas av lagen att tillhandahålla myndigheten de upplysningar och handlingar som behövs för kontrollen (7 kap. 3 §). Finner myndigheten skäl att misstänka att den som bedriver verksamhet som omfattas av lagen om elektronisk kommunikation inte efterlever lagen eller de föreskrifter som har meddelats med stöd av lagen, ska myndigheten underrätta den som bedriver verksamheten om detta förhållande och ge denne möjlighet att yttra sig (7 kap. 4 §). Post- och telestyrelsen får också meddela de förelägganden och förbud som behövs för att en rättelse av en överträdelse ska ske omedelbart eller inom skälig tid. Ett sådant föreläggande eller förbud får förenas med vite. Om föreläggandet inte följs, får Post- och telestyrelsen återkalla tillstånd, ändra tillståndsvillkor eller ytterst besluta att den som har åsidosatt en skyldighet helt eller delvis ska upphöra med verksamheten (7 kap. 5 §). Post- och telestyrelsens beslut enligt lagen eller enligt en föreskrift som har meddelats med stöd av lagen får överklagas hos allmän förvaltningsdomstol (8 kap. 19 §).

Post- och telestyrelsen har i andra sammanhang föreslagit att myndigheten ska få möjlighet att besluta om sanktionsavgifter för överträdelser av vissa bestämmelser i lagen om elektronisk kommunikation. I promemorian Genomförande av direktivet om inrättande av en kodex för elektronisk kommunikation, föreslås att

bestämmelserna om tillsyn i lagen om elektronisk kommunikation ska föras över till den nya lagen och i vissa delar utökas. Det föreslås också att Post- och telestyrelsen ska ha möjlighet att i vissa utpekade fall ta ut en sanktionsavgift. Förslagen bereds för närvarande i Regeringskansliet.

Eftersom registreringsskyldigheten enligt vårt förslag ska regleras i lagen om elektronisk kommunikation kommer Post- och telestyrelsen att ha tillsyn över efterlevnaden av de föreslagna bestämmelserna. Tillsynsområdet omfattar såväl operatörernas som återförsäljarnas agerande t.ex. i samband med en identitetskontroll. Det är vår bedömning att den tillsynsreglering som föreligger kan användas även för att säkerställa att registreringsskyldigheten efterlevs. Det kan dock finnas anledning att genomföra återkommande tillsynsinsatser för att tillse att registreringen och identifieringen genomförs på ett korrekt sätt.

De förslag som i andra sammanhang har lämnats om att Post- och telestyrelsen ska få möjlighet att meddela sanktionsavgift omfattar inte efterlevnaden av den av oss föreslagna registreringsskyldigheten. En möjlighet för tillsynsmyndigheten att ålägga operatörer och återförsäljare sanktionsavgift skulle dock kunna ge de inblandade aktörerna ekonomiska drivkrafter att efterleva regleringen. Beroende på hur tillsynsregleringen kommer att se ut framöver kan det därmed finnas anledning att överväga om möjligheterna att meddela sanktionsavgift bör omfatta även efterlevnaden av skyldigheten att registrera abonnemangsuppgifter avseende förbetalda tjänster och i samband därmed genomföra en identitetskontroll.

6 Verkställighetsfrågor

6.1 Inledning

Den andra delen av utredningsuppdraget avser vissa verkställighetsfrågor kopplade till de brottsbekämpande myndigheternas inhämtning av uppgifter på området för elektronisk kommunikation. Verkställighetsfrågorna kan sägas vara tre stycken. Den första avser reglerna om leverantörers skyldighet att anpassa sin verksamhet och medverka till att uppgifter lämnas ut till brottsbekämpande myndigheter så att de enkelt kan tas om hand. I uppdraget ingår att överväga om bestämmelser bör införas som medför att de utlämnade uppgifterna följer en gemensam standard. Syftet är att möjliggöra att de uppgifter som lämnas ut för brottsbekämpande ändamål ska kunna komma till avsedd användning på ett effektivt sätt. Den andra frågan gäller om nuvarande krav på skyndsamhet vid utlämnandena bör förtydligas och utvidgas till att omfatta fler uppgifter. Den tredje frågan handlar om rätten till ersättning för kostnader som uppstår vid utlämnande av uppgifter om elektronisk information till brottsbekämpande myndigheter. I uppdraget ingår att ta ställning till om reglerna om rätt till ersättning bör ändras och att föreslå nödvändiga författningsändringar. Samtliga ovannämnda frågor behandlas i detta avsnitt. Sist i avsnittet lämnar vi också ett förslag som innebär ett förtydligande av att abonnemangsuppgifter får lämnas ut för användning även i de brottsbekämpande myndigheternas underrättelseverksamhet. Det handlar alltså om ett förtydligande, inte någon ändring i sak.

6.2 Anpassningsskyldigheten

6.2.1 Gällande rätt

De leverantörer som enligt lagen (2003:389) om elektronisk kommunikation tillhandahåller allmänna kommunikationsnät eller elektroniska kommunikationstjänster (t.ex. den som tillhandahåller telefonabonnemang) spelar en viktig roll när brottsbekämpande myndigheter hämtar in uppgifter på området för elektronisk kommunikation. För att inhämtningen ska upprätthålla en rimlig effektivitet har leverantörerna ålagts vissa skyldigheter.

I 6 kap. 19 § första stycket LEK stadgas att verksamheten ska bedrivas så att beslut om hemlig avlyssning av elektronisk kommunikation (HAK) och hemlig övervakning av elektronisk kommunikation (HÖK) kan verkställas och så att verkställandet inte röjs. Enligt paragrafens andra stycke ska innehållet i och uppgifter om avlyssnade eller övervakade meddelanden göras tillgängliga så att informationen *enkelt kan tas om hand*. Denna s.k. anpassningsskyldighet infördes redan i den äldre telelagen (1993:597) och trädde i kraft i juli 1996. I fråga om den närmare innebörden av anpassningsskyldigheten angavs i förarbetena att den i praktiken innebär 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 tillgodose de krav som riktas mot dem. Vidare måste sådana personella och organisatoriska dispositioner vidtas som krävs för att hantera hjälpmedlen. Det angavs vidare att de begärda uppgifterna bör hållas tillgängliga inom viss tid, på visst sätt och på viss plats så att de enkelt kan tas om hand (se prop. 1995/96:180 s. 25 och 28).

Anpassningsskyldigheten gäller endast för vissa verksamheter, nämligen verksamheter som innefattar tillhandahållande av

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

2. tjänster inom ett allmänt kommunikationsnät vilka består av

a) en allmänt tillgänglig telefonitjänst till 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.

Regeringen eller den myndighet som regeringen bestämmer har enligt 6 kap. 19 § tredje stycket LEK rätt att meddela närmare föreskrifter i frågor som avses i första och andra styckena samt får i enskilda fall besluta om undantag från kravet i första stycket. Av 36 § förordningen (2003:396) om elektronisk kommunikation (FEK) framgår att Post- och telestyrelsen får, efter samråd med Åklagarmyndigheten, Polismyndigheten och Säkerhetspolisen, meddela de verkställighetsföreskrifter som behövs för HAK och HÖK enligt 6 kap. 19 § LEK. Post- och telestyrelsen får också i enskilda fall medge undantag från krav enligt 6 kap. 19 § första stycket. Sådana föreskrifter eller undantag har inte meddelats.

Lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (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. Det är en viss skillnad mellan bestämmelserna i 1 § inhämtningslagen och 27 kap. 19 § RB när det gäller tillstånd till hemlig övervakning av elektronisk kommunikation i realtid. Enligt inhämtningslagen får uppgifter hämtas in om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits. Lokaliseringsuppgifterna kan således hämtas in såväl i efterhand, och därmed avse historiska uppgifter, som i realtid. Inhämtningen av uppgifter om meddelanden (trafikuppgifter) får dock 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 hemlig övervakning av elektronisk kommunikation enligt 27 kap. 19 § RB. Det är vår uppfattning att uttrycket *hemlig övervakning av elektronisk kommunikation* i 6 kap. 19 § LEK rimligen måste 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.

Således är det vår uppfattning att anpassningsskyldigheten tar sikte även på fall när uppgifter om elektronisk kommunikation hämtas in med stöd av bestämmelserna i inhämtningslagen. Anpassningsskyldigheten gäller även i fråga om uppgifter som hämtas in efter beslut om HAK eller HÖK med stöd av lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen) eller lagen (1991:572) om särskild utlänningskontroll.

I promemorian Genomförande av direktivet om inrättande av en kodex för elektronisk kommunikation, föreslås bl.a. att tillsynsmyndigheten, alltså Post- och telestyrelsen, ska ha möjlighet att ta ut en sanktionsavgift av den som inte uppfyller kraven på att bedriva sin verksamhet så att beslut om HAK och HÖK kan verkställas i enlighet med en bestämmelse som motsvarar 6 kap. 19 § LEK eller föreskrifter som har meddelats med stöd av bestämmelsen. Enligt förslaget ska sanktionsavgifter också kunna tas ut av den som inte lämnar ut abonnemangsuppgifter enligt en bestämmelse som motsvarar 6 kap. 22 § LEK. Lagändringarna föreslås träda i kraft den 21 december 2020.

Det har ansetts nödvändigt med särskilda regler om anpassning för utlämnande i fråga om den som är skyldig att lagra trafikuppgifter 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 §). Enligt förarbetena innebär detta att de lagringsskyldiga måste se till att de brottsbekämpande myndigheterna utan ansträngning kan ta del av uppgifterna även om de skulle finnas i exempelvis krypterad eller komprimerad form hos den lagringsskyldige. Uppgifterna måste dock alltid överlämnas på ett sådant sätt att säkerheten och skyddet för uppgifterna inte eftersätts (se prop. 2010/11:46 s. 80 f.). Någon föreskriftsrätt för regeringen eller myndighet som regeringen bestämmer är inte kopplad till bestämmelsen i 6 kap. 16 f §.

För de situationer som uppkommer när uppgifter hämtas in av brottsbekämpande myndigheter med stöd av 6 kap. 22 § LEK finns inte någon särskild anpassningsskyldighet.

Av 27 kap. 25 § RB framgår att de brottsbekämpande myndigheterna får använda de tekniska hjälpmedel som behövs för att verkställa ett beslut om HAK eller HÖK. Regleringen har ansetts innebära en förpliktelse för leverantörer att i viss utsträckning med-

verka till att tvångsmedelsbeslutet kan verkställas (se prop. 1995/96:180 s. 22). I 9 § preventivlagen finns en motsvarande bestämmelse.

6.2.2 Problembeskrivning

Som tidigare framgått delas uppgifter om elektronisk kommunikation in i tre olika grupper; abonnemangsuppgifter, trafikuppgifter och lokaliseringsuppgifter. Var och en av de nämnda uppgiftskategorierna avser uppgifter av olika slag. Ett beslut om HÖK ger normalt upphov till uppgifter som kan brytas ned i mycket stora mängder data. Trafikuppgifter kan exempelvis inkludera uppgifter om typ av kommunikation, ett meddelandes ursprung och mål samt tid för kommunikationens början och slut liksom kommunikationens varaktighet. Trafikuppgifter kan även avse uppgifter som typ av sms och status på sms:et (t.ex. skickat, levererat eller avbruten leverans). Lokaliseringsuppgifter kan omfatta information om vilken cell (antenn på en basstation) som en viss utrustning har kopplat upp sig mot under en bestämd tidsperiod. Till kategorin lokaliseringsuppgifter hör även exempelvis information om geografiska koordinater för basstationens placering och om riktningen på den aktuella cellen.

Uppgifter om ett enstaka telefonsamtal kan avse en mängd uppgifter som kan vara relevanta för de brottsbekämpande myndigheterna. Det kan handla om exempelvis utrustningsidentitet, typ av tjänst och om den specifika tidpunkten för kontakten. Inhämtningen kan även omfatta information om exempelvis geografiska koordinater för den basstation som en mobiltelefon kopplar upp sig mot. Samtidigt krävs i normalfallet att uppgifter om ett mycket stort antal kommunikationstillfällen granskas och analyseras. Många gånger förekommer dessutom i samma ärende uppgifter som dels avser olika abonnemang och telefoner, dels kommer från olika leverantörer.

I de brottsbekämpande myndigheternas analysarbete ingår att söka efter mönster. Det kan handla om att utifrån spaningsuppslag eller andra underrättelser försöka ringa in vilka adresser (tidigare begrepp teleadresser) som har kommit till användning i ett visst moment under planeringsskedet av ett brott. Med utgångspunkt från en sådan analys kan ytterligare utredningsåtgärder vidtas för att

få fler ledtrådar i jakten på misstänkta. Det kan även handla om att analysera vilka basstationer som en viss utrustning med något slags regelbundenhet har kopplat upp sig mot under specifika tidsperioder. Analysarbetet kan syfta till att utreda ibland mycket komplexa relationer mellan olika adresser, telefoner och användare. Även mera lösryckta stycken av information kan utgöra viktiga pusselbitar vid analysen av en misstänkts kommunikation och andra förehavanden. Under förundersökningsstadiet kan uppgifter om elektronisk kommunikation användas t.ex. för att knyta en misstänkt till en viss plats eller till kommunikation som föregått ett brott.

Uppgifter om elektronisk kommunikation behandlas hos leverantörerna i olika datasystem, som varierar mellan leverantörerna. När uppgifter om elektronisk kommunikation hämtas in av brottsbekämpande myndigheter levereras de i det format som används av leverantören. Således får de brottsbekämpande myndigheterna tillgång till uppgifterna i skilda format beroende på vilken leverantör som tillhandahåller uppgifterna. Även sammanställningar från en och samma leverantör förekommer i olika format. De ingående uppgifternas inbördes ordning varierar beroende på vilken leverantör som innehar och sammanställer uppgifterna. Samma parametrar betecknas många gånger på olika sätt av olika leverantörer. Således saknar uppgiftssammanställningar från olika leverantörer en gemensam logik. Många gånger förutsätts att leverantören kan ge vägledning om innebörden av olika parametrar för att uppgifterna ska framgå. De listor som översänds kan inte heller alltid läsas maskinellt. De problem som anges avser främst uppgifter som hämtas in vid tillstånd till hemlig övervakning av elektronisk kommunikation enligt 27 kap. RB eller inhämtningslagen, men kan även avse abonnemangsuppgifter. Uppgifterna hämtas främst in från de fyra stora mobiloperatörer som också är nätägare. Abonnemangsuppgifter hämtas dock in från den mobiloperatör som ansvarar för aktuellt abonnemang.

För att informationen från leverantörerna ska kunna analyseras och användas för utredningsåtgärder krävs att informationen först bearbetas av de brottsbekämpande myndigheterna. Som läget är i dag kräver bearbetningsfasen en omfattande arbetsinsats. Bearbetningen behövs dels för att vissa värden ska göras begripliga, dels för att uppgifter från olika sammanställningar ska specificeras och ordnas enligt en gemensam standard. Först när uppgifterna på detta sätt har

ställts upp efter ett likvärdigt format är det möjligt att behandla informationen på ett effektivt sätt. Bearbetningen av uppgifterna tar i dagsläget ofta längre tid än själva analysarbetet.

Som exempel kan nämnas terrordådet på Drottninggatan i april 2017. Med anledning av dådet fick polisen tillgång till 1 551 excelfiler från de fyra största mobiloperatörerna. Innehållet bestod av drygt 2,3 miljoner rader med uppgifter om bl.a. telefonnummer och basstationer. Mobiloperatörerna lämnade sina samtalslistor i olika format. En mobiloperatör lämnade samma typ av lista i 50 olika format. Polisens arbete med att bearbeta filerna uppgick till cirka 500 arbetstimmar. Följden blev att analysarbetet blev kraftigt försenat. (Se Intern polisrapport: Det tog fem veckor för polisen att göra mobilanalyser, Dagens nyheter, 2017-12-26.)

Avsaknaden av en gemensam standard för de uppgifter som lämnas ut från leverantörerna medför alltså att tid och resurser måste läggas ned på att bearbeta uppgifterna. Arbetet är många gånger utdraget och krävande. Trots detta utgör bearbetningen inte någon garanti för att det eftersträvade resultatet kan uppnås. Många gånger ger bearbetningen upphov till felaktigheter som upptäcks först i analysfasen. Avsaknaden av en gemensam standard påverkar alltså även tillförlitligheten av de uppgifter som ingår i analysen. Tid och resurser går åt till att på nytt bearbeta uppgifter som har visat sig vara felaktiga. I vissa fall upptäcks felaktigheter i de lämnade uppgifterna först i ett skede när det på grund av lagringstiderna är för sent att inhämta kompletterande uppgifter.

6.2.3 Uppdraget

I vår uppdragsbeskrivning anges att en förklaring till de problem som föreligger avseende formatet på inhämtade uppgifter är att det inte i alla avseenden finns någon gemensam uppfattning om hur aktuella regler ska tillämpas. Det anges att den nuvarande ordningen kan vara en följd av hur bestämmelserna i 6 kap. 16 f och 19 §§ LEK är utformade. Bestämmelserna anges vara svåra att tolka och det kan i vissa situationer vara oklart hur reglerna förhåller sig till varandra. Det anges vidare att det kan vara svårt att avgöra om en fråga ska hänföras till anpassningsskyldigheten eller om den snarare ska bedömas i ljuset av den skyldighet att medverka som följer av 27 kap.

25 § RB eller allmänna principer. Även regeringens och Post- och telestyrelsens rätt att meddela föreskrifter på området har ansetts vara mindre klar. Det finns även fall när uppgifter om elektronisk information hämtas in av brottsbekämpande myndigheter utan att reglerna i 6 kap. 16 f eller 19 § LEK är tillämpliga, såsom när abonnemangsuppgifter hämtas in med stöd av 6 kap. 22 § LEK. När det gäller sådana situationer föreskrivs över huvud taget inte någon anpassningsskyldighet.

I uppdragsbeskrivningen anges att leverantörernas skyldighet att på olika sätt medverka vid verkställighet av beslut på området för elektronisk kommunikation behöver förtydligas. Det ligger därför i vårt uppdrag att se över och eventuellt förtydliga reglerna om leverantörers skyldighet att medverka och verksamhetsanpassa för att möjliggöra att utlämnade uppgifter enkelt kan tas om hand. Vi ska överväga om regler bör införas som möjliggör att inhämtade uppgifter följer en gemensam standard. Det anges att även de brottsbekämpande myndigheternas rutiner för att hämta in uppgifter bör analyseras och att vid behov bör förändringar av dessa övervägas.

6.2.4 Frågans tidigare behandling

I samband med att anpassningsskyldigheten infördes i dåvarande telelagen diskuterades om det borde fastställas standardiserade normer som ska gälla för samtliga operatörer som omfattas av kravet på anpassning. Regeringen uttalade då att detta knappast låter sig göras i praktiken. Enligt regeringen kan en operatör med ett mycket stort antal abonnenter 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 ansågs vara 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 anvis-

ningar om vad som bör krävas av varje operatör ansågs inte behöva anges direkt i lag eller annan författning. I stället ansågs att Post- och telestyrelsen 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 angavs att det i första hand bör ankomma på de brottsbekämpande myndigheterna och operatörerna att komma överens om vad som behöver göras. (Se prop. 1995/96:180 s. 28 f.).

Beredningen för rättsväsendets utveckling föreslog i sitt delbetänkande Tillgång till elektronisk kommunikation i brottsutredningar m.m. (SOU 2005:38) att anpassningsskyldigheten i 6 kap. 19 § LEK skulle utvidgas till att omfatta verksamheter som avser ett allmänt tillhandahållande av ett elektroniskt kommunikationsnät eller tjänster inom ett sådant nät. 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 (se SOU 2005:38 s. 272 ff.). 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 (se a.a. s. 339 ff.). Förslagen har inte lett till lagstiftning.

6.2.5 Pågående arbeten

I september 2018 anmälde Polismyndigheten de fyra största mobiloperatörerna till Post- och telestyrelsen för underlåtenhet att lämna historiska trafik- och lokaliseringsuppgifter på ett sådant sätt att de

enkelt kan tas om hand. Enligt Polismyndigheten stod mobiloperatörernas agerande i strid med anpassningsskyldigheten enligt 6 kap. 19 § LEK. I anledning av hemställan inledde Post- och telestyrelsen en tillsyn av de aktuella leverantörernas förfaranden. Under våren 2019 bjöd regeringen in Polismyndigheten, Säkerhetspolisen, Tullverket, Post- och telestyrelsen, branschorganisationen IT&Telekomföretagen och berörda mobiloperatörer till samtal om hur de problem som finns när det gäller utlämnandet av uppgifter från leverantörer till brottsbekämpande myndigheter bäst kan lösas. Vid mötet behandlades frågan om former för utlämnande av uppgifter. Närvarande aktörer var positiva till att inleda samtal och uttryckte en vilja att arbeta tillsammans för att lösa gemensamma problem.

Ett projekt som syftar till att standardisera de format som används vid utlämnande av uppgifter om elektronisk kommunikation från leverantörer till brottsbekämpande myndigheter pågår för närvarande. Polismyndigheten är sammankallande i projektet som kallas för FiLT (Formaterad Inhämtning Leverans Teleoperatörer). I projektet deltar Polismyndigheten, Säkerhetspolisen och Tullverket. Referensdeltagare är Post- och telestyrelsen samt de fyra största mobiloperatörerna. Projektet arbetar för att utlämnandet av historiska uppgifter om elektronisk kommunikation ska ske i ett gemensamt format. Förhoppningen är att de operatörer som omfattas av projektet ska kunna börja leverera i ett enhetligt format från sommaren 2020. Med anledning av det pågående projektet har Post- och telestyrelsen skrivit av tillsynsärendena mot de angivna mobiloperatörerna.

Inom FiLT-projektet används standarder som har tagits fram av ETSI – European Telecommunications Standards Institute – som är ett oberoende europeiskt standardiseringsorgan för telekommunikation i Europa. Förutom brottsbekämpande myndigheter är bl.a. tele- och internetoperatörer samt tillverkare och regulatoriska myndigheter medlemmar i organet. Standarderna i ETSI tas fram i samarbete mellan alla intressenter och förändras över tid när nya tekniker och kommunikationssätt utvecklas. Gällande inhämtning och överföring av uppgifter från och till brottsbekämpande myndigheter finns särskilda standarder framtagna. ETSI-formatet används redan i dag i Sverige vid utlämnande av realtidsuppgifter från leverantörerna till de brottsbekämpande myndigheterna.

Polismyndigheten driver också ett eget projekt kallat HTM-projektet (där HTM står för hemliga tvångsmedel). Projektet syftar till att utveckla Polismyndighetens förmåga och att skapa bättre förutsättningar för en effektiv och rättssäker hantering av hemliga tvångsmedel. Inom Polismyndigheten ska det införas sju regionala kontaktpunkter (kallade SPOC som står för single point of contact) som ska användas vid inhämtning av historiska uppgifter om elektronisk kommunikation. Även den Nationella operativa avdelningen, NOA, ska ha en sådan särskild kontaktpunkt. För realtidsuppgifter finns redan en särskild kontaktpunkt vid NOA, som gäller gemensamt för Polismyndigheten, Tullverket, Säkerhetspolisen och Ekobrottsmyndigheten. Syftet med särskilda kontaktpunkter är att enskilda poliser ska vända sig till sin regionala kontaktpunkt i de fall det finns frågor kring inhämtningen av historiska uppgifter om elektronisk kommunikation från leverantörerna. Endast kontaktpunkterna kommer i sin tur att stå i kontakt med leverantörerna. Tanken är att denna ordning ska förenkla samarbetet mellan de brottsbekämpande myndigheterna och leverantörerna.

Polismyndigheten arbetar också med att ta fram nya IT-verktyg och rutiner kring hur beställningen av historiska uppgifter om elektronisk kommunikation ska hämtas in. Samma formulär ska gälla även för inhämtning av abonnemangsuppgifter. Tanken är att frågor ska ställas i samma format som leverantörerna svarar i. Samma formulär ska också användas av alla brottsbekämpande myndigheter. Projektet förväntas vara klart i slutet av 2020 eller i början av 2021. En del regioner har redan börjat använda sig av en särskild funktion för hanteringen av hemliga tvångsmedel.

6.2.6 Överväganden och förslag

Anpassningsskyldighetens omfattning

Bedömning: Innebörden av 6 kap. 19 § första stycket LEK är oklar. Ett förtydligande av bestämmelsen vore önskvärt. Frågan är dock komplex och bör lämpligen utredas i ett större sammanhang.

Anpassningsskyldigheten i 6 kap. 19 § LEK innebär alltså att en leverantör ska bedriva verksamheten så att beslut om HAK och HÖK kan verkställas och så att verkställandet inte röjs. Dessutom ska innehållet i och uppgifter om avlyssnade eller övervakade meddelanden göras tillgängliga så att informationen enkelt kan tas om hand. Bestämmelserna om anpassningsskyldighet är i praktiken ofta en förutsättning för att beslut om HÖK och HAK över huvud taget ska kunna verkställas och att verkställandet kan ske i nära anslutning till tvångsmedelsbeslutet. När anpassningsskyldigheten infördes i den äldre telelagen uttalade regeringen att HAK och HÖK är betydelsefulla och oumbärliga hjälpmedel i kampen mot särskilt den grova brottsligheten och att det av effektivitetsskäl är ytterst angeläget att möjligheterna till verkställighet av tvångsmedlen på området upprätthålls (se prop. 1995/96: 180 s. 17 f.).

Enligt telelagen omfattade skyldigheten att anpassa sin verksamhet de leverantörer som hade fått tillstånd att inom ett allmänt tillgängligt telenät tillhandahålla telefonitjänst till fast nätanslutningspunkt, mobil teletjänst eller nätkapacitet, om verksamheten ansågs vara betydande. För en sådan leverantör omfattade skyldigheten enbart den tillståndsgivna verksamheten och inte annan verksamhet som den leverantören eventuellt bedrev (se a. prop. s. 26).

Lagen om elektronisk kommunikation utgår från en anmälningsplikt och inte en tillståndsplikt för leverantörerna avseende viss verksamhet. I samband med att telelagen upphörde att gälla förändrades även utformningen av den aktuella bestämmelsen om vilka verksamheter som omfattas av anpassningsskyldigheten.

Anpassningskravet omfattar enligt 6 kap. 19 § första stycket LEK de verksamheter som avser tillhandahållande av

- ett allmänt kommunikationsnät som inte enbart är avsett för utsändning till allmänheten av program som avses i 1 kap. 2 § YGL, eller
- tjänster inom ett allmänt kommunikationsnät vilka består av

– en allmänt tillgänglig telefonitjänst till 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

– en allmänt tillgänglig elektronisk kommunikationstjänst till mobil nätanslutningspunkt.

I 6 kap. 19 § första stycket LEK finns alltså angivet vilka verksamheter som omfattas av anpassningsskyldigheten. En del av de begrepp som används i bestämmelsen definieras i andra bestämmelser i lagen om elektronisk kommunikation. Vissa av definitionerna har ändrats sedan lagen infördes utan att det har föranlett någon ändring i 6 kap. 19 §. Med *allmänt kommunikationsnät* avses i dag ett elektroniskt kommunikationsnät som helt eller huvudsakligen används för att tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster och som stödjer informationsöverföring mellan nätanslutningspunkter. Med *elektronisk kommunikationstjänst* avses en tjänst som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät.

Anpassningsskyldigheten gäller fullt ut för de leverantörer som bedriver sådan verksamhet som omfattas av 6 kap. 19 § LEK. Skulle skyldigheterna bli allt för betungande framför allt när det gäller ekonomiska aspekter, kan den enskilde leverantören begära undantag hos Post- och telestyrelsen från kravet på anpassning. Det har såvitt bekant aldrig skett.

Utredningen om elektronisk kommunikation, som hade i uppgift att föreslå ny lagstiftning inom området, föreslog att anpassningsskyldigheten skulle omfatta dem som tillhandahåller allmänna telefonnät eller allmänt tillgängliga telefonitjänster (se SOU 2002:60 s. 505). I betänkandet uttalades att reglerna i telelagen angående hemlig teleavlyssning och hemlig teleövervakning skulle överföras till den nya lagen. Någon saklig ändring i förhållande till vad som gällde enligt telelagen var således inte avsedd. Enligt regeringens bedömning innebar emellertid utredningens förslag 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 ansågs det med hänsyn till den något ändrade terminologin i den nya lagen behöva klargöras att beträffande telefonitjänst till fast nätanslutningspunkt innefattar detta 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. (Se prop. 2002/03:110 s. 267 ff.)

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 omfatta fler och ej heller färre verksamheter än vad som omfattades enligt dåvarande regler. (Se a prop. s. 269.)

Beredningen för rättsväsendets utveckling angav i sitt tidigare nämnda delbetänkande att anpassningsskyldigheten i 6 kap. 19 § LEK är begränsad så till vida att den inte omfattar samtliga de verksamheter där sådana meddelanden som omfattas av tvångsmedlen befordras eller, om man så vill, samtliga de tekniker som är aktuella. Trots att den legala möjligheten finns att avlyssna eller övervaka ett visst meddelande enligt rättegångsbalken, medför avsaknaden av anpassningsskyldighet för vissa verksamheter stora effektivitetsförluster vid utredning av grova brott, eftersom tvångsmedelsbesluten med stor sannolikhet inte kan verkställas över huvud taget (se SOU 2005:38 s. 279). Utredningen föreslog att anpassningsskyldigheten skulle omfatta verksamheter som avser ett allmänt tillhandahållande av ett sådant elektroniskt kommunikationsnät som avses i 27 kap. RB eller tjänster inom ett sådant nät. Ett elektroniskt kommunikationsnät föreslogs samtidigt, enligt en ny bestämmelse i

27 kap. RB, avse detsamma som i lagen om elektronisk kommunikation med undantag för nät som enbart är avsett för utsändning av program i ljudradio eller television. Användandet av rekvisitet allmänt i 6 kap. 19 § LEK ansågs utesluta verksamheter som avser tillhandahållande av sådana nät eller tjänster som inte står till förfogande för användning av allmänheten och som samtidigt inte heller effektivt konkurrerar med sådan verksamhet. Företag, bostadsrättsföreningar eller andra sammanslutningar som internt tillhandahåller vissa tjänster skulle därmed generellt sett inte vara anpassningsskyldiga, även om beslut om tvångsmedel kan omfatta meddelanden som befordras i deras nät. I betänkandet angavs att den utvidgning av anpassningsskyldigheten som i praktiken skulle följa av förslagen skulle medföra att anpassningskravet också skulle omfatta verksamhet som avser tillhandahållande av internettjänster. Förslagen skulle också innebära att anpassningsskyldigheten i de fasta telenäten inte skulle vara begränsad till en viss lägsta datahastighet för funktionell tillgång till internet (se a.a. s. 278 ff. och 451). Som tidigare framgått har förslagen inte lett till lagstiftning.

Bestämmelserna i 6 kap. 19 § LEK ändrades språkligt i samband med att begreppen hemlig teleavlyssning och hemlig teleövervakning ersattes av begreppen HAK och HÖK. Någon ändring i sak var dock inte avsedd (se prop. 2011/12:55 s. 63 f. och 143).

Bestämmelserna i rättegångsbalken 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 faller under tvångsmedelsregleringen. Tillstånd till HAK och HÖK knöts tidigare först till viss fysisk teleanläggning och senare till viss teleadress, varmed avsågs ett abonnemang, en enskild anknytning, en kod eller adressen för elektronisk post. Även andra tillförlitliga identifieringar av telemeddelanden som den tekniska utvecklingen ger möjlighet till omfattades av begreppet (se prop. 1994/95:227 s. 21 och 31). Begreppet teleadress har därefter ersatts med enbart adress utan att någon förändring i sak har varit avsedd (se prop. 2011/12:55 s. 61 f.).

Hemlig avlyssning och övervakning 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 kommunikationssynpunkt (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 är sådana nät som är uppkopplade mot och används för kommunikation via allmänt tillgängliga kommunikationsnät eller större företagsnät och fristående datorer som via andra nätverk kommunicerar med varandra eller med t.ex. elektroniska anslagstavlor, informationsdatabaser eller andra informationssystem (se prop. 1994/95:227 s. 27 och 31).

Skyldigheten att lagra trafikuppgifter gäller för samtliga de leverantörer som är anmälningspliktiga enligt 2 kap. 1 § LEK. I den bestämmelsen anges att allmänna kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning eller allmänt tillgängliga elektroniska kommunikationstjänster endast får tillhandahållas efter anmälan till tillsynsmyndigheten (Post- och telestyrelsen). Av 2 kap. 2 § samma lag framgår att någon anmälan inte behöver göras för verksamheter som enbart består i att överföra signaler via tråd för utsändning till allmänheten av program som avses i 1 kap. 2 § YGL samt att Post- och telestyrelsen får meddela föreskrifter om ytterligare undantag från anmälningsplikten. Undantaget för verksamhet som består i trådsändningar som omfattas av grundlagsskyddet i yttrandefrihetsgrundlagen har sin grund i att vissa av de krav som lagen om elektronisk kommunikation ställer för bedrivande av anmälningspliktig verksamhet annars skulle komma i konflikt med etableringsfriheten i 3 kap. 1 § YGL för sådan sändningsverksamhet (se prop. 2010/11:46 s. 43). Lagringsskyldigheten omfattar i dag fler leverantörer än de som är anpassningsskyldiga enligt 6 kap. 19 § LEK (se a. prop. s. 50). 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 har framförts att internetoperatörer som inte tillhandahåller telefonitjänster kan omfattas av lagringsskyldigheten enligt 6 kap. 16 a § utan att omfattas av anpassningsskyldigheten i 6 kap. 19 §.

Som tidigare framgått har regeringen i promemorian Genomförande av direktivet om inrättande av en kodex för elektronisk kommunikation, lämnat förslag till en ny lag som ska ersätta den nuvarande lagen om elektronisk kommunikation. Den nya lagen ska bl.a. genomföra EU:s direktiv om inrättande av en kodex för elektronisk kommunikation. Enligt lagförslaget ska definitionen av elektronisk kommunikationstjänst vara vidare än i dag och bl.a. omfatta en s.k. *interpersonell kommunikationstjänst*. En sådan tjänst definieras i förslaget som en tjänst som vanligen tillhandahålls mot ersättning och som möjliggör 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. En tjänst som möjliggör interpersonell och interaktiv kommunikation enbart som en extrafunktion av mindre betydelse som är direkt kopplad till en annan tjänst omfattas dock inte. Som definitionen är utformad finns det inget krav på att interpersonella kommunikationstjänster helt eller huvudsakligen ska utgöras av överföring av signaler. Det innebär att vissa tjänster som tidigare inte har ansetts vara elektroniska kommunikationstjänster i fortsättningen kommer att vara det. Definitionen omfattar tjänster som traditionella röstsamtal mellan två fysiska personer, men även e-posttjänster, meddelandetjänster och gruppchattar. En interpersonell kommunikationstjänst kan vara nummeroberoende, dvs. inte använda nummer i nationella eller internationella nummerplaner och inte heller möjliggöra kommunikation med nummer i nationella eller internationella nummerplaner. En nummeroberoende interpersonell kommunikationstjänst använder andra identifierare än allmänt tilldelade nummerresurser, t.ex. användarnamn (se promemorian Genomförande av direktivet om inrättande av en kodex för elektronisk kommunikation, s. 421 ff.). Som exempel på nummeroberoende interpersonella kommunikationstjänster kan nämnas Whatsapp, Messenger och Viber.

I promemorian föreslås att bestämmelserna om anpassningsskyldighet i 6 kap. 19 § LEK förs över till den nya lagen. Eftersom

den nya definitionen av elektroniska kommunikationstjänster kommer att omfatta nummeroberoende interpersonella kommunikationstjänster, kommer också anpassningsskyldigheten enligt den nya lagen att omfatta de som tillhandahåller sådana tjänster. Dessa tillhandahållare kommer också att omfattas av uppgiftsskyldigheten enligt nuvarande 6 kap. 22 § LEK. Nummeroberoende interpersonella kommunikationstjänster omfattas dock enligt förslaget inte av anmälningsplikten enligt lagen och därmed inte av lagringsskyldigheten enligt nuvarande 6 kap. 16 a § LEK. I promemorian anges att riksdagen, i samband med att de nya reglerna om datalagring vid brottsbekämpning antogs, har tillkännagivit 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. Enligt promemorian finns det mot denna bakgrund skäl att framöver överväga ändringar i regleringarna om hemliga tvångsmedel och datalagring, t.ex. i fråga om nummeroberoende interpersonella kommunikationstjänster (se a.a. s. 332).

Det kan konstateras att bestämmelserna om anpassningsskyldighetens omfattning i 6 kap. 19 § första stycket LEK är ålderdomliga. Som har påpekats från olika håll under vårt utredningsarbete finns det goda skäl att förenkla regleringen. Den teknikutveckling som pågått länge och som fortfarande pågår innebär att olika typer av kommunikationstjänster flyter ihop och att det blir allt svårare att urskilja en specifik tjänst. Det har framförts att det bör utredas närmare vilka kommunikationstjänster som bör omfattas av anpassningsskyldigheten. Det har också framförts att anpassningsskyldigheten bör utvidgas till att omfatta ett allmänt tillhandahållande av elektroniska kommunikationsnät eller kommunikationstjänster. Mot bakgrund av den snabba tekniska utvecklingen vore det lämpligt att anpassningsskyldighetens omfattning regleras på ett så teknikneutralt sätt som möjligt, dvs. utan att viss typ av överföringsteknik anges i författningstexten. Lämpligen skulle bestämmelserna om anpassningsskyldighet i 6 kap. 19 § första stycket och lagringsskyldighet enligt 6 kap. 16 a § kunna utformas så att de träffar samma aktörer. Regelverket på området för elektronisk kommunikation är dock komplicerat och kräver en fördjupad analys som på grund av vår uppdragsbeskrivning inte kan göras inom ramen för denna utredning. Våra förslag får t.ex. inte innebära någon ändring när det

gäller vilka uppgifter som de brottsbekämpande myndigheterna får hämta in. Det är dock i praktiken ofta så att det är anpassningsskyldighetens omfattning som, tillsammans med lagringsskyldigheten, avgör vilka uppgifter om elektronisk kommunikation som kan hämtas in. Vi föreslår därför ingen ändring av 6 kap. 19 § första stycket LEK. Frågan om anpassningsskyldighetens omfattning bör dock lämpligen behandlas i ett annat sammanhang.

Vi har inte för avsikt att genom våra förslag förhindra den teknikutveckling som sker på området. Vi vill inte heller stå i vägen för de ökade krav på anpassning och möjligheter till inhämtning av uppgifter om elektronisk kommunikation som kan bli en följd av den nya kodexen om elektronisk kommunikation. Vi kommer i det följande att utforma våra förslag på anpassningsbestämmelser så att de inkluderar även sådana uppgifter om elektronisk kommunikation som framöver kan komma att hämtas in från nummeroberoende interpersonella kommunikationstjänster.

Gemensamma format

Förslag: Det ska i 6 kap. 19 § andra stycket LEK föreskrivas att när uppgifter som avses i 20 § första stycket lämnas ut för brottsbekämpning till Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som har till uppgift att ingripa mot brott, ska uppgifterna ordnas och göras tillgängliga i ett format som gör det möjligt att enkelt ta hand om dem. Regleringen ska gälla även vid utlämnande av lokaliseringsuppgifter som inte är trafikuppgifter.

Den särskilda regleringen om format i 6 kap. 16 f § för lagrade uppgifter ska upphävas.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela närmare föreskrifter om format. Post- och telestyrelsen ska i förordning bemyndigas att meddela föreskrifter om format.

Det ska i förordning regleras att leverantörerna och de brottsbekämpande myndigheterna gemensamt ska verka för att informationsöverföringen sker i gemensamma format på ett enhetligt sätt.

Inhämtning av historiska trafik- och lokaliseringsuppgifter och uppgifter om abonnemang utgör en stor och viktig del i de brottsbekämpande myndigheternas utrednings- och underrättelsearbete. Det är därför problematiskt att de uppgifter som lämnas ut från leverantörerna inte följer en gemensam standard. Problematiken gäller när historiska uppgifter hämtas in genom beslut om HAK eller HÖK med stöd av bestämmelserna i 27 kap. RB, preventivlagen, lagen om särskild utlänningskontroll eller inhämtningslagen, men kan också avse abonnemangsuppgifter som hämtas in enligt 6 kap. 22 § första stycket 2 LEK. Problemen är inte endast kopplade till sådana uppgifter som lagras hos leverantörerna med stöd av 6 kap. 16 a § LEK. Även uppgifter som leverantörerna lagrar för andra ändamål än brottsbekämpning omfattas således av problematiken. Realtidsuppgifter lämnas dock ut i ett gemensamt ETSI-format.

Att leverantörerna för sin egen behandling använder sig av olika format är i sig inte något konstigt då behandlingen sker hos olika oberoende aktörer. Avsaknaden av en gemensam standard för de uppgifter som lämnas ut till brottsbekämpande myndigheter medför dock att myndigheterna behöver lägga ner tid och resurser på att bearbeta de inhämtade uppgifterna. I värsta fall kan den fördröjning som bearbetningen innebär medföra att avgörande utredningsåtgärder inte kan genomföras eller att ett förestående brott inte kan utredas eller förhindras. Vidare innebär avsaknaden av en gemensam standard att tillförlitligheten av de uppgifter som ingår i en analys påverkas, vilket naturligtvis är allvarligt. Det är därför glädjande att de fyra största mobiloperatörerna och de brottsbekämpande myndigheterna har åtagit sig att verka för att utlämnandet av uppgifter om elektronisk information sker i gemensamma format. Enhetliga format för utlämnande även av historiska uppgifter och abonnemangsuppgifter skulle innebära stora fördelar för de brottsbekämpande myndigheterna vad gäller möjligheter att bearbeta informationen snabbt, korrekt och på ett kostnadseffektivt sätt. En användning av enhetliga format skulle enligt vår bedömning också effektivisera och underlätta arbetet för leverantörerna. Således kan ett system med gemensamma format för de uppgifterna som lämnas ut innebära fördelar för samtliga inblandade.

Med hänsyn till det pågående FiLT-projektet kan det finnas anledning att avvakta och se om frågan om gemensamma format kan lösas mellan brottsbekämpande myndigheter och leverantörer på

frivillig väg. Det förhållandet att det pågår ett projekt om gemensamma format innebär dock inte att det saknas skäl att införa förtydligande lagstiftning. Som påpekats av de brottsbekämpande myndigheterna är ett system som bygger på frivillighet känsligt för förändringar. Intresset av att samarbeta i frågan kan minska över tid. Även för leverantörerna kan det i sådana fall vara en fördel med klara regler som anger vilka skyldigheter som finns gentemot de brottsbekämpande myndigheterna. Med hänsyn härtill och till frågans stora betydelse för effektiviteten i det brottsbekämpande arbetet är det därför befogat att i detta läge förtydliga regelverket om leverantörernas skyldigheter att medverka vid utlämnandet av uppgifter om elektronisk kommunikation till brottsbekämpande myndigheter.

Som framgått ovan saknas närmare reglering om i vilket format uppgifter ska överföras från leverantörer till brottsbekämpande myndigheter. I 6 kap. 19 § andra stycket LEK anges visserligen att innehållet i och uppgifter om avlyssnade eller övervakade meddelanden ska göras tillgängliga så att informationen enkelt kan tas om hand. Ett liknande krav finns i 6 kap. 16 f § för lagrade uppgifter. Kravet innebär dock främst att leverantörerna i sin verksamhet ska använda sig av tekniska hjälpmedel som har vissa egenskaper och att de brottsbekämpande myndigheterna ska kunna ta del av uppgifter även om de hos en leverantör finns i exempelvis komprimerad eller krypterad form. Av bestämmelserna framgår inte att de uppgifter som görs tillgängliga direkt ska vara möjliga att använda av brottsbekämpande myndigheter i ett analysarbete. För abonnemangsuppgifter som inte omfattas av lagringsskyldigheten föreligger inte någon anpassningsskyldighet. För att komma till rätta med problemen med att ostrukturerade uppgifter lämnas i olika format bör det därför i lag införas ett krav på att de uppgifter som lämnas ut från leverantörerna till brottsbekämpande myndigheter ska ordnas och göras tillgängliga i ett format som gör det möjligt att enkelt ta hand om dem. Härmed blir det tydligt att uppgifter som lämnas ut inte enbart ska göras tillgängliga på ett sådant sätt att de är läsbara. Uppgifterna ska även vara sammanställda på ett sådant strukturerat sätt att de utan ytterligare bearbetning hos mottagarna kan komma till användning i det brottsbekämpande arbetet. Regleringen bör omfatta såväl innehållet i och uppgifter om avlyssnade och övervakade meddelanden samt uppgifter om abonnemang. Regleringen bör även omfatta sådana lokaliseringsuppgifter som inte är trafik-

uppgifter. Någon skillnad bör inte göras mellan uppgifter som hos leverantörerna lagras för brottsbekämpande ändamål eller för leverantörernas egna ändamål. Det bör inte heller göras någon skillnad beroende på vilket lagstöd som finns för utlämnandet. Således bör bestämmelsen omfatta utlämnanden som sker efter beslut om HAK eller HÖK som har sin grund i 27 kap. RB, inhämtningslagen, preventivlagen eller lagen om särskild utlänningskontroll. Även abonnemangsuppgifter som lämnas ut till brottsbekämpande myndigheter med stöd av 6 kap. 22 § första stycket 2 LEK bör omfattas.

Den föreslagna regleringen skulle kunna föras in i 27 kap. 25 § RB där det framgår att de brottsbekämpande myndigheterna får använda de tekniska hjälpmedel som behövs för att verkställa beslut om HAK eller HÖK. Regleringen har i tidigare lagstiftningsärenden ansetts innefatta en förpliktelse för leverantörer att i viss utsträckning medverka till att tvångsmedelsbeslutet kan verkställas (se prop. 1995/96:180 s. 22).

Enligt vår mening vore det dock mer ändamålsenligt att placera bestämmelsen tillsammans med övriga anpassningsfrågor i lagen om elektronisk kommunikation. Härmed blir det tydligare att regleringen omfattar även uppgifter som lämnas ut med stöd av bestämmelser i inhämtningslagen och 6 kap. 22 § första stycket 2 LEK. Enligt vår mening bör den nya regleringen föras in i 6 kap. 19 § andra stycket LEK där formerna för utlämnandet regleras i dag. Bestämmelsen ska läsas fristående från första stycket. Vi har övervägt att ta in regleringen i en ny paragraf för att tydliggöra att innebörden av den inte ska tolkas mot bakgrund av den snävare regleringen i 6 kap. 19 § första stycket. Vi har dock stannat för att inte föreslå en ny paragraf.

Den omständigheten att anpassningsskyldigheten ska gälla för uppgifter som lämnas ut *för brottsbekämpning* kommer rimligen att innebära att även uppgifter som lämnas ut för andra syften än brottsbekämpning till Polismyndigheten enligt 6 kap. 22 § första stycket LEK kommer att vara anpassade i fråga om format.

Eftersom den föreslagna regleringen omfattar alla slags uppgifter som lämnas ut från leverantörer till brottsbekämpande myndigheter för brottsbekämpning blir det inte nödvändigt med en särskild reglering för uppgifter som lagras med stöd av 6 kap. 16 a §. Vi återkommer nedan till betydelsen av att reglerna tas in i 6 kap. 19 §.

I dagsläget används inte HAK och HÖK för att hämta in uppgifter om elektronisk kommunikation från nummeroberoende interpersonella kommunikationstjänster. Den främsta anledningen till det är att lagen om elektronisk kommunikation inte anses tillämplig för dem som tillhandahåller sådana tjänster. Inte heller abonnemangsuppgifter avseende sådana tjänster hämtas in från de aktörerna med stöd av regleringen i 6 kap. 22 § LEK. Det är oklart huruvida brottsbekämpande myndigheter framöver kommer att hämta in uppgifter från nummeroberoende interpersonella kommunikationstjänster med stöd av beslut om HAK eller HÖK eller 6 kap. 22 § första stycket 2 LEK. Om de som tillhandahåller nummeroberoende interpersonella kommunikationstjänster framöver kommer att lämna ut uppgifter enligt här aktuellt regelverk kommer den föreslagna bestämmelsen om anpassningsskyldighet att träffa dem.

Det grundläggande kravet på leverantörerna att ordna och lämna ut uppgifter i ett format som gör det möjligt att enkelt ta hand om dem bör alltså framgå av lag. För att markera att frågan om vilka format som ska användas lämpligen löses gemensamt av de brottsbekämpande myndigheterna och berörda leverantörer bör det i förordningen om elektronisk kommunikation tas in en bestämmelse som anger att parterna gemensamt ska verka för att informationsöverföringen sker i gemensamma format på ett enhetligt sätt. Det bör dock på området också finnas en möjlighet att meddela närmare föreskrifter. Post- och telestyrelsen är tillsynsmyndighet enligt lagen om elektronisk kommunikation och har ett samlat ansvar inom området för elektronisk kommunikation. Myndigheten kan därför säkerställa att hänsyn tas till såväl leverantörernas som de brottsbekämpande myndigheternas intressen i formatfrågan. Post- och telestyrelsen har också goda förutsättningar att utreda effekterna på integritet för användare och kostnader för leverantörerna beroende på vilka tekniska krav som kan ställas. Det får således anses lämpligare att föreskriftsrätten anförtros Post- och telestyrelsen än t.ex. Polismyndigheten.

Det är viktigt att en ny reglering inte medför orimliga ekonomiska och administrativa konsekvenser för leverantörerna. Eventuella föreskrifter kan därför komma att behöva innehålla en möjlighet att ge undantag för mindre aktörer.

Den särskilda regleringen för lagrade uppgifter

Förslag: Den särskilda regleringen i 6 kap. 16 f § LEK för lagrade uppgifter ska upphävas.

Den föreslagna regleringen om anpassningsskyldighet i 6 kap. 19 § andra stycket LEK omfattar även den anpassningsskyldighet för lagrade uppgifter som i dag föreskrivs i 6 kap. 16 f § LEK. Den sistnämnda föreskriften bör därför, såvitt den avser krav på anpassning, nu upphävas. Vi återkommer senare till föreskrifterna om skyndsamhet och ersättning, där det i dag finns särskilda bestämmelser för lagrade uppgifter i 6 kap. 16 e och 16 f §§. Vi kommer att föreslå att även dessa frågor ska omfattas av en samlad reglering som tas in i 6 kap. 19 §.

6 kap. 16 f § kan i dag sägas omfatta tre krav, nämligen *att* uppgifter ska lämnas ut utan dröjsmål, *att* uppgifterna ska göra tillgängliga på ett sådant sätt att informationen enkelt kan tas om hand samt *att* verkställandet av utlämnandet inte röjs. De två förstnämnda frågorna ska enligt våra förslag regleras i 6 kap. 19 § andra stycket LEK. När det gäller den tredje frågan följer redan av 6 kap. 20 § att leverantörerna har en straffsanktionerad tystnadsplikt avseende innehållet i och uppgifter om avlyssnade eller övervakade meddelanden och abonnemangsuppgifter. Tystnadsplikten gäller visserligen inte i förhållande till bl.a. den som har tagit del i utväxlingen av ett meddelande. Dock följer av 6 kap. 21 § att leverantörerna har tystnadsplikt när det gäller uppgifter som hänför sig till angelägenhet som avser användning av hemlig avlyssning och övervakning av elektronisk kommunikation. Regleringen hänför sig till uppgifter som hämtas in med stöd av bestämmelserna i 27 kap. 18 eller 19 § RB och omfattar därmed även inhämtanden som har sin grund i preventivlagen och lagen om särskild utlänningskontroll. Regleringen omfattar också uppgifter som hämtas in med stöd av inhämtningslagen och gäller även en begäran om utlämnande av abonnemangsuppgifter enligt 6 kap. 22 § första stycket 2 LEK. Regleringen i 6 kap. 21 § innebär bl.a. att leverantören inte får informera en abonnent om att brottsbekämpande myndigheter hämtar in uppgifter om denne (se prop. 2011/12:55 s. 114 f.). Det är vår uppfattning att regleringen om tystnadsplikt i 6 kap. 20 och 21 §§ innebär att verkställandet av ett utlämnande inte får röjas.

Bestämmelser som överlappar varandra bör undvikas. På grund härav bör de särskilda bestämmelserna om lagrade uppgifter i 6 kap. 16 f § upphävas. Som redogörs för nedan bör även 6 kap. 16 e § upphävas.

De brottsbekämpande myndigheternas rutiner

Bedömning: De brottsbekämpande myndigheterna bör fortsätta sitt arbete med att begränsa antalet kontaktpunkter och att skapa enhetliga rutiner för inhämtande av uppgifter om elektronisk kommunikation.

Av de brottsbekämpande myndigheterna är Polismyndigheten den som hämtar in flest uppgifter om elektronisk kommunikation. För realtidsuppgifter sker inhämtningen via en gemensam kontaktpunkt, som delas av Polismyndigheten, Säkerhetspolisen, Tullverket och Ekobrottsmyndigheten. Denna sambandsfunktion är placerad vid NOA och har hand om alla kontakter med leverantörerna när det gäller inhämtning av elektronisk information i realtid.

För historiska uppgifter sker inhämtningen via varje myndighet för sig. Hos Polismyndigheten sker inhämtningen genom utredare och handläggare runtom i landet. Vissa regioner har ett mer centraliserat sätt att hämta in uppgifter, medan andra har det inte. Abonnemangsuppgifter kan i dagsläget begäras in av varje utredare och handläggare för sig. Det finns formulär för inhämtningen, men de används inte i alla fall. Säkerhetspolisen har en gemensam kontaktpunkt ut mot leverantörerna i samtliga frågor. Även Tullverket har en gemensam kontaktpunkt mot leverantörerna för inhämtning av historiska uppgifter. Abonnemangsuppgifter hämtas dock in av enskilda handläggare i verksamheten. Vid Ekobrottsmyndigheten hanteras inhämtningen av historiska uppgifter av ett tiotal operativa analytiker. Vid inhämtningen används det formulär som har fastställts av Polismyndigheten.

Förfrågningar från många olika handläggare hos de brottsbekämpande myndigheterna kan vara svåra att hantera för leverantörerna. För leverantörerna råder en straffbelagd tystnadsplikt som endast kan brytas under de förhållanden som är reglerade i lag. Således är det av stor vikt att uppgifter endast lämnas ut till en behörig person.

För leverantörerna kan det också vara betungande när förfrågningar inkommer på olika sätt och i olika format.

Som framgått ovan har Polismyndigheten ett pågående projekt, HTM-projektet, som syftar till att inhämtningen av uppgifter om elektronisk kommunikation ska ske på ett mer enhetligt och effektivt sätt. Arbete pågår med att införa regionala kontaktpunkter som ska sköta alla kontakter med leverantörerna vid inhämtningen av historiska uppgifter och abonnemangsuppgifter. Polismyndigheten arbetar också med att ta fram nya IT-verktyg och rutiner kring hur beställningen av historiska uppgifter och abonnemangsuppgifter ska gå till.

Det kan konstateras att såväl leverantörerna som de brottsbekämpande myndigheterna skulle gynnas av mer standardiserade beställningssystem. Enhetligt utformade beställningar som sker i ett gemensamt format kan antas leda till effektivare och snabbare utlämnanden. För det fall enhetliga rutiner används blir det också tydligare för leverantörerna att en beställning kommer från en behörig användare. Behörighetsfrågan skulle också underlättas om antalet kontaktpunkter vid de brottsbekämpande myndigheterna begränsades. Det är därför angeläget att Polismyndigheten och övriga brottsbekämpande myndigheter fortsätter sitt förändringsarbete i dessa frågor.

6.3 Skyndsamheten

6.3.1 Gällande rätt

Samtliga leverantörer som är lagringsskyldiga enligt 6 kap. 16 a § LEK ska enligt 6 kap. 16 f § bedriva sin verksamhet så att uppgifterna kan lämnas ut till brottsbekämpande myndigheter *utan dröjsmål*. Detta skyndsamhetskrav grundas på att det hos de brottsbekämpande myndigheterna i vissa situationer kan finnas ett akut behov av att få tillgång till uppgifterna. Utgångspunkten är att en leverantörs arbete med att överföra information med anledning av en begäran som inkommer under kontorstid ska inledas inom mycket kort tid. Leverantören förutsätts behöva arbeta med verkställigheten även utanför kontorstid. En överföring ska ske så snart någon uppgift finns tillgänglig. Det kan innebära att överföringar sker successivt så snart uppgifterna blir tillgängliga hos leverantören. Hur snabbt ett utläm-

nande ska ske i det enskilda fallet får avgöras av de brottsbekämpande myndigheterna och leverantörerna i varje situation. (Se prop. 2010/11:46 s. 51 och 80.)

Ett uttryckligt skyndsamhetskrav gäller endast uppgifter som omfattas av lagringsskyldigheten enligt 6 kap. 16 a § LEK. Som tidigare framgått anges i 6 kap. 19 § att innehållet i och uppgifter om avlyssnade eller övervakade meddelanden ska göras tillgängliga så att informationen enkelt kan tas om hand. I förarbetena till bestämmelsen uttalas att innehållet i telemeddelanden måste göras tillgängligt samtidigt som det förmedlas eller i vart fall omedelbart i anslutning till att det förmedlas (se prop. 1995/96:180 s. 27).

Post- och telestyrelsen har i anledning av en anmälan av Polismyndigheten gjort vissa uttalanden om med vilken grad av skyndsamhet uppgifter bör lämnas ut till följd av anpassningskravet i 6 kap. 19 § LEK. I beslut den 12 september 2017 (dnr 16-2818), som gällde Polismyndighetens möjligheter att i realtid få tillgång till lokaliseringsuppgifter för att utreda brott, anges att syftet med anpassningskravet inte kan anses vara uppfyllt om verkställighet följer efter ett långt dröjsmål. Enligt Post- och telestyrelsen krävs att verkställighet kan ske inom en viss tid som inte är så utdragen att ändamålet med det aktuella rättsmedlet riskerar att bli mer eller mindre verkningslöst, för att anpassningskravet ska anses vara uppfyllt. En beredskap som innebär att utlämnande endast kan ske under kontorstid är inte tillräcklig. Enligt Post- och telestyrelsen innebär en ändamålsenlig beredskap för verkställighet av beslut om HÖK enligt 6 kap. 19 § att verksamheten ska bedrivas så att ett påbörjande av verkställighet kan ske även efter kontorstid och att uppgifterna härefter lämnas ut så snart dessa finns tillgängliga för ett utlämnande.

6.3.2 Problembeskrivning

I förundersökningar om grov brottslighet uppstår inte sällan situationer som kräver snabba åtgärder. I takt med att den tekniska utvecklingen har gått framåt har de brottsbekämpande myndigheternas behov av att snabbt få tillgång till uppgifter om elektronisk kommunikation ökat. I 27 kap. 21 a § RB har det därför förts in en möjlighet för åklagare att meddela interimistiskt beslut om HAK eller HÖK, om det kan befaras att det skulle medföra en fördröjning

av väsentlig betydelse för utredningen att invänta rättens tillstånd. Möjligheten att besluta interimistiskt får endast användas i situationer där ändamålet med åtgärden riskerar att gå förlorat om rättens tillstånd skulle avvaktas, t.ex. om en misstänkt person som är föremål för hemlig avlyssning använder sig av ett telefonnummer som inte omfattas av rättens tillstånd vid en tidpunkt där det inte är möjligt att få till stånd ett domstolsbeslut (exempelvis på natten eller helgen). För att bl.a. kunna meddela sådana beslut finns det jouråklagare som bedriver verksamhet dygnet runt. Således kan beslut om HAK och HÖK fattas dygnet runt och under årets alla dagar. För att de brottsbekämpande myndigheterna ska få tillgång till de uppgifter som omfattas av besluten krävs dock först att dessa verkställs av leverantörerna.

Det har under vårt arbete framkommit att beslut om HAK och HÖK inte alltid kan verkställas under kvällar och helger eftersom leverantörerna inte har nödvändig beredskap för detta. Post- och telestyrelsen har, förutom det ovan nämnda tillsynsärendet, under en längre tid haft pågående tillsynsärenden mot två mobiloperatörer gällande skyndsamheten vid utlämnande av lokaliseringsuppgifter i realtid. Ärendena har skrivits av i mars 2020 sedan operatörerna infört organisatoriska möjligheter att påbörja verkställandet av beslut om HAK eller HÖK dygnet runt, årets alla dagar. Numera har de fyra största mobiloperatörerna möjlighet att verkställa beslut om HAK och HÖK avseende i vart fall realtidsuppgifter även utanför kontorstid. Dessa operatörer är bemannade dygnet runt. Under nätter och helger lämnas dock normalt inte historiska uppgifter eller abonnemangsuppgifter ut.

Inom kontorstid synes samtliga stora mobiloperatörer lämna ut realtidsuppgifter med nödvändig skyndsamhet, i vart fall samma dag som frågan inkommer. För historiska uppgifter och abonnemangsuppgifter förekommer det dock stora variationer mellan leverantörerna vad gäller tidsutdräkten. Historiska HÖK-uppgifter lämnas, enligt de uppgifter vi har fått del av, normalt inom någon till några dagar. Uppgifter hänförliga till ett efterfrågat geografiskt avgränsat område, som endast kan tas fram av personal med särskild kompetens, lämnas dock ut efter längre tid. När det gäller abonnemangsuppgifter kan tidsutdräkten vara längre. För någon leverantör kan det dröja mer än en vecka innan en abonnemangsuppgift lämnas ut. De brottsbekämpande myndigheterna har dock behov av att kunna

få tillgång till även historiska uppgifter och abonnemangsuppgifter snabbt. Sådana uppgifter kan vara nödvändiga för att det ska gå att säkerställa vem som är brukare av ett telefonnummer och som därmed bör omfattas av ett beslut om HAK eller HÖK. Således är uppgifter om abonnemang och andra historiska uppgifter ofta en förutsättning för att beslut om avlyssning eller övervakning i realtid ska kunna fattas. Utan tillgång till dessa uppgifter fördröjs alltså möjligheten att utverka beslut om de hemliga tvångsmedlen. Även för att snabbt kunna dra slutsatser av inhämtade uppgifter kan det vara nödvändigt att få tillgång till abonnemangsuppgifter. För att kunna tyda en telefonlista kan det t.ex. vara nödvändigt att få veta vem det är som har blivit uppringd. Sådana uppgifter kan exempelvis vara nödvändiga för att snabbt finna en misstänkt vid pågående brottslighet.

Möjligheten att snabbt få tillgång till uppgifter om elektronisk kommunikation kan variera beroende på vilken relation som har byggts upp mellan anställda hos de brottsbekämpande myndigheterna och leverantörerna. Det finns dock olika tillfällen när beslut om hemliga tvångsmedel inte har kunnat verkställas eller utverkas eftersom leverantörerna inte är tillgängliga eller inte erbjuder de tjänster som efterfrågas inom rimlig tid. Eftersom verkställigheten inte har kunnat genomföras eller avsevärt har fördröjts, har åtgärden inte heller lett till något resultat i det enskilda ärendet.

6.3.3 Uppdraget

I uppdragsbeskrivningen anges att det är otillfredsställande att möjligheterna för de brottsbekämpande myndigheterna att i brådskande fall hämta in uppgifter kan vara beroende av hur den enskilde leverantören har valt att organisera nödvändig beredskap. I uppdraget ingår därför att överväga om skyndsamhetskravet i 6 kap. 16 f § LEK behöver förtydligas. Vi ska även överväga ett uttryckligt skyndsamhetskrav även i fall som inte omfattas av regleringen i den nämnda paragrafen, t.ex. när inhämtningen sker i realtid och när inhämtningen avser abonnemangsuppgifter. Vi ska också överväga om regeringens föreskriftsrätt bör utvidgas.

6.3.4 Frågans tidigare behandling

Som tidigare framkommit föreslog Beredningen för rättsväsendets utveckling i sitt delbetänkande Tillgång till elektronisk kommunikation i brottsutredningar m.m. (SOU 2005:38) bl.a. att det i 27 kap. 25 § RB skulle föras in en bestämmelse som anger att en enskild (operatör) är skyldig att genast på begäran av en brottsutredande myndighet medverka vid verkställighet av beslut om avlyssning eller övervakning. I betänkandet diskuterades om det borde införas en tidsgräns för medverkan, alltså för den tid inom vilken operatören har att medverka genom att påbörja verkställighetsåtgärderna. Enligt utredningen skulle en skälig tidsgräns för samtliga operatörer kunna vara en timme från polisens begäran om medverkan under kontorstid (kl. 8-17). Det angavs vara i högsta grad rimligt att de operatörer som har personella resurser avdelade för drift- och nätövervakning även under annan tid, har samma tidsmässiga krav på sig att medverka även under den tiden. Eftersom förhållandena hos operatörerna ansågs variera så mycket fann dock utredningen att det i vart fall för tillfället inte borde införas någon generell gräns för medverkan. Det ansågs i stället tillräckligt att begreppet ”genast” användes i lagtexten, bl.a. för att markera att det som huvudregel inte får röra sig om mer än någon timmes väntetid för de brottsutredande myndigheterna (se SOU 2005:38 s. 339 ff.) Som tidigare framkommit har lagförslagen inte lett till lagstiftning.

6.3.5 Överväganden och förslag

Förslag: Det ska i 6 kap. 19 § andra stycket LEK föreskrivas att uppgifter som avses i 20 § första stycket utan dröjsmål ska lämnas ut för brottsbekämpning till Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som har till uppgift att ingripa mot brott. Regleringen ska gälla även vid utlämnande av lokaliseringsuppgifter som inte är trafikuppgifter.

Den särskilda regleringen för lagrade uppgifter i 6 kap. 16 f § ska upphävas.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela närmare föreskrifter om utlämnande av uppgifter utan dröjsmål. Post- och telestyrelsen ska i förordning bemyn-

digas att meddela föreskrifter om utlämnande av uppgifter utan dröjsmål.

Som tidigare har konstaterats kan det i det brottsbekämpande arbetet uppstå beaktansvärda behov av att använda hemliga tvångsmedel med mycket kort varsel. En snabb verkställighet kan i vissa fall vara absolut nödvändig för att skydda allmänheten eller föra en brådskande utredning framåt. Behovet av snabba beslut har påverkats av den utveckling som skett inom teknik och kommunikation. De förbättrade kommunikationsmöjligheterna innebär att planer kan ändras med kort varsel och att de misstänkta snabbt och ofta kan byta telefonnummer eller annan adress. Även abonnemangsuppgifter måste ibland hämtas in skyndsamt, inte minst för att inhämtningen av andra uppgifter ska kunna uppfylla sitt avsedda ändamål. Det kan i många fall vara nödvändigt att få kännedom om vem som är innehavare av ett visst abonnemang innan tillstånd till en begäran om hemligt tvångsmedel mot denna person kan inhämtas.

En snabb verkställighet är inte endast av vikt för inhemska intressen utan även för det internationella samarbetet, som inte sällan rör internationell grov organiserad brottslighet. Krav på en snabb verkställighet finns t.ex. i lagen (2017:1000) om en europeisk utredningsorder. Av 3 kap. 23 § andra stycket framgår att en verkställighet i ett brådskande ärende, som kan avse hemlig avlyssning eller övervakning av elektronisk kommunikation, om möjligt ska ske inom 24 timmar efter det att en verkställbarhetsförklaring har meddelats. Det är av stor vikt att Sverige kan erbjuda snabb rättslig hjälp till ansökande stater om svenska brottsbekämpande myndigheter ska kunna förvänta sig detsamma när de ansöker om rättslig hjälp i andra stater.

Det har framkommit att de brottsbekämpande myndigheternas behov av att snabbt få tillgång till eftersökta uppgifter inte alltid tillgodoses. Under senare tid har visserligen förändringar gjorts som innebär att samtliga fyra stora mobiloperatörer har möjlighet att lämna ut realtidsuppgifter även under nätter och helger. Det förekommer dock alltjämt att brottsbekämpande myndigheter kan behöva vänta längre tider innan de får tillgång till historiska uppgifter och till abonnemangsuppgifter. I vissa fall kan skyndsamma utlämnandefrågor lösas efter personliga kontakter mellan personal hos brottsbekämpande myndigheter och leverantörer. Det

kan dock konstateras att ett system som bygger på personkännedom är sårbart. Möjligheten för de brottsbekämpande myndigheterna att snabbt få tillgång till uppgifter om elektronisk kommunikation bör inte vara beroende av vem som begär ut uppgifterna.

Ett problem i sammanhanget är de krav på säkerhet m.m. som innebär att endast personer med speciell utbildning och behörighet får ombesörja utlämnandefrågorna hos leverantörerna. Strängare krav på skyndsamhet innebär att fler personer behöver hantera känsliga uppgifter med höjda kostnader som följd. Dessa frågor diskuterades även vid införandet av skyndsamhetskravet i 16 kap. 16 f § LEK. Regeringen anförde då att det finns intressen som talar i olika riktningar. Å ena sidan kan det hos de brottsbekämpande myndigheterna i vissa situationer finnas ett akut behov av att få tillgång till trafikuppgifter och å andra sidan innebär en ständig beredskap hos leverantörerna ökade kostnader och i vissa fall även ökade säkerhetsrisker. Enligt regeringens mening vägde dock brottsbekämpningsintresset i denna fråga mycket tungt (se prop. 2010/11:46 s. 51). Denna bedömning gör sig enligt vår mening alltjämt gällande. För att utlämnandena ska kunna ske med tillbörlig skyndsamhet är det därför nödvändigt att leverantörerna anpassar sin verksamhet så att begärda uppgifter kan lämnas ut med tillbörlig skyndsamhet.

De problem med sena verkställigheter som alltjämt föreligger talar för att det finns behov av att förtydliga och utöka regleringen gällande med vilken grad av skyndsamhet uppgifter om elektronisk kommunikation ska lämnas ut till brottsbekämpande myndigheter. Det kan konstateras att det i skyndsamhetsfrågan saknas skäl att göra någon skillnad mellan uppgifter som lagras för brottsbekämpande ändamål eller för leverantörernas egna ändamål. Det står också klart att en reglering i skyndsamhetsfrågan bör omfatta alla slags uppgifter som lämnas ut till de brottsbekämpande myndigheterna för brottsbekämpning. Regleringen bör alltså vara densamma oavsett om de uppgifter som ska lämnas ut avser realtidsuppgifter, historiska trafik- och lokaliseringsuppgifter eller abonnemangsuppgifter. Det bör inte heller göras någon skillnad beroende på vilket lagstöd som finns för utlämnandet. Ett skyndsamhetskrav bör således träffa samma slags uppgifter som omfattas av den föreslagna regleringen i formatfrågan, se föregående avsnitt.

Frågan om det bör införas en särskild tidsgräns för utlämnande av uppgifter som hämtas in efter beslut om HAK eller HÖK har tidigare diskuterats. Beredningen för rättsväsendets utveckling fann att en skälig tidsgräns för samtliga operatörer skulle kunna vara en timme från polisens begäran om medverkan, såväl inom som utom kontorstid. Eftersom förhållandena ansågs variera så mycket hos operatörerna stannade dock utredningen vid att det var tillräckligt att begreppet *genast* användes i lagtexten, bl.a. för att markera att det som huvudregel inte får röra sig om mer än någon timmes väntetid för de brottsutredande myndigheterna (se SOU 2005:38 s. 339 ff.). Vi delar utredningens bedömning och skälen härför att någon generell tidsgräns för medverkan inte bör införas i lag. Enligt vårt förslag bör regleringen omfatta även abonnemangsuppgifter, som kan hämtas in vid misstanke om all slags brottslighet. Det kan inte i alla situationer anses vara nödvändigt att de uppgifterna lämnas ut inom en så pass kort tidsram. Samma krav på skyndsamhet kan alltså inte anses föreligga i alla situationer. Vidare bör regleringen lämna visst utrymme för leverantörerna att göra egna prioriteringar, bl.a. beroende på hur många förfrågningar som de har att behandla vid samma tidpunkt. Vidare bör det beaktas att regleringen kommer att träffa aktörer av olika storlek som har olika stora möjligheter att snabbt efterkomma en begäran om utlämnande. Behovet av snabb verkställighet bör därför lämpligen markeras på annat sätt.

Enligt 23 kap. 4 § RB ska en förundersökning bedrivas så skyndsamt som omständigheterna medger. Vid användandet av personella tvångsåtgärder är det särskilt viktigt att förundersökningen bedrivs skyndsamt (jfr 24 kap. 12 och 18 §§ RB). För att de brottsbekämpande myndigheterna ska kunna leva upp till rättegångsbalkens krav är det nödvändigt att även leverantörerna tillhandahåller elektronisk kommunikation med motsvarande brådska. Kravet på leverantörerna skulle med hänsyn härtill kunna utformas som att uppgifterna ska lämnas ut *skyndsamt*.

Den nuvarande regleringen för lagrade uppgifter i 6 kap. 16 a–f §§ LEK har sin grund i det s.k. datalagringsdirektivet[1]. I direktivet anges att uppgifterna ska lagras på ett sådant sätt att de tillsammans med annan nödvändig information *utan dröjsmål* kan överföras till

[1] 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.

behöriga myndigheter när de begär det. Rekvisitet utan dröjsmål används av det skälet i 6 kap. 16 f § för att ange med vilken grad av skyndsamhet lagrade uppgifter ska lämnas ut. Rekvisitet fångar enligt vår mening väl den grad av skyndsamhet som är befogad vid utlämnandet av uppgifter till de brottsbekämpande myndigheterna. Det är lämpligt att samma rekvisit används för utlämnande av alla sorters uppgifter från leverantörerna till de brottsbekämpande myndigheterna. Rekvisitet utan dröjsmål bör därför användas för att beteckna graden av skyndsamhet vid utlämnandena.

Regleringen kan med fördel föras in i 6 kap. 19 § andra stycket LEK, där formerna för utlämnandet av uppgifter till brottsbekämpande myndigheter regleras. Eftersom den föreslagna bestämmelsen omfattar alla slags uppgifter som lämnas ut från leverantörer till brottsbekämpande myndigheter för brottsbekämpning blir det inte nödvändigt med en särskild reglering för utlämnande av uppgifter som lagras med stöd av 6 kap. 16 a §. För att undvika överlappande bestämmelser bör därför den särskilda regleringen för lagrade uppgifter i 6 kap. 16 f § upphävas. Vi har i föregående avsnitt behandlat betydelsen och följderna av att reglerna tas in i 6 kap. 19 §.

Begreppet utan dröjsmål bör tolkas mot bakgrund av hur stort behovet av skyndsamhet är och förutsättningarna för ett snabbt utlämnande i det enskilda fallet. Det är främst de tekniska förutsättningarna som bör avgöra hur snabbt ett utlämnande kan ske, men även andra faktorer kan beaktas. Ett visst mått av utrymme för prioriteringar bör inrymmas i begreppet. Utgångspunkten bör dock vara att behandlingen av en begäran som inkommer under kontorstid ska inledas inom mycket kort tid, dvs. samma dag. Större leverantörer förutsätts ha de tekniska och administrativa förutsättningarna för att påbörja en verkställighet dygnet runt, årets alla dagar (jfr Post- och telestyrelsens beslut den 12 september 2017 i dnr 16-2818, den 19 mars 2020 i dnr 18-3920 och den 20 mars 2020 i dnr 18-3923). Om behovet av skyndsamhet är stort bör verkställigheten således kunna påbörjas av dessa aktörer inom mycket kort tid även under kvällar och helger. De begärda uppgifterna ska härefter lämnas ut så snart de finns tillgängliga för ett utlämnande.

Post- och telestyrelsen bör ha en föreskriftsrätt när det gäller kravet på utlämnande av uppgifter utan dröjsmål. Det kan nämligen framöver komma att visa sig att en viss detaljreglering behövs, t.ex.

gällande någon viss inhämtningssituation. En sådan detaljreglering bör inte tas in i lag, men kan föras in på myndighetsnivå.

De gemensamma standarder och format som är på väg att införas kommer förhoppningsvis att förenkla arbetet och medföra att uppgifter kommer att kunna lämnas ut från leverantörerna snabbare. För det fall även de brottsbekämpande myndigheternas beställningar standardiseras och frågor ställs i samma format som svar ska erhållas i kommer troligen också processen att skyndas på. Det kan också vara lämpligt att de brottsbekämpande myndigheterna tydligt anger i vilka fall det finns behov av snabbt svar eller inte. På så sätt blir det enklare för leverantörerna att prioritera bland förfrågningarna och efterkomma dessa.

6.4 Ersättning för utlämnade uppgifter

6.4.1 Gällande rätt

Den nuvarande modellen för kostnadsfördelning mellan det allmänna och leverantörerna innebär att leverantörerna ska stå för kostnaderna för anpassning, drift och underhåll. Leverantörerna ska i sin tur ersättas av de brottsbekämpande myndigheterna för de kostnader som hänför sig till utlämnande av uppgifter i enskilda ärenden. (Se t.ex. prop. 1995/96:180 s. 30 f. och prop. 2010/11:46 s. 65 f.)

I 6 kap. 16 e § LEK stadgas att den som är lagringsskyldig enligt 6 kap. 16 a § har rätt till ersättning för kostnader som uppstår när lagrade uppgifter lämnas ut. Ersättningen ska betalas av den myndighet som har begärt uppgifterna. Enligt bestämmelsen har regeringen eller den myndighet som regeringen bestämmer rätt att meddela föreskrifter om ersättningen. Utgångspunkten är att leverantörerna ska få sina kostnader för att lämna ut trafikuppgifter i enskilda ärenden ersatta. Tanken är inte att ersättning ska utgå för varje utlämnad uppgift utan att ersättning ska betalas för varje begäran, alltså först när de uppgifter som hänför sig till en viss begäran har lämnats ut (se prop. 2010/11:46 s. 69 och 80).

Post- och telestyrelsen får, efter att ha hört Polismyndigheten, Säkerhetspolisen och Tullverket, meddela föreskrifter om ersättningen enligt 6 kap. 16 e § LEK (46 § FEK). Med stöd av detta bemyndigande har Post- och telestyrelsen meddelat föreskrifter

(Post- och telestyrelsens föreskrifter, 2013:5, om ersättning vid utlämnande av lagrade uppgifter för brottsbekämpande ändamål).

Det är således Post- och telestyrelsen som bestämmer ersättningens storlek när det gäller utlämnande av sådana uppgifter som omfattas av lagringsskyldigheten. De ersättningsnivåer som anges i föreskrifterna är baserade på uträkningar avseende den genomsnittliga tidsåtgång som varje begäran om utlämnande genererar hos leverantörerna. I föreskrifterna görs skillnad mellan utlämnanden av olika slags uppgifter och mellan utlämnanden som sker under eller efter kontorstid. För utlämnande av lagrade uppgifter hänförliga till ett efterfrågat geografiskt avgränsat område, som endast kan ske efter beredning av personal med särskild kompetens, ske ersättning utgå med 525 kr under kontorstid och 790 kr utanför kontorstid. För övriga utlämnanden av lagrade uppgifter uppgår ersättningen under kontorstid till 150 kr och utanför kontorstid till 170 kr. När kostnaderna för ett utlämnande avsevärt avviker från schablonersättningen får den lagringsskyldige begära ersättning som motsvarar kostnaderna i det enskilda fallet (se 3–4 §§ i nämnda föreskrifter).

Rätten till ersättning enligt 6 kap. 16 e § LEK gäller alltså endast vid utlämnande av sådana uppgifter som omfattas av lagringsskyldigheten, dvs. för uppgifter som leverantörerna sparar för brottsbekämpande ändamål. Bestämmelsen blir därmed tillämplig för kostnader som uppstår när uppgifter som lagras för brottsbekämpande ändamål lämnas ut till följd av beslut om HAK eller HÖK som har sin grund i bestämmelserna i 27 kap. RB, preventivlagen, lagen om särskild utlänningskontroll eller inhämtningslagen. Bestämmelsen gäller dock inte för kostnader som uppstår när besluten avser avlyssning eller övervakning i realtid. Regleringen är inte heller tillämplig exempelvis när Polismyndigheten begär ut uppgifter för att efterforska en försvunnen person (utan misstanke om brott) enligt 6 kap. 22 § första stycket 3 LEK. Inte heller är regleringen tillämplig för uppgifter som leverantörerna sparar endast för eget bruk, såsom för fakturering eller marknadsföring. I de fall som inte omfattas av bestämmelsen i 6 kap. 16 e § LEK bestäms ersättningsnivåerna efter förhandlingar mellan de brottsbekämpande myndigheterna och berörda leverantörer.

6.4.2 Problembeskrivning

Det förhållandet att Post- och telestyrelsen endast har mandat att meddela föreskrifter om ersättning vid utlämnande till brottsbekämpande myndigheter av vissa lagrade uppgifter har medfört att utlämnanden av mycket likartade uppgifter kan skilja sig väsentligt i pris för de brottsbekämpande myndigheterna. Ersättningen varierar beroende på om en viss uppgift hämtas in i realtid eller med någon dags fördröjning och skiljer sig också åt beroende på vilket lagstöd som åberopas. Priserna kan också variera mellan olika leverantörer.

De brottsbekämpande myndigheternas kostnader för inhämtning av uppgifter från leverantörerna uppgår till stora belopp. Enligt Polismyndigheten uppgår den ersättning som de brottsbekämpande myndigheterna betalar till mobiloperatörerna för verkställighet av endast realtidskopplingar av HAK och HÖK till cirka 30 miljoner kr årligen. Kostnaden för en inkoppling av en HÖK i realtid inom kontorstid uppgår till cirka 2 500 kr hos flera mobiloperatörer medan en HÖK avseende historiska uppgifter som omfattas av lagringsskyldigheten, kostar 150 kr alternativt 525 kr per beställning beroende på vilka uppgifter som avses. En inkoppling avseende HAK i realtid kostar 2 500 kr hos flera mobiloperatörer. I de fall beslut har fattats om hemlig avlyssning avseende en viss telefon (ett s.k. IMEI-nummer) men det inte är känt vilken mobiloperatör som är aktuell, kan samtliga fyra nätleverantörer behöva tillfrågas innan en HAK kan kopplas in. Varje förfrågan debiteras, vilket medför att kostnaderna för att få till stånd en enda avlyssning kan bli höga.

När det gäller lokaliseringsuppgifter i samband med efterforskning av försvunna personer utan misstanke om brott, har det framkommit att den ersättning som begärs av leverantörerna varierar stort. Vissa leverantörer lämnar ut uppgifterna utan kostnad medan andra begär över 6 000 kr för en lokaliseringsuppgift. Enligt Polismyndigheten kan kostnaderna för efterforskning av en försvunnen person uppgå till höga belopp eftersom det ofta är nödvändigt att positionera en försvunnen person mer än en gång. För det fall lokaliseringsuppgifterna i stället begärs ut av SOS Alarm tas ingen ersättning ut (se 5 kap. 7 § 2 LEK).

6.4.3 Uppdraget

Bestämmelserna om leverantörernas rätt till ersättning från brottsbekämpande myndigheter avser alltså endast sådana uppgifter som omfattas av lagringsskyldigheten. När det gäller ersättning för utlämnande av uppgifter som leverantörerna behandlar för andra ändamål saknas författningsreglering. I uppdragsbeskrivningen anges att det kan ifrågasättas om den nuvarande ordningen är rimlig. Vårt uppdrag i denna del är att se över den nuvarande ordningen för ersättning och vid behov lämna förslag på förändringar.

6.4.4 Överväganden och förslag

Förslag: Det ska i 6 kap. 19 § tredje stycket LEK föreskrivas att den som lämnar ut uppgifter som avses i 20 § första stycket till Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som har till uppgift att ingripa mot brott, har rätt till ersättning för kostnader som uppstår när uppgifter lämnas ut. Ersättningen ska betalas av den myndighet som har begärt uppgifterna. Regleringen ska gälla även vid utlämnande av lokaliseringsuppgifter som inte är trafikuppgifter.

Regleringen i 6 kap. 16 e § om ersättning för utlämnande av lagrade uppgifter ska upphävas.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela närmare föreskrifter om samtliga ersättningsfrågor. Post- och telestyrelsen ska i förordning bemyndigas att meddela föreskrifter om samtliga ersättningsfrågor.

Att det är en otillfredsställande ordning att utlämnandet av mycket likartade uppgifter kan skilja sig väsentligt i pris för de brottsbekämpande myndigheterna har uppmärksammats från flera håll. Frågan har bl.a. tagits upp av Utredningen om datalagring och EU-rätten (se SOU 2017:75 s. 284). Post- och telestyrelsen har också vid flera tillfällen påpekat att det vore mer ändamålsenligt att, på motsvarande sätt som gäller för ersättning vid utlämnande av uppgifter som lagras för brottsbekämpande ändamål, reglera ersättningen även vid utlämnande av uppgifter som behandlas på annan

grund. Myndigheten har också föreslagit att den ges mandat att besluta om ersättningen (se t.ex. Post- och telestyrelsens remissvar på SOU 2017:75 s. 3 f.). I regeringens proposition Datalagring vid brottsbekämpning – anpassningar till EU-rätten, förklarade regeringen att det kan finnas anledning att återkomma till frågan (se prop. 2018/19:86 s. 85). Ersättningsfrågan har också uppmärksammats av Polismyndigheten.

Från leverantörernas sida har framhållits att utlämnandet av uppgifter om elektronisk kommunikation till brottsbekämpande myndigheter är förenat med stora kostnader. Det ställs höga krav på leverantörerna när det gäller teknik, säkerhet och bemanning. Den ersättning som utgår för den utlämnade informationen är dock blygsam. En allmän uppfattning bland leverantörerna är att dagens taxor generellt sätt är för låga och bör ses över. Det har bl.a. av det skälet ifrågasatts om det är möjligt att genom schabloner standardisera även de ersättningsnivåer som ska gälla vid bl.a. realtidsutlämnanden. Flera leverantörer har dock framhållit att de inte har något emot användningen av schablonersättningar i sig. För att en verksamhet ska kunna fungera smidigt kan schabloner nämligen vara att föredra. Det som framhålls är dock att schablonerna bör ge tillräcklig kostnadstäckning. Det har också påpekats att en otydlig beställning medför merarbete för leverantörerna och därmed högre kostnader. Även för att hålla nere kostnaderna finns det därför anledning för de brottsbekämpande myndigheterna att standardisera sina beställningar.

Det står klart att utlämnandet av uppgifter till de brottsbekämpande myndigheterna innebär stora kostnader för leverantörerna. Med hänsyn till den kostnadsfördelningsmodell som föreligger och det kostnadsansvar det innebär för leverantörerna, kan det finnas anledning att göra regelbundna översyner av de föreskrifter som anger ersättningsnivåerna för utlämnandena. Det ingår dock inte i vårt uppdrag att föreslå en annan modell för kostnadsfördelningen i stort.

Det kan konstateras att det finns en rad fördelar med ett standardiserat förfarande för bestämmandet av den ersättning som ska betalas av brottsbekämpande myndigheter vid inhämtande av uppgifter om elektronisk kommunikation. Ett system med schablonersättningar ger en enkel och snabb handläggning för både leverantörer och brottsbekämpande myndigheter. Därmed kan resurser

såväl hos leverantörerna som hos de brottsbekämpande myndigheterna läggas på annat. Genom att ersättningen är bestämd på förhand är den också förutsebar för alla parter.

Det får anses vara en rimlig utgångspunkt att leverantörerna bör erhålla lika stor ersättning vid utlämnande av samma sorts uppgifter till de brottsbekämpande myndigheterna. Vidare är det rimligt att ersättningen i samtliga fall bör bestämmas enligt vissa schabloner som bygger på beräkningar av leverantörernas kostnader i olika typer av ärenden. Vi instämmer därför i Post- och telestyrelsens bedömning att det vore mer ändamålsenligt att, på motsvarande sätt som gäller för ersättning vid utlämnande av uppgifter som lagras för brottsbekämpande ändamål, författningsreglera ersättningen för utlämnande av uppgifter som behandlas på annan grund. Någon skillnad bör alltså inte göras beroende på om de uppgifter som lämnas ut avser realtidsuppgifter eller historiska uppgifter och inte heller om de avser trafikuppgifter, lokaliseringsuppgifter eller abonnemangsuppgifter. Det bör inte heller göras någon skillnad beroende på vilket lagstöd som finns för utlämnandet.

Post- och telestyrelsen är tillsynsmyndighet enligt lagen om elektronisk kommunikation och har ett samlat ansvar inom området för elektronisk kommunikation. Myndigheten kan därför säkerställa att hänsyn tas till såväl leverantörernas som de brottsbekämpande myndigheternas intressen. Myndigheten har dessutom redan erfarenhet av att bestämma den ersättning som ska utgå för de uppgifter som omfattas av lagringsskyldigheten. Post- och telestyrelsen ska också meddela föreskrifter om leverantörers ersättning vid medverkan i samband med verkställighet av hemlig dataavläsning (4 § förordningen [2020:172] om hemlig dataavläsning). En stor del av utredningen avseende leverantörernas åtgärder och därtill kopplade kostnader kan antas vara gemensamma för samtliga former av utlämnanden. Enligt vår mening bör därför Post- och telestyrelsen ges mandat att genom föreskrifter fastställa ersättningen vid utlämnande av uppgifter om elektronisk kommunikation till brottsbekämpande myndigheter i samtliga ovannämnda utlämnandesituationer.

Enligt vår mening löses frågan lämpligast genom att det i 6 kap. 19 § tredje stycket LEK förs in bestämmelser som anger att den som lämnar ut uppgifter som avses i 20 § första stycket, alltså uppgift om abonnemang samt innehållet i och uppgift som angår ett elektroniskt meddelande, till en brottsbekämpande myndighet har rätt till

ersättning för kostnader som uppstår när uppgifter lämnas ut. Detsamma bör gälla vid utlämnande av lokaliseringsuppgifter som inte avser trafikuppgifter. Av regleringen bör även framgå att ersättningen ska betalas av den myndighet som har begärt uppgifterna. Härigenom blir den princip om kostnadsersättning som gäller på området lagfäst. Vidare blir det tydligt att leverantörerna har rätt till ersättning vid utlämnande till brottsbekämpande myndigheter av alla slags uppgifter. Eftersom regleringen inte, såsom de föreslagna ändringarna i 6 kap. 19 § andra stycket, är begränsad till utlämnanden som sker i brottsbekämpande syfte, omfattar den även kostnader för utlämnanden av uppgifter om försvunna personer enligt 6 kap. 22 § första stycket 3.

Det bör också i 6 kap. 19 § LEK föras in ett bemyndigande som ger regeringen eller den myndighet regeringen bestämmer rätt att meddela närmare föreskrifter om ersättningen. Ett bemyndigande för Post- och telestyrelsen att meddela föreskrifter om ersättningen kan föras in i 36 § FEK.

Eftersom regleringen föreslås gälla även vid utlämnande av lagrade trafikuppgifter är den särskilda regleringen härom i 6 kap. 16 e § LEK inte längre nödvändig och bör därför upphävas. Det nuvarande bemyndigandet i 46 § FEK som ger Post- och telestyrelsen rätt att meddela föreskrifter om ersättning vid utlämnande av de lagrade uppgifterna bör samtidigt utgå.

Fastställandet av ersättningsnivåerna kommer att medföra vissa svårigheter eftersom kostnaderna kan variera mellan de olika leverantörerna och mellan olika uppgiftsslag. Utgångspunkten bör visserligen vara att leverantörerna ska få sina kostnader för att lämna ut uppgifter i det enskilda ärendet ersatta. Det ligger dock i sakens natur att en schablonersättning medför att en leverantör ibland kommer att få en högre ersättning än vad som är motiverat och ibland kommer att få en lägre ersättning än vad som motsvarar leverantörens kostnader. När kostnaderna för ett utlämnande avsevärt avviker från schablonersättningen bör dock leverantören, på samma sätt som gäller i dag, ha möjlighet att begära att schablonersättningen inte ska tillämpas, utan att ersättningen ska bestämmas till ett belopp som motsvarar kostnaderna i det enskilda fallet. Post- och telestyrelsens föreskriftsrätt bör således omfatta möjligheten att föreskriva om undantag från schablonersättningen. Det behöver inte

regleras särskilt i lag eller förordning utan följer av det bemyndigande som Post- och telestyrelsen föreslås få.

För att de brottsbekämpande myndigheterna ska ha möjlighet att påverka hur schablonbeloppen bestäms bör dessa, på samma sätt som gäller i dag, fastställas efter samråd med de brottsbekämpande myndigheter som begär in uppgifter om elektronisk kommunikation. Även leverantörernas synpunkter bör naturligtvis inhämtas.

6.5 Utlämnande av abonnemangsuppgifter i underrättelseverksamhet

Förslag: Bestämmelsen i 6 kap. 22 § första stycket 2 LEK ska förtydligas så att det helt klart framgår att uppgifter får hämtas in, utöver i en förundersökning, även i de brottsbekämpande myndigheternas underrättelseverksamhet.

Som tidigare framkommit har en leverantör som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst tystnadsplikt för bl.a. uppgifter om abonnemang (6 kap. 20 § första stycket 1 LEK). Trots tystnadsplikten har en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen eller någon annan myndighet som ska ingripa mot brottet (Tullverket, Kustbevakningen och Skatteverket) rätt att få tillgång till abonnemangsuppgifter, om uppgiften gäller misstanke om brott som myndigheten ska ingripa mot (6 kap. 22 § första stycket 2 LEK). Bestämmelsen är uppbyggd så att en uppgift om abonnemang ska lämnas ut på begäran om den gäller ”misstanke om brott”. En liknande skrivning fanns tidigare i 6 kap. 22 § första stycket 3 LEK (i dess lydelse före den 1 juli 2012). Enligt den bestämmelsen kunde brottsbekämpande myndigheter hämta in trafikuppgifter vid misstanke om brott. Trots ordalydelsen var bestämmelsen inte begränsad till en förundersökningssituation utan ansågs kunna användas även för att hämta in trafikuppgifter i underrättelseverksamheten (se SOU 2009:1 s. 72 f.).

Det har i tidigare utredningsarbeten slagits fast att regleringen i 6 kap. 22 § första stycket 2 inte är begränsad till en förundersökningssituation utan även kan användas för att hämta in uppgifter i underrättelseverksamhet (se SOU 2015:31 s. 198 f. och SOU 2017:71

s. 101). Vi har inte någon annan uppfattning. Regleringen tillämpas i praktiken också i de brottsbekämpande myndigheternas underrättelseverksamhet.

Datalagringsutredningen föreslog i SOU 2015:31 att 6 kap. 22 § första stycket 2 LEK ska justeras för att klargöra att abonnemangsuppgifter får hämtas in i underrättelseverksamhet. Förslaget har inte lett till lagstiftning. Tullverket har under vårt utredningsarbete framfört att det alltjämt finns anledning att tydliggöra att bestämmelsen kan tillämpas även i de brottsbekämpande myndigheternas underrättelseverksamhet. Vi delar den bedömningen. Av rättssäkerhetsskäl bör lagstiftning som innebär att brottsbekämpande myndigheter kan få tillgång till uppgifter som berör enskildas privatliv vara så tydlig som möjligt. Uttrycket ”misstanke om brott” kan föra tankarna till en redan begången konkret gärning. Med de brottsbekämpande myndigheternas underrättelseverksamhet avses dock främst arbete med insamling, bearbetning och analys av information i syfte att förhindra eller upptäcka brottslig verksamhet när det ännu inte finns misstankar om att något konkret brott har begåtts (se t.ex. prop. 2017/18:269 s. 294). För att klargöra att abonnemangsuppgifter får hämtas in även i underrättelseverksamhet bör därför bestämmelsen justeras.

Uttrycket ”brottslig verksamhet” används i lagstiftning för att avgränsa åtgärder som får vidtas i underrättelseverksamhet (se t.ex. 2 kap. 1 § lagen [2018:1693] om polisens behandling av personuppgifter inom brottsdatalagens område och 2 § inhämtningslagen). Med uttrycket avses verksamhet av viss konkretion (se prop. 2009/10:85 s. 362 f.). Däremot krävs inte att misstanken avser en konkretiserad gärning på samma sätt som vid förundersökning. Uttrycket bör användas även i lagen om elektronisk kommunikation.

7 Ikraftträdande- och övergångsbestämmelser

Förslag: Författningsförslagen ska träda i kraft den 1 januari 2022. Det ska införas en övergångsbestämmelse för förbetalda tjänster som har tillhandahållits innan regleringen trädde i kraft. Dessa tjänster ska vara möjliga att använda till den 1 juli 2022 utan att en registrering har skett.

Den föreslagna regleringen bör av effektivitetsskäl träda i kraft så snart som möjligt. Dock behöver leverantörerna ges rimlig tid att anpassa sina system och sin verksamhet, både när det gäller att leva upp till krav på registrering av abonnemangsuppgifter för förbetalda tjänster och när det gäller krav på gemensamma format och utlämnande av uppgifter om elektronisk kommunikation utan dröjsmål. Med hänsyn härtill föreslår vi att författningsförslagen ska träda i kraft den 1 januari 2022.

Reglerna ska börjas tillämpas genast vid ikraftträdandet. Vi har i avsnitt 5 föreslagit att en skyldighet att registrera abonnemangsuppgifter för förbetalda tjänster även ska omfatta tjänster som har tillhandahållits innan registreringsskyldigheten trädde i kraft. Arbetet med att låta genomföra en registrering av befintliga kunder bör kunna förberedas innan lagstiftningen träder i kraft. För att operatörer och enskilda ska ges tillräcklig tid att låta genomföra en registrering av samtliga befintliga förbetalda tjänster bör det dock införas en övergångsbestämmelse som anger att en förbetald tjänst som har tillhandahållits innan regleringen trädde i kraft ska vara möjlig att använda i ytterligare sex månader utan att en registrering har skett. Om en registrering inte har skett senast den 1 juli 2022 ska dock tillhandahållandet av tjänsten avbrytas.

Det finns i övrigt inte behov av några övergångsbestämmelser.

8 Förslagens konsekvenser

8.1 Inledning

Enligt uppdragsbeskrivningen ska vi analysera och redovisa de ekonomiska konsekvenserna av förslagen. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna ska vi föreslå hur de ska finansieras. Dessa frågor berörs i detta avsnitt. Vi kommer också att kort redogöra för förslagens konsekvenser för de mobiloperatörer som tillhandahåller kontantkort och för enskilda.

8.2 Konsekvenser för det allmänna

Bedömning: Förslagen kommer i viss utsträckning medföra ökade kostnader för berörda myndigheter. Dessa kostnader bedöms dock rymmas inom befintliga anslag.

Författningsförslagen syftar till att ge de brottsbekämpande myndigheterna bättre tillgång till uppgifter om elektronisk kommunikation. Förslaget om en skyldighet att registrera abonnemangsuppgifter för förbetalda tjänster som nås via kontantkort kommer att medföra att mobiloperatörerna har tillgång till fler uppgifter om enskildas abonnemang än vad de har i dag. Fler abonnemangsuppgifter kan därmed komma att hämtas in av de brottsbekämpande myndigheterna för användning i brottsbekämpningen. Tillgången till fler abonnemangsuppgifter kommer troligen att medföra att hemliga tvångsmedel kommer att användas i större utsträckning än i dag. Detta kan i sig leda till högra kostnader för de brottsbekämpande myndigheterna. Även inhämtningen av själva abonnemangsuppgifterna kan i sig leda till ökade kostnader för de brottsbekämpande myndigheterna i form av utbetald ersättning till

mobiloperatörerna. En ökad tillgång till abonnemangsuppgifter får dock samtidigt antas leda till ett effektivare brottsbekämpande arbete och till att fler brottsutredningar kan slutföras. Den ökade tillgången till abonnemangsuppgifter kan också medföra att olika tidskrävande utredningsåtgärder som i dag används för att få fram uppgifter om vem som är innehavare av ett kontantkort inte längre kommer att behöva användas i samma utsträckning. Härmed kan tid och resurser hos de brottsbekämpande myndigheterna läggas på annat.

Även de förslag som innebär att gemensamma format ska användas vid utlämnande av uppgifter om elektronisk kommunikation från leverantörer till brottsbekämpande myndigheter och om att uppgifterna ska lämnas ut utan dröjsmål, kan antas leda till ett effektivare brottsbekämpande arbete. Förslagen om att den ersättning som de brottsbekämpande myndigheterna ska betala till mobiloperatörerna ska utgå från en schablon i fler situationer än i dag, kan antas leda till en mer förutsebar ordning för de brottsbekämpande myndigheterna när det gäller kostnaderna kopplade till inhämtningen av uppgifter om elektronisk kommunikation. Detta förhållande kan balansera de ökade kostnader kopplade till inhämtningen som en registreringsskyldighet för kontantkort kan medföra.

Sammanfattningsvis är det vår bedömning att förslagen endast kommer att innebära marginella kostnadsökningar för de brottsbekämpande myndigheterna. Kostnadsökningarna får anses rymmas inom befintliga anslag.

En effektivare användning av uppgifter om elektronisk kommunikation i brottsbekämpningen skulle kunna leda till att kostnaderna ökar inom vissa sektorer av rättsväsendet. Om t.ex. polisen blir effektivare kan det leda till en ökad arbetsbörda med krav på ökade resurser för åklagare och domstolar. Totalt sett torde dock rättsväsendets olika insatser vid utredning och lagföring av allvarlig brottslighet effektiviseras. Vi bedömer att våra förslag i sig inte kommer att medföra behov av resursförstärkningar för rättsväsendet.

Förslaget om att mobiloperatörerna ska vara skyldiga att registrera vissa uppgifter om de abonnenter som använder förbetalda tjänster kommer att medföra ett utökat tillsynsområde för Post- och telestyrelsen. De samlade förslagen kommer också att innebära att Post- och telestyrelsen kommer att få möjlighet att meddela före-

skrifter i fler situationer än vad som sker i dag. De arbetsuppgifter som på detta sätt kan tillkomma för myndigheten bedöms dock inte medföra behov av ökade anslag.

8.3 Konsekvenser för företag

Bedömning: Förslagen kan medföra konsekvenser för de företag som tillhandahåller kontantkort, i form av försäljningsminskning och framför allt ökad administrativ börda.

Förslaget om en skyldighet att registrera abonnemangsuppgifter om de kunder som använder förbetalda tjänster kommer främst att beröra de mobiloperatörer som tillhandahåller dessa tjänster. Det finns för närvarande sex mobiloperatörer som säljer kontantkort och som därmed tillhandahåller förbetalda allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster eller förbetalda internetanslutningstjänster i Sverige. De fyra största mobiloperatörerna, Telia, Tele2, Telenor och Hi3G (Tre) innehar, via olika varumärken, sammanlagt 94 procent av marknaden. Kontantkort säljs också av Lycamobile och Wifog.

Registreringsskyldigheten kommer att medföra att de aktuella mobiloperatörerna behöver anpassa sina system och lagra fler uppgifter än förut, vilket innebär kostnadsökningar. Dels krävs en engångsinvestering i form av ombyggnad av systemen, dels krävs investeringar i och för löpande drift. Hur stora kostnadsökningarna kommer att bli är dock svårt att kvantifiera. Någon operatör har uppgett att en registreringsskyldighet skulle medföra att kostnaderna för operatörerna skulle skjuta i höjden och hamna på helt orimliga nivåer. En annan operatör har uppgett att system för att genomföra en registrering av samtliga kontantkortskunder i princip redan finns på plats, eftersom en registrering sker redan i dag av de kunder som har kontraktsabonnemang eller som på frivillig väg lämnar sina abonnemangsuppgifter till operatören. Det som tillkommer är eventuella kostnader kopplade till den personal som kan behövas för att genomföra en registrering.

Även om det är svårt att kvantifiera de kostnader som kan uppstå för operatörerna till följd av en registreringsskyldighet bedömer vi att dessa kommer att öka. I sammanhanget bör dock påpekas att flera

av mobiloperatörerna bedriver verksamhet i andra länder där det finns krav på att operatörerna ska registrera uppgifter om de kunder som innehar kontantkort. Således finns det, i olika stor utsträckning, redan upparbetade system och rutiner kring dessa frågor.

Som tidigare konstaterats finns det verksamhetsområden där samhället som en förutsättning för att tillåta ett företag att driva näringsverksamhet kräver att vissa samhälleliga intressen beaktas. Den som tillhandahåller kontantkort för mobiltelefoner är verksam inom ett sådant område och måste ibland anpassa sin verksamhet till vissa centrala intressen, däribland samhällets berättigade intresse att bekämpa brott. Regeringen har i tidigare sammanhang bedömt att operatörer kan vara skyldiga att vidta åtgärder för att underlätta den brottsutredande verksamheten och i viss utsträckning bära kostnaderna för detta (se prop. 2010/11:46 s. 67 och prop. 1995/96:180 s. 29 ff.).

En skyldighet att registrera abonnemangsuppgifter skulle kunna få till följd att enskilda väljer att avstå från att köpa ett kontantkort eller låta registrera sitt befintliga kontantkort, eventuellt för att en registrering uppfattas som krånglig. Förslagen är dock utformade i syfte att kunder inte ska uteslutas från möjligheten att fortsatt köpa och använda kontantkort. Den identifiering som krävs ska t.ex. kunna ske genom ett stort antal identitetshandlingar. För den som saknar identitetshandling ska identifieringen kunna ske på annat sätt. Således kommer alla grupper av människor, som t.ex. turister, asylsökande och flyktingar, kunna fortsätta använda kontantkort för sin mobilanvändning. Vidare innebär förslagen att registreringen kan ske på flera olika sätt, t.ex. via internet, via kontakt med mobiloperatörens kundtjänst eller i en fysisk butik. Det är därför vår bedömning att en registrering kommer att kunna genomföras även av t.ex. äldre personer eller andra som kan behöva hjälp med att genomföra en registrering. Således kommer inte en registreringsskyldighet att behöva medföra något större kundbortfall. Här kan tilläggas att en registreringsskyldighet som omfattar kontantkort sannolikt kommer att innebära en viss fördel för mobiloperatörerna eftersom de enklare kommer att kunna nå sina kontantkortskunder för marknadsföring.

Kontantkort säljs även av återförsäljare. Det finns i dag mellan 7 000 och 12 000 återförsäljare av kontantkort i Sverige. Flera av återförsäljarna är av sådan storlek att de bör kunna administrera en

registrering av abonnemangsuppgifter. Kontantkort säljs dock även av mindre fristående handlare som troligen inte har de tekniska och praktiska möjligheterna att kunna genomföra en registrering. Enligt en uppskattning säljer så många som cirka 7 000 fristående handlare kontantkort. Fristående handlare har i många fall små marginaler. Således skulle en minskad försäljning av kontantkort kunna bli märkbar för dessa aktörer. Den föreslagna registreringsskyldigheten hindrar dock inte fristående handlare från att fortsatt sälja kontantkort eller vouchers för påfyllnad. Som konstaterats ovan kan nämligen själva registreringen av abonnemangsuppgifterna utföras efter köpet t.ex. via internet, via kontakt med mobiloperatörens kundtjänst eller i mobiloperatörernas butiker. En registreringsskyldighet behöver därför inte innebära att de fristående handlarna kommer att förlora de ekonomiska förutsättningarna att fortsättningsvis bedriva sin verksamhet.

De förslag som lämnas i verkställighetsfrågorna omfattar samtliga leverantörer som kan komma att lämna ut uppgifter om elektronisk kommunikation till brottsbekämpande myndigheter. Leverantörerna utgörs av mer är 600 företag som erbjuder olika tjänster i form av mobiltelefoni, fast telefoni och internetabonnemang. Företagen har en mycket varierande marknadsandel och storlek mätt i omsättning. I praktiken kommer regleringen dock främst att träffa de fyra stora mobiloperatörerna, som är de aktörer som brottsbekämpande myndigheter vanligtvis vänder sig till för att få tillgång till uppgifter om elektronisk kommunikation. Tillsammans står dessa fyra företag för cirka 95 procent av mobilmarknaden.

Förslagen om att leverantörerna ska ordna och göra uppgifter om elektronisk kommunikation tillgängliga för brottsbekämpande myndigheter i ett format som gör det möjligt att enkelt ta hand om dem kommer att vara kostnadsdrivande för leverantörerna. Detsamma gäller för förslaget om att samtliga uppgifter ska lämnas ut utan dröjsmål. För de fyra stora mobiloperatörerna har arbetet med att införa gemensamma format dock redan påbörjats på frivillig väg. Det finns också redan i dag krav på att lagrade uppgifter ska lämnas ut med den föreslagna graden av skyndsamhet och de stora operatörerna förutsätts kunna verkställa beslut om hemlig avlyssning och övervakning av elektronisk kommunikation dygnet runt årets alla dagar. Den föreslagna regleringen kommer dock att innebära att höjda krav kommer att ställas även på de mindre

leverantörerna, vilket kan medföra ökade kostnader för dem. Som konstaterats ovan innebär dock den nuvarande modellen för kostnadsfördelning mellan det allmänna och leverantörerna att leverantörerna står för kostnaden för anpassning, drift och underhåll och de brottsbekämpande myndigheterna betalar en ersättning vid varje utlämnande av uppgifter. Det finns inte anledning att här föreslå någon annan modell för kostnadsfördelningen.

Förslagen i ersättningsdelen innebär att Post- och telestyrelsen ska bestämma storleken på den ersättning som ska betalas ut till leverantörerna i fler situationer än i dag. Regleringen kommer att medföra att ersättningsnivåerna kommer att bli mer likartade och därmed mer rättvisa mellan leverantörerna. Den föreslagna registreringsskyldigheten för kontantkort förväntas samtidigt innebära att de brottsbekämpande myndigheterna kommer att begära in abonnemangsuppgifter i större utsträckning än i dag. Detta kan i sig innebära större intäkter för de leverantörer som tillhandahåller kontantkort.

De kostnader som förslagen innebär för leverantörerna bör dessa huvudsakligen kunna föra över på sina kunder, dvs. såväl stat och kommuner som företag och privatpersoner. Enligt vår bedömning kan de eventuella merkostnader som på detta sätt kommer att drabba stat och kommuner rymmas inom befintliga ramar.

8.4 Konsekvenser för enskildas personliga integritet

Bedömning: Förslaget om en registreringsskyldighet för förbetalda tjänster innebär en begränsad inskränkning i enskildas rätt till personlig integritet.

Syftet med förslaget om att införa en registreringsplikt som omfattar uppgifter om de abonnenter som innehar kontantkort är att försvåra kriminell verksamhet. Som angetts i avsnitt 5.6.1 är det vår bedömning att den föreslagna regleringen är proportionerlig i förhållande till samhällsintresset av att bekämpa brott.

Den föreslagna regleringen kommer att innebära att fler uppgifter om enskilda kommer att hanteras av mobiloperatörerna. Uppgifterna kan också komma att lämnas ut till brottsbekämpande myndigheter och vissa andra myndigheter som räknas upp i 6 kap. 22 § LEK om så begärs och om den befintliga lagstiftningen tillåter

det. De uppgifter som enligt förslaget ska registreras har därför begränsats till att endast avse sådana uppgifter som är direkt nödvändiga för en identifiering. Några sådana uppgifter som i dataskyddssammanhang betecknas som känsliga personuppgifter omfattas inte. De uppgifter som ska registreras är enskildas telefonnummer, namn, adress och personnummer eller motsvarande. Sådana uppgifter behandlas av mobiloperatörerna redan i dag när det gäller de kunder som innehar kontraktsabonnemang eller som på frivillig väg har lämnat uppgifterna till sin mobiloperatör. Även om det genom förslagen införs en rättslig förpliktelse och därmed en ny rättslig grund för personuppgiftsbehandlingen (artikel 6.1 c i dataskyddsförordningen), kan det därmed inte sägas vara fråga om någon ny form av personuppgiftsbehandling.

De registrerade uppgifterna ska hos mobiloperatörerna behandlas i enlighet med befintlig dataskyddsreglering enligt den allmänna dataskyddsförordningen och lagen om elektronisk kommunikation. Regleringen innehåller uppgifter om hur länge uppgifterna får bevaras. Av dataskyddsregleringen följer också att mobiloperatörerna ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att uppgifterna behandlas på ett säkert sätt. Uppgifterna kommer också att omfattas av tystnadsplikt. Det är vår bedömning att den befintliga dataskydds- och sekretessregleringen utgör ett fullgott skydd även för de abonnemangsuppgifter som tillkommer genom en registreringsskyldighet.

Vi har i avsnitt 5.6.1 redogjort för de konsekvenser som en registreringsskyldighet som omfattar uppgifter om kontantkortskunder kommer att innebära för den som har ett befogat intresse av att undgå en registrering. Som framgår där kommer det även framöver att finnas möjligheter att kommunicera mobilt med andra utan att ens identitet röjs. Med hänsyn härtill, och till vad som anförts ovan om behandlingen av de registrerade uppgifterna, är det vår bedömning att registreringsskyldigheten kommer att innebära en begränsad inskränkning i enskildas rätt till personlig integritet.

Förslagen i verkställighetsfrågorna har till främsta syfte att effektivisera det utlämnande av uppgifter om elektronisk kommunikation från leverantörer till brottsbekämpande myndigheter som sker redan i dag. Förslagen i den delen innebär inte några direkta konsekvenser för enskilda och kan inte sägas påverka enskildas personliga integritet.

9 Författningskommentar

9.1 Förslaget till lag om ändring i lagen (2003:389) om elektronisk kommunikation

6 kap.

5 § Den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § ska utplåna eller avidentifiera lagrade eller på annat sätt behandlade trafikuppgifter som avser användare som är fysiska personer eller som avser abonnenter, när uppgifterna inte längre behövs för att överföra ett elektroniskt meddelande. Det gäller dock inte om uppgifterna sparas för sådan behandling som anges i 6, 13, 16 a, 16 c *eller 23 a §*.

I paragrafen återfinns huvudregeln om behandling av trafikuppgifter som avser användare som är fysiska personer eller som avser abonnenter. Huvudregeln innebär att när en sådan uppgift inte längre behövs för att överföra ett elektroniskt meddelande ska uppgiften utplånas eller avidentifieras. Det angivna gäller dock inte om uppgiften sparas för sådan behandling som anges i vissa uppräknade bestämmelser. Paragrafen har kompletterats med en hänvisning även till 6 kap. 23 a §, vilket innebär att även uppgifter som sparas med stöd av den bestämmelsen, dvs. abonnemangsuppgifter som avser förbetalda allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster eller förbetalda internetanslutningstjänster, är undantagna från huvudregeln.

19 § 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 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 kommunikationsnät vilka består av

a) en allmänt tillgänglig telefonitjänst till 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.

När uppgifter som avses i 20 § första stycket lämnas ut för brottsbekämpning till Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som har till uppgift att ingripa mot brott, ska uppgifterna ordnas och göras tillgängliga i ett format som gör det möjligt att enkelt ta hand om dem. Uppgifterna ska lämnas ut utan dröjsmål.

Den som lämnar ut uppgifter som avses i 20 § första stycket till Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som har till uppgift att ingripa mot brott, har rätt till ersättning för kostnader som uppstår när uppgifter lämnas ut. Ersättningen ska betalas av den myndighet som har begärt uppgifterna.

Vad som föreskrivs om uppgifter i andra och tredje styckena gäller även lokaliseringsuppgifter som inte är trafikuppgifter.

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

Paragrafen reglerar frågor som rör utlämnande av uppgifter om elektronisk kommunikation till brottsbekämpande myndigheter. Bestämmelserna har behandlats i avsnitt 6.

Första stycket är oförändrat.

I *andra stycket* första meningen föreskrivs att när uppgifter som avses i 20 § första stycket lämnas ut för brottsbekämpning till Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som har till uppgift att ingripa mot brott, ska uppgifterna ordnas och göras tillgängliga i ett format som gör det möjligt att enkelt ta hand om dem. Andra stycket ska läsas fristående från första stycket. Det omfattar fler aktörer än de som omfattas av första stycket. Regleringen träffar alla leverantörer som lämnar ut uppgifter om elektronisk kommunikation till en brottsbekämpande myndighet för att uppgifterna ska användas där i brottsbekämpande syfte. Kraven i bestämmelsen omfattar innehållet i och uppgifter om avlyssnade

eller övervakade meddelanden som lämnas ut efter beslut om HAK eller HÖK som har sin grund i 27 kap. RB, preventivlagen, lagen om särskild utlänningskontroll eller inhämtningslagen. Även abonnemangsuppgifter som lämnas ut till brottsbekämpande myndigheter med stöd av 6 kap. 22 § första stycket 2 LEK omfattas. I fjärde stycket föreskrivs att även lokaliseringsuppgifter som inte är trafikuppgifter omfattas av regleringen. Bestämmelsen i andra stycket träffar alla som är lagringsskyldiga enligt 6 kap. 16 a §, oavsett om det gäller telefonitjänster eller rena internettjänster. Det har ingen betydelse om uppgifterna behandlas hos leverantören på grund av lagringsskyldigheten i 6 kap. 16 a § LEK eller för leverantörens egna ändamål.

Kravet på att uppgifter ska ordnas och göras tillgängliga i ett format som gör det möjligt att enkelt ta hand om dem innebär att uppgifter som lämnas ut inte enbart ska göras tillgängliga på ett sådant sätt att de är läsbara. Uppgifterna ska även vara sammanställda på ett sådant strukturerat sätt att de utan ytterligare bearbetning hos mottagarna kan komma till användning i det brottsbekämpande arbetet. Ett sätt att uppfylla detta krav är att använda sig av etablerade standarder och i förväg överenskomna format baserade på standarder. Kravet på tillgängliggörande innebär inte att leverantören har en skyldighet att dekryptera meddelanden i de fall där denne inte tillhandahåller eller förfogar över krypteringssystemet. Leverantören förväntas således inte kunna avlämna meddelanden i klartext om abonnenten själv komprimerat eller krypterat sina meddelanden. Uppgifterna måste alltid överlämnas på ett sådant sätt att säkerheten och skyddet för uppgifterna inte eftersätts.

I andra styckets andra mening föreskrivs att de ovan angivna uppgifterna ska lämnas ut till de brottsbekämpande myndigheterna utan dröjsmål. Begreppet utan dröjsmål bör tolkas mot bakgrund av hur stort behovet av skyndsamhet är och förutsättningarna för ett snabbt utlämnande i det enskilda fallet. Det är främst de tekniska förutsättningarna som bör avgöra hur snabbt ett utlämnande kan ske, men även andra faktorer kan beaktas. Ett visst mått av utrymme för prioriteringar bör inrymmas i begreppet. Utgångspunkten är dock att behandlingen av en begäran som inkommer under kontorstid ska inledas inom mycket kort tid, dvs. samma dag. Om det tar olika lång tid att ta fram uppgifterna ut leverantörens system, bör utlämnandet ske successivt så snart uppgifterna blir tillgängliga för

leverantören. Större leverantörer förutsätts ha de tekniska och administrativa förutsättningarna för att påbörja en verkställighet dygnet runt, årets alla dagar. Om behovet av skyndsamhet är stort bör således verkställigheten kunna påbörjas av dessa aktörer inom mycket kort tid även under kvällar och helger. De begärda uppgifterna ska härefter lämnas ut så snart de finns tillgängliga för ett utlämnande.

I *tredje stycket* regleras kostnadsansvaret vid utlämnande av uppgifter om elektronisk kommunikation från leverantörer till Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som har till uppgift att ingripa mot brott. Stycket är tillämpligt även om utlämnandet inte sker i brottsbekämpande syfte. Det är således tillämpligt vid utlämnande av uppgifter om försvunna personer. Bestämmelsen innebär att en leverantör som lämnar ut uppgifter till en brottsbekämpande myndighet med stöd av 6 kap. 22 § första stycket LEK, 27 kap. RB, preventivlagen, lagen om särskild utlänningskontroll eller inhämtningslagen har rätt till ersättning för kostnader som uppstår när uppgifterna lämnas ut. Ersättningen ska betalas av den myndighet som har begärt uppgifterna. Post- och telestyrelsen har enligt 36 § FEK rätt att meddela föreskrifter om ersättningen.

I *fjärde stycket* anges att vad som föreskrivs om uppgifter i andra och tredje styckena även gäller lokaliseringsuppgifter som inte är trafikuppgifter. Således ska regleringen i andra och tredje styckena gälla även när de uppgifter som lämnas ut avser den geografiska positionen för en elektronisk kommunikationsutrustning utan att det är fråga om trafikuppgifter.

I *femte stycket* upplyses om att regeringen eller den myndighet regeringen bestämmer får meddela närmare föreskrifter om frågor som avses i första–fjärde styckena och får i enskilda fall besluta om undantag från kraven i första stycket. Ändringen innebär att regeringen eller den myndighet regeringen bestämmer får meddela närmare föreskrifter om format och om utlämnande av uppgifter utan dröjsmål liksom om leverantörers rätt till ersättning när uppgifter lämnas ut, under de förutsättningar som anges i andra–fjärde styckena. Av 36 § FEK framgår att Post- och telestyrelsen får meddela föreskrifter om kravet på format och utlämnande av uppgifter utan dröjsmål samt om leverantörernas rätt till ersättning när uppgifter lämnas ut.

22 § Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och därvid har fått del av eller tillgång till uppgift som avses i 20 § första stycket ska på begäran lämna

– –

2. uppgift som avses i 20 § första stycket 1 och som gäller misstanke om brott *eller brottslig verksamhet* till *Åklagarmyndigheten, Ekobrottsmyndigheten*, Polismyndigheten, Säkerhetspolisen eller någon annan myndighet som ska ingripa mot brottet *eller den brottsliga verksamheten*,

– –

Paragrafen innehåller bestämmelser om leverantörers skyldighet att på begäran lämna ut vissa uppgifter utan hinder av tystnadsplikt.

Mindre justeringar har gjorts i *första stycket 2*. Övervägandena finns i avsnitt 6.5. Det har i bestämmelsen förtydligats att leverantörernas skyldighet att lämna ut uppgifter om abonnemang gäller även i de fall en brottsbekämpande myndighet behöver uppgifterna i myndighetens underrättelseverksamhet. Det har också förtydligats att utlämnande får ske till både Åklagarmyndigheten och Ekobrottsmyndigheten.

23 a § *Den som tillhandahåller en förbetald allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst eller en förbetald internetanslutningstjänst får inte ge tillgång till tjänsten, om inte denne har registrerat abonnentens namn, adress, personnummer eller motsvarande och nummer för tjänsten. Uppgifterna ska finnas tillgängliga hos tillhandahållaren från registreringen och i ett år efter att tillhandahållandet har upphört.*

I samband med registreringen ska abonnentens identitet kontrolleras genom en giltig identitetshandling med fotografi eller en tillförlitlig elektronisk identifiering. Saknar abonnenten en identitetshandling ska identiteten göras sannolik på annat sätt. Identitetskontrollen ska dokumenteras.

Regeringen eller den myndighet som regeringen bestämmer får med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om identitetskontrollen enligt andra stycket.

I paragrafen, som är ny, föreskrivs en skyldighet att registrera abonnemangsuppgifter för förbetalda tjänster, dvs. kontantkort. Frågan har behandlats i avsnitt 5.6.2.

I *första stycket* anges att den som tillhandahåller en förbetald allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst eller en förbetald internetanslutningstjänst inte får ge tillgång till tjänsten om inte denne först har registrerat vissa uppgifter om

abonnenten. Registreringsskyldigheten omfattar de mobiloperatörer som tillhandahåller förbetalda tjänster som ger tillgång till telefoni eller internetanslutning. Regleringen gäller inte för den som tillhandahåller tjänster som helt eller huvudsakligen utgörs av överföring av signaler, såsom överföringstjänster som används för tillhandahållande av maskin till maskin-tjänster. De kontantkort som ska registreras är sådana kort som ger tillgång telefonitjänster eller internetanslutningstjänster och som därmed kan användas för att ringa, sända textmeddelanden eller surfa på internet. Det är tillgången till de förbetalda tjänsterna som avgör om det föreligger en registreringsplikt. För det fall kontantkort som ger tillgång till telefonitjänster eller internetanslutningstjänster används för kommunikation mellan maskiner omfattas de därför av registreringskravet.

De uppgifter som ska registreras avser den som har införskaffat ett kontantkort eller på annat sätt har ingått avtal med en mobiloperatör som tillhandahåller aktuella tjänster. Registreringsskyldigheten omfattar såväl fysiska som juridiska personer. De uppgifter som ska registreras är abonnentens nummer, namn, adress och personnummer eller motsvarande. Med begreppet motsvarande avses t.ex. samordningsnummer eller uppgift om när personen är född. Ett organisationsnummer innefattas också i begreppet för det fall abonnenten är en juridisk person. Tillhandahållaren ska registrera uppgifterna innan tjänsten får tas i bruk. Det ska alltså inte vara möjligt att ringa eller ta emot samtal eller att skicka eller ta emot textmeddelanden innan en registrering har skett. Inte heller ska det vara möjligt att surfa på internet om inte en registrering har gjorts. De registrerade uppgifterna ska finnas tillgängliga hos mobiloperatören från registreringen och i ett år efter att tillhandahållandet av tjänsten har upphört.

I *andra stycket* föreskrivs att abonnentens identitet ska kontrolleras genom en giltig identitetshandling med fotografi eller en tillförlitlig elektronisk identifiering. Med en giltig identitetshandling med fotografi avses t.ex. passhandling, id-kort, körkort eller liknade handling. Ett s.k. LMA-kort kan också godtas för identifieringen. Även utländska identitetshandlingar med fotografi kan godtas. Om en registrering sker via internet eller vid kontakt med kundtjänst kan identitetskontrollen ske genom en tillförlitlig elektronisk identifiering. Härmed avses i första hand en e-legitimation, såsom bankID.

För det fall en abonnent saknar identitetshandling kan identiteten göras sannolik på annat sätt. Om kunden t.ex. är ett barn som saknar identitetshandlingar kan en nära anhörig, med en godkänd svensk identitetshandling, intyga identiteten. För en kund som är en juridisk person kan lämnade uppgifter kontrolleras gentemot registerutdrag eller andra tillförlitliga uppgifter. Den som företräder den juridiska personen ska kunna styrka detta. Omfattningen av kontrollåtgärderna bör baseras på den risk för felaktig registrering som kan anses föreligga i det enskilda fallet. Identitetskontrollen ska dokumenteras. Detta kan ske t.ex. genom en anteckning om vilken identitetshandling som har använts.

I *tredje stycket* upplyses om att regeringen eller den myndighet regeringen bestämmer får meddela närmare föreskrifter om identitetskontrollen enligt andra stycket. Av 46 § FEK framgår att Post- och telestyrelsen får meddela föreskrifter om identitetskontrollen.

23 b § *Om en förbetald tjänst som har registrerats enligt 23 a § har överlåtits till någon annan utan att en ny registrering har skett, ska tillhandahållandet av tjänsten avbrytas.*

Vad som sägs i första stycket gäller inte om tjänsten

1. har överlåtits till en närstående,

2. har införskaffats av en juridisk person och används på dennes uppdrag, eller

3. har införskaffats på uppdrag av Försvarsmakten, Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som har till uppgift att ingripa mot brott.

Paragrafen är ny. Den reglerar överlåtelse av en registrerad förbetald tjänst. Frågan har behandlats i avsnitt 5.6.2.

I *första stycket* föreskrivs att om en förbetald tjänst som har registrerats enligt 23 a § har överlåtits till någon annan utan att en ny registrering har skett, ska tillhandahållandet av tjänsten avbrytas. I begreppet överlåtelse ligger att det ska vara fråga om en beständig överföring av en äganderätt. Bestämmelsen hindrar således inte att en förbetald tjänst vid något tillfälle utnyttjas av någon annan än den registrerade abonnenten, t.ex. för att ringa något samtal. Om tjänsten däremot säljs vidare, överlåts till annan på annat sätt eller inte helt kort lånas ut till annan utan att en ny registrering enligt 23 a § görs, och detta kommer till operatörens kännedom, ska tillhandahållandet av tjänsten avbrytas. En indikation på att en

förbetald tjänst har överlåtits utan att en ny registrering har skett kan vara att en enskild har låtit registrera sig som abonnent för en stor mängd förbetalda tjänster utan att det finns någon rimlig förklaring till det.

I *andra stycket* finns intaget vissa undantag från huvudregeln i första stycket. Vad som sägs i första stycket gäller för det första inte om en förbetald tjänst har överlåtits till en närstående. Det är således enligt regleringen möjligt att lämna kontantkort vidare till en närstående utan att en ny registrering behöver ske. Med närstående avses normalt abonnentens barn, maka eller make, sambo, föräldrar eller mor- och farföräldrar. Även andra personer bör dock kunna ses som närstående. En bedömning får göras i det enskilda fallet. För det andra behöver inte en ny registrering ske när en förbetald tjänst som har införskaffats av en juridisk person används på dennes uppdrag av t.ex. dennes personal eller uppdragstagare. För att undantagsregeln ska bli tillämplig förutsätts att den juridiska personen har kännedom om vem i personalen eller bland uppdragstagarna som använder den aktuella tjänsten. Om så inte är fallet, och detta kommer till operatörens kännedom, ska alltså tillhandahållandet av tjänsten avbrytas. För det tredje behöver inte en ny registrering ske när en förbetald tjänst som har införskaffats på uppdrag av Försvarsmakten, Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som har till uppgift att ingripa mot brott, lämnas vidare till annan.

Ikraftträdande- och övergångsbestämmelser

1. Denna lag träder i kraft den 1 januari 2022.

2. En förbetald allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst eller en förbetald internetanslutningstjänst som har tillhandahållits innan lagen trädde i kraft får tillhandahållas till och med den 1 juli 2022 trots att en registrering inte skett i enlighet med 6 kap. 23 a §.

Ikraftträdande- och övergångsbestämmelserna behandlas i avsnitt 7.

Enligt *punkt 1* träder bestämmelserna i kraft den 1 januari 2022.

Punkt 2 anger att en förbetald allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst eller en förbetald internetanslutningstjänst som har tillhandahållits innan lagen trädde i kraft får tillhandahållas till och med den 1 juli 2022 trots att en registrering

inte skett i enlighet med 6 kap. 23 a §. Det innebär att en förbetald tjänst som har tagits i bruk innan lagen trädde i kraft är möjlig att använda i sex månader efter lagens ikraftträdande utan att en registrering har skett. Om en registrering inte har skett inom denna tid ska dock tillhandahållandet av tjänsten upphöra.

Regeringskansliet

Promemoria

2019-08-27
Ju2019/02816/LP

Justitiedepartementet

Uppdrag att föreslå en registreringsskyldighet för kontantkort och att se över vissa frågor om verkställighet

Sammanfattning av uppdraget

En utredare ska biträda Justitiedepartementet och lämna förslag till regler om en skyldighet att registrera uppgifter om abonnemang för kontantkort. Syftet är att uppgifterna ska finnas tillgängliga för brottsbekämpande ändamål.

I utredarens uppdrag ingår även att se över vissa verkställighetsfrågor. Utredaren ska överväga behovet av förändrade regler dels för leverantörers skyldighet att medverka till att uppgifter kan hämtas in av brottsbekämpande myndigheter, dels för leverantörers skyldighet att bedriva sin verksamhet på ett sätt som innebär att uppgifter görs tillgängliga så att informationen enkelt kan tas om hand av de brottsbekämpande myndigheterna. Syftet är att möjliggöra att de uppgifter som lämnas ut för brottsbekämpande ändamål ska kunna komma till avsedd användning på ett effektivt sätt. I uppdraget ingår även att se över kraven på leverantörers skyndsamhet vid utlämning av uppgifter och ordningen för ersättning när uppgifter lämnas ut. Slutligen ska utredaren ta ställning till behovet av förändrade rutiner hos de brottsbekämpande myndigheterna när uppgifter hämtas in från leverantörerna.

Uppdraget ska redovisas senast den 1 juni 2020.

Uppdraget att föreslå en registreringsskyldighet för kontantkort till mobiltelefoner

Det finns ett påtagligt behov av uppgifter för brottsbekämpande ändamål på området för elektronisk kommunikation

Tillgången till uppgifter från elektronisk kommunikation är ofta avgörande för att utredningar om allvarlig brottslighet ska föras framåt. Bestämmelser som ger de brottsbekämpande myndigheterna tillgång till sådana uppgifter finns främst i 27 kap. rättegångsbalken.

Uppgifterna är även avgörande för att i underrättelseverksamhet upptäcka, förebygga och förhindra brottslig verksamhet. Förutsättningarna för att få tillgång till uppgifterna utanför en förundersökning regleras i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen), lagen (1991:572) om särskild utlänningskontroll (LSU) och lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen).

I lagen (2003:389) om elektronisk kommunikation (LEK) regleras de brottsbekämpande myndigheternas tillgång till uppgifter på det aktuella området i vissa andra fall, t.ex. tillgången till uppgift om abonnemang som gäller misstanke om brott (6 kap. 22 § första stycket 2).

Uppgifter om abonnemang är ofta en förutsättning för hemliga tvångsmedel

Både i underrättelseverksamhet och i förundersökningsverksamhet behöver brottsbekämpande myndigheter ofta veta vem som har ett visst telefonnummer eller vilket telefonnummer en viss person har. Det är normalt en förutsättning för att myndigheterna ska få tillstånd att avlyssna eller övervaka elektronisk kommunikation och för att sådana beslut ska kunna verkställas (se t.ex. 27 kap. 20 och 21 §§ rättegångsbalken, 8 § preventivlagen, se även prop. 1994/95:227 s. 21). Uppgifter om abonnemang kan också läggas till grund för utredningsåtgärder som inte kräver att hemliga tvångsmedel används.

Nuvarande ordning innebär att tillgången till abonnemangsuppgifter ytterst beror på om tjänsteleverantören behöver uppgifterna för egna ändamål

För att säkerställa tillgången till vissa uppgifter för brottsbekämpande ändamål föreskrivs en skyldighet för vissa leverantörer att lagra data, däribland sådana uppgifter om abonnemang som är nödvändiga för att spåra och identifiera kommunikationskällan (6 kap. 16 a § LEK, se även prop. 2018/19:86 om den s.k. Tele2-domen och om regeringens förslag till anpassningar av reglerna).

Lagringsskyldigheten förutsätter dock att den enskilde leverantören har genererat eller behandlat uppgiften (6 kap. 16 a § andra stycket LEK). Uppgiften behöver inte ha varit föremål för en mer konkret hantering eller användning men lagringsskyldigheten förutsätter att uppgiften någon gång har funnits hos leverantören, även om det bara rör sig om en ytterst kort tid. Leverantörer har däremot varken någon rätt eller skyldighet att samla in abonnemangsuppgifter som de inte behöver för egna ändamål även om uppgifterna omfattas av lagringsskyldigheten. (Se prop. 2010/11:46 s. 77.)

Möjligheten för brottsbekämpande myndigheter att få tillgång till abonnemangsuppgifter är sålunda avhängig av vilka uppgifter som leverantören behandlar. Detta är i sin tur beroende av vilka uppgifter som leverantören behöver för egna ändamål.

Behovet av en utredning om en registreringsskyldighet för kontantkort

Som framgår ovan behöver den misstänkte i regel kunna knytas till ett telefonnummer för att en avlyssning eller en övervakning ska kunna komma till stånd. Eftersom identiteten hos den som har ett kontantkort sällan behövs för fakturering förblir sådana abonnenter i regel anonyma för leverantören. Det leder till att de brottsbekämpande myndigheterna inte har möjlighet att få ut abonnemangsuppgifter som ofta är nödvändiga för att avlyssna eller övervaka elektronisk kommunikation. Många personer involverade i organiserad brottslighet känner till detta och använder oregistrerade kontantkort i syfte att försvåra för brottsbekämpande myndigheter att knyta telefonnumret till den misstänkte och sålunda kunna avlyssna eller övervaka elektronisk kommunikation. En registrerings-skyldighet skulle kunna leda till en säkrare tillgång till abonnemangsuppgifter och därmed till förbättrade förutsättningar att bekämpa allvarlig brottslighet.

Frågan om det borde införas en skyldighet för leverantörer att registrera uppgifter om abonnemang för kontantkort har övervägts i ett tidigare lagstiftningsärende (prop. 2011/12:55). Den dåvarande regeringen gjorde bedömningen att en sådan skyldighet inte borde införas. Regeringen uttalade visserligen att de brottsutredande myndigheternas hade ett påtagligt behov av att få tillgång till uppgifter om abonnemang avseende kontantkort men bedömde samtidigt att det fanns stora problem förknippade med ett system för registrering av abonnemangsuppgifter till kontantkort. Regeringen konstaterade att en registreringsskyldighet skulle innebära dels ett åliggande för leverantörer med kostnader som följd, dels en skyldighet för den som köper ett kontantkort att ge upp sin anonymitet. Regeringen konstaterade också att det var osäkert hur effektiv en registreringsskyldighet skulle bli från brottsbekämpningssynpunkt. Tvivlen på effektiviteten grundades bl.a. på att man inte heller med en registreringsskyldighet skulle kunna säkerställa att den som har eller använder ett visst telefonnummer också alltid är den som finns registrerad. En registreringsskyldighet skulle inte heller förhindra att anonyma kontantkort köptes utomlands och utnyttjades i Sverige i brottsliga sammanhang. (Se samma prop. s. 104–105.)

Det är problematiskt att tillgången till betydelsefulla verktyg i brottsbekämpningen är kringskuren för att grundläggande abonnemangsuppgifter ofta inte finns att tillgå när telefonnumret är hänförligt till en förbetald tjänst i form av ett kontantkort. Det finns dessutom tecken på att behovet att avlyssna och övervaka elektronisk kommunikation ökar. Det gäller särskilt i förundersökningar som avser våldsbrott. Till exempel har det antagits att den ökning som har noterats av antalet beviljade tillstånd till hemlig avlyssning av elektronisk kommunikation är kopplad till en ökning av det grova våldet mellan kriminella aktörer med koppling till kriminella nätverk i utsatta områden (skr. 2018/19:19). Oregistrerade kontantkort är vanligt förekommande bland personer med koppling till den organiserade brottsligheten (se t.ex. SOU 2012:44 s. 221 och SOU 2017:89 s. 185). Det kan visserligen noteras att ökningen av våldsbrott mellan kriminella aktörer också har lett till en viss ökning av antalet beviljade tillstånd. Samtidigt kan det antas att de brottsbekämpande myndigheterna på grund av förekomsten av oregistrerade kontantkort i många fall saknar tillgång till nödvändiga uppgifter om abonnemang som har koppling till kriminella nätverk.

Kontantkort används även av personer med koppling till internationell terrorism (se t.ex. Säkerhetspolisens årsbok 2018 s. 55–56). Med hjälp av oregistrerade kontantkort inköpta i Sverige kan konton för webbaserade tjänster skapas i anonymitet och användas för krypterad kommunikation mellan medlemmar i utländska terroristorganisationer.

En registreringsskyldighet skulle kunna bidra till att uppgifter från elektronisk kommunikation oftare kan göras åtkomliga för brottsbekämpande ändamål. Vissa av de tvivel som tidigare har förts fram i fråga om effektiviteten i en registreringsskyldighet kan dock vara giltiga alltjämt och bör undersökas närmare, liksom möjligheten att begränsa användandet av oregistrerade kontantkort köpta utomlands.

De bedömningar som görs och de förslag som lämnas måste naturligtvis vara förenliga med svensk grundlag. Över huvud taget är det viktigt att skyddet för grundläggande fri- och rättigheter, t.ex. tryck- och yttrandefriheten, noga beaktas. I det sammanhanget kan det noteras att det kan finnas högst legitima behov av att kunna teckna abonnemang utan att avslöja sin identitet, exempelvis när den grundlagsskyddade meddelarfriheten utövas. Det kan även noteras att de praktiska förutsättningarna för olika grupper i samhället att styrka sin identitet varierar och att det finns de som saknar ekonomiska förutsättningar att teckna abonnemang på kredit.

Nyttan av en registreringsskyldighet måste vägas mot de ekonomiska konsekvenserna och andra effekter för leverantörer och andra som berörs. Leverantörerna är visserligen verksamma inom ett område där skyddet för centrala samhällsintressen ibland måste tillåtas få genomslag (prop. 1995/96:180 s. 32 och prop. 2010/11:46 s. 66). Hänsyn måste dock tas till intresset av att enskilda och myndigheter har tillgång till säkra och effektiva elektroniska kommunikationer och största möjliga utbyte vad gäller urvalet av elektroniska kommunikationstjänster samt deras pris och kvalitet (1 § första stycket LEK).

I ljuset av den utveckling som skett finns det sammantaget skäl att på nytt överväga frågan om en registreringsskyldighet avseende kontantkort bör införas.

En utredare ska

- ta ställning till om det bör införas en skyldighet att registrera uppgifter om abonnemang avseende kontantkort för att säkerställa att uppgifterna finns tillgängliga för brottsbekämpande ändamål, och
- lämna förslag till regler om en skyldighet att registrera uppgifter om abonnemang avseende kontantkort, även om ställningstagandet inte föranleder det.

I uppdraget ingår att överväga om nuvarande regler om tillsyn och sanktioner är tillräckliga för att säkerställa att en registreringsskyldighet efterlevs.

Uppdraget att se över vissa frågor om verkställighet

Leverantörer är skyldiga att anpassa sin verksamhet och att medverka när ett tvångsmedelsbeslut verkställs

De leverantörer som enligt LEK tillhandahåller allmänna kommunikationsnät eller en elektronisk kommunikationstjänst (t.ex. den som tillhandahåller telefonabonnemang) spelar en viktig roll när brottsbekämpande myndigheter hämtar in uppgifter på området för elektronisk kommunikation. För att inhämtningen ska upprätthålla en rimlig effektivitet har leverantörer ålagts vissa skyldigheter. De är bl.a. skyldiga att bedriva sin verksamhet så att uppgifter görs tillgängliga på ett sådant sätt att informationen enkelt kan tas om hand. I fråga om den närmare innebörden av den s.k. anpassningsskyldigheten sägs i lagmotiven att den i praktiken innebär främst ett krav på leverantören att använda sig av tekniska hjälpmedel som har vissa egenskaper. Det sägs dessutom att sådana personella och organisatoriska dispositioner måste vidtas som krävs för att hantera hjälpmedlen. (Se prop. 1995/96:180 s. 25.)

Vid sidan av anpassningsskyldigheten anses leverantörer vara skyldiga att medverka i viss utsträckning till att tvångsmedelsbeslut kan verkställas (samma prop. s. 22).

Att uppgifter lämnas ut i skilda format medför ett resurskrävande och tidsödande arbete

Trots den ovan nämnda anpassningsskyldigheten och skyldigheten att medverka har det framkommit att utlämnade uppgifter förekommer i skilda

format beroende på vilken leverantör som tillhandahåller uppgifterna. Även sammanställningar från en och samma leverantör förekommer ibland i olika format. De ingående uppgifternas inbördes ordning kan skifta och de specificeras inte med utgångspunkt från någon gemensam teknisk standard. Många gånger förutsätts att leverantören kan ge vägledning om innebörden av olika upplysningar för att det ska framgå vad de betyder.

Myndigheterna behöver konvertera uppgifterna innan de kan komma till avsedd användning i analysarbetet. Konverteringen är nödvändig för att ordna och specificera uppgifter från olika sammanställningar enligt en gemensam standard, liksom för att göra vissa specifikationer läsbara.

Avsaknaden av en gemensam standard för utlämnade uppgifter medför alltså att värdefull tid och viktiga resurser går åt till att konvertera uppgifter till ett likvärdigt och läsbart format. Enligt vad som har framkommit kan detta arbete många gånger vara utdraget och komplicerat. Till detta kommer att konverteringen inte utgör någon garanti för att det eftersträvade resultatet kan uppnås. När uppgifterna behandlas kan nämligen felaktigheter uppkomma som upptäcks först i analysfasen. Avsaknaden av en gemensam standard påverkar alltså även tillförlitligheten av de uppgifter som ingår i analysen.

Det är problematisk att de brottsbekämpande myndigheternas tillgång till uppgifter på området för elektronisk kommunikation försvåras av att utlämnade uppgifter förekommer i olika format. Särskilt allvarligt är detta i brådskande fall. Den tid som går åt till att behandla uppgifter i skilda format kan i värsta fall medföra att avgörande utredningsåtgärder inte kan genomföras eller att ett förestående brott inte kan förhindras.

Behovet av en utredning om vissa verkställighetsfrågor

Skyldigheterna att medverka och att verksamhetsanpassa kan behöva förtydligas

En förklaring till de problem som redogörs för i det föregående är att det inte i alla avseenden finns någon gemensam uppfattning om hur reglerna ska tillämpas. Den nuvarande ordningen kan vara en följd av hur reglerna i 6 kap. 16 f och 19 §§ LEK är utformade. Bestämmelserna kan vara svåra att tolka och i vissa situationer är det dessutom oklart hur reglerna förhåller sig till varandra. Det förekommer dessutom fall där det kan vara svårt att avgöra

om en fråga ska hänföras till anpassningsskyldigheten eller om den snarare ska bedömas i ljuset av den skyldighet att medverka som följer av 27 kap. 25 § rättegångsbalken eller allmänna principer (jfr prop. 1995/96:180 s. 22).

Det kan härtill ifrågasättas om regeringens rätt att meddela föreskrifter om anpassningsskyldigheten kan läggas till grund för att lösa de tillämpningssvårigheter som finns (6 kap. 19 § tredje stycket LEK). En följd av de otydligheter som föreligger är nämligen att även bemyndigandets räckvidd kan framstå som mindre klart. Av samma skäl kan det ifrågasättas om Post- och telestyrelsen har rätt att meddela föreskrifter, t.ex. regler som innebär att ett visst gemensamt format ska tillämpas för utlämnade uppgifter. Till detta kommer att det över huvud taget inte finns någon föreskriftsrätt kopplad till den särskilda anpassningsskyldighet som regleras i 6 kap. 16 f § LEK.

Det finns även fall när uppgifter hämtas in utan att reglerna i vare sig 6 kap. 16 f eller 19 § LEK är tillämpliga. Som exempel kan nämnas vissa av de situationer som föreligger när uppgifter hämtas in med stöd av 6 kap. 22 § LEK eller inhämtningslagen. Med avseende på sådana situationer föreskrivs över huvud taget inte någon anpassningsskyldighet.

Det är viktigt att en acceptabel kvalitet och effektivitet kan upprätthållas när uppgifter från elektronisk kommunikation hämtas in för brottsbekämpande ändamål. Tydligare regler kan bidra till detta. Tydliga regler ger också goda förutsättningar för leverantörer och brottsbekämpande myndigheterna att hitta gemensamma lösningar på vissa av de problem som finns. Leverantörers skyldighet att på olika sätt medverka vid verkställighet av beslut på området för elektronisk kommunikation behöver förtydligas. Detsamma gäller i fråga om anpassningsskyldigheten. Tydligare krav på leverantörerna skulle kunna förbättra förutsättningarna att bekämpa allvarlig brottslighet och därmed tillgodose ett tungt vägande samhällsintresse. Det är samtidigt viktigt att regleringens ekonomiska och administrativa konsekvenser för leverantörerna står i rimlig proportion till vad som står att vinna med den. Det är likaså viktigt att de brottsbekämpande myndigheterna hämtar in uppgifter på ett sätt som underlättar för leverantörerna att hantera framställningarna. Det kan finnas fördelar med att enhetliga rutiner tillämpas för hur en begäran ska utformas och framställas.

Det finns mot den angivna bakgrunden skäl att se över reglerna om leverantörers skyldighet att medverka och verksamhetsanpassa för att

möjliggöra att utlämnade uppgifter enkelt kan tas om hand. Det kan då övervägas om regler bör införas som möjliggör att inhämtade uppgifter följer en gemensam standard. Även de brottsbekämpande myndigheternas rutiner för att hämta in uppgifter bör analyseras och vid behov bör ändringar av dessa övervägas.

Skyndsamhetskravet kan behöva utvidgas och förtydligas

Som har konstaterats i tidigare lagstiftningsärenden kan det uppstå beaktansvärda behov att använda tvångsmedel med mycket kort varsel. Även abonnemangsuppgifter måste ibland hämtas in skyndsamt, inte minst för att inhämtningen av andra uppgifter ska kunna uppfylla sitt avsedda ändamål. En snabb verkställighet kan i vissa fall vara absolut nödvändig för att skydda allmänheten eller för att kunna föra en utredning framåt. Som också har framhållits har behovet av snabba beslut påverkats av den utveckling som skett inom teknik och kommunikation, bl.a. eftersom de förbättrade kommunikationsmöjligheterna innebär att planer med kort varsel kan ändras samt att de misstänkta snabbt och ofta kan byta telefonnummer eller annan adress. (Se prop. 2013/14:237 s. 138 med hänvisningar.) Det är självklart att fattade beslut också måste kunna verkställas skyndsamt. Behovet att snabbt få tillgång till uppgifter kan uppstå även vid tider när leverantörers beredskap för detta normalt är begränsad.

Det framgår av 6 kap. 16 f § LEK att lagringsskyldiga leverantörer, förutom att göra uppgifter tillgängliga så att informationen enkelt kan tas om hand, ska bedriva verksamheten så att uppgifter kan lämnas ut utan dröjsmål (jfr Post- och telestyrelsens beslut den 12 september 2017, dnr 16-2818).

De tillämpningssvårigheter som nämnts när det gäller anpassningsskyldigheten i allmänhet gäller också i fråga om skyndsamhetskravets tillämpning i vissa fall. Det finns delade meningar om det närmare tillämpningsområdet för det skyndsamhetskrav som föreskrivs i 6 kap. 16 f § LEK. Det finns dessutom olika uppfattningar om den närmare innebörden av det krav på skyndsamhet som kan anses följa av anpassningsskyldigheten i 6 kap. 19 § LEK. Över huvud taget finns oklarheter när det gäller den skyndsamhet som gäller i olika situationer. Det har vidare framkommit att de brottsbekämpande myndigheternas behov att snabbt få tillgång till eftersökta uppgifter inte alltid tillgodoses.

Det är otillfredsställande att möjligheterna att i brådskande fall hämta in uppgifter kan vara beroende av hur den enskilde leverantören har valt att organisera nödvändig beredskap.

Det finns mot bakgrund av detta skäl att överväga om skyndsamhetskravet i 6 kap. 16 f § LEK behöver förtydligas. Det kan vidare finnas skäl att överväga ett uttryckligt skyndsamhetskrav även i fall som inte omfattas av regleringen i nämnda paragraf. Det bör till exempel övervägas om ett generellt skyndsamhetskrav bör gälla även i fall när inhämtningen sker i realtid och när inhämtningen avser abonnemangsuppgifter. Det kan i det sammanhanget behöva övervägas om regeringens föreskriftsrätt bör utvidgas.

Reglerna om rätt till ersättning för kostnader när uppgifter lämnas ut kan behöva ändras

Den som är skyldig att lagra uppgifter enligt 6 kap. 16 a § LEK har rätt till ersättning för kostnader som uppstår när lagrade uppgifter lämnas ut (6 kap. 16 e §). Ersättningen ska betalas av den myndighet som har begärt uppgifterna. Utgångspunkten är att leverantörerna ska få sina kostnader för att lämna ut trafikuppgifter ersatta (prop. 2010/11:46 s. 69).

Regeringen har tidigare uttalat att rätten till ersättning enligt 6 kap. 16 e § LEK avser endast sådana uppgifter som omfattas av lagringsskyldigheten (prop. 2018/19:86 s. 85). Detta innebär att Post- och telestyrelsens bemyndigande att meddela föreskrifter om ersättningen inte gäller kostnader som uppstår när uppgifter hämtas in i realtid (46 § förordningen [2003:396] om elektronisk kommunikation).

När det gäller kostnader som uppstår vid utlämnande av uppgifter som faller utanför regleringen bestäms ersättningsnivåerna efter förhandlingar mellan de brottsbekämpande myndigheterna och berörda leverantörer. Det innebär att ersättningsnivåerna kan variera mellan olika leverantörer. Det kan ifrågasättas om det är en rimlig ordning. Utredaren bör därför se över den nuvarande ordningen för ersättning och vid behov lämna förslag på förändringar.

Hänsyn bör tas till intresset av en sammanhållen reglering

De problem som beskrivits varierar till art och omfattning beroende dels på vilka regler som läggs till grund för att hämta in uppgifterna, dels på den typ

av uppgifter som eftersöks, dels på om inhämtningen avser uppgifter från förfluten tid eller inte. I ytterligare andra fall görs det skillnad mellan uppgifter som omfattas av lagringsskyldigheten och andra uppgifter. Utredaren ska vid utarbetandet av sina förslag ta hänsyn till intresset av en sammanhållen reglering. I denna del kan det noteras att de brottsbekämpande myndigheternas möjligheter att låta inhämtade uppgifter komma till avsedd användning ofta beror på regler i olika författningar som är avsedda att samspela.

Utredarens förslag ska dock inte innebära någon ändring av vilka uppgifter som de brottsbekämpande myndigheterna får hämta in. Det ligger inte heller i utredarens uppdrag att lämna förslag som innebär att lagringsskyldighetens omfattning ändras.

Närmare om uppdraget om vissa verkställighetsfrågor

Utredaren ska

- ta ställning till behovet av tydligare krav på hur och med vilken skyndsamhet uppgifter ska lämnas ut i fall när uppgifter hämtas in för brottsbekämpande ändamål, för att uppgifterna ska kunna komma till avsedd användning på ett effektivt sätt och lämna de förslag på författningsändringar som ställningstagandet föranleder,
- ta ställning till behovet av förändrade rutiner hos de brottsbekämpande myndigheterna när uppgifter hämtas in och föreslå nödvändiga förändringar, och
- ta ställning till om reglerna om rätt till ersättning för kostnader som uppstår när uppgifter lämnas ut för brottsbekämpande ändamål behöver ändras och föreslå nödvändiga författningsändringar.

Genomförande och redovisning av uppdraget

Utredaren får ta upp även andra frågor som har samband med de frågeställningar som ska utredas, om det bedöms nödvändigt.

Utredaren ska hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet och utredningsväsendet. Utredaren ska särskilt beakta arbetet med betänkandet Hemlig dataavläsning (SOU 2017:89) liksom regeringens förslag i propositionen Datalagring vid brottsbekämpning – anpassningar till EU-rätten (prop. 2018/19:86). Utredaren ska även beakta arbetet med att genomföra Europaparlamentets och rådets direktiv (EU)

2018/1972 om inrättande av en europeisk kodex för elektronisk kommunikation. Utredaren ska vidare beakta arbetet med kommissionens förslag till förordning om integritet och elektronisk kommunikation (COM [2017] 10). Utredaren kan även behöva beakta kommissionens förslag till förordning om tillgång till e-bevisning (COM [2018] 225) och direktiv om utseende av företrädare för insamling av e-bevisning (COM [2018] 226).

Utredaren ska beakta Sveriges EU-rättsliga och andra folkrättsliga förpliktelser. Utredaren ska i förhållande till dessa förpliktelser bedöma konsekvenserna av de förslag som lämnas och i det sammanhanget ta hänsyn bl.a. till EU-rättens krav på proportionalitet.

Utredaren ska beskriva förslagens effekter för företag. I det sammanhanget ska hänsyn tas bl.a. till vilka förändringar i verksamheten som företagen kan behöva vidta och till de kostnadsmässiga konsekvenserna av förslagen. Vidare måste hänsyn tas till intresset av att reglerna för företagen är enkla. De förslag som lämnas bör inte vara mer ingripande än vad som är nödvändigt med hänsyn till det som står att vinna med dem (jfr 2 § LEK).

Utredaren ska hämta in nödvändiga synpunkter och upplysningar från Polismyndigheten, Säkerhetspolisen, Tullverket och Post- och telestyrelsen samt från andra myndigheter och verksamhetsutövare som berörs av de aktuella frågorna.

Utredaren ska analysera och redovisa de ekonomiska konsekvenserna av förslagen. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna ska utredaren föreslå hur de ska finansieras.

Uppdraget ska redovisas senast den 1 juni 2020.

Departementsserien 2020

Kronologisk förteckning

1. Ett nytt brott om olovlig befattning med betalningsinstrument. Genomförande av non-cash-direktivet. Ju.
2. Uppenbart ogrundade ansökningar och fastställande av säkra ursprungsländer. Ju.
3. Konkurrensverkets befogenheter. N.
4. Klimatdeklaration för byggnader. Fi.
5. Kompletterande bestämmelser till utträdesavtalet mellan Förenade kungariket och EU i fråga om medborgarnas rättigheter. Ju.
6. Material och produkter avsedda att komma i kontakt med livsmedel. N.
7. Inkomstpensionstillägg. S.
8. En ny växtskyddslag. N.
9. Utökad målgrupp för Allmänna arvsfonden. S.
10. Ny lag om källskatt på utdelning. Fi.
11. Säkerhetsskyddsreglering för Regeringskansliet, utlandsmyndigheterna och kommittéväsendet. Ju.
12. Registrering av kontantkort, m.m. Ju.

Departementsserien 2020

Systematisk förteckning

En departementspromemoria arbetas fram inom Regeringskansliet. Den publiceras i departementsserien, förkortad Ds.

NORSTEDTS JURIDIK | KARNOV GROUP

106 47 Stockholm Tel 08-598 191 90 kundservice@nj.se www.nj.se

ISBN 978-91-38-25054-9 ISSN 0284-6012