Lagrådsremiss

Registrering av kontantkort – förbättrad tillgång till uppgifter för brottsbekämpande myndigheter

Regeringen överlämnar denna remiss till Lagrådet.

Stockholm den 10 februari 2022

Morgan Johansson

David Brandell
(Justitiedepartementet)

Lagrådsremissens huvudsakliga innehåll

Det är mycket vanligt att oregistrerade och anonyma kontantkort till mobiltelefoner används i samband med brottslig verksamhet. Det gör att brottsbekämpande myndigheter går miste om viktig och ibland avgörande information. I syfte att underlätta för brottsbekämpande myndigheter och försvåra för kriminella föreslår regeringen en registreringsskyldighet för vissa förbetalda tjänster som kan nås via till exempel kontantkort. Den som tillhandahåller en förbetald tjänst ska registrera uppgifter om abonnenten och kontrollera abonnentens identitet innan tjänsten börjar användas. Om en förbetald tjänst används av någon annan än den registrerade abonnenten ska tjänsten som huvudregel avbrytas.

Dessutom föreslår regeringen ändrade regler om utlämnande av uppgifter om elektronisk kommunikation till brottsbekämpande myndigheter. Förslagen innebär ett tydligare krav på format, ett utvidgat skyndsamhetskrav och en utvidgad reglering om ersättning.

Lagändringen föreslås träda i kraft den 1 augusti 2022.

Innehållsförteckning

1 Beslut

Regeringen har beslutat att inhämta Lagrådets yttrande över förslag till lag om ändring i lagen (2022:000) om elektronisk kommunikation.

2 Förslag till lag om ändring i lagen (2022:000) om elektronisk kommunikation

Härigenom föreskrivs i fråga om lagen (2022:000) om elektronisk kommunikation

dels att 9 kap. 23–25 §§ ska upphöra att gälla,

dels att nuvarande 9 kap. 26 § ska betecknas 9 kap. 23 §,

dels att 8 kap. 5 §, den nya 9 kap. 23 §, 9 kap. 29 och 33 §§, 12 kap. 1 § och rubriken närmast före 9 kap. 29 § ska ha följande lydelse,

dels att det ska införas fem nya paragrafer, 9 kap. 24–26, 29 a och 29 b §§, och närmast före 9 kap. 24 § en ny rubrik av följande lydelse,

dels att det närmast före 9 kap. 30 § ska införas en ny rubrik som ska lyda ”Signalspaning”.

Lydelse enligt lagrådsremissen Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation	*Föreslagen lydelse*
8 kap.	
5 §	
Den som är skyldig att lagra uppgifter enligt 9 kap. 19 § ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling.	
	Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § och som har förelagts enligt 27 kap. 16 § rättegångsbalken att bevara en viss lagrad uppgift ska avseende den uppgiften vidta sådana åtgärder som anges i första stycket.
Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om sådana skyddsåtgärder.	
9 kap.	
26 §	*23 §*
Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om	
1. vilka uppgifter som ska lagras enligt 19 §,	1. vilka uppgifter som ska lagras enligt 19 §, *och*
2. lagringstiden enligt 22 § första stycket*, och*	2. lagringstiden enligt 22 § första stycket*.*
3. ersättningen enligt 23 §.	

Registrering av förbetalda tjänster

24 §

Den som tillhandahåller en förbetald allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst eller en förbetald internetanslutningstjänst får inte ge tillgång till tjänsten utan att dessförinnan ha registrerat

1. abonnentens namn och postadress,

2. abonnentens personnummer, samordningsnummer, organisationsnummer eller annat identifieringsnummer, och

3. nummer eller annan beteckning för tjänsten.

Tillhandahållaren ska även ange tidpunkten för registreringen.

Uppgifterna ska finnas tillgängliga hos tillhandahållaren från och med registreringen till och med ett år efter att tillhandahållandet av tjänsten har upphört.

25 §

I samband med en registrering enligt 24 § ska abonnentens identitet kontrolleras genom en giltig identitetshandling eller en tillförlitlig elektronisk identifiering. Om abonnenten saknar sådana handlingar och verktyg får identiteten göras sannolik på annat sätt. Identitetskontrollen ska dokumenteras.

Om abonnenten är en juridisk person, gäller första stycket den som företräder den juridiska personen.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om identitetskontrollen.

26 §

Om en förbetald tjänst används av någon annan än den abonnent som har registrerats enligt 24 § utan att en ny registrering har

gjorts, ska tillhandahållandet av tjänsten avbrytas.

Första stycket gäller inte om

1. tjänsten endast tillfälligt används av någon annan än den registrerade abonnenten,

2. tjänsten används av en närstående till den registrerade abonnenten,

3. den registrerade abonnenten är en juridisk person och tjänsten används på dennes uppdrag,

4. tjänsten har införskaffats på uppdrag av Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som ska ingripa mot brott, eller

5. tjänsten har införskaffats på uppdrag av en myndighet som bedriver verksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet.

Hemlig avlyssning och signalspaning

Anpassning och ersättning för kostnader

29 §

En verksamhet ska bedrivas så att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs, om verksamheten avser tillhandahållande av

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

2. tjänster inom ett allmänt elektroniskt kommunikationsnät som består av

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

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

Innehållet i och uppgifter om avlyssnade eller övervakade meddelanden ska göras tillgängliga så att informationen enkelt kan tas om hand.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd 8 kap. 7 § regeringsformen meddela närmare före-

Regeringen eller den myndighet som regeringen bestämmer kan med stöd *av* 8 kap. 7 § regeringsformen meddela närmare före-

skrifter om frågor som avses i *denna paragraf* samt får i enskilda fall besluta om undantag från kravet i första stycket.

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

29 a §

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

Första stycket gäller även lokaliseringsuppgifter som inte är trafikuppgifter.

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

29 b §

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

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

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

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

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

33 §

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

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

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

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

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

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

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

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

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

h) Polismyndigheten, om myndigheten bedömer att uppgiften behövs i samband med underrättelse, efterforskning eller identifiering vid olyckor

eller dödsfall eller för att myndigheten ska kunna fullgöra en uppgift som avses i 12 § polislagen (1984:387),

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

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

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

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

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

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

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

12 kap.

1 §

Tillsynsmyndigheten ska ta ut en sanktionsavgift av den som inte

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

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

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

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

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

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

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

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

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

10. underrättar om integritetsincidenter i enlighet med 8 kap. 8 § och föreskrifter som har meddelats med stöd av den paragrafen,

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

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

13. *gör innehållet i och* uppgifter *om avlyssnade eller övervakade meddelanden* tillgängliga *så att informationen* enkelt kan tas om hand i enlighet med 9 kap. *29 § andra stycket* och föreskrifter som har meddelats i anslutning till det stycket,

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

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

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

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

---

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

2. En förbetald allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst eller en förbetald internetanslutningstjänst som har

tillhandahållits före ikraftträdandet får, även om någon registrering enligt 9 kap. 24 § inte har gjorts, tillhandahållas till och med den 1 februari 2023 eller den senare tidpunkt då en ny förbetalning görs.

3 Ärendet och dess beredning

Regeringen beslutade i juni 2014 att ge en särskild utredare i uppdrag att göra en översyn av vissa bestämmelser om elektronisk kommunikation i brottsbekämpningen (dir. 2014:101). Utredningen, som antog namnet Datalagringsutredningen, överlämnade i mars 2015 betänkandet Datalagring och integritet (SOU 2015:31). En sammanfattning av betänkandet i relevanta delar finns i *bilaga 1*. Utredningens lagförslag i relevanta delar finns i *bilaga 2*. Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 3*. Remissyttrandena finns tillgängliga i Justitiedepartementet (Ju2015/03153). I lagrådsremissen behandlar regeringen utredningens förslag om ett förtydligande av en bestämmelse om inhämtning av abonnemangsuppgifter. Utredningens övriga lagförslag har redan behandlats och i vissa fall lett till lagstiftning, se propositionen Datalagring vid brottsbekämpning – anpassningar till EU-rätten (prop. 2018/19:86, bet. 2018/19:JuU27, rskr. 2018/19:296).

I augusti 2019 fick en utredare i uppdrag att biträda Justitiedepartementet med att lämna förslag till regler om en skyldighet att registrera uppgifter om abonnemang för kontantkort i syfte att säkerställa att uppgifterna finns tillgängliga för brottsbekämpande ändamål. I uppdraget ingick även att se över vissa verkställighetsfrågor kopplade till de brottsbekämpande myndigheternas inhämtning av uppgifter på området för elektronisk kommunikation (Ju2019/02816). Utredaren överlämnade i juni 2020 departementspromemorian Registrering av kontantkort, m.m. (Ds 2020:12). En sammanfattning av promemorian och dess lagförslag finns i *bilaga 4* respektive *bilaga 5*. Promemorian har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 6*. Remissyttrandena finns tillgängliga i Justitiedepartementet (Ju2020/02095). I lagrådsremissen behandlar regeringen promemorians lagförslag.

Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (e-kodexdirektivet) ska genomföras i Sverige. Genom e-kodexdirektivet inrättas ett harmoniserat ramverk för bl.a. elektroniska kommunikationsnät och tjänster. För att genomföra direktivet har regeringen i lagrådsremissen Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation lämnat förslag till en ny lag om elektronisk kommunikation (nya LEK) som ska träda i kraft den 1 juni 2022 och ersätta lagen (2003:389) om elektronisk kommunikation (LEK). Regeringen utgår i detta lagstiftningsärende från att nya LEK kommer att få det innehåll som föreslås i den lagrådsremissen.

4 Registrering av kontantkort

4.1 Det bör införas en registreringsskyldighet för kontantkort

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

Promemorians bedömning överensstämmer med regeringens.

Remissinstanserna: En majoritet av remissinstanserna instämmer i eller har inga invändningar mot promemorians bedömning, däribland *Brottsförebyggande rådet*, *Ekobrottsmyndigheten*, *Hi3G Access AB*, *Kammarrätten i Stockholm*, *Polismyndigheten*, *Säkerhetspolisen*, *Tullverket*, *Åklagarmyndigheten* och *Säkerhets- och integritetsskyddsnämnden*. Ekobrottsmyndigheten framhåller särskilt att en registreringsskyldighet kan leda till en effektivare brottsbekämpning och ha en viss brottsförebyggande effekt. Även Åklagarmyndigheten och Tullverket framhåller att en registreringsskyldighet kan förväntas få positiva effekter för brottsbekämpningen. *Riksdagens ombudsmän* godtar avvägningen mellan å ena sidan behovet och nyttan för de brottsbekämpande myndigheterna och å andra sidan konsekvenserna för enskilda som i dag kommunicerar via oregistrerade kontantkort.

Unizon ställer sig positivt till syftet med en registreringsskyldighet, att försvåra kriminell verksamhet, och pekar på att mäns våld mot kvinnor också utövas via telefon och andra digitala kommunikationsmedel. Unizon anser dock att det är av högsta vikt att kvinnor och barn som utsätts för mäns våld har tillgång till anonym kommunikation.

Post- och telestyrelsen (PTS) konstaterar att det i promemorian förs ett utförligt resonemang kring varför en registreringsplikt bör införas och ifrågasätter inte att de brottsbekämpande myndigheterna har ett påtagligt behov av uppgifterna. Enligt PTS innebär en registreringsskyldighet samtidigt att en möjlighet att kommunicera anonymt försvinner. PTS framhåller dock att tillhandahållarna har en straffbelagd tystnadsplikt för de uppgifter de behandlar och att en registreringsskyldighet inte i sig innebär att den enskilda kontantkortsinnehavarens identitet röjs. PTS bedömer att tillhandahållarnas arbete för att skydda behandlade uppgifter kan antas bli än viktigare om en registreringsskyldighet införs.

Vissa remissinstanser, däribland S*veriges advokatsamfund*, *TU – Medier i Sverige (TU)* och *Utgivarna*, anser att det har gjorts en felaktig intresseavvägning på så sätt att fördelarna för brottsbekämpningen har överskattats medan nackdelarna för andra intressen har underskattats. Advokatsamfundet instämmer dock i att en registrering av kontantkort i och för sig skulle kunna försvåra för kriminella och underlätta för brottsbekämpande myndigheter. Flera aktörer inom telekom- och mediebranscherna, däribland *IT&Telekomföretagen*, *Journalistförbundet*, *Sveriges Radio AB* och *Tele2 Sverige AB*, motsätter sig att det införs en skyldighet att registrera uppgifter om abonnemang för kontantkort.

Journalistförbundet, Sveriges Radio AB, TU och Utgivarna anser att förslaget kan leda till negativa konsekvenser för den journalistiska verksamheten. Aktörerna pekar på att oregistrerade kontantkort används av personer som kontaktar media och att journalister kan förse källor med eller själva använda sig av sådana kontantkort. Tele2 Sverige AB anser att en registreringsskyldighet skulle innebära att kontantkortsmarknaden i Sverige skulle förändras i grunden och att betydande ekonomiska värden skulle riskera att omfördelas.

Justitiekanslern anser att registreringsskyldighetens inverkan på meddelarskyddet behöver övervägas mera noggrant i det fortsatta lagstiftningsarbetet. *Integritetsskyddsmyndigheten* (tidigare Datainspektionen) anser att en förutsättning för att det ska vara godtagbart att införa en registreringsskyldighet för kontantkort är att effektiviteten och det förväntade värdet av en sådan reglering väger tyngre än intrånget i den personliga integriteten och skyddet av enskildas fri- och rättigheter. *Hi3G Access AB* efterlyser klargöranden av uttrycket uppgift om abonnemang.

Skälen för regeringens bedömning

Abonnemangsuppgifter och andra uppgifter 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.

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

I samband med införandet av nya regler om datalagring 2019 anförde regeringen att det kunde ifrågasättas om det är lämpligt eller ens möjligt att definiera uppgifter om abonnemang endast utifrån vilken uppgift det är fråga om. Det ansågs i stället 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. Vissa remissinstanser hade då efterfrågat en definition i författningstext. Regeringen ansåg emellertid att det framgick av förarbeten och praxis vad som anses utgöra en uppgift om abonnemang. Mot denna bakgrund, och då det saknades beredningsunderlag, såg regeringen ingen möjlighet till och inte heller något omedelbart behov av

en författningsreglering (prop. 2018/19:86 s. 93 och 94). *Hi3G Access AB* efterlyser nu ytterligare klargöranden av vad som utgör abonnemangsuppgifter. Regeringen gör dock ingen annan bedömning än i det tidigare lagstiftningsärendet utan anser att det varken finns beredningsunderlag för eller något omedelbart behov av att definiera uttrycket uppgift om abonnemang i författning.

Brottsbekämpande myndigheters tillgång till abonnemangsuppgifter

Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst som inte är en nummeroberoende interpersonell kommunikationstjänst har tystnadsplikt i fråga om bl.a. uppgifter om abonnemang (9 kap. 31 § första stycket 1 nya LEK).

Trots tystnadsplikten har de brottsbekämpande myndigheterna rätt att få tillgång till abonnemangsuppgifter från tillhandahållarna, om uppgifterna gäller misstanke om brott som myndigheten ska ingripa mot (9 kap. 33 § första stycket 2 nya LEK). Abonnemangsuppgifter får också lämnas ut till brottsbekämpande myndigheter i vissa andra situationer, bl.a. vid delgivning samt efterforskning av försvunna personer (9 kap. 33 § första stycket 1 a och 4 nya LEK). Myndigheterna kan vidare få tillgång till abonnemangsuppgifter via tjänster för abonnentupplysning på samma sätt som enskilda personer, om abonnenten har samtyckt till att uppgifter publiceras i en abonnentförteckning (9 kap. 18 § nya LEK).

För att säkerställa tillgången till vissa uppgifter om elektronisk kommunikation för brottsbekämpande ändamål är tillhandahållare som omfattas av kravet på anmälan i 2 kap. 1 § nya LEK skyldiga att lagra vissa uppgifter, däribland sådana uppgifter om abonnemang som är nödvändiga för att spåra och identifiera kommunikationskällan. För att lagringsskyldigheten ska inträda krävs att den enskilda tillhandahållaren har genererat eller behandlat uppgifterna (9 kap. 19 § nya LEK). Uppgifterna behöver inte ha varit föremål för en mer konkret hantering eller användning, men lagringsskyldigheten förutsätter att uppgifterna någon gång har funnits hos tillhandahållaren. Tillhandahållarna har däremot inte någon skyldighet att samla in abonnemangsuppgifter som de inte behöver för egna ändamål, även om uppgifterna omfattas av lagringsskyldigheten, jfr propositionen Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG (prop. 2010/11:46 s. 77).

Huruvida de brottsbekämpande myndigheterna har möjlighet att få tillgång till abonnemangsuppgifter från tillhandahållarna beror därmed på vilka uppgifter som tillhandahållarna behandlar. Det är i sin tur avhängigt vilka uppgifter som tillhandahållarna behöver för sina egna ändamål. Tillhandahållarna har behov av att hålla register med uppgifter över abonnenter som har kontraktsabonnemang, främst för att kunna sköta sin fakturering. Eftersom en kontantkortsabonnents identitet sällan behövs för fakturering, förblir sådana abonnenter i regel anonyma för tillhandahållarna. Visserligen kan en registrering av en kontantkortskund göras hos en tillhandahållare av andra orsaker, t.ex. för att kunden ska få tillgång till vissa tjänster. Registreringen görs dock endast om kunden själv väljer det. Det stora flertalet kontantkortsabonnenter förblir oregistrerade och därmed anonyma för tillhandahållarna. Det innebär att de brottsbekämpande

myndigheterna saknar möjlighet att genom tillhandahållarnas försorg få tillgång till uppgifter om kontantkortsabonnenter.

Behovet och nyttan av en registreringsskyldighet

Det är mycket vanligt att oregistrerade och anonyma kontantkort till mobiltelefoner används i samband med brottslig verksamhet. I kriminella kretsar köps, byts och slängs såväl mobiltelefoner som oregistrerade kontantkort frekvent. I samband med grov brottslighet är det inte ovanligt att ett kontantkort aktiveras kort tid före brottet och därefter slängs. Under senare år har det i olika sammanhang konstaterats att användningen av oregistrerade kontantkort är vanligt förekommande bland personer med koppling till den organiserade brottsligheten, se betänkandena Datalagring och integritet (SOU 2015:31 s. 165) och Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet (SOU 2017:89 s. 185). Den anonymitet som användningen av oregistrerade kontantkort för med sig försvårar de brottsbekämpande myndigheternas arbete och gör att myndigheterna går miste om viktig och ibland avgörande information för att upptäcka, förebygga och förhindra brottslig verksamhet och för att beivra brott.

Tillgång till information om elektronisk kommunikation är ofta avgörande för framgång i brottsutredningar, särskilt utredningar om allvarlig brottslighet liksom brott som begås över internet. Detsamma gäller för att i underrättelseverksamhet upptäcka, förebygga och förhindra brottslig verksamhet. Exempel på tvångsmedel som kan ge tillgång till information om elektronisk kommunikation under en förundersökning är hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation, som regleras i rättegångsbalken. Förutsättningarna för att få tillgång till sådan information utanför en förundersökning regleras huvudsakligen 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. Sedan den 1 april 2020 finns också ett nytt hemligt tvångsmedel, hemlig dataavläsning, som enligt lagen (2020:62) om hemlig dataavläsning kan användas såväl under som utanför en förundersökning. Hemliga tvångsmedel kan också aktualiseras inom ramen för Sveriges internationella samarbete enligt lagen (2017:1000) om en europeisk utredningsorder och lagen (2000:562) om internationell rättslig hjälp i brottmål.

En förutsättning för att få använda hemlig avlyssning av elektronisk kommunikation är att åtgärden kan hänföras till antingen en adress, t.ex. ett telefonnummer, eller en elektronisk kommunikationsutrustning, t.ex. en 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. Att åtgärden konkretiseras med avseende på adress eller kommunikationsutrustning är en förutsättning såväl för tillstånd som för att beslutet ska vara praktiskt verkställbart (se t.ex. 27 kap. 20 och 21 §§ rättegångsbalken och 2 och 8 §§ preventivlagen.) I

normalfallet krävs att adressen eller utrustningen har en viss närmare anknytning till den misstänkte. Det är inte alltid nödvändigt att känna till den misstänktes namn, men de uppgifter som finns om personen ska vara i så hög grad särskiljande att förväxlingsrisk i praktiken saknas (JO 2006/07 s. 30). Kopplingen kan vara hänförlig till antingen ett innehav eller ett användande. Kravet innebär 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 adressen eller utrustningen under den tid som tillståndet avser (27 kap. 20 § första stycket rättegångsbalken, jfr 2 § preventivlagen).

För att det ska vara möjligt att utröna om det finns en koppling mellan ett telefonnummer och den skäligen misstänkte är det nödvändigt att ha tillgång till uppgifter om innehavaren av numret. Kunskap om innehavarens 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. Med hjälp av abonnemangsuppgifter som innehas av tillhandahållarna kan brottsbekämpande myndigheter på ett effektivt sätt knyta en viss person till ett visst nummer. Den möjligheten finns emellertid inte när det gäller oregistrerade kontantkort, eftersom abonnenterna i de fallen är anonyma för tillhandahållaren.

Utan tillgång till abonnemangsuppgifter som innehas av tillhandahållarna har 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 förundersökningsverksamhet och underrättelseverksamhet. 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.

I vissa situationer är det dock möjligt att använda hemlig övervakning av elektronisk kommunikation utan att ett nummer kan knytas till en misstänkt. Tvångsmedlet kan bl.a. användas för att hämta in uppgifter om vilka elektroniska kommunikationsutrustningar, t.ex. mobiltelefoner, 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 (s.k. basstationstömning, se 27 kap. 19 § första stycket 2 och 20 § andra stycket rättegångsbalken). Möjligheterna att använda tvångsmedlet i detta syfte är dock begränsade. När en sådan basstationstömning har gjorts medför avsaknaden av abonnemangsuppgifter dessutom att det är svårt att ur det inhämtade materialet sålla fram de uppgifter som är intressanta att arbeta vidare med. Om samtliga kontantkortskunder hade varit registrerade så hade det däremot 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, medför användningen av oregistrerade kontantkort även andra problem. Tillgången till abonnemangsuppgifter har betydelse för möjligheten att

utreda och beivra sådana brott som begås med hjälp av elektronisk kommunikation, t.ex. hot, bedrägerier och trakasserier via telefon. *Unizon* pekar i detta sammanhang på att mäns våld mot kvinnor också kan utövas via telefon och andra digitala kommunikationsmedel. Vidare kan abonnemangsuppgifter användas för att utreda vuxnas kontakter med barn i sexuellt syfte. Ett ytterligare problem är att oregistrerade kontantkort kan fungera som mobilt bredband och därmed användas för anonym kommunikation över internet. Oregistrerade kontantkort används även av brottsaktiva inom Säkerhetspolisens verksamhetsområde, t.ex. av personer inom extremistmiljöer.

Säkerhetspolisen har under de senaste åren även kunnat se ett nytt användningsområde för oregistrerade svenska kontantkort, nämligen att stödja terrorism i bl.a. Syrien och Irak. Det har visat sig att våldsbejakande islamistiska aktörer i konfliktområden använder nummer från oregistrerade svenska kontantkort i krypterade chattappar där brottsplaner kan diskuteras och propaganda spridas. Säkerhetspolisen har uppmärksammat flera fall av massdistribution av telefonnummer i form av inloggningsuppgifter till terrorkopplade aktörer utomlands. Ett förbud mot oregistrerade kontantkort skulle enligt Säkerhetspolisen försvåra för dessa aktörer. I dagsläget är det mer sannolikt att ett svenskt nummer i konfliktområdet Syrien och Irak inte tillhör en svensk person – ett fenomen som enligt Säkerhetspolisen är unikt för just Sverige (Säkerhetspolisens årsbok 2018 s. 55–57).

Sveriges advokatsamfund anser att det inte har gjorts någon närmare beskrivning eller analys av problemen med nuvarande metoder för att identifiera innehavare av kontantkort. *Tele2 Sverige AB* anser att behovsbedömningen som görs i promemorian inte stämmer med verkliga förhållanden, eftersom hemlig avlyssning och övervakning av elektronisk kommunikation inte förutsätter tillgång till abonnemangsuppgifter. Enligt bolagets statistik har närmare nio av tio hemliga tvångsmedel utförts på nummer för vilka det saknas abonnemangsuppgifter. Bolaget framhåller också att tillhandahållarna har uppgifter om transaktioner, vilka är mer effektiva och tillförlitliga för att etablera en koppling mellan ett telefonnummer och en misstänkt än vad abonnemangsuppgifter är.

I promemorian konstateras att de brottsbekämpande myndigheterna i dag lägger 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 förlita sig på andra metoder för att fastställa vem som innehar telefonnumret. Det arbetet tar mycket tid och resurser i anspråk. Det är dessutom inte säkert att uppgifterna leder till att en viss person kan identifieras som innehavare av ett kontantkort. Mycket tid och arbete behöver också läggas ned på att sortera bort de kontantkortsnummer som används av personer som inte är intressanta för den aktuella brottsutredningen. Dessa problem är enligt promemorian desamma i både underrättelse- och förundersökningsarbetet.

Även om hemliga tvångsmedel i dag kan avse oregistrerade kontantkort, har de brottsbekämpande myndigheterna alltså många gånger tvingats lägga ned omfattande resurser på att få fram den nödvändiga kopplingen mellan den relevanta personen och kontantkortet. Det arbetet är inte

synligt för tillhandahållarna och inte heller de fall där arbetet inte har lett till att en koppling kunnat fastställas. Det är visserligen riktigt att transaktionsuppgifter ibland kan leda till att användaren av ett oregistrerat kontantkort identifieras, men om transaktionen t.ex. har gjorts med kontanter kan personen förbli anonym. Att ta fram relevanta transaktionsuppgifter kräver dessutom ett flertal utredningsåtgärder och är därför mindre effektivt än att begära ut abonnemangsuppgifter från en tillhandahållare.

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. En skyldighet att registrera abonnemangsuppgifter för kontantkort skulle innebära att de brottsbekämpande myndigheterna skulle kunna få tillgång till dessa uppgifter på ett effektivt sätt, antingen genom olika webbplatser för nummerupplysning, om abonnenten samtyckt till publicering i abonnentförteckning, eller genom att begära ut uppgifterna från tillhandahållarna. Regeringen instämmer således i promemorians bedömning att de brottsbekämpande myndigheterna har ett påtagligt behov av tillgång till uppgifter om vem som innehar ett kontantkort och att en registreringsskyldighet skulle medföra ett effektivare brottsbekämpande arbete. Det finns inte heller någon mindre ingripande åtgärd som kan tillgodose behovet.

En registreringsskyldighet skulle vara till nytta trots eventuella möjligheter att kringgå den

Enligt *Sveriges advokatsamfund* skulle ett krav på registrering i realiteten inte bli ett sådant effektivt hjälpmedel i de brottsbekämpande myndigheternas arbete som hävdas i promemorian. Advokatsamfundet pekar i det sammanhanget på de möjligheter att kringgå en registreringsskyldighet som behandlas i promemorian och framhåller att användningen av kontantkort torde bli närmast obefintlig bland kriminella om de behöver registrera sina abonnemang. Även *Journalistförbundet*, *Tele2 Sverige AB* och *IT&Telekomföretagen* framför liknande invändningar.

Inledningsvis måste det framhållas att eventuella möjligheter att kringgå en registreringsskyldighet inte i sig utgör skäl för att avstå från att införa en sådan skyldighet. Regeringen instämmer i promemorians bedömning att en registreringsskyldighet för kontantkort, trots eventuella möjligheter att kringgå den, skulle försvåra för de kriminella och effektivisera de brottsbekämpande myndigheternas arbete.

Frågan om att införa en registreringsskyldighet för kontantkort är inte ny, utan har övervägts tidigare. Då gjordes bedömningen att det inte borde införas någon registreringsskyldighet, bl.a. eftersom en sådan skyldighet inte skulle kunna förhindra att anonyma kontantkort köps utomlands och utnyttjas i Sverige i brottsliga sammanhang, se propositionen De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation (prop. 2011/12:55 s. 104 och 105). De möjligheter till s.k. fri roaming som finns inom EU medför att det är förhållandevis enkelt att använda utländska oregistrerade kontantkort här. Sedan frågan om en skyldighet att registrera abonnemangsuppgifter för kontantkort utreddes

förra gången har emellertid ett stort antal länder i världen infört en sådan skyldighet. Enligt promemorian har minst 155 länder och mer än hälften av Europas länder infört någon form av registreringsskyldighet som omfattar kontantkort. Frågan utreds också i flera länder. 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. Som framgår ovan har det framkommit att telefonnummer som tillhör svenska oregistrerade kontantkort i stor omfattning används av terrorkopplade aktörer utomlands. Det är inte acceptabelt att avsaknaden av en registreringsskyldighet för svenska kontantkort underlättar för kriminella i andra länder att planera sin brottsliga verksamhet.

Ett sätt att kringgå en registreringsskyldighet är att låta registreringen utföras av andra personer än de verkliga innehavarna, dvs. av en sorts målvakter. Även problemet med målvakter var något som ansågs tala emot en registreringsskyldighet enligt tidigare bedömningar (prop. 2011/12:55 s. 105). Risken för ett sådant agerande finns fortfarande. 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. Men i det fall ett kontantkort skulle vara registrerat på en målvakt har de brottsbekämpande myndigheterna i vart fall uppgifter om den personen och en ingång att börja nysta i. Det får förutsättas ge bättre förutsättningar att fastställa vem som har ett visst telefonnummer eller vilket telefonnummer en viss person har, än om det inte finns några uppgifter alls. Därmed skulle en registreringsskyldighet innebära fördelar i förhållande till dagens system, även om vissa registrerade uppgifter skulle kunna avse målvakter.

En registreringsskyldighet för kontantkort kan även innebära att fler kriminella väljer att kommunicera via appar och andra tjänster som möjliggör kommunikation i krypterad och anonymiserad form. *Tele2 Sverige AB* anför som ett skäl mot en registreringsskyldighet att ett sådant teknikskifte skulle försämra de brottsbekämpande myndigheternas möjligheter att förhindra och utreda brottslighet. För att de brottsbekämpande myndigheterna ska kunna få tillgång till information som kommuniceras på detta sätt infördes det emellertid den 1 april 2020 ett nytt hemligt tvångsmedel genom lagen om hemlig dataavläsning. Vidare gav regeringen i augusti 2021 en särskild utredare i uppdrag att analysera förutsättningarna för att leverantörer av nummeroberoende interpersonella kommunikationstjänster, vilket omfattar bl.a. olika kommunikationsappar, ska kunna omfattas av skyldigheten att lagra och ge tillgång till uppgifter om elektronisk kommunikation samt ta ställning till om en sådan skyldighet bör införas (dir. 2021:58). Dessutom är det möjligt att genom hemlig övervakning av elektronisk kommunikation få tillgång till uppgifter som talar om var en persons kommunikationsutrustning har funnits, under förutsättning att det går att koppla utrustningen till personen. Det kan t.ex. handla om en mobiltelefon. En registreringsskyldighet kan på så sätt medföra att en person kan positioneras i närheten av en brottsplats.

Noggrant planerade brott kommer alltid att kunna ge upphov till vissa svårigheter för de brottsbekämpande myndigheterna. Långt ifrån alla grova brott föregås dock av noggrann planering och begås inte alltid av

personer med hög säkerhetsförmåga. En skyldighet att registrera uppgifter om kontantkortsabonnenter skulle i vart fall försvåra för den som avser att använda ett kontantkort för att försöka dölja spår med 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.

Även om det för den som planerar sin brottslighet kan finnas sätt att kringgå en registreringsskyldighet för kontantkort, kommer en sådan skyldighet att innebära att kriminellas verksamhet försvåras och att de brottsbekämpande myndigheternas arbete effektiviseras. De brottsbekämpande myndigheterna är också positiva till en registreringsskyldighet. *Ekobrottsmyndigheten*, *Åklagarmyndigheten* och *Tullverket* framhåller särskilt att en sådan skyldighet förväntas ha positiva effekter för brottsbekämpningen. En skyldighet att registrera uppgifter om abonnemang för kontantkort skulle alltså innebära tydliga fördelar i förhållande till dagens system och vara till nytta för brottsbekämpningen, särskilt i fråga om möjligheten att förebygga, förhindra, utreda och beivra allvarligare brottslighet.

En begränsad inskränkning av enskildas fri- och rättigheter

En skyldighet att registrera abonnemangsuppgifter för kontantkort skulle beröra många kontantkortsabonnenter och innebära att fler uppgifter om enskilda hanteras av tillhandahållarna. Uppgifterna skulle också på begäran kunna lämnas ut från tillhandahållarna till vissa myndigheter, bl.a. de brottsbekämpande myndigheterna, i de fall det finns lagstöd för det.

I 2 kap. 6 § andra stycket regeringsformen anges att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Begränsningar i detta skydd får endast ske genom lag och endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningarna får inte heller gå utöver vad som är nödvändigt eller utgöra ett hot mot den fria åsiktsbildningen (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 som åtgärden innebär beaktas. Bestämmelsen i 2 kap. 6 § andra stycket regeringsformen 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 propositionen En reformerad grundlag (prop. 2009/10:80 s. 250.)

I artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) anges att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Rätten innefattar även skydd av person-

uppgifter. Offentlig myndighet får inte inskränka dessa rättigheter annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt bl.a. med hänsyn till statens säkerhet och den allmänna säkerheten, till förebyggande av oordning och brott eller till skydd för andra personers fri- och rättigheter. Konventionen gäller som svensk lag, se lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna. Lag eller annan föreskrift får inte meddelas i strid med Sveriges åtaganden på grund av Europakonventionen (2 kap. 19 § regeringsformen).

Artikel 8 i Europakonventionen ger emellertid inte bara upphov till negativa förpliktelser för det allmänna att avhålla sig från omotiverade inskränkningar i denna rättighet, utan även positiva skyldigheter för det allmänna att se till att enskilda tillförsäkras skydd för sina rättigheter gentemot andra enskilda. Det innebär t.ex. att staten i vissa fall kan vara skyldig att införa straffrättslig reglering för att skydda enskilda mot intrång i rättigheter från andra enskilda. Det innebär också att staten för sådana fall behöver säkerställa att brott kan utredas och att så också sker när det är befogat. 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. Att ha en väl fungerande brottsbekämpning innebär t.ex. att myndigheterna ska ha tillgång till effektiva utredningsverktyg, även i den elektroniska miljön (se t.ex. prop. 2018/19:86 s. 27). När så inte har varit fallet har staten ansetts kränka de rättigheter som följer av Europakonventionen. Ett exempel på det är när en person som gjort sig skyldig till förtal eller möjligen sexuellt ofredande av ett tolvårigt barn inte kunde identifieras på grund av att den nationella lagstiftningen inte möjliggjorde att uppgift om vem som låg bakom en ip-adress kunde hämtas in från tillhandahållaren. I det aktuella fallet uttalade Europadomstolen att konfidentialitet för kommunikation och yttrandefrihet ibland måste få vika för brottsbekämpande ändamål (Europadomstolens dom den 2 december 2008 i mål K.U. mot Finland, mål nr 2872/02).

En bestämmelse om rätt till respekt för bl.a. privatliv finns också i artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna (EU:s rättighetsstadga). I artikel 8 i EU:s rättighetsstadga regleras även en rätt till skydd av personuppgifter. Varje begränsning i utövandet av de fri- och rättigheter som erkänns i EU:s rättighetsstadga måste vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa fri- och rättigheter. Begränsningar får, med beaktande av proportionalitetsprincipen, göras endast om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors fri- och rättigheter (artikel 52.1). I den mån stadgan omfattar rättigheter som motsvarar sådana som garanteras av Europakonventionen, ska de ha samma innebörd och räckvidd som enligt konventionen. Det hindrar dock inte unionsrätten från att tillförsäkra ett mer långtgående skydd (artikel 52.3). För att säkerställa rätten till respekt för privatliv 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. Direktivet

är genomfört i svensk rätt främst genom bestämmelser i LEK, vilka föreslås föras över till nya LEK.

Vidare innehåller FN:s konvention om barnets rättigheter (barnkonventionen) bestämmelser om barns rätt till privatliv. Av artikel 16 följer att inget barn får utsättas för godtyckliga eller olagliga ingripanden i sitt privat- och familjeliv. Vidare framgår av artikel 3 att vid alla åtgärder som rör barn ska i första hand beaktas vad som bedöms vara barnets bästa. Barnets bästa kan inte frikopplas från övriga rättigheter i konventionen. Rättigheterna ska ses om en helhet. Barnkonventionen gäller som svensk lag sedan den 1 januari 2020, se lagen (2018:1197) om Förenta nationernas konvention om barnets rättigheter.

När det gäller frågan om en skyldighet att registrera abonnemangsuppgifter i enskilda fall kan utgöra en inskränkning i nämnda rättigheter gör regeringen följande bedömning. 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 (jfr prop. 2009/10:80 s. 176).

De uppgifter som tillhandahållarna skulle vara skyldiga att registrera kan inte anses vara särskilt känsliga ur integritetssynpunkt. Även om abonnemangsuppgifter naturligtvis är skyddsvärda, avser de inte uppgifter om innehållet i den kommunikation som har ägt rum, uppgifter om geografisk position (lokaliseringsuppgifter) eller uppgifter som skapas med anledning av en viss kommunikation (trafikuppgifter). Abonnemangsuppgifter möjliggör i princip enbart att en adress, t.ex. ett telefonnummer, kan hänföras till sin innehavare och att en indikation kan erhållas om vem som använder adressen. Abonnemangsuppgifterna ger alltså inte i sig besked om t.ex. vem som har ringt till vem eller vad som har framkommit vid telefonsamtalen. Uppgifter om abonnemang kan således inte användas för att dra några mer precisa slutsatser om berörda personers privatliv (se t.ex. prop. 2018/19:86 s. 94 och rättsfallet RK 2018:1). I detta fall är det dessutom endast vissa abonnemangsuppgifter som ska registreras (avsnitt 4.2.2).

Att denna typ av uppgifter endast kan ge begränsad information om berörda personers privatliv beaktades av Europadomstolen när den prövade om den registreringsskyldighet för kontantkort som införts i Tyskland stred mot rätten till respekt för privatliv (Europadomstolens dom den 30 januari 2020 i målet Breyer mot Tyskland, mål nr 50001/12). Domstolen fann att skyldigheten att registrera uppgift om namn, adress, födelsedatum, telefonnummer och tidpunkt för avtalets ingående endast innebar en begränsad inskränkning i rätten till respekt för privatliv (punkt 92–95). Även EU-domstolen har framhållit att identitetsuppgifter för innehavare av simkort respektive uppgifter om den fysiska identiteten för användare av elektroniska kommunikationsmedel har begränsad betydelse för enskildas privatliv (EU-domstolens dom den 2 oktober 2018 i målet C-207/16 punkt 60 och dom den 6 oktober 2020 i de förenade målen C-511/18, C-512/18 och C-520/18 punkt 157).

Tillhandahållarna behandlar redan i dag abonnemangsuppgifter om de kunder som innehar kontraktsabonnemang, dvs. flertalet användare av mobiltelefoner. Det förekommer också att kontantkortskunders abonnemangsuppgifter registreras på frivillig väg. En registreringsskyldighet kommer därmed inte i sig att leda till någon ny form av personuppgiftsbehandling. Den dataskyddsreglering som gäller enligt EU:s dataskyddsförordning, lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) och nya LEK kommer att vara tillämplig även för de abonnemangsuppgifter som skulle behandlas på grund av en registreringsskyldighet. Om registrerade abonnemangsuppgifter lämnas ut till brottsbekämpande myndigheter kommer de personuppgifter som behandlas hos myndigheterna dessutom att vara omgärdade av integritetsskyddande lagstiftning, huvudsakligen brottsdatalagen (2018:1177) med tillhörande registerförfattningar, t.ex. lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område. Det säkerställer att uppgifter behandlas korrekt och med respekt för enskildas personliga integritet.

Mot denna bakgrund gör regeringen bedömningen, i likhet med den som görs i promemorian, att en registrering av abonnemangsuppgifter för kontantkort endast skulle innebära ett begränsat intrång i enskildas personliga integritet och en begränsad inskränkning i enskildas rätt till respekt för privatliv och rätt till skydd av personuppgifter. Förslaget aktualiserar redan av det skälet inte tillämpningen av bestämmelsen i 2 kap. 6 § andra stycket regeringsformen. Syftet med registreringen är att uppgifterna ska finnas tillgängliga för brottsbekämpande ändamål, vilket är ett godtagbart syfte enligt såväl Europakonventionen som EU-rätten.

Enskildas legitima intresse av att kommunicera utan att röja sin identitet

Som *Sveriges Radio AB* pekar på finns det fall när uppgifter om identitet kan vara mycket känsliga. Till skillnad från när oregistrerade kontantkort används i samband med brottslig verksamhet finns det tillfällen när enskilda har ett legitimt intresse av att kunna kommunicera utan att röja sin identitet. Ett sådant exempel är enskilda som vill utnyttja den grundlagsskyddade meddelarfriheten för att lämna uppgifter till medier i syfte att dessa ska göras offentliga (se 1 kap. 7 § tryckfrihetsförordningen och 1 kap. 10 § yttrandefrihetsgrundlagen). Ett annat viktigt exempel är förföljda personer som lever gömda från t.ex. en tidigare partner eller familjemedlem.

Journalistförbundet, *Sveriges Radio AB*, *TU* och *Utgivarna* betonar vikten av oregistrerade kontantkort för meddelarfriheten men också för andra aspekter av den journalistiska verksamheten och anser att registreringsskyldighetens negativa konsekvenser för denna verksamhet kraftigt har underskattats. Dessa remissinstanser pekar i det sammanhanget på den användning som beskrivs i promemorian, dvs. att oregistrerade kontantkort används av personer som kontaktar media och att journalister kan förse källor med eller själva använda sig av sådana kontantkort. Sveriges Radio AB, Utgivarna och TU anser också att tillhandahållarnas tystnadsplikt inte räcker som skydd. Sveriges Radio AB framhåller i det sammanhanget att en källa kan vara en person som utreds av polis och vars elektroniska utrustning övervakas. *Justitiekanslern* anser

att registreringsskyldighetens inverkan på meddelarskyddet behöver övervägas mera noggrant. *Unizon* anser att det är av stor vikt att kvinnor och barn som utsätts för mäns våld har möjlighet att kommunicera anonymt. Enligt *Sveriges advokatsamfund* riskerar insikten om att det finns en möjlighet att övervaka och spåra den enskilda individen att få ytterst menlig inverkan på utövandet av en mängd demokratiska fri- och rättigheter.

Regeringen konstaterar att en registreringsskyldighet för kontantkort inte kommer att innebära att enskildas abonnemangsuppgifter blir allmänt kända. Uppgifterna kommer, som Justitiekanslern och *PTS* pekar på, att omfattas av en straffsanktionerad tystnadsplikt hos tillhandahållarna och få röjas endast om den enskilde har samtyckt till det eller det annars är tillåtet enligt lag. En registreringsskyldighet innebär alltså inte i sig att den enskilda kontantkortsinnehavarens identitet röjs. Det finns också, som Justitiekanslern framhåller, ett grundlagsreglerat förbud för det allmänna att efterforska vem som har lämnat uppgifter till en journalist i publiceringssyfte. Varken abonnemangsuppgifter eller hemliga tvångsmedel får användas av brottsbekämpande myndigheter för att ta reda på vem som har lämnat uppgifter till en journalist. Inte heller i övrigt medför en registreringsskyldighet någon förändring av meddelarskyddet eller dess beståndsdelar. Reglerna om meddelarfrihet, rätt till anonymitet och repressalieförbud kommer alltså fortfarande att gälla. I sammanhanget kan det också påpekas att hemlig avlyssning inte får avse samtal eller andra meddelanden där den som yttrar sig har tystnadsplikt på grund av källskyddet (27 kap. 22 § rättegångsbalken och 11 § preventivlagen). Det kan även noteras att många medieföretag har krypterade tjänster där enskilda anonymt kan lämna tips och inleda kontakter med journalister.

Sammantaget anser regeringen att det legitima intresse som finns av att kommunicera utan att röja sin identitet kan tillgodoses genom det skydd som befintlig lagstiftning erbjuder, även om en registreringsskyldighet för kontantkort införs.

Betydelsen för företag

Införandet av en registreringsskyldighet kommer att beröra de företag som tillhandahåller kontantkort. Enligt promemorian finns det för närvarande sex sådana företag. Sedan promemorian togs fram har dock ett av dessa företag meddelat att tjänsten kommer upphöra och att företagets alla kontantkort avslutas den 31 mars 2022.

Tele2 Sverige AB anser att konsekvenserna för tillhandahållarna har underskattats och anför följande. Genom en registreringsskyldighet skulle betydande ekonomiska värden riskera att omfördelas. Vissa värden skulle riskera att fördelas till andra marknader i Sverige, t.ex. marknaden för internetbaserade telefoniappar, och vissa värden skulle riskera att omfördelas till följd av återförsäljning i Sverige av utländska kontantkort. På grund av dessa förväntade effekter måste kontantkortsmarknadens omsättning förväntas minska. Vidare skulle tillhandahållarna på den svenska kontantkortsmarknaden belastas med implementeringskostnader.

Registreringsskyldigheten kommer medföra att de aktuella tillhandahållarna behöver anpassa sina system och lagra fler uppgifter än tidigare, vilket innebär kostnadsökningar. Enligt promemorian krävs dels

en engångsinvestering i form av ombyggnad av system, dels investeringar för den löpande driften. Hur stora kostnadsökningarna kommer att bli är dock svårt att kvantifiera. I promemorian anges att någon tillhandahållare har uppgett att en registreringsskyldighet skulle medföra att kostnaderna skulle hamna på orimliga nivåer. En annan tillhandahållare har däremot uppgett att system för att genomföra en registrering av samtliga kontantkortskunder i princip redan finns på plats, eftersom en registrering redan i dag görs av de kunder som har kontraktsabonnemang eller som på frivillig väg lämnar sina abonnemangsuppgifter till tillhandahållaren. Det som enligt tillhandahållaren skulle tillkomma är eventuella kostnader kopplade till den personal som kan behövas för att genomföra en registrering.

Det är alltså svårt att kvantifiera de kostnader som kan uppstå för tillhandahållarna till följd av en registreringsskyldighet. Regeringen instämmer dock i promemorians bedömning att kostnaderna kommer att öka. I sammanhanget bör dock påpekas att flera av tillhandahållarna bedriver verksamhet i andra länder där det finns krav på att de ska registrera uppgifter om de kunder som innehar kontantkort. Således bör det i viss utsträckning finnas upparbetade system och rutiner kring dessa frågor. Dessutom registreras abonnemangsuppgifter redan i dag avseende andra kunder än kontantkortsinnehavare. En registreringsskyldighet skulle således endast innebära en utvidgning av nuvarande system.

Det finns 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. Det har från lagstiftarens sida tidigare bedömts att tillhandahållarna kan vara skyldiga att vidta åtgärder för att underlätta den brottsutredande verksamheten och i viss utsträckning bära kostnaderna för detta, se prop. 2018/19:86 s. 110 och 111, prop. 2010/11:46 s. 67 och propositionen Teleoperatörernas skyldigheter vid hemlig teleavlyssning och hemlig teleövervakning (prop. 1995/96:180 s. 29–36). Regeringen anser att så bör fortsatt vara fallet.

Kontantkort säljs även av återförsäljare. Det finns, enligt uppgift i promemorian, 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 genomföra en registrering. *IT&Telekomföretagen* efterfrågar en analys av de ekonomiska konsekvenserna för dessa handlare. Enligt en uppskattning som framgår av promemorian säljer ca 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. Registreringsskyldigheten kan dock utformas på ett sådant sätt att fristående handlare inte hindras från att fortsatt sälja kontantkort eller vouchers för påfyllnad (avsnitt 4.2.1). En registreringsskyldighet behöver därför inte medföra några betydande ekonomiska konsekvenser för de fristående handlarna.

Det är proportionerligt att 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. Som konstateras ovan finns det ett påtagligt behov av de uppgifter som en registreringsskyldighet ger tillgång till i det brottsbekämpande arbetet. Det kan även konstateras att en registreringsskyldighet kommer att få konsekvenser för enskilda som i dag kommunicerar via oregistrerade kontantkort och för tillhandahållare och återförsäljare av 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 kan få tillgång till uppgifter genom 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 är involverade i grov brottslighet genom så pass enkla åtgärder som det är fråga om kan förbli anonyma och därmed undvika att bli föremål för effektiva utredningsåtgärder. Detta leder till att brottslighet i många fall inte kan avslöjas, utredas eller beivras. I andra fall kommer avslöjandet av vem som döljer sig bakom ett oregistrerat kontantkort inte att kunna ske utan att brottsbekämpande myndigheter förbrukar betydande resurser.

Som konstaterats ovan kan det finnas vägar att kringgå en registrerings-skyldighet för kontantkort. Det finns också andra sätt att kommunicera där det kan vara svårt för de brottsbekämpande myndigheterna att följa kommunikationen. En registreringsskyldighet är således inte en åtgärd som ensam kan lösa samtliga svårigheter som kan uppstå när brotts-bekämpande myndigheter behöver ta del av kriminellas kommunikation. Däremot kan en registreringsskyldighet vara en betydelsefull del 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 därmed medföra att uppgifter om elektronisk kommunikation oftare kan göras åtkomliga för brottsbekämpande ändamål. På så sätt kan det brottsbekämpande arbetet effektiviseras. Därigenom skapas förbättrade förutsättningar att bekämpa brottslighet, särskilt när det gäller allvarlig brottslighet.

Det är ofta nödvändigt att göra en avvägning mellan integritetsintresset och intresset av att myndigheterna har effektiva metoder för brottsbekämpning. Det ligger i sakens natur att sådana metoder ofta innefattar ett integritetsintrång. I det sammanhanget bör det dock beaktas att de abonnemangsuppgifter som skulle behandlas till följd av en registreringsskyldighet 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 respekt för privatliv och rätt till skydd av personuppgifter. Möjligheten att kommunicera utan att lämna ifrån sig vissa uppgifter till tillhandahållare kommer dock att minska. Som framgår ovan innebär en

registreringsskyldighet emellertid inte att enskildas abonnemangsuppgifter blir allmänt kända, utan de skulle skyddas av befintlig reglering om bl.a. tystnadsplikt och dataskydd. När det gäller tillhandahållare och återförsäljare bedöms det inte uppstå orimliga kostnader och de ekonomiska konsekvenserna kan till viss del begränsas genom utformningen av registreringsskyldigheten.

Sammanfattningsvis anser regeringen att det brottsbekämpande intresset väger tungt och att det intrång i den personliga integriteten som registreringen ger upphov till är förhållandevis begränsat och inte sträcker sig längre än vad som är nödvändigt för att nå det eftersträvade syftet. Att införa ett krav på tillhandahållare att registrera vissa uppgifter om kontantkortsabonnenter bedöms därmed utgöra en proportionerlig begränsning av rätten till respekt för privatlivet och rätten till skydd av personuppgifter. Införandet av en registreringsskyldighet är därmed också förenligt med artikel 8 i Europakonventionen och artiklarna 7 och 8 i EU:s rättighetsstadga. De brottsbekämpande myndigheternas behov och nytta av en registreringsskyldighet väger alltså tyngre än de intressen som talar mot en sådan skyldighet. Regeringen anser därför att det bör införas en registreringsskyldighet.

4.2 Utformningen av registreringsskyldigheten

4.2.1 Vilka tjänster som ska omfattas

Regeringens förslag: Registreringsskyldigheten omfattar förbetalda allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster och förbetalda internetanslutningstjänster. Den som tillhandahåller en sådan tjänst får inte ge tillgång till tjänsten utan att dessförinnan ha gjort en registrering.

Registreringsskyldigheten regleras i den nya lagen om elektronisk kommunikation.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: En majoritet av remissinstanserna är positiva till förslaget eller har ingen invändning mot det. Enligt *Ekobrottsmyndigheten*, *Säkerhetspolisen* och *Åklagarmyndigheten* måste det säkerställas att de tjänster för kommunikation mellan maskiner som undantas inte kan användas på annat sätt, eftersom registreringsskyldigheten annars riskerar att bli verkningslös. Säkerhetspolisen anser att det av promemorian inte framgår om det finns simkort med förbetalda tjänster som enbart kan användas för kommunikation mellan maskiner och om simkorten i så fall är tekniskt begränsade att användas på något annat sätt. *Polismyndigheten* framför liknande synpunkter. *Telenor Sverige AB* och *IT&Telekomföretagen* anser att det inte har presenterats tillräckliga skäl för att inkludera förbetalda datatjänster i registreringsskyldigheten och pekar på möjligheten att få tillgång till internet utan simkort genom ett wifi-nätverk. *Tele2 Sverige AB* och *IT&Telekomföretagen* pekar på problem med att kontantkort avsedda för maskin-till-maskin-kommunikation som kan ge tillgång till samtalstjänster eller datatjänster omfattas av registreringsskyldigheten. Tele2 Sverige AB anser att det behövs en tydligare

avgränsning i förhållande till maskin-till-maskin-tjänster. Enligt bolaget vore det rimligt att ta utgångspunkt i de nummerserier som specifikt ska allokeras till och användas för maskin-till-maskin-tjänster. Tjänster med sådana nummer bör enligt bolaget undantas i sin helhet från registreringskravet, oavsett om telefoni- eller internetaccessfunktionalitet har adderats i det enskilda fallet. Tele2 Sverige AB framhåller att maskin-till-maskin-tjänster kan innehålla telefoni eller internetanslutning utan att vara relevanta för ett registreringskrav. Ett exempel är de hundratusentals maskin-till-maskin-simkort som i Sverige används för larmutrustning. I dessa fall är simkortet ofta utrustat med kapacitet att ringa larmsamtal från användaren till larmcentral via en mikrofon som utgör en del av larmutrustningen. Simkorten skulle dessutom vara registrerade på tillhandahållaren av larmtjänsten och inte på slutanvändaren. Detta skulle ytterligare minska den förväntade nyttan av abonnemangsuppgifterna. Enligt IT&Telekomföretagen vore det rimligt att undanta alla kontantkort som används för maskin-till-maskin-kommunikation, oavsett vilka funktioner som är kopplade till dem. *Kammarrätten i Stockholm* pekar på att registreringsskyldigheten enligt promemorian inte ska gälla för vissa tjänster som t.ex. tillhandahållande av maskin-till-maskin-tjänster. Enligt kammarrätten kan bestämmelsen behöva förtydligas så att det klart framgår vilka förbetalda tjänster som ska omfattas av registreringsskyldigheten.

PTS instämmer i bedömningen att registreringsskyldigheten bör regleras i LEK, bl.a. eftersom frågor om tillhandahållarnas lagring och övrig behandling av personuppgifter inom sektorn för elektronisk kommunikation huvudsakligen regleras där.

Skälen för regeringens förslag

Registreringsskyldigheten bör omfatta förbetalda samtals- och datatjänster

Det finns olika modeller för hur en registreringsskyldighet kan utformas. Bland de länder som har infört en registreringsskyldighet är den vanligaste modellen att tillhandahållarna är skyldiga att samla in och bevara uppgifter om sina kunder. Även en svensk registreringsskyldighet bör utformas på detta sätt. Fördelen med en sådan ordning är att uppgifterna därmed kommer att föras vidare till brottsbekämpande myndigheter endast i de fall där det begärs och befintlig lagstiftning tillåter det.

Utmärkande för kontantkort är att den enskilde betalar för tjänsten i förskott. Som framgår ovan är det detta förhållande som gör att kontantkortsabonnenterna i dag oftast är anonyma för tillhandahållarna. Eftersom det även är möjligt att få tillgång till förbetalda tjänster via inbyggda simkort, s.k. e-sim, bör regleringen emellertid 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 (i fortsättningen kommer dock e-sim inte att omnämnas särskilt). De aktörer som tillhandahåller sådana förbetalda tjänster bör omfattas av registreringskravet.

Ett kontantkort kan avse enbart samtalstjänster, enbart datatjänster (mobilt bredband) eller både samtalstjänster och datatjänster. Som framgår av promemorian är det vanligast att ett mobilabonnemang ger tillgång till

både samtalstjänster och datatjänster. Det finns även simkort som använder telefonnummer och som används för kommunikation mellan maskiner, s.k. maskin-till-maskin-tjänster. Vid maskin-till-maskin-tjänster används simkort för t.ex. övervakning, mätning, styrning, transport och logistik. Simkorten kan på detta sätt användas i exempelvis bilar, tåg, elmätare, hemlarm och gräsklippare. Även kontantkort kan användas för maskin-till-maskin-tjänster, men enligt promemorian är det ovanligt.

Enligt nya LEK kan elektroniska kommunikationstjänster vara av tre slag: internetanslutningstjänster, interpersonella kommunikationstjänster eller tjänster som helt eller huvudsakligen utgörs av överföring av signaler, såsom överföringstjänster som används för tillhandahållande av maskin-till-maskin-tjänster. Med en internetanslutningstjänst avses en allmänt tillgänglig elektronisk kommunikationstjänst som erbjuder anslutning till internet. Med en interpersonell kommunikationstjänst avses en tjänst som vanligen tillhandahålls mot ersättning och som möjliggör ett direkt interpersonellt och interaktivt informationsutbyte via elektroniska kommunikationsnät mellan ett begränsat antal personer, varigenom de personer som inleder eller deltar i kommunikationen bestämmer vem eller vilka som ska vara mottagare av denna, dock inte en tjänst som möjliggör interpersonell och interaktiv kommunikation enbart som en extrafunktion av mindre betydelse. 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. En nummeroberoende interpersonell kommunikationstjänst är en interpersonell kommunikationstjänst som varken etablerar en förbindelse till nummer i nationella eller internationella nummerplaner eller möjliggör kommunikation med sådana nummer (1 kap. 7 § nya LEK, jfr även artikel 2 i e-kodexdirektivet).

I nya LEK används uttrycket allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst för att beskriva de samtalstjänster som tillhandahålls via bl.a. kontantkort. För att beskriva de datatjänster som kan nås via kontantkort används ordet internetanslutningstjänst (se t.ex. 7 kap. 34 §). Samma ord och uttryck bör användas när det gäller registreringsskyldigheten.

Det står klart att regleringen bör omfatta de kontantkort som ger tillgång till traditionella samtalstjänster. Detta bör komma till uttryck på det sättet att regleringen ska omfatta tillhandahållande av förbetalda allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster. Därmed omfattas också de kontantkort som ger tillgång till både samtalstjänster och datatjänster.

En reglering som inte omfattar de kontantkort som enbart ger tillgång till datatjänster skulle kunna medföra att enskilda i större utsträckning kommer att använda sig av dessa tjänster för att få åtkomst till appar eller andra internetbaserade tjänster som gör det möjligt att kommunicera krypterat. Som *Telenor Sverige AB* och *IT&Telekomföretagen* pekar på krävs det visserligen inte ett simkort, utan endast en internetuppkoppling, för att det ska vara möjligt att via exempelvis en mobiltelefon få tillgång till internet och därmed till krypterade tjänster. En registreringsskyldighet som omfattar internetanslutningstjänster kan ändå förväntas få stor

betydelse för brottsbekämpningen. Genom hemlig övervakning av elektronisk kommunikation kan man 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 datatjänster. 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 av stort värde att få tillgång till registrerade uppgifter om vem som innehar även sådana kontantkort. De aktuella uppgifterna blir också allt viktigare i takt med att kriminella väljer att kommunicera över internet i stället för via traditionell telefoni. Vidare kan kontantkort som endast ger tillgång till datatjänster användas för att ta emot den kod som krävs för att aktivera ett konto i en internetbaserad kommunikationstjänst. Det finns visserligen andra sätt att ta emot koden. Ett registreringskrav som även omfattar sådana kontantkort skulle dock försvåra för de kriminella som har satt i system att via kontantkort starta konton i appar och vidarebefordra uppgifter om dessa till andra personer för krypterad och anonym kommunikation.

Mot denna bakgrund anser regeringen, i enlighet med promemorians förslag, att även förbetalda datatjänster (internetanslutningstjänster) bör omfattas av registreringsskyldigheten. På så sätt blir regleringen också mer teknikneutral.

Som *Ekobrottsmyndigheten*, *Säkerhetspolisen* och *Åklagarmyndigheten* framhåller skulle registreringsskyldigheten riskera att bli verkningslös om det gjordes ett undantag för kontantkort som är avsedda för kommunikation mellan maskiner, men som ändå ger tillgång till samtals- eller datatjänster. Regeringen anser därför, till skillnad från *Tele2 Sverige AB* och *IT&Telekomföretagen*, att det avgörande för registreringsskyldigheten bör vara vilka tjänster som ett kontantkort ger tillgång till.

Regleringen bör sammanfattningsvis omfatta förbetalda allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster och förbetalda internetanslutningstjänster, men inte förbetalda tjänster som endast kan användas för kommunikation mellan maskiner. Det är tillgången till de förbetalda tjänsterna som bör avgöra om det föreligger en registreringsskyldighet, inte huruvida tjänsterna faktiskt används. Tillhandahållarna bör alltså vara skyldiga att göra en registrering om ett kontantkort ger tillgång till de angivna tjänsterna.

Abonnenten bör inte kunna få tillgång till tjänsten före registreringen

Det bör inte vara möjligt att använda förbetalda tjänster innan en registrering har gjorts. I annat fall riskerar regleringen att bli mindre effektiv. Om tjänsterna skulle kunna användas utan att en registrering har gjorts 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 före registreringen. Det bör t.ex. inte vara möjligt att dessförinnan ta emot samtal eller sms. Inte heller bör internetanslutningstjänster vara möjliga att utnyttja före registreringen. Av regleringen bör det alltså framgå att den som tillhandahåller en förbetald

tjänst inte ska få ge tillgång till tjänsten utan att dessförinnan ha genomfört en registrering.

Att en förbetald tjänst inte bör kunna tas i bruk före registreringen hindrar inte att kontantkort säljs utan att en registrering har gjorts. 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 aktuella tillhandahållaren eller hos en större återförsäljare. Man kan också tänka sig att registreringen kan utföras via internet eller vid kontakt med en kundtjänst.

Skyldigheten bör regleras i den nya lagen om elektronisk kommunikation

Registreringsskyldigheten kommer att innebära sådana åligganden för tillhandahållarna att regleringen bör införas i lag. I linje med *PTS* synpunkter är det lämpligt att bestämmelserna förs in i nya LEK, där frågor om tillhandahållarnas lagring och övrig behandling av personuppgifter regleras. Det framstår också som lämpligt med hänsyn till att andra frågor om abonnenter samt tillhandahållarnas tystnadsplikt regleras i den lagen.

4.2.2 Vilka uppgifter som ska registreras och hur länge de ska finnas tillgängliga

Regeringens förslag: Följande uppgifter ska registreras:
- abonnentens namn och postadress
- abonnentens personnummer, samordningsnummer, organisationsnummer eller annat identifieringsnummer
- nummer eller annan beteckning för tjänsten.

Tillhandahållaren ska även ange tidpunkten för registreringen.

Uppgifterna ska finnas tillgängliga hos tillhandahållaren från och med registreringen till och med ett år efter att tillhandahållandet av tjänsten har upphört.

Promemorians förslag överensstämmer i huvudsak med regeringens. I promemorians förslag till lagtext nämns inte samordningsnummer, organisationsnummer eller annan beteckning för tjänsten än nummer. I promemorian föreslås inte att tidpunkten för registreringen ska anges.

Remissinstanserna: Endast *Säkerhetspolisen* och *Åklagarmyndigheten* yttrar sig särskilt över förslaget om vilka uppgifter som ska registreras. Enligt Åklagarmyndigheten bör registreringsskyldigheten omfatta även tidpunkten för registreringen, eftersom det bör vara möjligt att avgränsa tidsperioden som en viss person haft tillgång till den förbetalda tjänsten. Även Säkerhetspolisen anser att tidpunkten för registreringen ska omfattas. Säkerhetspolisen anser att en uppgift om när en registrering har gjorts, vid inköp från en tillhandahållare eller vid en överlåtelse, är oerhört viktig i arbetet med att bekämpa brott. Utan en sådan uppgift kan det vara svårt att i efterhand knyta en misstänkt till en förbetald tjänst vid en viss tid.

När det gäller den förslagna lagringstiden yttrar sig endast *Ekobrottsmyndigheten* och *Hi3G Access AB* särskilt. Ekobrottsmyndigheten anser att förslaget framstår som väl avvägt och framhåller att det är av vikt för de brottsbekämpande myndigheterna att uppgifterna finns tillgängliga

under en tid även efter det att tjänsten avslutats. Hi3G Access AB anser däremot att det inte är motiverat med ett års lagring efter att tillhandahållandet har upphört och pekar på att sex månader tidigare har angetts som huvudregel (prop. 2018/19:86 s. 49–51). Vidare anser bolaget att uttrycket tillhandahållandet har upphört är oklart. Enligt bolaget vore det lämpligt att förtydliga att med uttrycket avses den tidpunkt då abonnenten inte längre har tillgång till tjänsten på grund av t.ex. genomförd utportering eller inaktivering till följd av att tjänsten inte har använts under en längre tid.

Skälen för regeringens förslag

Vilka uppgifter som bör registreras

Registreringsskyldigheten bör omfatta uppgifter om den som genom att köpa ett kontantkort eller på annat sätt ingår avtal med en tillhandahållare om att den ska tillhandahålla en förbetald tjänst. Registreringen bör således avse abonnenten och dennes abonnemangsuppgifter. De uppgifter som bör registreras är sådana som identifierar abonnenten. Enligt promemorians förslag ska abonnentens namn, adress, personnummer eller motsvarande samt nummer för tjänsten registreras. Eftersom ordet adress förekommer i nya LEK med en annan betydelse (se definitionen av ordet lokaliseringsuppgift 1 kap. 7 §) bör i stället ordet postadress användas i detta sammanhang. Med hänsyn till vikten av en säker identifiering bör en registreringsskyldighet även omfatta personnummer eller samordningsnummer om abonnenten är en fysisk person och organisationsnummer om abonnenten är en juridisk person. I promemorians förslag används uttrycket personnummer eller motsvarande för att beskriva vilka identifieringsnummer som bör registreras. Regeringen bedömer emellertid att regleringen blir tydligare om även samordningsnummer och organisationsnummer uttryckligen anges. För den som saknar personnummer och samordningsnummer, t.ex. en utländsk turist, bör det vara möjligt att i stället registrera exempelvis födelsedatum och passnummer. Den möjligheten kan lämpligen beskrivas genom uttrycket annat identifieringsnummer. Regeringen anser att vikten av en säker identifiering överväger de integritetsrisker som en behandling av personnummer eller samordningsnummer innebär för den enskilde. Det får därför anses vara klart motiverat att registreringsskyldigheten omfattar personnummer eller samordningsnummer (jfr 3 kap. 10 § dataskyddslagen). I enlighet med promemorians förslag bör också numret för tjänsten registreras. Om tjänsten inte har något nummer bör i stället en annan beteckning för tjänsten registreras.

Som *Åklagarmyndigheten* och *Säkerhetspolisen* framhåller är det av vikt att uppgift om tidpunkten för registreringen finns tillgänglig för brottsbekämpande myndigheter. Registreringsskyldigheten bör därför, i tillägg till promemorians förslag, omfatta även den uppgiften.

Sammanfattningsvis bör registreringsskyldigheten omfatta abonnentens namn och postadress, personnummer, samordningsnummer, organisationsnummer eller annat identifieringsnummer samt nummer eller annan beteckning för tjänsten. Tillhandahållaren bör även vara skyldig att ange tidpunkten för registreringen.

Hur länge uppgifterna bör finnas tillgängliga hos tillhandahållarna

Nya LEK innehåller vissa bestämmelser om lagring som även omfattar abonnemangsuppgifter. Huvudregeln är att en trafikuppgift ska utplånas eller avidentifieras när den inte längre behövs för att överföra ett elektroniskt meddelande (9 kap. 1 §). Från denna huvudregel finns flera undantag. En tillhandahållare kan exempelvis, med den enskildes samtycke, lagra sådana uppgifter en viss tid för marknadsföring (9 kap. 2 §). Den lagringsskyldighet för brottsbekämpande ändamål som följer av 9 kap. 19 § 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. Skyldigheten att lagra uppgifter omfattar uppgifter som genereras eller behandlas vid telefonitjänst och meddelandehantering via mobil nätanslutningspunkt samt vid internetåtkomst. Uppgifterna ska lagras i två–tio månader beroende på typen av uppgifter. Lagringstiden räknas från den dag kommunikationen avslutades (9 kap. 22 §).

För att säkerställa att de abonnemangsuppgifter som avser kontantkort lagras och kan lämnas ut till brottsbekämpande myndigheter är det nödvändigt med särskilda bestämmelser om lagring, även om det medför en viss dubbelreglering i förhållande till lagringsskyldigheten i 9 kap. 19 § nya LEK. Lagringsskyldigheten enligt den paragrafen förutsätter nämligen att tillhandahållaren har genererat eller behandlat uppgifterna. Det är inte säkert att tillhandahållarna skulle fortsätta att behandla de registrerade uppgifterna efter registrering utan en skyldighet att göra det. Om abonnenten exempelvis inte lämnat samtycke till behandling i marknadsföringssyfte kan tillhandahållaren sakna skäl att behandla uppgifterna för egna ändamål. Om ett kontantkort skulle användas för kommunikation först en viss tid efter registrering skulle därmed situationen kunna uppstå att tillhandahållaren inte har några abonnemangsuppgifter att lagra enligt 9 kap. 19 §. Vidare förekommer det att telefonnummer kopplade till kontantkort endast används för att starta konton i vissa appar. I sådant fall sker ingen sådan kommunikation som gör att lagringsskyldigheten aktualiseras. 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 avseende kort som ännu inte har använts för kommunikation.

Vid en internationell utblick kan det konstateras att abonnemangsuppgifter om kontantkortskunder bevaras under olika lång tid i olika europeiska länder. I något fall ska uppgifterna raderas direkt efter att ett avtal har upphört och i något fall bevaras de i tre år. I Tyskland ska de insamlade uppgifterna raderas i slutet av kalenderåret året efter det att avtalet har upphört. Europadomstolen konstaterade i det ovan nämnda 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 som tjänsten är i bruk. Med hänsyn till att en brottsutredning kan pågå en längre tid än den tid en förbetald tjänst tillhandahålls bör uppgifterna, som

Ekobrottsmyndigheten också påpekar, lagras en viss tid efter det. Som framgått förekommer det t.ex. att telefonnummer som tillhör kontantkort används för att aktivera konton i olika 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 kontona, kan de brottsbekämpande myndigheterna därför ha behov av att få tillgång till abonnemangsuppgifterna efter en längre tid. Samtidigt kommer en lagring av de abonnemangsuppgifter som avser kontantkortskunder att medföra att tillhandahållarna har tillgång till uppgifter om ett stort antal enskilda, varav de flesta inte är av intresse för brottsbekämpande myndigheter. Som framhålls ovan kan uppgifterna dock inte anses särskilt känsliga ur integritetssynpunkt. Mot denna bakgrund anser regeringen, i likhet med promemorian och Ekobrottsmyndigheten men till skillnad från *Hi3G Access AB*, att ett år efter det att tillhandahållandet av tjänsten har upphört utgör en rimlig och proportionerlig lagringstid. De registrerade uppgifterna bör således finnas tillgängliga hos tillhandahållaren från och med registreringen till och med ett år efter att tillhandahållandet av tjänsten har upphört. Att tillhandhållandet har upphört kan, som Hi3G Access AB anför, t.ex. bero på en nummerportering, dvs. att ett nummer lämnas över till en annan tillhandahållare, eller att tillhandahållaren avslutar tjänsten på grund av att den inte har använts under en längre tid.

4.2.3 Abonnentens identitet ska kontrolleras

Regeringens förslag: I samband med en registrering ska abonnentens identitet kontrolleras genom en giltig identitetshandling eller en tillförlitlig elektronisk identifiering. Om abonnenten saknar sådana handlingar och verktyg får identiteten göras sannolik på annat sätt. Identitetskontrollen ska dokumenteras.

Om abonnenten är en juridisk person ska identitetskontrollen avse den som företräder den juridiska personen.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om identitetskontrollen.

Promemorians förslag överensstämmer i huvudsak med regeringens. Promemorians förslag innehåller ingen bestämmelse om identitetskontroll av den som företräder en juridisk person. I promemorian föreslås inget normgivningsbemyndigande.

Remissinstanserna: Ingen remissinstans motsätter sig att abonnentens identitet ska kontrolleras. Enligt *Hi3G Access AB* är det viktigt att den som tillhandahåller tjänsten inte ska behöva tillämpa och i verksamheten anpassa sig efter alla i promemorian godkända metoder för identifiering, utan kunna tillämpa en av dessa metoder, t.ex. elektronisk identifiering. Vidare anser bolaget att det är oklart hur identifieringen ska gå till när det gäller juridiska personer, vid godmansförordnanden och förvaltarskap samt när en vårdnadshavare ska intyga ett barns identitet. När det gäller juridiska personer undrar bolaget om den juridiska personens firma och organisationsnummer ska kontrolleras och om det ska genomföras en identitetskontroll på behörig företrädare för den juridiska personen. *Tele2 Sverige AB* anser att det är oklart hur en identitetskontroll ska göras digitalt

för det fall en kontantkortskund saknar bank-id. Bolaget anser även att det bör förtydligas att en identitetskontroll inte behöver utföras med tekniska hjälpmedel. Vidare framhåller bolaget att det bör vara möjligt att erbjuda kunder som påbörjat ett digitalt köp av ett kontantkort, men som inte har kunnat identifiera sig med bank-id, att dels få kontantkortet hemskickat till den adress som i folkbokföringsdatabasen är registrerad på det namn som anges vid det digitala köpet, dels kunna hämta ut kontantkortet hos valfri butik eller agent mot uppvisande av identitetshandling med fotografi. Metoden med folkbokföringsadress tillämpas i dag för abonnemangstjänster. *IT&Telekomföretagen* pekar på att förslaget, vid försäljning online, riskerar att öka den digitala klyftan eftersom inte alla har eller kan få tillgång till en e-legitimation och därmed inte kan bevisa sin identitet digitalt. *PTS* anför att det är av vikt att enskilda inte utesluts från möjligheten att använda kontantkort på grund av att de inte har tillgång till en viss identitetshandling. *Umeå universitetet* framför liknande synpunkter. Vissa remissinstanser pekar på ett behov av närmare myndighetsföreskrifter, däribland *Ekobrottsmyndigheten*, *PTS* och *Hi3G Access AB*.

Skälen för regeringens förslag: Det måste säkerställas att de uppgifter som lämnas om enskilda abonnenter av förbetalda tjänster är korrekta. De identitetsuppgifter som lämnas bör därför kontrolleras. Kontrollen bör i första hand ske gentemot en identitetshandling. Som framgår av promemorian finns det ett flertal olika identitetshandlingar som normalt godtas för identifiering i Sverige och flera andra handlingar som godtas för identifiering i vissa fall. Som *PTS* framhåller är det viktigt att enskilda inte utesluts från möjligheten att använda kontantkort på grund av att de inte har tillgång till en viss identitetshandling. För att få registrera sig som abonnent av en förbetald tjänst bör det därför vara tillräckligt att en enskild uppvisar någon form av giltig identitetshandling. Med detta avses t.ex. en passhandling, ett id-kort eller ett körkort. Även ett sådant tjänstekort som regleras i förordningen (1958:272) om tjänstekort bör kunna godtas. För att inte utestänga personer som saknar en svensk identitetshandling, t.ex. turister och andra personer som tillfälligt besöker Sverige, från möjligheten att använda svenska kontantkort bör även utländska identitetshandlingar godtas.

Identitetskontrollen bör inte bara kunna göras i samband med besök i en fysisk butik utan även vid registrering via internet eller vid kontakt med en kundtjänst. En sådan identitetskontroll bör i första hand göras med hjälp av en e-legitimation som t.ex. bank-id. I lagtexten kan detta lämpligen, med 12 kap 2 § spellagen (2018:1138) som förebild, uttryckas så att abonnentens identitet får kontrolleras genom användning av en tillförlitlig elektronisk identifiering, jfr propositionen En omreglerad spelmarknad (prop. 2017/18:220 s. 318). Uttrycket elektronisk identifiering definieras i artikel 3.1 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. Som *IT&Telekomföretagen* pekar på finns det visserligen personer som inte har tillgång till en e-legitimation. För dessa personer finns det emellertid andra godtagbara sätt att kontrollera identiteten.

Sammanfattningsvis anser regeringen att det bör införas ett krav på att abonnentens identitet ska kontrolleras genom en giltig identitetshandling eller en tillförlitlig elektronisk identifiering.

Det finns personer som saknar identitetshandlingar och inte heller har tillgång till en e-legitimation. Det kan t.ex. handla om barn. För att sådana personer inte ska utestängas från möjligheten att använda kontantkort, bör deras identitet få göras sannolik på annat sätt. Ett barns identitet bör t.ex. kunna kontrolleras genom att en nära anhörig, som har en godtagbar identitetshandling, intygar barnets identitet.

Ett krav på identitetskontroll innebär inte att den som ska utföra registreringen måste anpassa verksamheten efter alla godtagbara metoder för identifiering, vilket *Hi3G Access AB* önskar ett klargörande av. Det är tillräckligt att den identitetskontroll som faktiskt genomförs uppfyller kraven. Vidare bör, som *Tele2 Sverige AB* anför, identitetskontrollen av den som påbörjat ett digitalt köp kunna göras i samband med att personen hämtar ut ett kontantkort i en butik. Regeringen anser däremot inte, till skillnad från Tele2 Sverige AB, att det bör vara möjligt att få kontantkortet hemskickat till den adress som i folkbokföringsdatabasen är registrerad på det namn som anges vid det digitala köpet. Ett sådant förfarande kan inte anses förenligt med ett krav på att abonnentens identitet ska kontrolleras.

Det bör även finnas en kontrollmekanism för att identitetskontrollen utförs på ett korrekt sätt. Regleringen bör därför innehålla ett krav på att identitetskontrollen ska dokumenteras. En sådan dokumentation skulle t.ex. kunna avse en anteckning om vilken identitetshandling som har använts.

Som *Hi3G Access AB* pekar på framgår det inte uttryckligen av promemorians lagförslag hur identitetskontrollen ska gå till när abonnenten är en juridisk person. För att göra regleringen så tydlig som möjligt och för att undvika att juridiska personer används för att kringgå registreringsskyldigheten, bör det införas en särskild bestämmelse om detta. Det framstår som en ändamålsenlig ordning att identitetskontrollen, i de fall abonnenten är en juridisk person, ska avse den fysiska person som företräder den juridiska personen vid registreringen. Av ett sådant krav får det även anses följa att företrädaren måste kunna styrka sin rätt att företräda den juridiska personen. Hi3G Access AB anser vidare att det är oklart hur identitetskontrollen ska gå till när abonnenten har god man eller förvaltare. Förslaget innebär att även sådana abonnenter omfattas av kravet på identitetskontroll. I de fall en god man eller förvaltare har införskaffat ett kontantkort för sin huvudmans räkning behöver huvudmannens identitet alltså kontrolleras innan tjänsten börjar användas.

I promemorian föreslås en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela närmare föreskrifter om identitetskontrollen. Regeringen instämmer i att bestämmelserna om identitetskontroll kan behöva kompletteras med föreskrifter på lägre nivå än lag. För att säkerställa att det finns stöd för att meddela de föreskrifter som behövs, anser regeringen att det bör finnas ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela ytterligare föreskrifter om identitetskontrollen.

4.3 Tjänster som används av någon annan än den registrerade abonnenten

Regeringens förslag: Om en förbetald tjänst används av någon annan än den registrerade abonnenten utan att en ny registrering har gjorts, ska tillhandahållandet av tjänsten avbrytas. Detta gäller dock inte om

- tjänsten endast tillfälligt används av någon annan än den registrerade abonnenten
- tjänsten används av en närstående till den registrerade abonnenten
- den registrerade abonnenten är en juridisk person och tjänsten används på dennes uppdrag
- tjänsten har införskaffats på uppdrag av Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som ska ingripa mot brott
- tjänsten har införskaffats på uppdrag av en myndighet som bedriver försvarsunderrättelseverksamhet.

Promemorians förslag överensstämmer i huvudsak med regeringens. Enligt promemorians förslag är det avgörande momentet att tjänsten har överlåtits utan att en ny registrering har skett. Promemorians förslag innehåller inget undantag för myndigheter som bedriver försvarsunderrättelseverksamhet.

Remissinstanserna: En majoritet av remissinstanserna är positiva till förslaget eller har ingen invändning mot det. *Säkerhetspolisen* framhåller att förslaget är en viktig del av regleringen, men anser att det avgörande momentet överlåtelse medför en risk för luckor i regleringen för de fall den registrerade påstår sig ha tappat bort eller på annat sätt blivit av med sitt kontantkort. Det bör enligt Säkerhetspolisen framgå att tillhandahållaren även i dessa fall ska avbryta tjänsten. *Förvaltningsrätten i Stockholm*, *Hi3G Access AB* och *PTS* pekar på svårigheter för tillhandahållare och tillsynsmyndigheten att kontrollera vem som använder en tjänst och om en tjänst har överlåtits i enlighet med något undantag. PTS anför att regleringen därmed främst torde innebära en möjlighet för brottsbekämpande myndigheter att uppmärksamma tillhandahållarna på de fall där det inom ramen för utredningar framkommer att en förbetald tjänst används av någon annan än den registrerade abonnenten. Hi3G Access AB och *IT&Telekomföretagen* pekar på oklarheter när det gäller vilket underlag som ska krävas för att tillhandahållaren ska avbryta tjänsten. Båda remissinstanserna anser att den omständigheten att en brottsbekämpande myndighet har uppmärksammat tillhandahållaren på att en överlåtelse torde ha ägt rum, inte bör vara tillräcklig och tar upp tillhandahållarens skadeståndsansvar gentemot abonnenten. IT&Telekomföretagen anser vidare att det är tveksamt om den föreslagna regeln kan bli särskilt effektiv för brottsbekämpningen samtidigt som regeln är svårtillämpad och lägger ett stort utredningsansvar på tillhandahållaren. IT&Telekomföretagen avstyrker därför förslaget. Enligt *Hi3G Access AB* bör det tydliggöras att tillhandahållarens åtgärd att avbryta tjänsten på grund av utebliven registrering inte utgör en integritetsincident som behöver rapporteras till tillsynsmyndigheten. *Telenor Sverige AB* anser att ett beslut om nedstängning riktat mot tillhandahållaren innebär myndig-

hetsutövning mot enskild och att ett sådant beslut inom ramen för en brottsutredning i praktiken är ett hemligt tvångsmedel. En laglig grund för en myndighets beslut om att stänga ned en tjänst bör enligt bolaget i stället lämpligen föras in i rättegångsbalkens kapitel om hemliga tvångsmedel.

Vissa remissinstanser yttrar sig över den del av förslaget som handlar om undantag från registreringsskyldigheten vid överlåtelse. *Försvarsmakten* tillstyrker förslaget att undanta myndigheten men anser att det behöver klargöras att undantaget omfattar samtliga delar av myndighetens verksamhet. *Försvarets materielverk*, *Försvarets radioanstalt* och *Totalförsvarets forskningsinstitut* anser att förslaget bör kompletteras med en punkt som undantar myndigheter som bedriver verksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet från kravet på registrering vid överlåtelse. Enligt Försvarets materielverk och Försvarets radioanstalt kan det alternativt övervägas om regeringen bör få mandat att meddela undantag från kravet. *Tullverket* är positivt till att myndigheten undantas från registreringsskyldigheten vid överlåtelse. *Kammarrätten i Stockholm* noterar att undantaget för juridiska personer enligt promemorian förutsätter att den juridiska personen har kännedom om vem i personalen eller bland uppdragstagarna som använder den aktuella tjänsten, vilket inte framgår av lagtexten. *Tullverket* anser att undantaget omfattar en alltför vid krets av personer. Vidare anser Tullverket att förslaget kan behöva kompletteras med en undersökningsplikt för tillhandahållarna.

Skälen för regeringens förslag

Ny registrering när tjänsten används av någon annan

Som framgår av avsnitt 4.2.2 föreslås en registrering avse uppgifter om abonnenten, dvs. den som har ingått ett avtal med en tillhandahållare om en förbetald tjänst. Det kan dock uppstå situationer där den registrerade abonnenten därefter väljer att låta någon annan använda tjänsten. Exempelvis kan en person köpa och registrera sig som abonnent för tjänster som är knutna till ett kontantkort som senare överlåts till hans eller hennes barn eller någon annan anhörig. 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 övertas av någon annan. Ett sådant förfarande väcker frågan om det bör införas något lagkrav gällande överföringar av registrerade förbetalda tjänster.

Enligt promemorian föreskrivs i den belgiska regleringen 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 särskilt angivna 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 tillhandahållaren. Vid överträdelser av regleringen kan sanktioner beslutas.

En lagreglering som innebär att det är den som tagit över en förbetald tjänst som också ska vara registrerad som abonnent av tjänsten skulle vara

till nytta för brottsbekämpningen. Genom en sådan reglering skulle det i högre grad vara möjligt att säkerställa att de abonnemangsuppgifter som har registrerats avser den verkliga brukaren av tjänsten. På så sätt skulle de registrerade uppgifterna i större utsträckning kunna komma till nytta i det brottsbekämpande arbetet.

Visserligen lär det, som bl.a. *PTS* och *Förvaltningsrätten i Stockholm* framhåller, vara svårt för tillhandahållarna och tillsynsmyndigheten att kontrollera om den registrerade abonnenten också är den som faktiskt använder tjänsten. En reglering i frågan skulle ändå vara av värde. En regel som innebär att en ny registrering ska göras om en förbetald tjänst övertagits av någon annan skulle rimligtvis efterföljas av de allra flesta. För de kriminella skulle regleringen i vart fall innebära ett försvårande. Denna effekt skulle sannolikt bli större om regleringen innehåller ett krav på att tillhandahållaren ska stänga av en förbetald tjänst som har övertagits av någon annan utan att en ny registrering har gjorts. Med en sådan reglering skulle det dessutom vara möjligt för en brottsbekämpande myndighet att vända sig till en tillhandahållare 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.

Regeringen anser mot denna bakgrund att det bör införas ett krav på tillhandahållaren att avbryta tillhandahållandet av en förbetald tjänst om det framkommer att tjänsten har övertagits av en annan person utan att en ny registrering har gjorts. Som *Säkerhetspolisen* framhåller är detta en viktig del av regleringen av registrering av förbetalda tjänster.

Promemorians förslag är utformat på så sätt att det avgörande momentet är att en förbetald tjänst har överlåtits. Bestämmelsen bör enligt regeringens mening emellertid omfatta vissa situationer som inte innefattar en överlåtelse, t.ex. långvariga lån av kontantkort. Som *Säkerhetspolisen* påpekar är det också tveksamt om promemorians förslag ger stöd för att avbryta tillhandahållandet av en tjänst om en abonnent påstår sig ha tappat bort eller på annat sätt blivit av med ett kontantkort. Regeringen anser mot denna bakgrund att kravet på ny registrering bör gälla om en förbetald tjänst används av någon annan än den registrerade abonnenten.

Kravet på ny registrering innebär, till skillnad från vad *Telenor Sverige AB* anför, inte att en brottsbekämpande myndighet med stöd av regleringen kan besluta att en tillhandahållare ska avbryta tillhandahållandet av en tjänst. Det är tillhandahållaren som ska vara skyldig att avbryta tillhandahållandet och som ska avgöra om skyldigheten har inträtt. När det gäller underlaget för det ställningstagandet, som *Hi3G Access AB* och *IT&Telekomföretagen* efterfrågar vägledning kring, får tillhandahållaren göra en bedömning i det enskilda fallet. Ytterst har tillsynsmyndigheten tillsyn över att regleringen följs (11 kap. 1 § nya LEK). Tillhandahållarna har emellertid i normalfallet anledning att förlita sig på uppgifter från de brottsbekämpande myndigheterna. Avsikten med kravet på en ny registrering är inte att tillhandahållarna ska vara skyldiga att på eget initiativ kontrollera vem som använder en viss registrerad tjänst. Med

anledning av det förtydligande som *Hi3G Access AB* efterfrågar kan det slutligen tilläggas att ett avbrytande inte i sig utgör en integritetsincident.

Undantag från kravet på ny registrering

Det finns vissa situationer då det inte är lämpligt att kräva en ny registrering, trots att en förbetald tjänst används av någon annan än den registrerade abonnenten. Det bör därför införas vissa undantag. Det skulle vara alltför långtgående att kräva en ny registrering om tjänsten endast tillfälligt används av någon annan, t.ex. för att ringa något eller några samtal. Det bör därför införas ett undantag för den situationen. Vidare framstår det inte som problematiskt att en tjänst används av en närstående till den registrerade abonnenten, t.ex. ett barn. Sådan användning bör därför vara undantagen från kravet på ny registrering. För att inte lägga en onödig administrativ börda på företag bör det också vara tillåtet för en juridisk person att låta anställda och uppdragstagare använda förbetalda tjänster som har registrerats på den juridiska personen. En förutsättning bör vara att tjänsten används på den juridiska personens uppdrag. Att den juridiska personen ska ha kännedom om vem som använder tjänsten är, som *Kammarrätten i Stockholm* noterar, inget krav som uttryckligen följer av förslaget. För att tjänsten ska kunna anses användas på den juridiska personens uppdrag, får det emellertid förutsättas att den juridiska personen har kännedom om vem bland anställda eller uppdragstagare som använder tjänsten. Slutligen finns det vissa myndigheter som har behov av att låta personer använda förbetalda tjänster utan att dessa personer ska behöva registreras hos tillhandahållarna. Ett tydligt behov av en sådan hantering finns inom brottsbekämpningen, där kontantkort kan behöva användas av informatörer. Mot denna bakgrund bör kravet på ny registrering inte gälla om en tjänst har införskaffats på uppdrag av Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som har till uppgift att ingripa mot brott. Ett behov av att kunna använda förbetalda tjänster utan krav på registrering av användaren finns även inom försvarsunderrättelseverksamhet. Myndigheter som bedriver verksamhet enligt lagen om försvarsunderrättelseverksamhet bör därför, som bl.a. *Försvarets materielverk* och *Försvarets radioanstalt* föreslår, vara undantagna från kravet på ny registrering. Eftersom Försvarsmakten är en sådan myndighet behöver den, till skillnad från hur förslaget är utformat i promemorian, inte särskilt anges som en sådan myndighet som har till uppgift att ingripa mot brott. I detta sammanhang bör det, i enlighet med *Försvarsmaktens* önskemål om ett förtydligande, framhållas att det föreslagna undantaget är begränsat till vissa myndigheter, inte till viss verksamhet som myndigheterna bedriver.

Regeringen delar inte *Tullverkets* uppfattning att det föreslagna undantaget omfattar en alltför vid krets av personer. Regeringen ser inte heller ett behov av en sådan undersökningsplikt som Tullverket efterfrågar.

4.4 Ingen begränsning av antalet registrerade förbetalda tjänster eller av användningen av utländska kontantkort

Regeringens bedömning: Det bör inte införas någon begränsning av det antal förbetalda tjänster som en enskild fysik eller juridisk person får registrera eller av möjligheten att använda utländska kontantkort.

Promemorians bedömning överensstämmer med regeringens.

Remissinstanserna: Endast *Tullverket* yttrar sig särskilt i denna del. Tullverket anser att bedömningen att det inte bör införas någon begränsning av antalet registrerade tjänster medför en risk för användning av många målvakter. För att om möjligt kunna begränsa problemet föreslår Tullverket att tillhandahållarna ges ett lagligt stöd att kunna uppmärksamma de brottsbekämpande myndigheterna på risken för målvakter. Förslagsvis kan en bestämmelse införas som gör det möjligt för en tillhandahållare att i samband med en förfrågan även informera den brottsbekämpande myndigheten om att en privatperson innehar ett visst antal abonnemang för kontantkort.

Skälen för regeringens bedömning: Syftet med att införa en begränsning av det antal förbetalda tjänster som får registreras av en enskild skulle vara att minska risken för att målvakter används för registreringen. En begränsning gällande hur många kontantkort som får innehas finns enligt promemorian i Ungern och Turkiet, men inte i några andra europeiska länder. Regeringen anser, i enlighet med promemorians bedömning, att det finns skäl som talar mot att införa en sådan begränsning. Ett tak för hur många tjänster som får registreras av en viss fysisk eller juridisk person skulle t.ex. innebära att tillhandahållarna skulle bli tvungna att göra kontroller sinsemellan inför varje registrering. Visserligen kan man tänka sig en ordning där varje tillhandahållare endast får registrera ett visst antal förbetalda tjänster på en viss person och att en kontroll mot andra tillhandahållare därmed inte skulle behöva göras. Ett system med en begränsning av antalet tjänster som får registreras skulle dock innebära ytterligare åligganden för tillhandahållarna. Det kan också konstateras att det antal 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 eller andra närstående. 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. Regeringen anser därför att övervägande skäl talar mot en begränsning av antalet registrerade förbetalda tjänster.

Tullverket föreslår att det införs en bestämmelse som gör det möjligt för en tillhandahållare att i samband med en förfrågan även informera den brottsbekämpande myndigheten om att en privatperson innehar ett visst antal abonnemang för kontantkort. Det kan konstateras att det kommer att vara möjligt för brottsbekämpande myndigheter att, med stöd av befintliga regler om inhämtning av abonnemangsuppgifter, begära in uppgifter om antalet registrerade förbetalda tjänster. Regeringen finner därför inte

anledning att föreslå en sådan särskild bestämmelse som Tullverket efterfrågar.

När det gäller frågan om att begränsa möjligheten att använda utländska kontantkort framgår det av promemorian att det finns tekniska hinder mot att införa en begränsning som enbart skulle gälla kontantkort och inte kontraktsabonnemang. En begränsning för även med sig EU-rättsliga problem och någon motsvarande lagstiftning har inte införts i någon annan medlemsstat i EU. Regeringen instämmer därför i promemorians bedömning att det inte bör införas någon begränsning av användningen av utländska kontantkort, vilket ingen remissinstans invänder mot.

Sammanfattningsvis anser regeringen att det inte bör införas någon begränsning av antalet förbetalda tjänster som en enskild fysisk eller juridisk person får registrera eller av möjligheten att använda utländska kontantkort.

4.5 Tillsyn

Regeringens bedömning: Det behövs inga särskilda bestämmelser om tillsyn avseende registreringsskyldigheten.

Promemorians bedömning överensstämmer med regeringens.

Remissinstanserna: De remissinstanser som yttrar sig särskilt i denna del, *Säkerhetspolisen* och *Brottsförebyggande rådet*, anser att det bör övervägas att införa en möjlighet att ta ut en sanktionsavgift av den som inte uppfyller registreringskravet.

Skälen för regeringens bedömning: Eftersom registreringsskyldigheten föreslås regleras i nya LEK kommer tillsynsmyndigheten, dvs. PTS, att ha tillsyn över efterlevnaden av de föreslagna bestämmelserna. Tillsynsområdet omfattar såväl tillhandahållarnas som återförsäljarnas agerande t.ex. i samband med en identitetskontroll. Tillsynsmyndigheten har bl.a. rätt att för tillsynen få tillträde till områden, lokaler och vissa andra utrymmen där verksamhet som omfattas av nya LEK bedrivs. Tillsynsmyndigheten får också meddela förelägganden som kan förenas med vite. Den tillsynsreglering som finns kan användas även för att säkerställa att registreringsskyldigheten följs. Det behövs därför inga särskilda bestämmelser om tillsyn avseende registreringsskyldigheten.

I och med nya LEK föreslås att tillsynsmyndigheten ska ta ut sanktionsavgifter vid vissa överträdelser. Inom ramen för detta lagstiftningsärende är det inte möjligt att, som *Säkerhetspolisen* och *Brottsförebyggande rådet* efterfrågar, överväga om möjligheten att ta ut sanktionsavgifter bör omfatta även registreringskravet för kontantkort.

5 Tydligare regler om utlämnande av uppgifter om elektronisk kommunikation

5.1 Ett tydligare krav på hur uppgifter ska göras tillgängliga för brottsbekämpande myndigheter

Regeringens förslag: När den som bedriver verksamhet som ska anmälas enligt den nya lagen om elektronisk kommunikation lämnar ut uppgifter om abonnemang, uppgifter som avser innehållet i ett elektroniskt meddelande, andra uppgifter som angår ett särskilt elektroniskt meddelande eller lokaliseringsuppgifter som inte är trafikuppgifter till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott, ska uppgifterna, om de gäller brottslig verksamhet eller misstanke om brott, ordnas och göras tillgängliga i ett format som gör att de enkelt kan tas om hand.

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

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om format.

Bestämmelsen om sanktionsavgifter vid överträdelser av kravet på hur uppgifter ska göras tillgängliga utvidgas till att avse även andra uppgifter än sådana som avser avlyssnade eller övervakade meddelanden.

De särskilda bestämmelserna om tillgängliggörande av uppgifter som lagras för brottsbekämpande ändamål, uppgifter som är föremål för ett föreläggande om bevarande och uppgifter som avser avlyssnade eller övervakade meddelanden upphör att gälla.

Promemorians förslag överensstämmer i huvudsak med regeringens. Promemorians förslag innehåller ingen avgränsning till anmälningspliktig verksamhet. I promemorian föreslås inget normgivningsbemyndigande eller någon möjlighet att besluta om undantag i enskilda fall. I promemorian föreslås inte någon möjlighet att ta ut sanktionsavgift.

Remissinstanserna: En majoritet av remissinstanserna, däribland *Brottsförebyggande rådet*, *Ekobrottsmyndigheten*, *Polismyndigheten*, *PTS*, *Riksdagens ombudsmän*, *Säkerhetspolisen*, *Säkerhets- och integritetsskyddsnämnden*, *Tullverket* och *Unizon*, är positiva till förslaget eller har inget att invända mot det. Tullverket anser att förslaget bör kunna effektivisera inhämtningen av uppgifter i underrättelseverksamhet och under förundersökning genom att de inhämtade uppgifterna inte behöver bearbetas ytterligare för att kunna analyseras. Polismyndigheten framhåller att det är angeläget att förslaget genomförs så snart som möjligt så att man kommer till rätta med de oklarheter som i dag råder kring i vilket format uppgifter ska lämnas ut. *Hi3G Access AB* anser att ett krav på ett gemensamt format är rimligt eftersom det torde förbättra, förenkla och kanske även påskynda tillhandahållarnas verkställighet mot brotts-bekämpande myndigheter.

Telenor Sverige AB pekar på att det mot bakgrund av det pågående arbetet mellan brottsutredande myndigheter och tillhandahållare när det gäller enhetliga format inte finns något uttalat behov av lagreglering på området. *Verizon Sweden AB* anser att ett lagkrav om att uppgifter ska lämnas i ett speciellt format bör införas på EU-nivå, eftersom ett sådant nationellt krav innebär att det uppstår ytterligare hinder mot förverkligandet av den digitala inre marknaden. Bolaget anför vidare att nyttan med att ha ett gemensamt format inte uppväger kostnaden för att underhålla ett sådant system för tillhandahållare som endast lämnar ut ett mindre antal uppgifter. *Hi3G Access AB* anser att det bör införas en skyldighet för de brottsbekämpande myndigheterna att använda det gemensamma formatet i sina förfrågningar till tillhandahållarna. *PTS* betonar vikten av att de brottsbekämpande myndigheterna fortsätter sitt arbete med att begränsa antalet kontaktpunkter och att skapa enhetliga rutiner för inhämtandet av uppgifter om elektronisk kommunikation. *Tullverket* och *Förvaltningsrätten i Stockholm* framför vissa lagtekniska synpunkter.

Skälen för regeringens förslag

Den nuvarande regleringen orsakar problem för brottsbekämpande myndigheter

Det saknas närmare reglering om i vilket format uppgifter om elektronisk kommunikation ska lämnas ut från tillhandahållare till brottsbekämpande myndigheter. I nya LEK anges att innehållet i och uppgifter om avlyssnade eller övervakade meddelanden ska göras tillgängliga så att informationen enkelt kan tas om hand (9 kap. 29 § andra stycket). Kravet infördes redan i den äldre telelagen (1993:597) och angavs innebära att om teleoperatören kodar, komprimerar eller krypterar telemeddelandena måste dessa levereras i klartext (prop. 1995/96:180 s. 27 och 28). Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om kravet (9 kap. 29 § tredje stycket nya LEK). Några sådana föreskrifter har inte meddelats. För uppgifter som lagras för brottsbekämpande ändamål finns ett särskilt krav på att uppgifterna ska göras tillgängliga på ett sådant sätt att informationen enkelt kan tas om hand (9 kap. 24 § nya LEK). Enligt förarbetena innebär kravet att de lagringsskyldiga måste se till att de brottsbekämpande myndigheterna utan ansträngning kan ta del av uppgifterna även om uppgifterna skulle finnas i exempelvis krypterad eller komprimerad form hos den lagringsskyldige (prop. 2010/11:46 s. 81). Det finns inte någon föreskriftsrätt för regeringen eller den myndighet som regeringen bestämmer kopplad till 9 kap. 24 § nya LEK. Sedan den 1 maj 2021 gäller kravet i bestämmelsen på motsvarande sätt för en uppgift som omfattas av ett föreläggande om bevarande som har meddelats med stöd av 27 kap. 16 § rättegångsbalken (9 kap. 25 § nya LEK).

I dag finns det alltså vissa krav på hur uppgifterna ska göras tillgängliga när det gäller uppgifter som lagras för brottsbekämpande ändamål, som omfattas av ett föreläggande om bevarande eller som avser meddelanden som är föremål för hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation. Av de beskrivna bestämmelserna framgår dock inte att de uppgifter som lämnas ut ska vara möjliga att utan

bearbetning användas av brottsbekämpande myndigheter i sitt analysarbete. Dessutom faller bl.a. abonnemangsuppgifter som varken omfattas av lagringsskyldigheten eller ett föreläggande om bevarande utanför kraven på hur uppgifter ska göras tillgängliga.

Av promemorian framgår att bristen på närmare reglering om i vilket format uppgifter ska lämnas ut från tillhandahållare till brottsbekämpande myndigheter orsakar problem. Uppgifter om elektronisk kommunikation behandlas hos tillhandahållarna i olika datasystem som varierar mellan tillhandahållarna och uppgifterna levereras i det format som används av tillhandahållaren. Därmed får de brottsbekämpande myndigheterna tillgång till uppgifter i skilda format beroende på vilken aktör som tillhandahåller uppgifterna. Även sammanställningar från en och samma tillhandahållare förekommer i olika format. Vidare betecknas många gånger samma parametrar på olika sätt av olika tillhandahållare. Uppgiftssammanställningar från olika tillhandahållare saknar alltså en gemensam struktur. Många gånger förutsätts att tillhandahållarna kan ge vägledning om innebörden av olika parametrar för att uppgifterna ska gå att utläsa. De listor som översänds kan inte heller alltid läsas maskinellt. Enligt promemorian gäller problematiken när historiska uppgifter hämtas in genom beslut om hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation med stöd av bestämmelserna i 27 kap. rättegångsbalken, preventivlagen, lagen om särskild utlänningskontroll eller inhämtningslagen, men kan också avse abonnemangsuppgifter som hämtas in vid misstanke om brott (9 kap. 33 § första stycket 2 nya LEK). Uppgifterna hämtas främst in från de fyra största mobiloperatörerna som också är nätägare. Abonnemangsuppgifter hämtas dock in från den tillhandahållare som ansvarar för det aktuella abonnemanget. Problemen är enligt promemorian inte endast kopplade till sådana uppgifter som lagras hos tillhandahållarna för brottsbekämpande ändamål (9 kap. 19 § nya LEK), utan omfattar även uppgifter som tillhandahållarna lagrar för andra ändamål. Realtidsuppgifter lämnas dock ut i ett gemensamt format.

För att informationen från tillhandahållarna ska kunna analyseras och användas för utredningsåtgärder krävs att informationen först bearbetas av de brottsbekämpande myndigheterna. På grund av de beskrivna problemen krävs en omfattande arbetsinsats under bearbetningsfasen. 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 analysera informationen på ett effektivt sätt. Bearbetningen av uppgifter tar i dagsläget ofta längre tid än själva analysarbetet.

Problematiken kan illustreras med ett exempel som tas upp i promemorian. I samband med terrordådet på Drottninggatan i Stockholm i april 2017 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. Tillhandahållarna lämnade sina samtalslistor i olika format. En tillhandahållare lämnade samma typ av lista i 50 olika format. Polisens arbete med att bearbeta filerna uppgick till ca 500 arbetstimmar. Följden blev att analysarbetet i brottsutredningen blev kraftigt försenat.

Avsaknaden av en gemensam standard för de uppgifter som lämnas ut från tillhandahållarna medför alltså att tid och resurser måste läggas ned på att bearbeta uppgifterna. Arbetet är många gånger utdraget och krävande och det finns ingen garanti för att det eftersträvade resultatet kan uppnås. I värsta fall kan den fördröjning som bearbetningen innebär medföra att avgörande utredningsåtgärder inte kan genomföras eller att ett förestående brott inte kan förhindras. Många gånger ger bearbetningen dessutom upphov till felaktigheter som upptäcks först i analysfasen. Avsaknaden av en gemensam standard påverkar alltså även tillförlitligheten av de uppgifter som ingår i analysen.

Kravet på tillgängliggörande bör utvidgas och skärpas

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 tillhandahållarna inte följer en gemensam standard. Regeringen bedömer i likhet med *Tullverket* att enhetliga format för utlämnande även av historiska uppgifter och abonnemangsuppgifter skulle innebära stora fördelar för de brottsbekämpande myndigheterna. Myndigheterna skulle då få möjlighet att bearbeta informationen snabbt, korrekt och kostnadseffektivt. En användning av enhetliga format bör också, som *Hi3G Access AB* framhåller, effektivisera och underlätta arbetet för tillhandahållarna.

Som framgår av promemorian pågår det för närvarande ett projekt som syftar till att standardisera de format som används vid utlämnande av uppgifter om elektronisk kommunikation från tillhandahållare till brottsbekämpande myndigheter. Polismyndigheten är sammankallande i projektet som kallas för FiLT (Formaterad inhämtning Leverans Teleoperatörer). I projektet deltar Polismyndigheten, Säkerhetspolisen och Tullverket. Referensdeltagare är PTS och de fyra största mobiloperatörerna. Syftet med projektet är att historiska uppgifter om elektronisk kommunikation ska lämnas ut i ett gemensamt format.

Det förhållandet att det pågår ett projekt om gemensamma format innebär inte, i motsats till vad *Telenor Sverige AB* anför, att det saknas skäl att författningsreglera frågan. Ett system som bygger på frivillighet är känsligt för förändringar och intresset av att samarbeta kan minska över tid. Även för tillhandahållarna kan det vara en fördel med klara regler som anger vilka skyldigheter som finns gentemot de brottsbekämpande myndigheterna. Inte heller finns det, till skillnad från vad *Verizon Sweden AB* framför, anledning att avstå från lagstiftning för att den innebär en nationell särreglering. Med hänsyn till detta och till frågans stora betydelse för effektiviteten i det brottsbekämpande arbetet är det därför befogat att utvidga och skärpa regelverket om i vilken form uppgifter om elektronisk kommunikation ska lämnas ut från tillhandahållare till brottsbekämpande myndigheter.

För att komma till rätta med problemen med att ostrukturerade uppgifter lämnas i olika format bör det i lag införas ett, i förhållande till dagens reglering, skärpt krav på i vilken form som uppgifter ska lämnas ut. Kravet bör lämpligen innebära att de uppgifter som lämnas ut från tillhandahållare till brottsbekämpande myndigheter ska ordnas och göras tillgängliga i ett

format som gör att de enkelt kan tas om hand. Genom en sådan reglering blir det tydligt att uppgifter som lämnas ut inte enbart ska göras tillgängliga på ett sådant sätt att de är läsbara, som i princip är fallet med dagens reglering, utan att de även ska vara sammanställda på ett sådant strukturerat sätt att de enkelt kan komma till användning i det brottsbekämpande arbetet.

På samma sätt som i dag bör kravet på hur uppgifter ska göras tillgängliga endast gälla vid utlämnande till brottsbekämpande myndigheter. Av lagtekniska skäl behöver dessa myndigheter, till skillnad från i dag, uttryckligen pekas ut i regleringen. Det bör därför framgå att bestämmelsen gäller när uppgifter lämnas ut till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott.

För att regleringen ska bli mer enhetlig bör den också utvidgas till att omfatta fler typer av uppgifter. Bestämmelsen bör lämpligen omfatta sådana uppgifter som omfattas av tillhandahållarnas tystnadsplikt enligt 9 kap. 31 § första stycket nya LEK, dvs. uppgifter om abonnemang, uppgifter som avser innehållet i ett elektroniskt meddelande och andra uppgifter som angår ett särskilt elektroniskt meddelande. Dessutom bör bestämmelsen omfatta lokaliseringsuppgifter som inte är trafikuppgifter, exempelvis uppgifter som genereras av en mobiltelefons kontakt med en basstation utan att det har varit fråga om kommunikation. Eftersom sådana uppgifter inte omfattas av tystnadsplikten behöver det särskilt anges att bestämmelsen omfattar dessa uppgifter. Någon skillnad bör inte göras mellan uppgifter som lagras hos tillhandahållarna för brottsbekämpande ändamål eller för tillhandahållarnas egna ändamål. I förhållande till dagens reglering bör alltså tillämpningsområdet utvidgas till att omfatta även andra uppgifter än sådana som lagras för brottsbekämpande ändamål, som omfattas av ett föreläggande om bevarande eller som avser meddelanden som är föremål för hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation. Det kan t.ex. röra sig om abonnemangsuppgifter eller lokaliseringsuppgifter som inte är trafikuppgifter, vilka lagras för tillhandahållarens egna ändamål och inte omfattas av ett föreläggande om bevarande.

På samma sätt som i dag bör det krävas att uppgifterna lämnas ut för brottsbekämpande ändamål. I promemorian föreslås att det i lagtexten ska anges att det handlar om uppgifter som lämnas ut för brottsbekämpning. Regeringen anser dock att avgränsningen hellre bör uttryckas genom att bestämmelsens tillämplighet förutsätter att uppgifterna gäller brottslig verksamhet eller misstanke om brott. På så sätt blir det tydligt att regleringen gäller oavsett om uppgifterna hämtas in inom ramen för en förundersökning eller i underrättelseverksamhet.

I promemorian föreslås ingen avgränsning i fråga om vilka aktörer som ska omfattas av kravet på tillgängliggörande. Tillhandahållare av nummeroberoende interpersonella kommunikationstjänster, vilket omfattar bl.a. olika kommunikationsappar, omfattas emellertid inte av någon skyldighet enligt nya LEK att lagra uppgifter för brottsbekämpande ändamål eller att lämna ut uppgifter till brottsbekämpande myndigheter (9 kap. 19 och 33 §§). Regeringen anser därför att bestämmelsen om hur uppgifter ska göras tillgängliga för brottsbekämpande myndigheter, i linje med regleringen i 9 kap. 24, 25 och 29 §§, bör avgränsas till att gälla den som

bedriver verksamhet som ska anmälas enligt 2 kap. 1 §. Regeringen har gett en särskild utredare i uppdrag att analysera förutsättningarna för att tillhandahållare av nummeroberoende interpersonella kommunikationstjänster ska kunna omfattas av skyldigheten att lagra och ge tillgång till uppgifter om elektronisk kommunikation samt ta ställning till om en sådan skyldighet bör införas. I uppdraget ingår även att analysera anpassningsskyldighetens omfattning och ta ställning till hur en reglering kan utformas på ett så tydligt, enhetligt, säkert och teknikneutralt sätt som möjligt (dir. 2021:58).

De avgränsningar som beskrivs ovan innebär att den föreslagna bestämmelsen kommer att omfatta uppgifter som lämnas ut efter beslut om hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation enligt 27 kap. rättegångsbalken, inhämtningslagen, preventivlagen, lagen om särskild utlänningskontroll, lagen om internationell rättshjälp i brottmål eller lagen om en europeisk utredningsorder. Kravet kommer även att omfatta abonnemangsuppgifter och uppgifter om vilka tillhandahållare som har deltagit vid överföringen av ett meddelande som lämnas ut med stöd av 9 kap. 33 § första stycket 2 eller 5 nya LEK.

Sammanfattningsvis bör regleringen innebära att när tillhandahållare som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § nya LEK lämnar ut uppgifter om abonnemang, uppgifter som avser innehållet i ett elektroniskt meddelande, andra uppgifter som angår ett särskilt elektroniskt meddelande eller lokaliseringsuppgifter som inte är trafikuppgifter till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott, ska uppgifterna, om de gäller brottslig verksamhet eller misstanke om brott, ordnas och göras tillgängliga i ett format som gör att de enkelt kan tas om hand.

Enligt promemorians förslag ska regleringen föras in i 6 kap. 19 § andra stycket LEK, vilket motsvarar 9 kap. 29 § andra stycket nya LEK, men läsas fristående från den paragrafens första stycke. Bestämmelserna i 9 kap. 29 § nya LEK handlar om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation och är begränsade till vissa angivna tillhandahållare. För att undvika risken att den nya regleringen tolkas mot bakgrund av den snävare regleringen i 9 kap. 29 § första stycket anser regeringen, i likhet med *Tullverket* och *Förvaltningsrätten i Stockholm*, att regleringen i stället bör införas i en ny paragraf.

Den föreslagna bestämmelsen innebär att 9 kap. 29 § andra stycket nya LEK, som gäller uppgifter som avser avlyssnade eller övervakade meddelanden, blir överflödig. Detsamma gäller bestämmelserna om hur uppgifter som lagras för brottsbekämpande ändamål och uppgifter som är föremål för ett föreläggande om bevarande ska göras tillgängliga (9 kap. 24 och 25 §§). De bestämmelserna bör därför upphöra att gälla.

Enligt 12 kap. 1 § första stycket 13 nya LEK ska tillsynsmyndigheten ta ut en sanktionsavgift av den som inte gör innehållet i och uppgifter om avlyssnade eller övervakade meddelanden tillgängliga så att informationen enkelt kan tas om hand i enlighet med 9 kap. 29 § andra stycket och föreskrifter som har meddelats i anslutning till det stycket. Någon motsvarande bestämmelse finns inte för kravet på tillgängliggörande avseende uppgifter som lagras för brottsbekämpande ändamål eller som är föremål för ett föreläggande om bevarande. Eftersom dessa frågor nu

föreslås regleras i en generell bestämmelse, framstår det som lämpligt att även möjligheten att ta ut en sanktionsavgift ska gälla generellt. Bestämmelsen om sanktionsavgifter bör därför omfatta överträdelser av den nya bestämmelsen och föreskrifter som har meddelats i anslutning till den.

Det grundläggande kravet på tillhandahållare att ordna uppgifter och göra dem tillgängliga i ett format som gör att de enkelt kan tas om hand bör alltså framgå av lag. De närmare detaljerna, t.ex. beträffande vilka format som ska användas, bör emellertid kunna regleras i föreskrifter på lägre nivå. Promemorians lagförslag innehåller en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela verkställighetsföreskrifter. För att säkerställa att det finns stöd för att meddela de föreskrifter som behövs, anser regeringen att det bör finnas ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela ytterligare föreskrifter om format.

Verizon Sweden AB anser att nyttan med ett gemensamt format inte uppväger kostnaden för att underhålla ett sådant system för tillhandahållare som endast lämnar ut ett mindre antal uppgifter. Regeringen instämmer i att det är viktigt att en ny reglering inte medför alltför stora ekonomiska och administrativa konsekvenser för tillhandahållarna. I promemorian görs bedömningen att eventuella föreskrifter kan behöva innehålla en möjlighet att ge undantag från det föreslagna kravet på format. Regeringen delar uppfattningen att det bör vara möjligt att genom beslut i enskilda fall, dvs. förvaltningsbeslut, ge undantag från kravet på format. För att ett sådant undantag ska få beslutas bör det krävas särskilda skäl, t.ex. att kravet blir alltför betungande för en mindre tillhandahållare. Möjligheten att besluta om undantag bör, till skillnad från i promemorians förslag, komma till uttryck redan i lagtexten. En sådan lösning ligger i linje med regleringen av anpassningsskyldigheten i 9 kap. 29 § nya LEK. Tillsynsmyndigheten bör mot denna bakgrund i enskilda fall få besluta om undantag från kravet på format, om det finns särskilda skäl för det.

5.2 Ett utvidgat skyndsamhetskrav

Regeringens förslag: När den som bedriver verksamhet som ska anmälas enligt den nya lagen om elektronisk kommunikation lämnar ut uppgifter om abonnemang, uppgifter som avser innehållet i ett elektroniskt meddelande, andra uppgifter som angår ett särskilt elektroniskt meddelande eller lokaliseringsuppgifter som inte är trafikuppgifter till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott, ska utlämnandet, om uppgifterna gäller brottslig verksamhet eller misstanke om brott, göras utan dröjsmål och på ett sådant sätt att utlämnandet inte röjs.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om dessa frågor.

De särskilda bestämmelserna om att uppgifter som lagras för brottsbekämpande ändamål eller är föremål för ett föreläggande om

bevarande ska lämnas ut utan dröjsmål och så att verkställandet av utlämnandet inte röjs, upphör att gälla.

Promemorians förslag överensstämmer i huvudsak med regeringens. Promemorians förslag innehåller ingen avgränsning till anmälningspliktig verksamhet. Promemorians förslag innehåller inget krav på att uppgifterna ska lämnas ut på ett sådant sätt att utlämnandet inte röjs. I promemorian föreslås inget normgivningsbemyndigande.

Remissinstanserna: En majoritet av remissinstanserna, däribland *Brottsförebyggande rådet*, *Ekobrottsmyndigheten*, *Förvaltningsrätten i Stockholm*, *Polismyndigheten*, *PTS*, *Säkerhetspolisen*, *Säkerhets- och integritetsskyddsnämnden*, *Unizon* och *Åklagarmyndigheten*, är positiva till förslaget eller har inget att invända mot det. Åklagarmyndigheten anser att förslaget kan förväntas få positiva effekter för brottsbekämpningen. Polismyndigheten framhåller att det är angeläget att förslaget genomförs så snart som möjligt så att man kommer till rätta med de oklarheter som i dag råder kring med vilken skyndsamhet uppgifter ska lämnas ut.

PTS delar uppfattningen i promemorian att uttrycket utan dröjsmål bör tolkas mot bakgrund av hur stort behovet av skyndsamhet är och de tekniska förutsättningarna för ett snabbt utlämnande i det enskilda fallet. Myndigheten framhåller att eftersom bestämmelsen omfattar en mängd olika typer av verksamheter kan såväl tekniska som administrativa förutsättningar samt antalet förfrågningar variera stort. *Hi3G Access AB* anser att förslaget är rimligt förutsatt att det finns utrymme för tillhandahållarna att göra egna prioriteringar i förhållande till den sammantagna mängden förfrågningar, den aktuella typen av förfrågan och till hur myndigheten själv uppger att man prioriterar förfrågan. *Telenor Sverige AB* kan tillstyrka att det genomgående hänvisas till uttrycket utan dröjsmål, under förutsättning att det inte görs något försök att sätta respons och verkställighetstider generellt i timmar och minuter. Enligt bolaget är det även viktigt att begärande myndigheter har standardiserade sätt att visa hur bråttom det är, så att tillhandahållaren kan göra de prioriteringar som ger störst nytta.

IT&Telekomföretagen och *Verizon Sweden AB* anser att det vore oproportionerligt att ålägga alla tillhandahållare att ha beredskap dygnet runt och anser att uppgifterna ska lämnas ut skyndsamt i stället för utan dröjsmål. Verizon Sweden AB anför att kravet på att uppgifter ska lämnas ut utan dröjsmål i vart fall endast bör ställas på tillhandahållare som frekvent lämnar ut uppgifter till brottsbekämpande myndigheter. *Kammarrätten i Stockholm* framhåller att förslaget innebär ett relativt omfattande krav som riktar sig mot enskilda och skulle kunna innebära ett krav på bemanning dygnet runt hos tillhandahållarna.

Tullverket efterlyser förtydliganden och anser att det bör övervägas om uttrycket utan dröjsmål kan ersättas med ordet genast. Vidare anser Tullverket att det av den nya regleringen om format och skyndsamhet också bör framgå att utlämnandet inte får röjas.

Skälen för regeringens förslag

Det nuvarande skyndsamhetskravet gäller bara i vissa situationer

I dagsläget finns det ett uttryckligt skyndsamhetskrav endast för utlämnande av uppgifter som ska lagras för brottsbekämpande ändamål eller som omfattas av ett föreläggande om bevarande. Regleringen innebär att tillhandahållarna ska bedriva sin verksamhet så att uppgifterna kan lämnas ut utan dröjsmål (9 kap. 24 och 25 §§ nya LEK). Utgångspunkten är att en tillhandahållares arbete med att överföra information med anledning av en begäran som kommer in under kontorstid ska inledas inom mycket kort tid. Tillhandahållaren kan också komma att behöva arbeta med verkställigheten 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 tillhandahållaren. Hur snabbt ett utlämnande ska ske i det enskilda fallet får avgöras av de brottsbekämpande myndigheterna och tillhandahållarna i varje situation (prop. 2010/11:46 s. 51 och 80).

Regleringen av anpassningsskyldigheten i 9 kap. 29 § nya LEK innehåller inget uttryckligt skyndsamhetskrav. När motsvarigheten till den paragrafen infördes i den då gällande telelagen anfördes att telesystemet vid varje givet tillfälle bör innehålla de egenskaper som behövs för att ett beslut om hemlig teleavlyssning eller hemlig teleövervakning genast ska kunna verkställas. Det uttalades även, beträffande hemlig teleavlyssning, att innehållet i ett telemeddelande måste göras tillgängligt samtidigt som det förmedlas eller i vart fall i omedelbar anslutning till att det förmedlas. Vad som sagts om innebörden av teleoperatörernas förpliktelser beträffande hemlig teleavlyssning ansågs i allt väsentligt gälla också för hemlig teleövervakning (prop. 1995/96:180 s. 25, 27 och 28). Vidare har PTS i flera tillsynsärenden gjort uttalanden om med vilken grad av skyndsamhet realtidsuppgifter bör lämnas ut till följd av anpassningsskyldigheten i 6 kap. 19 § LEK (9 kap. 29 § nya LEK). Myndigheten har bedömt att anpassningsskyldigheten innebär att tjänstetillhandahållare med mer betydande verksamhet som omfattas av bestämmelsen, ska bedriva sin verksamhet på ett sådant sätt att verkställigheten ska kunna påbörjas även efter kontorstid, dvs. i princip dygnet runt.

I det brottsbekämpande arbetet kan det uppstå beaktansvärda behov av att använda hemliga tvångsmedel med mycket kort varsel. En snabb verkställighet kan i vissa fall vara nödvändig för att skydda allmänheten eller för att föra en brådskande brottsutredning framåt. Behovet av snabba beslut har påverkats av den utveckling som skett inom teknik och kommunikation. De förbättrade kommunikationsmöjligheterna innebär att misstänktas 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 ett hemligt tvångsmedel 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.

Av promemorian framgår att de brottsbekämpande myndigheternas behov av att snabbt få tillgång till uppgifter om elektronisk kommunikation inte alltid tillgodoses. Under senare tid har visserligen förändringar gjorts som innebär att de fyra största mobiloperatörerna har möjlighet att lämna ut realtidsuppgifter även under nätter och helger. Det förekommer dock alltjämt att brottsbekämpande myndigheter kan behöva vänta längre 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 tillhandahållare. 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.

Skyndsamhetskravet bör utvidgas

Som *Polismyndigheten* framhåller är det angeläget att komma till rätta med de oklarheter som i dag råder kring vilken skyndsamhet som krävs när uppgifter om elektronisk kommunikation lämnas ut till brottsbekämpande myndigheter. Det finns därför ett behov av att utvidga regleringen. En sådan förändring kan, vilket *Åklagarmyndigheten* pekar på, förväntas få positiva effekter för brottsbekämpningen.

Ett utvidgat krav på skyndsamhet kan innebära ökade kostnader för tillhandahållarna. Regeringen anser dock att brottsbekämpningsintresset väger mycket tungt i detta sammanhang. Det framstår därför som rimligt att kräva att tillhandahållarna ska anpassa sin verksamhet så att begärda uppgifter kan lämnas ut med tillbörlig skyndsamhet. Det saknas skäl att i fråga om kravet på skyndsamhet göra någon skillnad mellan uppgifter som lagras för brottsbekämpande ändamål respektive för tillhandahållarnas egna ändamål. En reglering av frågan bör därför omfatta alla slags uppgifter som lämnas ut till brottsbekämpande myndigheter för brottsbekämpande ändamål. Regleringen bör på samma sätt som kravet på format avgränsas till att gälla tillhandahållare som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § nya LEK. Ett skyndsamhetskrav bör således träffa samma slags utlämnanden av uppgifter som den föreslagna regleringen om format (avsnitt 5.1). På så sätt kommer regleringen att omfatta bl.a. historiska uppgifter som lagras för tillhandahållarnas egna ändamål, vilka i dag faller utanför regleringen om utlämnande utan dröjsmål i de fall uppgifterna inte omfattas av ett föreläggande om bevarande. Även uppgifter som hämtas in i realtid, som kan avse både innehållet i ett meddelande och uppgifter om ett meddelande, kommer att omfattas av ett uttryckligt skyndsamhetskrav.

Samma krav på skyndsamhet kan inte anses finnas i alla situationer. Regeringen anser därför, i likhet med *Telenor Sverige AB* och bedömningen i promemorian, att det inte i lag bör införas någon specifik tidsgräns för när uppgifter ska lämnas ut. Det bör även, som *PTS* påpekar, beaktas att regleringen på samma sätt som i dag kommer att träffa aktörer av olika storlek som har olika stora möjligheter att snabbt tillgodose en begäran om utlämnande. Behovet av snabb verkställighet markeras därför lämpligen på ett annat sätt. Som beskrivs ovan används uttrycket utan dröjsmål för uppgifter som lagras för brottsbekämpande ändamål eller som

omfattas av ett föreläggande om bevarande. Regeringen anser, till skillnad från *Tullverket*, *IT&Telekomföretagen* och *Verizon Sweden AB* men i enlighet med promemorians bedömning, att rekvisitet väl fångar den grad av skyndsamhet som är befogad när uppgifter lämnas ut till de brottsbekämpande myndigheterna. Som *PTS* framhåller kan uttrycket tolkas mot bakgrund av hur stort behovet av skyndsamhet är och de tekniska förutsättningarna för ett snabbt utlämnande i det enskilda fallet. Vidare ger det, som *Hi3G Access AB* tar upp, utrymme för tillhandahållarna att göra prioriteringar i förhållande till den sammantagna mängden förfrågningar, den aktuella typen av förfrågan och till hur myndigheten anger att förfrågan bör prioriteras. Det är därför lämpligt att nuvarande krav på utlämnande utan dröjsmål utvidgas till att omfatta utlämnanden av samma uppgifter som den föreslagna regleringen om format. Regleringen kan med fördel föras in i den nya paragraf där formerna för utlämnande av uppgifter till brottsbekämpande myndigheter regleras.

Eftersom den föreslagna regeln omfattar samma uppgifter som den föreslagna bestämmelsen om format blir det inte nödvändigt med en särskild reglering om skyndsamhet för utlämnanden av uppgifter som lagras för brottsbekämpande ändamål eller omfattas av ett föreläggande om bevarande (9 kap. 24 och 25 §§ nya LEK). Dessa bestämmelser bör därför upphävas.

Bestämmelserna i 9 kap. 24 och 25 §§ nya LEK omfattar, förutom ett skyndsamhetskrav, även ett krav på att uppgifterna ska lämnas ut så att verkställandet av utlämnandet inte röjs. I promemorian görs bedömningen att ett sådant krav följer av lagens bestämmelser om tystnadsplikt och att kravet därför kan tas bort. Regeringen bedömer dock att det aktuella kravet på hur uppgifter ska lämnas ut och bestämmelserna om tystnadsplikt fyller delvis olika funktioner. Kravet på att uppgifterna ska lämnas ut på ett sådant sätt att utlämnandet inte röjs bör därför, som *Tullverket* föreslår, föras över till den nya paragrafen om hur uppgifter ska lämnas ut.

Sammanfattningsvis anser regeringen att när tillhandahållare som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § nya LEK lämnar ut uppgifter om abonnemang, uppgifter som avser innehållet i ett elektroniskt meddelande, andra uppgifter som angår ett särskilt elektroniskt meddelande eller lokaliseringsuppgifter som inte är trafikuppgifter till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott, ska utlämnandet, om uppgifterna gäller brottslig verksamhet eller misstanke om brott, göras utan dröjsmål och på ett sådant sätt att utlämnandet inte röjs.

Det grundläggande skyndsamhetskravet bör framgå av lag. Det kan emellertid uppstå behov av mer detaljerade föreskrifter, t.ex. om vilken grad av skyndsamhet som ska krävas vid olika typer av utlämnanden. Promemorians lagförslag innehåller en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela verkställighetsföreskrifter om detta. För att säkerställa att det finns stöd för att meddela de föreskrifter som behövs, anser regeringen att det bör finnas ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela ytterligare föreskrifter om hur snabbt uppgifter ska

lämnas ut. Ett sådant bemyndigande bör även omfatta frågan om hur uppgifter ska lämnas ut för att utlämnandet inte ska röjas.

5.3 En utvidgad reglering om ersättning

Regeringens förslag: Den som bedriver verksamhet som ska anmälas enligt den nya lagen om elektronisk kommunikation har rätt till ersättning för kostnader som uppstår när uppgifter om abonnemang, uppgifter som avser innehållet i ett elektroniskt meddelande, andra uppgifter som angår ett särskilt elektroniskt meddelande eller lokaliseringsuppgifter som inte är trafikuppgifter lämnas ut till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott. I de fall det är särskilt föreskrivet ska ersättningen beräknas enligt schablon. Ersättningen ska betalas av den myndighet som har begärt uppgifterna.

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

Promemorians förslag överensstämmer i huvudsak med regeringens. Promemorians förslag innehåller ingen avgränsning till anmälningspliktig verksamhet. Promemorians förslag innehåller ingen bestämmelse om att ersättningen i vissa fall ska beräknas enligt schablon. I promemorian föreslås inget normgivningsbemyndigande.

Remissinstanserna: En majoritet av remissinstanserna, däribland *Kammarrätten i Stockholm*, *Polismyndigheten*, *PTS*, *Riksdagens ombudsmän*, *Säkerhetspolisen*, *Telenor Sverige AB* och *Åklagarmyndigheten*, är positiva till förslaget eller har inget att invända mot det. Polismyndigheten anser att det är viktigt att förslaget genomförs så snart som möjligt så att man kommer till rätta med de oklarheter som i dag råder kring ersättningen vid utlämnande till brottsbekämpande myndigheter. *Hi3G Access AB* och *IT&Telekomföretagen* betonar att det bör vara tillhandahållarens faktiska kostnader för utlämnandet som ska ersättas. Hi3G Access AB anser att den i promemorian angivna utgångspunkten att tillhandahållarna bör erhålla lika stor ersättning vid utlämnande av samma sorts uppgifter bygger på en felaktig bild. Enligt bolaget finns det en rad omständigheter som påverkar prissättningen och som gör att det kan finnas fog för variationer även när det gäller likartade uppgifter. Bolaget pekar bl.a. på att utlämnande av realtidsuppgifter ställer högre krav på säkerhet, bemanning och tillgänglighet jämfört med utlämnande av historiska uppgifter. *Tullverket* anser däremot att det inte bör göras någon skillnad på om utlämnandet avser realtidsuppgifter eller historiska uppgifter.

Skälen för regeringens förslag

Den nuvarande regleringen gäller bara i vissa situationer

Den nuvarande modellen för kostnadsfördelning mellan tillhandahållare och det allmänna när det gäller utlämnande av uppgifter om elektronisk kommunikation innebär att tillhandahållarna ska stå för kostnaderna för

anpassning, drift och underhåll. Tillhandahållarna ska däremot ersättas av de brottsbekämpande myndigheterna för kostnader som hänför sig till utlämnanden av uppgifter i enskilda ärenden (prop. 1995/96:180 s. 29–36 och prop. 2010/11:46 s. 65–68).

För uppgifter som lagras för brottsbekämpande ändamål finns en uttrycklig reglering om ersättning i nya LEK. Enligt 9 kap. 23 § har den som är lagringsskyldig enligt 9 kap. 19 § rätt till ersättning för kostnader som uppstår när lagrade uppgifter lämnas ut. Ersättningen ska betalas av den myndighet som har begärt uppgifterna. I 9 kap. 26 § 3 finns en upplysning om möjligheten för regeringen eller den myndighet som regeringen bestämmer att meddela närmare föreskrifter om ersättningen. I förarbetena uttalas att principerna för den ersättning som myndigheterna ska betala bör vara att tillhandahållarna ska få sina kostnader för att lämna ut uppgifter i enskilda ärenden ersatta. Ersättningens storlek bör dock bestämmas enligt vissa schabloner som bygger på beräkningar av tillhandahållarnas kostnader i olika typer av ärenden. Om avvikelserna från de faktiska kostnaderna blir för stora bör det dock kunna föreskrivas att schablonersättningen inte ska tillämpas, utan att en ersättning i stället ska bestämmas till ett belopp som motsvarar kostnaderna i det enskilda fallet. Tanken är inte att ersättning ska betalas 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 (prop. 2010/11:46 s. 69, 70 och 80). Sedan den 1 maj 2021 gäller bestämmelsen om ersättning på motsvarande sätt för uppgifter som omfattas av ett föreläggande om bevarande (9 kap. 25 §).

PTS har meddelat föreskrifter om ersättning (PTSFS 2021:5). I föreskrifterna görs skillnad mellan utlämnanden av olika slags uppgifter och mellan utlämnanden som sker under eller efter kontorstid. När kostnaderna för ett utlämnande avsevärt avviker från schablonersättningen får den lagringsskyldige begära ersättning som motsvarar kostnaderna i det enskilda fallet (3–5 §§).

Rätten till ersättning gäller alltså, på samma sätt som dagens reglering om utlämnande utan dröjsmål, vid utlämnanden av uppgifter som lagras för brottsbekämpande ändamål eller omfattas av ett föreläggande om bevarande. Bestämmelserna om ersättning gäller inte för kostnader som uppstår när uppgifter hämtas in i realtid. Regleringen är inte heller tillämplig när en brottsbekämpande myndighet hämtar in uppgifter för andra ändamål än för brottsbekämpning. Det kan exempelvis handla om när Polismyndigheten, utan misstanke om brott, begär ut uppgifter för att efterforska en försvunnen person enligt 9 kap. 33 § första stycket 4 nya LEK. När det gäller uppgifter som tillhandahållare sparar endast för egna ändamål, t.ex. för fakturering eller marknadsföring, gäller dagens reglering endast i den utsträckning som uppgifterna omfattas av ett föreläggande om bevarande. I de fall som inte omfattas av bestämmelserna i 9 kap. 23 och 25 §§ nya LEK bestäms ersättningsnivåerna efter förhandlingar mellan de brottsbekämpande myndigheterna och berörda tillhandahållare.

Den nuvarande regleringen innebär 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 tillhandahållare. Enligt promemorian uppgår de brottsbekämpande myndigheternas kostnader för inhämtning av uppgifter från tillhandahållarna till betydande belopp.

Regleringen om ersättning bör utvidgas

Det är en otillfredsställande ordning att utlämnandet av mycket likartade uppgifter kan skilja sig åt väsentligt i pris för de brottsbekämpande myndigheterna. Det framstår också som angeläget att ersättningen i fler fall kan bestämmas enligt schabloner som baseras på tillhandahållarnas kostnader i olika typer av ärenden. Ett system med schablonersättningar ger en enkel och snabb handläggning för både tillhandahållare och brottsbekämpande myndigheter. Därmed kan tillhandahållarnas och de brottsbekämpande myndigheternas resurser läggas på annat. Genom att ersättningen är bestämd på förhand är den också förutsebar för alla parter.

Regleringen om tillhandahållarnas ersättning bör mot denna bakgrund utvidgas till att gälla även andra utlämnanden till brottsbekämpande myndigheter än de som omfattas av de nuvarande bestämmelserna. Ersättningsregleringen bör gälla oberoende av om de uppgifter som lämnas ut är realtidsuppgifter, historiska uppgifter, trafikuppgifter, lokaliseringsuppgifter eller abonnemangsuppgifter. Det bör inte heller göras någon skillnad beroende på vilket lagstöd som finns för utlämnandet. Regleringen bör därmed omfatta samma uppgifter som de föreslagna bestämmelserna om format och skyndsamhet. Regleringen bör vidare på samma sätt som kraven på format och skyndsamhet avgränsas till att gälla tillhandahållare som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § nya LEK.

Behovet av en tydlig ersättningsreglering gör sig gällande även när uppgifter hämtas in för andra ändamål än brottsbekämpning. De nya bestämmelserna om ersättning bör därför, till skillnad från den föreslagna regleringen om format och skyndsamhet, gälla vid alla utlämnanden till brottsbekämpande myndigheter. Det kan t.ex. handla om att Polismyndigheten, utan misstanke om brott, begär ut uppgifter för att efterforska en försvunnen person. Skälen för att avvika från den i promemorian föreslagna placeringen av regleringen av format och skyndsamhet gäller också för bestämmelserna om ersättning. Till skillnad från förslaget i promemorian bör ersättningsfrågan därför regleras i en ny paragraf i nya LEK. Av regleringen bör det på samma sätt som i dag framgå att ersättningen ska betalas av den myndighet som har begärt uppgifterna.

Hi3G Access AB och *Tullverket* har synpunkter på beräkningen av ersättningen för realtidsuppgifter och historiska uppgifter. Vidare betonar Hi3G Access AB och *IT&Telekomföretagen* att det bör vara tillhandahållarens faktiska kostnader för utlämnandet som ska ersättas. Utgångspunkten bör visserligen på samma sätt som i dag vara att tillhandahållaren ska få sina kostnader för att lämna ut uppgifter i det enskilda ärendet ersatta. För att göra det tydligt att ersättning ska kunna beräknas enligt schablon bör det, till skillnad från i promemorians förslag, finnas en bestämmelse som anger det. Det ligger i sakens natur att en schablonersättning kan medföra att en tillhandahållare ibland får en högre

ersättning och ibland en lägre ersättning än vad som motsvarar tillhandahållarens faktiska kostnader i det enskilda fallet.

Sammanfattningsvis bör den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § nya LEK ha rätt till ersättning för kostnader som uppstår när uppgifter om abonnemang, uppgifter som avser innehållet i ett elektroniskt meddelande, andra uppgifter som angår ett särskilt elektroniskt meddelande eller lokaliseringsuppgifter som inte är trafikuppgifter lämnas ut till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott. Vidare bör det i bestämmelsen anges att ersättningen ska beräknas enligt schablon i de fall det är särskilt föreskrivet. Den myndighet som har begärt uppgifterna bör vara skyldig att betala ersättningen.

Förslaget innebär att de bestämmelser som gäller ersättning för utlämnande av uppgifter som lagras för brottsbekämpande ändamål och uppgifter som omfattas av ett föreläggande om bevarande blir överflödiga (9 kap. 23 och 25 §§ nya LEK). De bestämmelserna bör därför upphöra att gälla.

På samma sätt som i dag bör det finnas en möjlighet att meddela föreskrifter om ersättning på lägre nivå än lag, t.ex. gällande vilka schabloner som ska gälla i olika situationer. Promemorians lagförslag innehåller en upplysning om att regeringen eller den myndighet som regeringen bestämmer kan meddela verkställighetsföreskrifter om ersättningen. För att säkerställa att det finns stöd för att meddela de föreskrifter som behövs, anser regeringen att det bör finnas ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela ytterligare föreskrifter ersättningen och schablonberäkningen.

5.4 Ett förtydligande av att abonnemangsuppgifter får hämtas in i underrättelseverksamhet

Regeringens förslag: En tillhandahållares skyldighet att på begäran lämna en uppgift om abonnemang till en brottsbekämpande myndighet utvidgas till att omfatta uppgifter som gäller brottslig verksamhet. Ekobrottsmyndigheten, Åklagarmyndigheten och Tullverket läggs till som exempel på brottsbekämpande myndigheter.

Datalagringsutredningens förslag överensstämmer i huvudsak med regeringens. I utredningens lagförslag nämns inte Tullverket.

Remissinstanserna: *Polismyndigheten*, *Åklagarmyndigheten, Ekobrottsmyndigheten*, *Tullverket* och *Institutet för Juridik och Internet* tillstyrker förslaget. Ingen remissinstans invänder mot förslaget.

Promemorians förslag överensstämmer i huvudsak med regeringens. I promemorians lagförslag nämns inte Tullverket.

Remissinstanserna: Endast *Säkerhetspolisen* och *Tullverket* yttrar sig särskilt i denna del och välkomnar förslaget. Tullverket framhåller dock att bestämmelsen skulle vinna i tydlighet om även Tullverket uttryckligen anges som en av de myndigheter som omfattas av bestämmelsen.

Skälen för regeringens förslag: Brottsbekämpande myndigheter har rätt att få tillgång till abonnemangsuppgifter om uppgiften gäller misstanke om ett brott som myndigheten ska ingripa mot (9 kap. 33 § första stycket 2 nya LEK). Uttrycket misstanke om brott kan föra tankarna till ett konkret begånget brott. En sådan tolkning är mindre väl anpassad till de brottsbekämpande myndigheternas underrättelseverksamhet som främst avser 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. propositionen Brottsdatalag – kompletterande lagstiftning (prop. 2017/18:269 s. 294). Som framhålls både av utredningen och i promemorian är bestämmelsen dock inte begränsad till en förundersökning och tillämpas även i de brottsbekämpande myndigheternas underrättelseverksamhet. Av rättssäkerhetsskäl bör lagstiftningen vara så tydlig som möjligt. För att klargöra att abonnemangsuppgifter får hämtas in även i underrättelseverksamhet bör bestämmelsen därför justeras.

Uttrycket brottslig verksamhet används i lagstiftning för att avgränsa åtgärder som får vidtas i underrättelseverksamhet, se t.ex. 2 kap. 1 § lagen om polisens behandling av personuppgifter inom brottsdatalagens område och 2 § inhämtningslagen. Uttrycket bör användas även i detta sammanhang.

Av tydlighetsskäl bör, i enlighet med *Tullverkets* synpunkt, även Tullverket anges som en av de myndigheter som omfattas av bestämmelsen.

6 Ikraftträdande- och övergångsbestämmelser

Regeringens förslag: Lagändringen träder i kraft den 1 augusti 2022.

En förbetald allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst eller en förbetald internetanslutningstjänst som har tillhandahållits före ikraftträdandet får, även om någon registrering inte har gjorts, tillhandahållas till och med den 1 februari 2023 eller den senare tidpunkt då en ny förbetalning görs.

Promemorians förslag överensstämmer i huvudsak med regeringens. I promemorian föreslås ett tidigare ikraftträdande. Promemorians förslag innehåller ingen möjlighet att använda oregistrerade tjänster till och med tidpunkten för en ny förbetalning.

Remissinstanserna: En majoritet av remissinstanserna är positiva till förslaget eller har inget att invända mot det. *Telenor Sverige AB* föreslår att registreringskravet inte ska gälla för förbetalda maskin-till-maskin-tjänster som har tillhandahållits före ikraftträdandet, även om de har stöd för meddelande- eller internetaccesstjänst. Bolaget anför att det saknas förståelse för hur maskin-till-maskin-tjänster fungerar och att det finns en risk för allvarliga konsekvenser. Merparten av förbetalda tjänster som används till maskin-till-maskin-applikationer använder just meddelandetjänst eller internetaccess för att fungera. Dessa simkort är installerade i

tusentals utrustningar, såsom larm, sensorer, mätinstrument, uppvärmningsanläggningar och olika hushållsapparater, och många av dessa fyller en helt avgörande roll för kritiska funktioner inom säkerhet och egendomsskydd. Dessa utrustningar är inte konstruerade för att läsa och förstå inkommande sms. Därmed kommer ett besked från tillhandahållaren om att simkortet kommer att avaktiveras om det inte registreras att gå obemärkt förbi. Viktiga funktioner kommer att sluta fungera när tillhandahållaren avaktiverar tjänsten, utan att abonnenten har fått någon förvarning. Om regeringen ändå går vidare med lagförslaget i denna del, krävs en omfattande informationskampanj. *IT&Telekomföretagen* anser att oklarheterna kring vilka maskin-till-maskin-användningar som är undantagna från registreringsskyldigheten kan medföra stora konsekvenser. Organisationen undrar om t.ex. trygghetslarm på äldreboenden är att betrakta som maskin-till-maskin-tjänster som undantas och vad konsekvenserna skulle bli om de inte undantas. Enligt *Hi3G Access AB* kommer det att vara en utmaning att nå ut till samtliga kontantkortsinnehavare och få dem att registrera kontantkortet, framför allt när det gäller internetanslutningstjänster. För dessa tjänster finns det enligt bolaget normalt sett inte några kontaktvägar till kunden. Även *PTS* pekar på att en viktig fråga är hur befintliga kontantkortskunder ska få information om att deras kort måste registreras inom sex månader.

Skälen för regeringens förslag

Ikraftträdande

Lagändringen bör träda i kraft så snart som möjligt. Tillhandahållarna bör dock ges rimlig tid att anpassa sina system och sin verksamhet, både när det gäller att leva upp till kravet på registrering av abonnemangsuppgifter för förbetalda tjänster och när det gäller kraven på format och skyndsamhet vid utlämnande av uppgifter om elektronisk kommunikation. Regeringen anser mot denna bakgrund att lagändringen bör träda i kraft den 1 augusti 2022.

Övergångsbestämmelser

Andra europeiska länder som har infört en registreringsskyldighet som omfattar kontantkort har enligt promemorian 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.

Det finns i dag miljontals kontantkort i Sverige. Vidare har det framkommit att telefonnummer kopplade till svenska oregistrerade kontantkort används av terrorkopplade aktörer utomlands. Om befintliga kontantkort inte skulle omfattas av den föreslagna regleringen om registrering skulle det vara möjligt att fortsatt använda dessa kort anonymt. Det skulle också kunna uppstå en andrahandsmarknad för befintliga kontantkort för personer som vill undgå en registrering. För att undvika en sådan situation krävs att även de tjänster som tillhör befintliga kontantkort registreras. En registreringsskyldighet som omfattar befintliga kontantkort framstår som rimlig även med beaktande av den ytterligare administrativa bördan för tillhandahållarna.

Tillhandahållare och enskilda kommer att behöva viss tid för att genomföra registreringen. Därför bör det, liksom i andra europeiska länder, införas en övergångsperiod inom vilken enskilda kan låta registrera sina befintliga förbetalda tjänster. Det görs lämpligen genom att det i en övergångsbestämmelse införs ett undantag som innebär att förbetalda tjänster som har tillhandahållits innan registreringsskyldigheten började gälla får användas en viss tid därefter utan att en registrering har gjorts. Tillhandahållarnas arbete med att genomföra en registrering av befintliga kunder bör också kunna förberedas innan lagstiftningen träder i kraft. Regeringen anser mot denna bakgrund, i enlighet med promemorians förslag, att sex månader är en tillräckligt lång tid för att de som vill fortsätta använda befintliga tjänster ska ha möjlighet att registrera dem.

Regeringens förslag i avsnitt 4.2.1 innebär att registreringsskyldigheten omfattar kontantkort som i huvudsak är avsedda för maskin-till-maskin-tjänster, men som även ger tillgång till samtals- eller datatjänster. När det gäller sådana kontantkort kan det i vissa fall vara svårt för tillhandahållaren att inom sexmånadersperioden informera användaren om att det måste göras en registrering. Som *Hi3G Access AB* påpekar kan detta även gälla internetanslutningstjänster. Enligt *Telenor Sverige AB* och *IT&Telekomföretagen* kan det förekomma att kontantkort för maskin-till-maskin-tjänster används i utrustning som är av stor betydelse för säkerhet och egendomsskydd, t.ex. larm. Av promemorian framgår visserligen att det är ovanligt att maskin-till-maskin-tjänster är förbetalda. Regeringen anser ändå att det är angeläget att säkerställa att kontantkort som används för maskin-till-maskin-tjänster inte måste stängas av utan att abonnenten har kunnat förvarnas om detta. Det bör därför, utöver den generella sexmånadersfristen, införas en ventil som innebär att oregistrerade tjänster kan fortsätta att användas till dess att abonnenten kan informeras om registreringskravet. Ett lämpligt tillfälle för sådan information är i samband med en ny förbetalning, dvs. när kontantkortet fylls på. Tillhandahållaren kan då meddela abonnenten att en registrering måste göras för att det ska vara möjligt att använda tjänsten även efter förbetalningen.

Regeringen anser sammanfattningsvis att en förbetald allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst eller en förbetald internetanslutningstjänst som har tillhandahållits före den 1 augusti 2022, även om tjänsten inte har registrerats, bör få tillhandahållas till och med den 1 februari 2023 eller den senare tidpunkt då en ny förbetalning görs. Avsikten med regeringens förslag är inte att en tillhandahållare ska vara skyldig att tillhandahålla tjänsten efter sexmånadersfristens utgång. Det bör alltså vara upp till tillhandahållaren att välja om den vill utnyttja möjligheten att tillhandahålla tjänsten till och med tidpunkten för en ny förbetalning.

Det finns i övrigt inte behov av några övergångsbestämmelser.

7 Konsekvenser

Regeringens bedömning: Förslagen leder till att den brotts-bekämpande verksamheten effektiviseras.

Förslagen medför marginella kostnadsökningar för de brottsbekämpande myndigheterna. Kostnadsökningarna kan hanteras inom befintliga anslag.

Förslagen medför ökade kostnader för tillhandahållare.

Promemorians bedömning överensstämmer med regeringens.

Remissinstanserna: *Ekobrottsmyndigheten* instämmer i bedömningen att förslagen i viss mån kan medföra ökade kostnader för berörda myndigheter, däribland Ekobrottsmyndigheten. *Kammarrätten i Stockholm* efterfrågar en analys av vilka konsekvenser förslagen får för de allmänna förvaltningsdomstolarna och betonar vikten av att domstolarna får de eventuella resurser som kan behövas om kostnaderna skulle öka. *PTS* anför att de samlade förslagen innebär att myndigheten kommer att få ett utökat tillsynsområde och möjlighet att meddela föreskrifter i fler situationer än i dag. Enligt PTS kommer de nya arbetsuppgifterna att kräva ökade resurser, vilka i förlängningen torde finansieras genom att myndigheten tar ut avgifter från marknadens aktörer. På så vis kommer förslagen enligt PTS att innebära konsekvenser för de företag som verkar inom sektorn. *Regelrådet* anser att konsekvensutredningen är bristfällig när det gäller beskrivningarna av storleken på de företag som berörs av förslagen, förslagens påverkan på företagens kostnader och verksamhet, förslagens konkurrenspåverkan på berörda företag och om särskilda hänsyn behöver tas till små företag.

Skälen för regeringens bedömning

Konsekvenser för det allmänna

En skyldighet att registrera abonnemangsuppgifter för förbetalda tjänster kan förväntas leda till en säkrare tillgång till abonnemangsuppgifter och därmed medföra att uppgifter från elektronisk kommunikation oftare kan göras åtkomliga för brottsbekämpande ändamål. På så sätt kan det brottsbekämpande arbetet effektiviseras. Därigenom skapas förbättrade förutsättningar att bekämpa brottslighet, särskilt när det gäller allvarlig brottslighet. Även förslagen om ett tydligare krav på format, ett utvidgat skyndsamhetskrav och en utökad reglering om ersättning kan antas leda till ett effektivare brottsbekämpande arbete.

Den förbättrade tillgången till abonnemangsuppgifter kan förväntas få till följd att hemliga tvångsmedel kommer att användas i större utsträckning än i dag. Det kan leda till ökade kostnader för de brottsbekämpande myndigheterna. Fler inhämtade abonnemangsuppgifter kan också i sig leda till ökade kostnader för de brottsbekämpande myndigheterna i form av ersättning till tillhandahållarna. Samtidigt kommer registreringsskyldigheten att 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. Den effektiviseringen kommer att minska kostnaderna.

En effektivare tillgång till 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 för åklagare och domstolar. Totalt sett torde dock

rättsväsendets olika insatser vid utredning och lagföring av allvarlig brottslighet effektiviseras.

Sammanfattningsvis instämmer regeringen i promemorians bedömning att förslagen endast kommer att innebära marginella kostnadsökningar för de brottsbekämpande myndigheterna och att kostnadsökningarna kan hanteras inom befintliga anslag.

När det gäller konsekvenserna för de allmänna förvaltningsdomstolarna, som *Kammarrätten i Stockholm* saknar en analys av, kommer förslaget om en registreringsskyldighet att medföra ett utökat tillsynsområde för tillsynsmyndigheten. Därmed skulle antalet överklagade tillsynsbeslut kunna öka. Även förändringarna av kraven på format och skyndsamhet skulle kunna leda till fler tillsynsbeslut och därmed fler överklaganden. Detsamma gäller förslaget om att utvidga bestämmelsen om sanktionsavgifter vid överträdelser av kravet på format. Sammantaget torde ökningen av antalet mål i allmän förvaltningsdomstol emellertid inte uppgå till mer än några enstaka mål per år. De eventuella kostnadsökningarna blir därmed marginella och bör kunna hanteras inom befintliga anslag.

Som *PTS* anför innebär de samlade förslagen att tillsynsmyndigheten kommer att få ett utökat tillsynsområde och möjlighet att meddela föreskrifter i fler situationer än i dag. Tillsynsmyndigheten kommer också att få något större möjlighet att ta ut sanktionsavgifter. Dessa förhållanden bedöms dock inte medföra behov av ökade anslag för tillsynsmyndigheten men kan, som PTS anför, få ekonomiska konsekvenser för de företag som verkar inom sektorn. Konsekvenserna bör dock vara begränsade.

Konsekvenser för företag

Konsekvenserna av förslaget om en skyldighet att registrera abonnemangsuppgifter för förbetalda tjänster beskrivs i avsnitt 4.1 under rubriken Betydelsen för företag. I avsnittet gör regeringen även bedömningen att det är proportionerligt att införa en registreringsskyldighet. Det kan tilläggas att de föreslagna bestämmelserna är utformade på ett sådant sätt att kunder inte ska behöva uteslutas från möjligheten att fortsatt köpa och använda förbetalda tjänster, bl.a. genom kontantkort. Den identifiering som krävs ska t.ex. kunna ske genom ett stort antal identitetshandlingar. För den som saknar en identitetshandling ska identifieringen kunna ske på ett annat sätt. Således kommer t.ex. turister fortsatt att kunna använda kontantkort. Vidare innebär förslagen att registreringen kan göras på flera olika sätt, t.ex. via internet, via kontakt med tillhandahållarens kundtjänst eller i en fysisk butik. Registreringen ska därmed kunna genomföras även av personer som kan behöva hjälp med registreringen. Mot denna bakgrund kan den föreslagna registreringsskyldigheten inte antas medföra något större kundbortfall. Det kan i sammanhanget noteras att en av de fyra största mobiloperatörerna har slutat att sälja startpaket och påfyllning för kontantkort och kommer avsluta alla sina kontantkort den 31 mars 2022.

Förslagen om utlämnande av uppgifter om elektronisk kommunikation omfattar alla tillhandahållare som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § nya LEK och som kan komma att lämna ut sådana uppgifter till brottsbekämpande myndigheter. Av promemorian framgår

att förslagen kan beröra mer än 600 företag som erbjuder olika typer av tjänster. Företagen har en mycket varierande marknadsandel och storlek. Enligt promemorian kommer dock regleringen i praktiken träffa främst de fyra största mobiloperatörerna, som är de aktörer som de brottsbekämpande myndigheterna vanligtvis vänder sig till för att få tillgång till uppgifter om elektronisk kommunikation. Enligt promemorian står dessa fyra företag tillsammans för ca 95 procent av den svenska mobilmarknaden.

Förslaget om ett tydligare krav på format kommer att vara kostnadsdrivande för tillhandahållarna. De fyra största mobiloperatörerna har emellertid redan på frivillig väg påbörjat arbetet med att införa gemensamma format. Den föreslagna regleringen kommer dock innebära att höjda krav kommer att ställas även på de mindre tillhandahållarna, vilket kan medföra ökade kostnader för dem. Även förslaget om att utvidga skyndsamhetskravet kan medföra ökade kostnader för tillhandahållarna.

Förslaget om att utvidga regleringen om ersättning innebär bl.a. att tillsynsmyndigheten får möjlighet att bestämma storleken på den ersättning som ska betalas ut till tillhandahållarna i fler situationer än i dag. Regleringen kan därför förväntas medföra att tillhandahållarnas handläggning effektiviseras och att ersättningen blir mer förutsebar. Det kan tilläggas att mer likartade ersättningsnivåer medför en mer rättvis ersättning tillhandahållarna emellan.

Tillhandahållarna bör huvudsakligen kunna föra över de kostnader som förslagen innebär på sina kunder, dvs. företag, privatpersoner, staten och kommuner. Regeringen instämmer i promemorians bedömning att de eventuella merkostnader som på detta sätt kommer att drabba staten ryms inom befintliga ramar. Eventuella ekonomiska konsekvenser för kommuner och regioner bedöms bli marginella.

Konsekvenser för skyddet av enskildas personliga integritet

Konsekvenserna av förslaget om en registreringsskyldighet för skyddet av enskildas personliga integritet beskrivs i avsnitt 4.1 under rubriken En begränsad inskränkning av enskildas fri- och rättigheter. Där görs bedömningen att en registrering av abonnemangsuppgifter för kontantkort endast skulle innebära ett begränsat intrång i enskildas personliga integritet och en begränsad inskränkning i enskildas rätt till respekt för privatliv och rätt till skydd av personuppgifter.

Förslagen som gäller utlämnande av uppgifter om elektronisk kommunikation innebär inte att de brottsbekämpande myndigheternas rätt att ta del av uppgifter utvidgas. Förslagen kan därför inte sägas påverka skyddet av enskildas personliga integritet.

Övriga konsekvenser

Samtliga förslag är könsneutrala. Förslaget om registrering av kontantkort syftar bl.a. till att förbättra möjligheten att utreda brott som begås via telefon och andra digitala kommunikationsmedel. Det kan t.ex. handla om kvinnor som utsätts för brott av en partner eller före detta partner. Förslaget om registrering av kontantkort kan därmed bidra till att uppnå det jämställdhetspolitiska målet att kvinnor och män ska ha samma makt

att forma samhället och sina egna liv, särskilt det sjätte delmålet att mäns våld mot kvinnor ska upphöra.

Förslagen bedöms inte ha någon påverkan på möjligheten att nå de integrationspolitiska målen.

8 Författningskommentar

Förslaget till lag om ändring i lagen (2022:000) om elektronisk kommunikation

Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (e-kodexdirektivet) ska genomföras i Sverige. Genom e-kodexdirektivet inrättas ett harmoniserat ramverk för bl.a. elektroniska kommunikationsnät och tjänster. För att genomföra direktivet har regeringen i lagrådsremissen Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation lämnat förslag till en ny lag om elektronisk kommunikation som ska träda i kraft den 1 juni 2022 och ersätta lagen (2003:389) om elektronisk kommunikation. Författningskommentaren utgår från att nuvarande lydelse av lagtexten är den som föreslås i den lagrådsremissen.

8 kap.

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

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

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

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

Andra stycket, som är nytt, motsvarar delvis nuvarande 9 kap. 25 §, vilken upphör att gälla (jfr prop. 2020/21:72 s. 30, 31 och 73). Bestämmelsen innebär att tillhandahållaren ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de bevarade uppgifterna vid behandling. Någon ändring i sak är inte avsedd.

Tredje stycket motsvarar nuvarande andra stycket.

9 kap.

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

1. vilka uppgifter som ska lagras enligt 19 §, *och*
2. lagringstiden enligt 22 § första stycket.

Paragrafen upplyser om möjligheten att meddela föreskrifter på lägre nivå än lag.

I paragrafen, som i nuvarande lydelse betecknas 26 §, görs en ändring som innebär att tredje punkten tas bort. Ändringen är en följd av att nuvarande 23 §, som delvis motsvarar 29 a §, upphör att gälla.

24 § *Den som tillhandahåller en förbetald allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst eller en förbetald internetanslutningstjänst får inte ge tillgång till tjänsten utan att dessförinnan ha registrerat*

1. abonnentens namn och postadress,

2. abonnentens personnummer, samordningsnummer, organisationsnummer eller annat identifieringsnummer, och

3. nummer eller annan beteckning för tjänsten.

Tillhandahållaren ska även ange tidpunkten för registreringen.

Uppgifterna ska finnas tillgängliga hos tillhandahållaren från och med registreringen till och med ett år efter att tillhandahållandet av tjänsten har upphört.

Paragrafen, som är ny, behandlar en skyldighet att registrera uppgifter om abonnenter avseende vissa förbetalda tjänster. Övervägandena finns i avsnitt 4.2.1 och 4.2.2.

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 utan att dessförinnan ha registrerat vissa uppgifter. Innebörden av uttrycket allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst och ordet internetanslutningstjänst framgår av 1 kap. 7 §. Med interpersonell kommunikationstjänst avses en tjänst som vanligen tillhandahålls mot ersättning och som möjliggör ett direkt interpersonellt och interaktivt informationsutbyte via elektroniska kommunikationsnät mellan ett begränsat antal personer, varigenom de personer som inleder eller deltar i kommunikationen bestämmer vem eller vilka som ska vara mottagare av denna, dock inte en tjänst som möjliggör interpersonell och interaktiv kommunikation enbart som en extrafunktion av mindre betydelse som är direkt kopplad till en annan tjänst. Med nummerbaserad interpersonell kommunikationstjänst avses en interpersonell kommunikationstjänst som etablerar en förbindelse till nummer i nationella eller internationella nummerplaner eller som möjliggör kommunikation med sådana nummer. Med internetanslutningstjänst avses enligt artikel 2.2 i den s.k. TSM-förordningen (EU) 2015/2120 en allmänt tillgänglig elektronisk kommunikationstjänst som erbjuder anslutning till internet och därigenom möjlighet till anslutning mellan praktiskt taget alla ändpunkter på internet, oberoende av vilken nätteknik och terminalutrustning som används. Registreringsskyldigheten omfattar den som tillhandahåller förbetalda tjänster som kan användas för att ringa, sända textmeddelanden eller surfa på internet. Det kan röra sig om tjänster som utnyttjas genom fysiska kontantkort, men också genom s.k. e-sim (embedded sim). Det är tillgången till tjänsterna som avgör om det föreligger en registreringsskyldighet. Om ett kontantkort ger tillgång till allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster eller internetanslutningstjänster, ska tillhandahållaren av tjänsterna göra en registrering. Även ett kontantkort som är avsett för

kommunikation mellan maskiner omfattas av registreringsskyldigheten, om kortet ger tillgång de angivna tjänsterna. Om ett kontantkort däremot endast kan användas för kommunikation mellan maskiner omfattas det inte av registreringskravet. Vissa uppgifter om abonnenten ska registreras. Uppgifterna utgör sådana uppgifter om abonnemang som enligt 9 kap. 31 § första stycket 1 omfattas av tystnadsplikt. Ordet abonnent definieras i 1 kap. 7 §. Abonnenten är i det här fallet den som har köpt ett kontantkort eller på annat sätt har ingått avtal med en tillhandahållare av aktuella tjänster. Registreringsskyldigheten omfattar både fysiska och juridiska personer. Vid nummerportering, dvs. att ett nummer lämnas över till en annan tillhandahållare, omfattas den nya tillhandahållaren av kravet på registrering.

Enligt *första punkten* ska abonnentens namn och postadress registreras. Av *andra punkten* framgår att abonnentens personnummer, samordningsnummer, organisationsnummer eller annat identifieringsnummer ska anges. Med annat identifieringsnummer avses för fysiska personer t.ex. passnummer eller födelsedatum för den som saknar svenskt personnummer eller samordningsnummer. När det gäller juridiska personer kan ett annat identifieringsnummer t.ex. vara en utländsk motsvarighet till organisationsnummer. *Tredje punkten* innebär att någon form av identifierande beteckning för tjänsten, t.ex. ett telefonnummer, ska registreras. Tillhandahållaren ska registrera uppgifterna innan tjänsten tas i bruk. Det ska alltså inte vara möjligt att t.ex. ringa, ta emot samtal eller surfa på internet om inte en registrering har gjorts.

Enligt *andra stycket* ska tillhandahållaren även ange tidpunkten för registreringen.

Av *tredje stycket* framgår att uppgifter som registreras enligt första och andra styckena ska finnas tillgängliga hos tillhandahållaren från och med registreringen till och med ett år efter att tillhandahållandet av tjänsten har upphört. Att tillhandahållandet upphör kan t.ex. bero på en nummerportering eller att tillhandahållaren avslutar tjänsten på grund av att den inte har använts under en längre tid.

25 § *I samband med en registrering enligt 24 § ska abonnentens identitet kontrolleras genom en giltig identitetshandling eller en tillförlitlig elektronisk identifiering. Om abonnenten saknar sådana handlingar och verktyg får identiteten göras sannolik på annat sätt. Identitetskontrollen ska dokumenteras.*

Om abonnenten är en juridisk person, gäller första stycket den som företräder den juridiska personen.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om identitetskontrollen.

Paragrafen, som är ny, innehåller bestämmelser om identitetskontroll. Övervägandena finns i avsnitt 4.2.3.

Av *första stycket* framgår att det ska göras en identitetskontroll i samband med att abonnentuppgifter registreras enligt 24 §. Det är tillhandahållaren av tjänsten som ansvarar för att identitetskontrollen genomförs. Abonnentens identitet ska kontrolleras genom en giltig identitetshandling eller genom en tillförlitlig elektronisk identifiering. Med en giltig identitetshandling avses t.ex. ett pass, ett id-kort eller ett körkort. Även utländska identitetshandlingar kan godtas. Identitets-

kontrollen kan också ske genom en elektronisk identifiering. Uttrycket elektronisk identifiering definieras i artikel 3.1 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. Den elektroniska identifieringen ska vara tillförlitlig. Med det avses i första hand användning av en e-legitimation, t.ex. bank-id. Om en abonnent inte har tillgång till någon identitetshandling eller kan använda sig av en tillförlitlig elektronisk identifiering, får identiteten göras sannolik på annat sätt. Om abonnenten t.ex. är ett barn som saknar både identitetshandling och e-legitimation, kan barnets identitet göras sannolik genom att en nära anhörig, som har en giltig identitetshandling, intygar barnets identitet. Identitetskontrollen ska dokumenteras.

Om abonnenten är en juridisk person, följer det av *andra stycket* att identitetskontrollen ska avse den fysiska person som företräder den juridiska personen vid registreringen. Företrädarens identitet ska alltså kontrolleras på samma sätt som när abonnenten är en fysisk person. Företrädaren ska även kunna styrka sin rätt att företräda den juridiska personen.

I *tredje stycket* finns ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela ytterligare föreskrifter om identitetskontrollen.

26 § *Om en förbetald tjänst används av någon annan än den abonnent som har registrerats enligt 24 § utan att en ny registrering har gjorts, ska tillhandahållandet av tjänsten avbrytas.*

Första stycket gäller inte om

1. tjänsten endast tillfälligt används av någon annan än den registrerade abonnenten,

2. tjänsten används av en närstående till den registrerade abonnenten,

3. den registrerade abonnenten är en juridisk person och tjänsten används på dennes uppdrag,

4. tjänsten har införskaffats på uppdrag av Polismyndigheten, Säkerhetspolisen, Tullverket eller någon annan myndighet som ska ingripa mot brott, eller

5. tjänsten har införskaffats på uppdrag av en myndighet som bedriver verksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet.

Paragrafen, som är ny, innehåller regler om när någon annan än den registrerade abonnenten använder en förbetald tjänst. Övervägandena finns i avsnitt 4.3.

Av *första stycket* följer att den som tillhandahåller en förbetald tjänst som har registrerats enligt 24 § är skyldig att avbryta tillhandahållandet om tjänsten används av någon annan än den registrerade abonnenten utan att en ny registrering har gjorts. Bedömningen att en tjänst används av någon annan än den registrerade abonnenten kan grundas på uppgifter från brottsbekämpande myndigheter. Kravet innebär inte att tillhandahållaren är skyldig att på eget initiativ kontrollera vem som använder en registrerad tjänst. En indikation på att en förbetald tjänst används av någon annan kan vara att en abonnent är registrerad avseende ett stort antal förbetalda tjänster utan att det finns någon rimlig förklaring till det.

I *andra stycket* anges vissa undantag från huvudregeln i första stycket. Av *första punkten* följer att det inte behöver göras en ny registrering om

tjänsten endast tillfälligt används av någon annan än den registrerade abonnenten. Huruvida användningen är tillfällig får avgöras utifrån omständigheterna i det enskilda fallet. Det kan t.ex. handla om att tjänsten används för att ringa något eller några samtal. Om ett kontantkort har överlåtits, tillgripits eller tappats bort, kan tillhandahållaren utgå från att en ny innehavares användning av tjänsten inte är av tillfällig karaktär. Detsamma gäller om det konstateras att en tjänst används i utlandet samtidigt som den registrerade abonnenten uppehåller sig i Sverige. Enligt *andra punkten* kan en närstående till den registrerade abonnenten använda en förbetald tjänst utan att det behöver göras en ny registrering. Med närstående avses i första hand abonnentens barn, maka, make, sambo, förälder eller mor- eller farförälder. Även andra personer bör dock i vissa fall kunna ses som närstående, t.ex. personer med andra typer av släktskap som är sammanboende med abonnenten. Av *tredje punkten* framgår att en ny registrering inte behöver göras om den registrerade abonnenten är en juridisk person och tjänsten används på dennes uppdrag, t.ex. av den juridiska personens anställda eller uppdragstagare. För att användningen av en tjänst ska kunna anses ske på den juridiska personens uppdrag får det normalt förutsättas att den juridiska personen har kännedom om vem som använder tjänsten. Enligt *fjärde punkten* behöver det aldrig göras någon ny registrering om en förbetald tjänst har införskaffats på uppdrag av en myndighet som har till uppgift att ingripa mot brott, t.ex. Polismyndigheten, Säkerhetspolisen eller Tullverket. Detsamma gäller enligt *femte punkten* om tjänsten har införskaffats av en myndighet som bedriver verksamhet enligt lagen (2000:130) om försvarsunderrättelseverksamhet, dvs. Försvarsmakten, Försvarets radioanstalt, Försvarets materielverk eller Totalförsvarets forskningsinstitut, se 2 § förordningen (2000:131) om försvarsunderrättelseverksamhet. Undantagen i fjärde och femte punkterna gäller även om tjänsten inte har införskaffats inom ramen för en förundersökning eller i försvarsunderrättelseverksamhet.

29 § En verksamhet ska bedrivas så att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs, om verksamheten avser tillhandahållande av

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

2. tjänster inom ett allmänt elektroniskt kommunikationsnät som består av

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

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

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

Paragrafen innebär en skyldighet för tillhandahållare att anpassa sin verksamhet så att beslut om hemlig avlyssning av elektronisk

kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs. Övervägandena finns i avsnitt 5.1.

Det nuvarande andra stycket tas bort och ersätts av en delvis motsvarande bestämmelse i 29 b § andra stycket.

I *andra stycket*, som motsvarar nuvarande tredje stycket, görs språkliga och redaktionella ändringar.

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

Första stycket gäller även lokaliseringsuppgifter som inte är trafikuppgifter.

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

I paragrafen, som är ny, finns bestämmelser om ersättning vid utlämnande av uppgifter till brottsbekämpande myndigheter. Övervägandena finns i avsnitt 5.3.

Första och andra styckena motsvarar delvis nuvarande 23 och 25 §§, vilka upphör att gälla. I förhållande till de paragraferna utvidgas tillämpningsområdet till att omfatta även andra uppgifter än sådana som lagras för brottsbekämpande ändamål enligt 19 § eller som omfattas av ett föreläggande om bevarande enligt 27 kap. 16 § rättegångsbalken. De nya bestämmelserna omfattar alltså även uppgifter som tillhandahållare lagrar för egna ändamål och som inte omfattas av ett föreläggande om bevarande samt uppgifter som lämnas ut i realtid.

Enligt *första stycket* finns en rätt till ersättning för den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § och som lämnar ut uppgifter som avses i 31 § första stycket, dvs. uppgifter om abonnemang, uppgifter som avser innehållet i ett elektroniskt meddelande och andra uppgifter som angår ett särskilt elektroniskt meddelande. Bestämmelsen gäller om uppgifterna lämnas ut till Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten eller någon annan myndighet som ska ingripa mot brott. Exempel på andra myndigheter som ska ingripa mot brott är Kustbevakningen och Skatteverket. Rätten till ersättning är inte begränsad till viss verksamhet hos myndigheterna utan gäller även om uppgifterna ska användas t.ex. inom underrättelse-verksamhet. Rätten till ersättning gäller oavsett vilket lagligt stöd som finns för utlämnandet. På samma sätt som tidigare är det inte meningen att ersättning ska utgå för varje utlämnad uppgift utan ersättningen ska betalas för varje begäran, alltså först när de uppgifter som hänför sig till en viss begäran har lämnats ut (jfr prop. 2010/11:46 s. 80). Utgångspunkten är på samma sätt som tidigare att tillhandahållaren har rätt till ersättning för kostnader som uppstår när uppgifterna lämnas ut. Av en ny bestämmelse framgår dessutom att ersättningen, i de fall det är särskilt föreskrivet, ska beräknas enligt schablon. Schablonerna kan bygga på beräkningar av tillhandahållarnas kostnader i olika typer av ärenden.

Av *andra stycket* följer att regleringen även omfattar lokaliseringsuppgifter som inte är trafikuppgifter. Det kan t.ex. handla om uppgifter som avser en mobiltelefon som är påslagen men inte används.

I *tredje stycket* finns ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela ytterligare föreskrifter om ersättningen och schablonberäkningen.

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

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

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

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

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

Paragrafen, som är ny, behandlar hur uppgifter ska lämnas ut till brottsbekämpande myndigheter. Övervägandena finns i avsnitt 5.1 och 5.2.

Paragrafen gäller när den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § lämnar ut uppgifter som avses i 31 § första stycket. Paragrafen är vidare på samma sätt som 29 a § tillämplig endast om uppgifterna lämnas ut till en myndighet som ska ingripa mot brott. En skillnad i förhållande till 29 a § är att paragrafen endast gäller vid utlämnande av uppgifter som gäller brottslig verksamhet eller misstanke om brott. Uttrycket omfattar alla uppgifter som lämnas ut för brottsbekämpande ändamål, oavsett om uppgifterna hämtas in inom ramen för en förundersökning eller i underrättelseverksamhet. Kraven på hur uppgifter ska lämnas ut omfattar således uppgifter som lämnas ut efter beslut om hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation enligt 27 kap. rättegångsbalken, lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott, lagen (1991:572) om särskild utlänningskontroll, lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, lagen (2000:562) om internationell rättshjälp i brottmål eller lagen (2017:1000) om en europeisk utredningsorder. Kraven omfattar även abonnemangsuppgifter och uppgifter om vilka tillhandahållare som har deltagit vid överföringen av ett meddelande som lämnas ut med stöd av 33 § första stycket 2 eller 5.

Enligt *första stycket* ska uppgifterna lämnas ut utan dröjsmål. Kravet motsvarar det som gäller enligt nuvarande 24 § (jfr prop. 2010/11:46 s. 80). I förhållande till den bestämmelsen utvidgas tillämpningsområdet till att gälla även andra uppgifter än sådana som lagras för brottsbekämpande ändamål enligt 19 § eller omfattas av ett föreläggande om bevarande enligt 27 kap. 16 § rättegångsbalken. Det kan t.ex. handla om uppgifter som lämnas ut i realtid eller abonnemangsuppgifter som inte lagras för brottsbekämpande ändamål. På samma sätt som enligt nu-

varande 24 § innebär skyndsamhetskravet att tillhandahållaren kan behöva arbeta med utlämnanden även utanför kontorstid (jfr prop. 2010/11:46 s. 80). När det gäller realtidsuppgifter innebär det uttryckliga skyndsamhetskrav som införs inte att det ställs lägre krav på skyndsamhet jämfört med vad som har ansetts följa av anpassningsskyldigheten i 6 kap. 19 § lagen (2003:389) om elektronisk kommunikation (9 kap. 29 § denna lag). Mer detaljerade föreskrifter om vilken grad av skyndsamhet som krävs i olika situationer kan meddelas med stöd av normgivningsbemyndigandet i tredje stycket. Första stycket innebär också att uppgifterna, på samma sätt som tidigare gällt för uppgifter som lagras för brottsbekämpande ändamål, ska lämnas ut på ett sådant sätt att utlämnandet inte röjs.

I *andra stycket* anges att uppgifterna ska ordnas och göras tillgängliga i ett format som gör att de enkelt kan tas om hand. Stycket motsvarar delvis bestämmelserna i nuvarande 24 och 25 §§ och 29 § andra stycket (jfr prop. 1995/96:180 s. 27 och 28 och prop. 2010/11:46 s. 81). I förhållande till de bestämmelserna utvidgas tillämpningsområdet till att omfatta även andra uppgifter än sådana som lagras för brottsbekämpande ändamål enligt 19 §, som omfattas av ett föreläggande om bevarande enligt 27 kap. 16 § rättegångsbalken eller som avser meddelanden som är föremål för hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation. Det kan t.ex. handla om abonnemangsuppgifter som inte lagras för brottsbekämpande ändamål. Stycket innebär vidare att det ställs högre krav på i vilken form uppgifterna ska lämnas ut. Kravet innebär inte enbart att uppgifter som lämnas ut ska göras tillgängliga på ett sådant sätt att de är läsbara, vilket i princip är fallet med dagens reglering (prop. 1995/96:180 s. 27 och 28 och prop. 2010/11:46 s. 81). Uppgifterna ska även vara sammanställda på ett sådant strukturerat sätt att de enkelt kan komma till användning i det brottsbekämpande arbetet. Ett sätt att uppfylla kravet kan vara att använda sig av i förväg överenskomna format baserade på etablerade standarder. Mer detaljerade föreskrifter om i vilket format uppgifter ska lämnas ut kan meddelas med stöd av normgivningsbemyndigandet i tredje stycket. På samma sätt som gäller enligt nuvarande 29 § andra stycket innebär kravet på tillgängliggörande inte att tillhandahållaren har en skyldighet att dekryptera meddelanden i de fall där denne inte tillhandahåller eller förfogar över krypteringssystemet.

Av *tredje stycket* följer att första och andra styckena även gäller lokaliseringsuppgifter som inte är trafikuppgifter.

Tillsynsmyndigheten får enligt *fjärde stycket* i enskilda fall besluta om undantag från kravet i andra stycket på att uppgifterna ska ordnas och göras tillgängliga i ett format som gör att de enkelt kan tas om hand, om det finns särskilda skäl för det. Undantag kan t.ex. medges om kravet blir alltför betungande för en mindre tillhandahållare.

I *femte stycket* finns ett bemyndigande för regeringen eller den myndighet som regeringen bestämmer att meddela ytterligare föreskrifter om hur uppgifterna ska lämnas ut.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Paragrafen innehåller bestämmelser om en skyldighet att på begäran lämna ut vissa uppgifter som enligt 31 § första stycket omfattas av tystnadsplikt. Övervägandena finns i avsnitt 5.4.

I *första stycket 2* görs ett tillägg om att uppgifter som gäller brottslig verksamhet omfattas av skyldigheten att lämna ut uppgifter om abonnemang. Ändringen innebär ett förtydligande av att uppgiftsskyldigheten gäller även i de fall en brottsbekämpande myndighet behöver uppgifterna i sin underrättelseverksamhet. Dessutom förtydligas att uppgifter får lämnas ut till, utöver Polismyndigheten och Säkerhetspolisen, bl.a. Åklagarmyndigheten, Ekobrottsmyndigheten och Tullverket.

12 kap.

1 § Tillsynsmyndigheten ska ta ut en sanktionsavgift av den som inte

1. tillhandahåller en sammanfattning av avtalet i enlighet med 7 kap. 1 §, föreskrifter som har meddelats med stöd av den paragrafen och genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 102.3 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,
2. tillämpar villkor om bindningstid och uppsägningstid i enlighet med 7 kap. 8, 13 eller 14 §,
3. uppfyller kraven på nummerportabilitet i enlighet med 7 kap. 19 och 20 §§ och föreskrifter om nummerportabilitet som har meddelats med stöd av 7 kap. 21 § första stycket,
4. vidtar åtgärder för att hantera risker som hotar säkerheten i nät och tjänster i enlighet med 8 kap. 1 §, föreskrifter som har meddelats med stöd av den paragrafen och genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,
5. rapporterar om säkerhetsincidenter i enlighet med 8 kap. 3 §, föreskrifter som har meddelats med stöd av den paragrafen och genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,
6. informerar om hot om säkerhetsincidenter i enlighet med 8 kap. 4 §, föreskrifter som har meddelats med stöd av den paragrafen och genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,
7. vidtar skyddsåtgärder enligt 8 kap. 5 § och föreskrifter som har meddelats med stöd av den paragrafen,
8. vidtar åtgärder för att säkerställa skydd av uppgifter som behandlas i samband med tillhandahållandet av en tjänst i enlighet med 8 kap. 6 § och föreskrifter som har meddelats med stöd av den paragrafen,
9. informerar abonnenten om särskilda risker för bristande skydd av behandlade uppgifter i enlighet med 8 kap. 7 §,
10. underrättar om integritetsincidenter i enlighet med 8 kap. 8 § och föreskrifter som har meddelats med stöd av den paragrafen,
11. behandlar uppgifter i ett elektroniskt meddelande eller trafikuppgifter som hör till detta meddelande i enlighet med 9 kap. 27 §,

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

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

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

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

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

Paragrafen reglerar vilka överträdelser som tillsynsmyndigheten ska besluta om sanktionsavgift för. Övervägandena finns i avsnitt 5.1.

Ändringarna i *första stycket 13* är en följd av att nuvarande 9 kap. 29 § andra stycket ersätts av en delvis motsvarande bestämmelse i 9 kap. 29 b § andra stycket.

Ikraftträdande- och övergångsbestämmelser

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

2. En förbetald allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst eller en förbetald internetanslutningstjänst som har tillhandahållits före ikraftträdandet får, även om någon registrering enligt 9 kap. 24 § inte har gjorts, tillhandahållas till och med den 1 februari 2023 eller den senare tidpunkt då en ny förbetalning görs.

Övervägandena om ikraftträdande- och övergångsbestämmelserna finns i avsnitt 6.

Enligt *punkt 1* träder lagen i kraft den 1 augusti 2022.

Övergångsbestämmelsen i *punkt 2* innebär att en oregistrerad förbetald allmänt tillgänglig nummerbaserad interpersonell kommunikationstjänst eller en oregistrerad förbetald internetanslutningstjänst som har tillhandahållits före den 1 augusti 2022 får tillhandahållas till och med den 1 februari 2023 eller den senare tidpunkt då en ny förbetalning görs. Om en registrering inte har gjorts inom denna tid ska tillhandahållandet av tjänsten upphöra. Bestämmelsen om förbetalning innebär att en registrering måste göras senast i samband med den första förbetalning som görs efter den 1 februari 2023. När det gäller kontantkort är det alltså fråga om att kontantkortet fylls på. En oregistrerad tjänst ska inte vara möjlig att använda efter det att en förbetalning har genomförts. Det är upp till tillhandahållaren att välja om den vill utnyttja möjligheten att tillhandahålla tjänsten till och med tidpunkten för en ny förbetalning. Tillhandahållaren är alltså inte skyldig att tillhandahålla en oregistrerad tjänst efter den 1 februari 2023.

Sammanfattning av betänkandet Datalagring och integritet (SOU 2015:31)

Inhämtning av abonnemangsuppgifter

En av de brister i datalagringsdirektivet som EU-domstolen pekade på i sin dom var att direktivet inte angav några objektiva kriterier för att avgränsa de nationella myndigheternas tillgång till och användning av de lagrade uppgifterna. Domstolen noterade också att direktivet inte krävde att tillgången till uppgifter skulle vara underkastad någon förhandskontroll av en domstol eller oberoende myndighet som har till uppgift är att se till att tillgången begränsas till vad som är strikt nödvändigt.

Abonnemangsuppgifter som lagras med stöd av de svenska datalagringsreglerna får lämnas ut till brottsbekämpande myndigheter utan krav på att den brottslighet som uppgifterna lämnas ut för ska vara av någon viss svårhetsgrad. Vidare får uppgifter hämtas in efter beslut av den brottsbekämpande myndigheten och således utan föregående kontroll av en oberoende instans.

Vi har mot den bakgrunden övervägt ett flertal olika åtgärder som skulle kunna bidra till att stärka kontrollen över de brottsbekämpande myndigheternas tillämpning av reglerna om inhämtning av abonnemangsuppgifter. Bland annat har vi övervägt om ett tillsynsorgan bör få i uppgift att utöva tillsyn som specifikt tar sikte på tillämpningen av dessa regler. Vi gör dock bedömningen att nackdelarna med en sådan ordning överväger fördelarna. Däremot föreslår vi att beslut om inhämtning av abonnemangsuppgifter ska få fattas endast av vissa särskilt utpekade befattningshavare inom den myndighet som begär uppgifterna. Vidare föreslår vi att beslut om inhämtning av sådana uppgifter ska dokumenteras på visst sätt. Dessa åtgärder bedöms kunna bidra till högre kvalitet i beslutsfattandet och till att den tillsyn som bedrivs av JO, JK, Datainspektionen och SIN blir mer effektiv. Vidare lämnar vi förslag på vissa förtydliganden i bestämmelsen om inhämtning av abonnemangsuppgifter. Syftet är att göra det tydligt att bestämmelsen kan tillämpas i de brottsbekämpande myndigheternas underrättelseverksamhet.

Betänkandets lagförslag

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

Härigenom föreskrivs att 6 kap. 22 § lagen (2003:389) om elektronisk kommunikation ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

6 kap.

22 §[1]

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 misstanke om brott till en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen eller någon annan myndighet som ska ingripa mot brottet,	2. uppgift som avses i 20 § första stycket 1 och som gäller misstanke om brott *eller brottslig verksamhet* till en åklagarmyndighet, 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),

[1] Senaste lydelse 2014:734.

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, och

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.

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

Denna lag träder i kraft den 1 juli 2016.

Förteckning över remissinstanserna

Remissyttranden över betänkandet Datalagring och integritet (SOU 2015:31) har lämnats av följande instanser: Riksdagens ombudsmän, Göta hovrätt, Stockholms tingsrätt, Malmö tingsrätt, Kammarrätten i Stockholm, Förvaltningsrätten i Umeå, Förvaltningsrätten i Göteborg, Justitiekanslern, Domstolsverket, Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Säkerhets- och integritetsskyddsnämnden, Kriminalvården, Brottsförebyggande rådet, Datainspektionen, Kustbevakningen, Försvarsmakten, Försvarets radioanstalt, Statens inspektion för försvarsunderrättelseverksamheten, Försvarsunderrättelsedomstolen, Tullverket, Försäkringskassan, Skatteverket, Statskontoret, Post- och telestyrelsen, Lunds universitet (Juridiska fakulteten), Stockholms universitet (Juridiska fakulteten), Göteborgs universitet (Juridiska institutionen), Kungl. Tekniska högskolan, Blekinge tekniska Högskola, Diskrimineringsombudsmannen, Sveriges advokatsamfund, TULL-KUST, Tidningsutgivarna, Journalistförbundet, Utgivarna, Svenska kyrkan, Sveriges kristna råd, Svenska Stadsnätsföreningen, IT&Telekomföretagen, Com Hem AB, Hi3G Access AB, Tele2 Sverige AB, TeliaSonera Sverige AB, Stiftelsen för internetinfrastruktur, SNUS (Swedish Network Users' Society), Svensk biblioteksförening, Konstnärliga och Litterära Yrkesutövares Samarbetsnämnd, Rättighetsalliansen, Föreningen för Digitala fri- och rättigheter, Institutet för Juridik och Internet och Swedish institute of Computer Science.

Yttrande har också inkommit från Dataskydd.net, Föreningen fri kultur och programvara, Piratpartiet, Swedish Doctors for Human Rights, Tankesmedjan Fores och Ung pirat.

Följande instanser har inbjudits att yttra sig men avstått: Sveriges psykologförbund, Sveriges läkarförbund, Judiska centralrådet i Sverige, Islamiska förbudet i Sverige, Amnesty international Sverige, Svenska avdelningen av Internationella Juristkommissionen, Civil Rights Defenders, Centrum för rättvisa, Alltele Privat AB, Bahnhof AB, TDC Sverige AB, Telenor Sverige AB, Filmproducenternas rättighetsförening, IFPI Sverige och Netnod Internet Exchange.

Sammanfattning av promemorian Registrering av kontantkort, m.m. (Ds 2020:12)

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 internet-anslutningstjänster. 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.

Promemorians lagförslag

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 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 överföra ett elektroniskt meddelande. Det gäller dock inte om uppgifterna sparas för sådan behandling som anges i 6, 13, 16 a *eller* 16 c §.	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 §*.
Hemliga 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] 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.
[3] Senaste lydelse 2012:285.
[4] Senaste lydelse 2018:1917.

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.

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 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 misstanke om brott till *en åklagarmyndighet*, Polismyndigheten, Säkerhetspolisen eller någon annan myndighet som ska ingripa mot brottet,	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,*

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

[5] Senaste lydelse 2016:1311.

(EU) nr 596/2014 av den 16 april 2014 om marknadsmissbruk (marknadsmissbruksförordning) och om upphävande av Europaparlamentets och rådets direktiv 2003/6/EG och kommissionens direktiv 2003/124/EG, 2003/125/EG och 2004/72/EG.

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 §.

Förteckning över remissinstanserna

Efter remiss har yttranden över departementspromemorian Registrering av kontantkort, m.m. (Ds 2020:12) lämnats av Brottsförebyggande rådet, Datainspektionen, Ekobrottsmyndigheten, Försvarets radioanstalt, Försvarsmakten, Förvaltningsrätten i Stockholm, Göteborgs universitet (Juridiska institutionen), Hi3G Access AB, IT&Telekomföretagen, Journalistförbundet, Justitiekanslern, Kammarrätten i Stockholm, Kustbevakningen, Polismyndigheten, Post- och telestyrelsen, Regelrådet, Riksdagens ombudsmän, Sveriges advokatsamfund, Sveriges Radio AB, Säkerhets- och integritetsskyddsnämnden, Säkerhetspolisen, Tele2 Sverige AB, Telenor Sverige AB, Tullverket, TU – Medier i Sverige, Umeå universitet (Juridiska institutionen), Unizon och Åklagarmyndigheten.

Com Hem AB, Föreningen grävande journalister, Företagarna, Lycamobile Sweden AB, Pensionärernas riksorganisation, Riksorganisationen för kvinnojourer och tjejjourer i Sverige (Roks), Småföretagarnas Riksförbud, Telia Sverige AB och Wifog Sverige AB har inte svarat på remissen.

Synpunkter har även lämnats av Försvarets materielverk, Samhällsmagasinet Avsnitt, Totalförsvarets forskningsinstitut, Utgivarna och Verizon Sweden AB.