Kommittédirektiv

Datalagring och EU-rätten

Dir. 2017:16

Beslut vid regeringssammanträde den 16 februari 2017

Sammanfattning

En särskild utredare ska se över bestämmelserna om skyldigheten att lagra uppgifter om elektronisk kommunikation som gäller för leverantörer av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster, samt bestämmelserna om de brottsbekämpande myndigheternas tillgång till sådana uppgifter. Översynen ska ske i syfte att anpassa det svenska regelverket till EU-rätten såsom den uttolkats av EU-domstolen i förhandsavgörandet den 21 december 2016 i de förenade målen C-203/15 och C-698/15. Utredaren ska föreslå de förändringar som är nödvändiga för att det svenska regelverket ska vara proportionerligt och ha en ändamålsenlig balans mellan skyddet för enskildas personliga integritet och behovet av uppgifter för att kunna förebygga, förhindra, upptäcka, utreda och lagföra brott.

Utredaren ska också se över rättssäkerhetsgarantierna och mekanismerna som ska skydda den personliga integriteten när hemliga tvångsmedel för särskilt allvarlig eller på annat sätt samhällsfarlig brottslighet används.

Uppdraget ska redovisas senast den 16 augusti 2018. Den del av uppdraget som ges med anledning av EU-domstolens förhandsavgörande om datalagring ska delredovisas senast den 9 oktober 2017.

Reglerna om datalagring och om vissa hemliga tvångsmedel behöver ses över

Leverantörer av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster

(leverantörerna) ska enligt lagen (2003:389) om elektronisk kommunikation (LEK) lagra vissa uppgifter om bl.a. telefonsamtal, internettrafik och meddelandehantering för att uppgifterna ska kunna användas vid brottsbekämpning. Villkoren för de brottsbekämpande myndigheternas inhämtning av dessa uppgifter regleras närmare i LEK, rättegångsbalken och lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen).

EU-domstolen har, efter en begäran om ett förhandsavgörande från Kammarrätten i Stockholm, nyligen prövat om de svenska reglerna om datalagring och om tillgången till lagrade uppgifter stämmer överens med EU-rätten. Avgörandet klargör att svensk rätt inte stämmer överens med EU-rätten på ett flertal punkter. Lagstiftningen behöver därför ses över och ändras.

Den 1 januari 2015 permanentades ett antal bestämmelser om hemliga tvångsmedel som fram till dess varit tidsbegränsade. I samband med uppdraget att se över frågorna om datalagring och åtkomst till lagrade uppgifter finns det även skäl att se över hur rättssäkerhetsgarantierna och mekanismerna som ska skydda den personliga integriteten när man använder dessa hemliga tvångsmedel fungerar.

Uppdraget att se över den svenska datalagringsregleringen i ljuset av EU-domstolens förhandsavgörande om datalagring

Den svenska regleringen har prövats av EU-domstolen

EU-domstolen (förenade målen C 293/12 och C 594/12) ogiltigförklarade i april 2014 det s.k. datalagringsdirektivet (Europaparlamentets och rådets direktiv 2006/24/EG om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG). Syftet med direktivet var att harmonisera medlemsstaternas bestämmelser om skyldighet att lagra vissa uppgifter om elektronisk kommunikation för att

säkerställa att uppgifterna är tillgängliga för utredning, avslöjande och åtal av brott som medlemsstaterna anser vara allvarliga. Enligt domstolens bedömning överskred EU:s lagstiftande församlingar sina befogenheter när direktivet antogs, eftersom det inte levde upp till proportionalitetsprincipen när det gällde artiklarna 7, 8 och 52.1 i EU:s stadga om de grundläggande rättigheterna (EU-stadgan). Artikel 7 reglerar rätten till respekt för bl.a. privat- och familjelivet och artikel 8 rätten till skydd av personuppgifter. Enligt artikel 52.1 måste varje begränsning i utövandet av fri- och rättigheter som erkänns i EU-stadgan vara föreskriven i lag och vara förenlig med det väsentliga innehållet i dessa fri- och rättigheter. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras 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.

Till följd av ogiltigförklaringen faller nu EU-rätten när det gäller datalagring för brottsbekämpning tillbaka på artikel 15.1 i Europaparlamentets och rådets direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (direktiv 2002/58). Där anges närmare under vilka förutsättningar medlemsstaterna får vidta åtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som anges i direktivet. Direktivet är inte tillämpligt på verksamheter som avser allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättens område (artikel 1.3).

Det ogiltigförklarade direktivet genomfördes i svensk rätt genom ändringar i framför allt LEK (prop. 2010/11:46, bet. 2011/12:JuU28, rskr. 2011/12:166). Enligt 6 kap. 16 a § i den lagen är leverantörerna skyldiga att lagra vissa uppgifter som genereras eller behandlas i samband med att tjänster tillhandahålls, för att uppgifterna ska kunna användas vid brottsbekämpning. Lagringsskyldigheten gäller i sex månader från den dag kommunikationen avslutades. Som huvudregel ska

den lagringsskyldige sedan genast utplåna uppgifterna (6 kap. 16 d § LEK).

Skyldigheten att lagra data enligt de svenska bestämmelserna ifrågasattes efter EU-domstolens dom där datalagringsdirektivet ogiltigförklarades. Flera leverantörer meddelade att de tänkte sluta lagra uppgifter enligt de tvingande reglerna i LEK, och i vissa fall att man tänkte radera redan lagrade uppgifter. Post- och telestyrelsen förelade därför flera leverantörer att fortsätta med sin lagring. Med anledning av ett överklagande av ett sådant föreläggande begärde Kammarrätten i Stockholm ett förhandsavgörande från EU-domstolen (mål nr 7380-14). Frågorna tog sikte på rättsläget enligt artikel 15.1 i direktiv 2002/58, i dess lydelse enligt Europaparlamentets och rådets direktiv 2009/136/EG, och artiklarna 7, 8 och 52.1 i EU-stadgan.

EU-domstolen besvarade kammarrättens begäran om förhandsavgörande genom en dom den 21 december 2016 (förenade målen C-203/15 och C-698/15). EU-domstolens slutsats var bl.a. att en generell och odifferentierad lagring av uppgifter om elektronisk kommunikation inte är förenlig med EU-rätten. Domstolen framhöll bl.a. att dessa uppgifter sammantagna kan göra det möjligt att dra mycket precisa slutsatser om privatlivet för de personer vars uppgifter har lagrats, och att kartlägga de berörda personerna på ett sätt som är lika känsligt ur integritetssynpunkt som själva innehållet i kommunikationerna. Domstolen gjorde även vissa uttalanden om förutsättningarna för de brottsbekämpande myndigheternas åtkomst till lagrade uppgifter samt om säkerheten för uppgifterna.

Kammarrätten beslutade dagen därpå att Post- och telestyrelsens föreläggande om fortsatt lagring tills vidare inte ska gälla. Kammarrätten har inte slutligt avgjort målet.

Uppgifter som kan lagras

Den centrala bestämmelsen om lagringsskyldighetens omfattning finns i 6 kap. 16 a § LEK. Skyldigheten omfattar uppgifter som anges som nödvändiga för vissa bestämda syften.

Dessa är preciserade som uppgifter som är nödvändiga för att spåra och identifiera kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och varaktighet för den, typ av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning vid kommunikationens början och slut. Även uppgifter som genereras eller behandlas vid misslyckade uppringningar ska lagras. Innehållet i kommunikationen lagras däremot inte. Lagringsskyldigheten är närmare strukturerad i vissa teknikslag. Dessa är angivna som telefonitjänst, meddelandehantering, internetåtkomst och tillhandahållande av kapacitet för att få internetåtkomst (anslutningsform). I 39–43 §§ förordningen (2003:396) om elektronisk kommunikation (FEK) finns ytterligare bestämmelser om vilka uppgifter som ska lagras.

EU-domstolen har i förhandsavgörandet slagit fast att lagringsskyldigheten enligt LEK överskrider gränserna för vad som är strängt nödvändigt och att den inte kan anses motiverad i ett demokratiskt samhälle i enlighet med artikel 15.1 i direktiv 2002/58 jämförd med artiklarna 7, 8, 11 och 52.1 i EU-stadgan. En generell och odifferentierad lagring av uppgifter – utan att det görs någon åtskillnad, begränsning eller undantag utifrån syftet att bekämpa brott – är alltså inte tillåten. I sammanhanget påpekas bl.a. att den omständigheten att lagringen och den senare användningen av uppgifterna sker utan att abonnenten är underrättad om det kan ge de berörda personerna en känsla av att deras privatliv står under ständig övervakning. Det finns enligt EU-domstolen däremot inget hinder mot att i förebyggande syfte tillämpa en riktad lagring i syfte att bekämpa grov brottslighet. En sådan datalagring förutsätter dock att lagringen begränsas till vad som är strängt nödvändig när det gäller vilka slags uppgifter som ska lagras, vilka kommunikationsmedel som avses, vilka personer som berörs och hur länge lagringen ska ske.

Att kunna få tillgång till lagrade uppgifter om elektronisk kommunikation är av mycket stort värde för rättsväsendets myndigheter i arbetet med att förebygga, förhindra, upptäcka, utreda och lagföra brott, inte minst när det gäller grov brottslighet. Genom att sådana uppgifter finns lagrade – och

därmed kan hämtas in av de brottsbekämpande myndigheterna – går det att klarlägga händelser som anknyter till såväl själva brottstillfället som till t.ex. planläggning eller flykt. I många fall, t.ex. vid barnpornografibrott, kan uppgifter om elektronisk kommunikation vara avgörande för att man ska kunna identifiera en misstänkt gärningsman. Uppgifterna har även stor betydelse för att man ska kunna bekräfta brottsmisstankar.

Inom ramen för de riktlinjer EU-domstolen drar upp bör det även i fortsättningen, vid sidan av de uppgifter leverantörerna lagrar frivilligt, finnas ett utrymme för att i lagstiftningen kunna ha tvingande regler för leverantörernas lagring av uppgifter om elektronisk kommunikation. Hur stort detta utrymme är och vilket behov det finns av det måste dock utredas. Målsättningen är att upprätthålla ett starkt skydd för de grundläggande rättigheterna som står sig väl vid en rättslig prövning, samtidigt som de brottsbekämpande myndigheternas möjligheter att upprätthålla sin förmåga att förebygga, förhindra, upptäcka, utreda och lagföra brott kan tillgodoses. En särskild fråga i sammanhanget är också vilken effekt domen har på verksamhet som avser Sveriges säkerhet, dvs. sådan verksamhet som ligger inom Säkerhetspolisens ansvarsområde.

Utredaren ska

- analysera hur reglerna om lagring av uppgifter enligt 6 kap. 16 a § LEK och 39–43 §§ FEK förhåller sig till EU-domstolens dom,
- med beaktande av skyddet för den personliga integriteten och yttrandefriheten, överväga olika alternativ till förändringar i de delar reglerna inte bedöms vara förenliga med domen och belysa fördelarna och nackdelarna med dessa alternativ, och
- föreslå de författningsändringar och andra åtgärder som behövs.

Tillgången till lagrade uppgifter

EU-domstolen uttalar sig i domen också om vilka villkor som ska gälla för att behöriga nationella myndigheter ska få tillgång till lagrade uppgifter. För att begränsa tillgången till vad som är

strängt nödvändigt krävs, enligt EU-domstolen, i princip att uppgifterna rör personer som misstänks planera, begå eller ha begått ett allvarligt brott eller som på något annat sätt är inblandade i ett sådant brott. När vitala intressen för nationell säkerhet, försvar eller allmän säkerhet hotas av terrorism kan tillgång dock även ges till uppgifter om andra personer. Vidare ska tillgången normalt – utom i brådskande fall – kräva förhandskontroll av en domstol eller en oberoende myndighet. Den person som de inhämtade uppgifterna rör ska dessutom underrättas om åtgärden så snart en sådan upplysning inte riskerar att skada utredningen.

Bestämmelser om tillgången till uppgifter som ska lagras finns i flera olika regleringar. Regler om inhämtning av abonnemangsuppgifter finns i 6 kap. 22 § första stycket 2 LEK, regler om inhämtning av trafik- och lokaliseringsuppgifter under förundersökning i 27 kap. 19 § rättegångsbalken och regler om inhämtning av trafik- och lokaliseringsuppgifter i underrättelseverksamhet finns i inhämtningslagen.

Det stora flertalet av de brottstyper som omfattas av regleringen om hemlig övervakning av elektronisk kommunikation har ett straffminimum på sex månaders fängelse. Tvångsmedlet får dock även användas i vissa andra fall, t.ex. vid dataintrång, barnpornografibrott och samhällsfarliga brott inom Säkerhetspolisens verksamhetsområde. Det får dessutom i förekommande fall användas vid förundersökning om försök, förberedelse eller stämpling till sådan brottslighet. Det finns också vissa bestämmelser i andra lagar som utvidgar tillämpningsområdet för tvångsmedlet. Enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott får exempelvis hemlig övervakning av elektronisk kommunikation användas för brott som inte uppfyller kraven på brottets svårhet enligt reglerna i rättegångsbalken.

Huvudregeln är att hemlig övervakning av elektronisk kommunikation bara får användas efter förhandsprövning och beslut av domstol. Tillstånd får under vissa förutsättningar dock även ges interimistiskt av åklagare i avvaktan på domstolens prövning. Enskilda som har utsatts för användning av

tvångsmedlet ska enligt huvudregeln underrättas om åtgärden i efterhand.

I princip motsvarande uppgifter som kan hämtas in enligt reglerna om hemlig övervakning av elektronisk kommunikation kan i Polismyndighetens, Säkerhetspolisens och Tullverkets underrättelseverksamhet hämtas in enligt inhämtningslagen. Uppgifterna får under vissa förutsättningar hämtas in för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott med ett straffminimum på två års fängelse, eller som avser vissa särskilt angivna brott inom Säkerhetspolisens ansvarsområde. Till skillnad från regleringen om hemlig övervakning av elektronisk kommunikation är beslut om inhämtning av uppgifter enligt inhämtningslagen inte föremål för någon utomstående förhandsprövning utan fattas på egen hand av respektive myndighet. Lagen innehåller inte heller någon motsvarighet till rättegångsbalkens krav på underrättelse till enskilda.

Inte heller vid inhämtning av abonnemangsuppgifter enligt LEK finns det något krav på föregående kontroll av en oberoende instans. Uppgifterna får alltså hämtas in efter beslut av den brottsbekämpande myndigheten själv. Regleringen ställer inte heller några krav på underrättelse i efterhand eller att den brottslighet som uppgifterna lämnas ut för ska vara av en viss svårhetsgrad. De brottsbekämpande myndigheterna har således rätt att få tillgång till uppgifter om abonnemang – t.ex. abonnentens nummer, namn och adress – vid alla typer av brott utom sådana brott där åtal enbart får väckas av målsäganden. Bestämmelsens utformning motiverades med att trakasserier via internet av olika slag, nätmobbning och förtal liksom vuxnas kontakter med barn i sexuella syften (grooming), hade blivit ett allt större problem och att möjligheten att ingripa mot sådana brott ofta var begränsade eftersom det saknades tillgång till abonnemangsuppgifter som kunde identifiera abonnenten (prop. 2011/12:55, s. 102). Abonnemangsuppgifter hämtas även in i underrättelseskedet (SOU 2015:31, s. 198 f.)

EU-domstolens dom innebär att regelverkens nuvarande utformning behöver ses över när det gäller de närmare förutsättningarna för myndigheternas tillgång till uppgifter. Det

gäller t.ex. vilka krav som bör ställas på brottets allvar för att uppgifterna ska få hämtas in. En annan sådan fråga är vad som sägs i domen om krav på underrättelse till enskilda. Även beslutsordningen för att få hämta in lagrade uppgifter behöver ses över liksom frågan om det behövs ett särskilt skydd för uppgifter som omfattas av yrkesmässig tystnadsplikt.

Utredaren ska

- analysera hur dagens regler om tillgång till uppgifter som lagras förhåller sig till EU-domstolens dom,
- överväga olika alternativ till förändringar i de delar reglerna inte bedöms vara förenliga med domen och belysa fördelarna och nackdelarna med dessa alternativ, och
- föreslå de författningsändringar och andra åtgärder som behövs.

Vid utformningen av förslagen bör den gräns som i dag råder mellan underrättelseverksamhet och brottsutredande verksamhet inom ramen för en förundersökning beaktas så långt som möjligt.

Skyddet och säkerheten för de lagrade uppgifterna

Den som är skyldig att lagra uppgifter enligt reglerna i LEK är också ansvarig för att skydda uppgifterna. Den lagringsskyldige ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling (6 kap. 3 a § första stycket LEK). Ytterligare föreskrifter om säkerheten för de lagrade uppgifterna finns i bl.a. 37 § FEK. Det finns inget krav i Sverige på att uppgifterna ska lagras inom ett visst område, t.ex. inom EU.

Uppgifterna ska vidare utplånas vid lagringstidens slut eller, om en begäran om utlämnande har inkommit men inte hunnit behandlas inom denna tid, så fort uppgifterna har lämnats ut (6 kap. 16 d § LEK). Att reglerna följs står under tillsyn av Post- och telestyrelsen.

EU-domstolen uttalar sig i förhandsavgörandet även i dessa frågor. Med hänsyn till att det bl.a. handlar om en stor mängd uppgifter av känslig natur måste leverantörerna av elektroniska kommunikationstjänster, för att säkerställa fullständig integritet

och konfidentialitet för uppgifterna, garantera en särskilt hög skydds- och säkerhetsnivå. EU-domstolen konstaterar också att den nationella lagstiftningen i synnerhet måste föreskriva att lagringen sker inom unionen och att uppgifterna oåterkalleligen förstörs när deras lagringstid gått ut. I domen pekas även på vikten av kontroll av en oberoende myndighet.

Utredaren ska

- analysera hur nuvarande regler om skydd av och säkerhet för uppgifter som lagras förhåller sig till EU-domstolens dom,
- överväga olika alternativ till förändringar i de delar reglerna inte bedöms vara förenliga med domen och belysa fördelarna och nackdelarna med dessa alternativ, och
- föreslå de författningsändringar och andra åtgärder som behövs.

Internationell utblick

Utredaren ska redovisa gällande rätt och pågående arbete i Finland och Danmark och de övriga länder som bedöms vara relevanta för utredningsuppdraget, t.ex. Österrike, Tyskland och Nederländerna, och i övrigt göra de internationella jämförelser som utredaren bedömer befogade.

Utredaren ska även följa arbetet med EU-kommissionens förslag till förordning om integritet och elektronisk kommunikation (COM [2017], 10 final, 2017/0003 [COD]) och, i den mån det bedöms nödvändigt, eventuellt arbete på EU-nivå med anledning av EU-domstolens förhandsavgörande.

Målet i kammarrätten

Enligt EU-domstolen ankommer det på Kammarrätten i Stockholm att pröva om och i så fall i vilken utsträckning den svenska regleringen uppfyller kraven enligt artikel 15.1 i direktiv 2002/58 jämfört med artiklarna 7, 8, 11 och artikel 52.1 i EU-stadgan, såsom de preciseras i förhandsavgörandet, när det gäller behöriga nationella myndigheters tillgång till lagrade uppgifter och skyddet av och säkerheten för uppgifterna.

Utredaren ska vid utformningen av sina förslag, i den mån utredaren bedömer det relevant, beakta utfallet av kammarrättens prövning.

Närliggande frågor

Utredaren får ta upp sådana närliggande frågor som har samband med de frågeställningar som ska utredas, under förutsättning att uppdraget ändå bedöms kunna redovisas i tid. Exempel på sådana frågor är vilken efterhandskontroll som bör finnas samt om någon myndighet bör ha tillsyn över att uppgifter om elektronisk kommunikation lämnas ut på ett korrekt sätt.

Uppdraget att se över rättssäkerhetsgarantierna och mekanismerna som ska skydda den personliga integriteten vid användning av hemliga tvångsmedel för vissa allvarliga brott

Permanentningen av reglerna om hemliga tvångsmedel

Under senare år har kriminaliteten blivit alltmer komplex och svårutredd. Att information kan hämtas in är som nämnts centralt för att de brottsbekämpande myndigheterna på ett effektivt sätt ska kunna förebygga, förhindra och utreda brott. När det gäller särskilt allvarlig eller på annat sätt samhällsfarlig brottslighet är inhämtning av information genom användning av hemliga tvångsmedel i många fall de enda verktyg som kan användas för att driva en brottsutredning framåt.

Regler om hemliga tvångsmedel för den typen av brottslighet finns framför allt i rättegångsbalken och i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott. Lagen, som reglerar möjligheten att använda hemliga tvångsmedel utan att en förundersökning pågår, var tidigare tidsbegränsad men gjordes permanent genom lagändringar som trädde i kraft den 1 januari 2015. Genom en överflyttning till rättegångsbalken permanentades samtidigt även bestämmelserna i två andra tidsbegränsade lagar med

bestämmelser om hemliga tvångsmedel för särskilt allvarlig eller på annat sätt samhällsfarlig brottslighet, nämligen lagen (2007:978) om hemlig rumsavlyssning och lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott (prop. 2013/14:237, bet. 2014/15:JuU2, rskr. 2014/15:22).

En avvägning mellan enskildas rätt till integritet och rättssäkerhet och behovet av en effektiv brottsbekämpning

Det är samtidigt av grundläggande betydelse i en rättsstat att rätten till skydd för privat- och familjelivet respekteras. De hemliga tvångsmedlen inskränker de rättigheter som var och en har enligt regeringsformen och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). Varje befogenhet för staten att i hemlighet bereda sig tillgång till personlig information, och varje utnyttjande av denna befogenhet, leder till ingrepp i den personliga integriteten. Graden av integritetsintrång varierar med befogenhetens (tvångsmedlets) utformning och tillämpning. Regleringen om hemliga tvångsmedel bygger på en avvägning mellan å ena sidan samhällets behov av en effektiv brottsbekämpning till skydd för medborgarna och å andra sidan enskildas rätt till integritet och rättssäkerhet i förhållande till staten.

Rättssäkerhetsgarantier och mekanismer till skydd för den personliga integriteten

Avvägningen har resulterat i att regleringen omgärdas av ett antal rättssäkerhetsgarantier och mekanismer för att säkerställa att reglerna och deras tillämpning lever upp till högt ställda krav på rättssäkerhet och att intrånget i den personliga integriteten minimeras. De har tillkommit bl.a. för att möta de krav som regeringsformen och Europakonventionen ställer i dessa avseenden. För tillstånd till hemliga tvångsmedel krävs det normalt prövning i domstol. Vid domstolsprövningen av flertalet av de hemliga tvångsmedlen ska ett offentligt ombud kallas att närvara för att bevaka enskildas integritetsintressen. Det offentliga ombudet ska ha tillgång till allt material som

ligger till grund för domstolens prövning och har rätt att överklaga domstolens beslut. I samband med permanentningen av de tidsbegränsade reglerna togs möjligheten för domstolen att fatta beslut om hemliga tvångsmedel, utan att ett offentligt ombud har medverkat, bort. Till rättssäkerhetsgarantierna räknas också skyldigheten att i efterhand underrätta vissa personer om att hemliga tvångsmedel har använts. Även den tillsyn och kontroll som Säkerhets- och integritetsskyddsnämnden utövar över de brottsbekämpande myndigheterna räknas hit. Nämnden har som övergripande mål att bidra till att värna rättssäkerheten och skyddet för den personliga integriteten inom den brottsbekämpande verksamheten. Tillsynen ska särskilt syfta till att säkerställa att verksamheten bedrivs i enlighet med lag eller annan författning. Nämnden är också på begäran av en enskild skyldig att kontrollera om han eller hon har utsatts för hemliga tvångsmedel och om hanteringen i så fall har varit lagenlig. Den enskilde underrättas om att kontrollen har utförts men kan p.g.a. sekretess som regel inte informeras närmare om vad som har funnits vid kontrollen.

Även regleringen av användningen av överskottsinformation har tillkommit mot bakgrund av regeringsformens och Europakonventionens krav. Vidare finns det av integritets-hänsyn ett förbud mot avlyssning av vissa samtal eller meddelanden. Utgångspunkten för förbudet – som utvidgades i samband med permanentningen av de tidsbegränsade bestämmelserna – är att uppgifter som inte får inhämtas genom vittnesförhör i domstol inte heller ska kunna inhämtas genom avlyssning.

Tidigare översyner

Rättssäkerhetsgarantierna och mekanismerna till skydd för den personliga integriteten har setts över i olika sammanhang. Utredningen om rättssäkerhet vid hemliga tvångsmedel gjorde t.ex. bedömningen att systemet med offentliga ombud fungerade väl och att inga förändringar behövdes (SOU 2006:98). Några år senare konstaterade Utredningen om

utvärdering av vissa hemliga tvångsmedel att befintliga rättssäkerhetsgarantier och kontrollmekanismer utgör ett tillräckligt gott skydd mot otillbörliga intrång i den personliga integriteten (SOU 2009:70). Även Utredningen om vissa hemliga tvångsmedel gjorde en översyn i samband med att man tog ställning till de tre tidsbegränsade lagarnas fortsatta giltighet och hur den framtida regleringen av hemliga tvångsmedel för särskilt allvarlig eller annars samhällsfarlig brottslighet borde utformas. Enligt utredningen lever rättssäkerhetsgarantierna upp till regeringsformens och Europakonventionens krav (SOU 2012:44).

Rättssäkerhetsgarantierna och mekanismerna till skydd för den personliga integriteten bör ses över på nytt

Det är viktigt att rättssäkerhetsgarantierna och mekanismerna till skydd för den personliga integriteten fungerar. Den senaste översynen sträcker sig till utgången av 2011. Det finns när det gäller de bestämmelser om hemliga tvångsmedel för särskilt allvarlig eller på annat sätt samhällsfarlig brottslighet, som permanentades den 1 januari 2015, skäl att nu följa upp tillämpningen av befintliga rättssäkerhetsgarantier och mekanismer till skydd för enskildas personliga integritet. Syftet är att säkerställa att de tillämpas på ett sådant sätt att systemet lever upp till de krav som Europakonventionen och regeringsformen ställer på rättssäkerhet och skydd för den personliga integriteten. Det är i detta sammanhang särskilt angeläget att bedöma effekterna avseende skyddet för enskildas personliga integritet med anledning av permanentningen (prop. 2014/15:1, uo 4, s. 23). Bland annat bör utredaren göra en analys av om det sedan permanentningen har uppstått något behov av att justera rättssäkerhetsgarantierna och mekanismerna till skydd för enskildas personliga integritet. Vid genomförandet av uppdraget ska beaktas vad som tidigare har uttalats om att en sådan ingående undersökning som gjordes inför permanentningen av de tidsbegränsade reglerna inte kan förväntas ske löpande (se prop. 2013/14:237, s. 168).

Utredaren ska

- undersöka hur rättssäkerhetsgarantierna och mekanismerna till skydd för den personliga integriteten vid användning av hemliga tvångsmedel för särskilt allvarlig eller på annat sätt samhällsfarlig brottslighet har tillämpats från och med den 1 januari 2012,
- analysera om regelverket är förenligt med de krav regeringsformen och Europakonventionen ställer, och
- föreslå de författningsändringar och andra åtgärder som behövs om regleringen enligt utredarens bedömning inte skulle vara förenlig med kraven.

Konsekvensbeskrivningar

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen för det allmänna och konsekvenserna i övrigt av förslagen, inklusive förslagens betydelse för möjligheten att förebygga, förhindra, upptäcka, utreda och lagföra brott. Om förslagen kan antas försämra möjligheten i dessa avseenden ska detta belysas. Om förslagen kan förväntas medföra kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras.

Samråd och redovisning av uppdraget

Utredaren ska föra dialog med och inhämta upplysningar från Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Post- och telestyrelsen, Säkerhets- och integritetsskyddsnämnden samt andra myndigheter i den utsträckning utredaren finner lämpligt. Utredaren ska också hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet och utredningsväsendet.

Uppdraget ska redovisas senast den 16 augusti 2018. Den del av uppdraget som ges med anledning av EU-domstolens förhandsavgörande om datalagring ska delredovisas senast den 9 oktober 2017.

(Justitiedepartementet)