



Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG

Till justitieutskottet

Justitieutskottet beslutade den 18 januari 2011 att ge bl.a. konstitutionsutskottet tillfälle att yttra sig över proposition 2010/11:46 och motioner i de delar som berör utskottens respektive beredningsområden.

Utskottets överväganden

Datalagringsdirektivet

Syfte och genomförande

Datalagringsdirektivet¹ beslutades 2006, och enligt artikel 15 i direktivet ska medlemsstaterna senast den 15 september 2007 sätta i kraft de bestämmelser i lagar och andra författningar som är nödvändiga för att följa direktivet. Varje medlemsstat får t.o.m. den 15 mars 2009 skjuta upp tillämpningen av direktivet i fråga om lagringen av kommunikationsuppgifter som rör Internetåtkomst, Internettelefoni och Internetbaserad e-post.

I ingressen till direktivet anges att rådet har understrukt att eftersom användningen av elektronisk kommunikation har ökat avsevärt är uppgifter om användningen av sådan kommunikation särskilt viktiga och därför ett värdefullt verktyg när det gäller att förebygga, utreda, avslöja och åtala brott, särskilt organiserad brottslighet.

Vidare noteras i ingressen att enligt artikel 8 i europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna har alla personer rätt till skydd för sitt privatliv och sin korrespondens. En offentlig myndighets inblandning i utövandet av denna rättighet får bara ske i enlighet med vad som är stadgat i lag och om det är nödvändigt i ett demokratiskt samhälle, bl.a. med hänsyn till landets nationella säkerhet eller den allmänna säkerheten, för att förebygga oordning eller brott eller för att skydda andra personers fri- och rättigheter.

Det anförs vidare att med tanke på hur viktiga trafik- och lokaliseringsuppgifter är för att kunna utreda, avslöja och åtala brott, något som enligt ingressen framkommit både genom forskning och genom medlemsstaternas praktiska erfarenheter, är det viktigt att på europeisk nivå säkerställa att uppgifter som vid tillhandahållande av kommunikationstjänster genereras eller behandlas av leverantörer av kommunikationstjänster eller kommunikationsnät lagras under en viss tid.

Lagringsskyldighetens omfattning

Lagringsskyldigheten enligt direktivet omfattar uppgifter som genereras eller behandlas av leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät vid leverans av kommunikationstjänster, i den utsträckning det sker inom statens territorium. Däremot ställs inte några krav på lagring av uppgifter om samtal som inte kopplats fram. Inga uppgifter som avslöjar kommunikationens innehåll får lagras. Uppgifterna ska lagras i minst sex månader.

¹ Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/85/EG.

Uppgifter som ska lagras

De uppgifter som ska lagras är sådana som är nödvändiga för att spåra och identifiera en kommunikationskälla. Vidare rör det sig om uppgifter som är nödvändiga för att identifiera slutmålet för en kommunikation. Lagringsskyldigheten omfattar dessutom datum, tidpunkt och varaktighet för kommunikationen, typen av kommunikation samt vilken utrustning som har använts. Exempel på kategorier av uppgifter som enligt direktivet ska lagras är bl.a. uppgifter om uppringt telefonnummer och abonnentens namn och adress vid telefoni samt användar-ID, namn och adress till den abonnent som en IP-adress har tilldelats.

Propositionen

Utgångspunkter för genomförandet

I propositionen anförts att de brottsbekämpande myndigheterna i stor utsträckning använder sig av trafikuppgifter för att avslöja, utreda och lagföra brott. I direktivet om lagring av trafikuppgifter framhålls också att trafikuppgifter är ett nödvändigt och effektivt redskap för de brottsbekämpande myndigheterna.

Vidare anförts i propositionen att möjligheterna för de brottsbekämpande myndigheterna att få tillgång till trafikuppgifter är beroende av vilka uppgifter som leverantörerna har lagrat för andra syften. Vilka uppgifter som lagras och den tid de lagras styrs enligt propositionen därför av helt andra faktorer än de brottsbekämpande myndigheternas behov. Enligt propositionen kan utvecklingen inom området elektronisk kommunikation förväntas leda till att nät- och tjänsteleverantörer i framtiden inte behöver lagra uppgifter för sin egen verksamhet i lika stor utsträckning som tidigare. Det medför att möjligheterna för de brottsbekämpande myndigheterna att få tillgång till sådana uppgifter kan komma att minska. Genom att införa en skyldighet att lagra vissa trafikuppgifter säkerställer direktivet enligt propositionen att trafikuppgifter finns tillgängliga för att användas i brottsutredningar.

Det är enligt propositionen enbart de trafikuppgifter som den enskilda leverantören genererar eller behandlar som omfattas av den lagringsskyldighet som följer av direktivet. Direktivet kan inte tolkas på så sätt att en uppgift måste genereras och behandlas även om uppgiften inte behövs för att kunna tillhandahålla det nät eller den tjänst som kan vara aktuell. Enligt propositionen innebär direktivet ingen genererings- eller behandlings-skyldighet.

I propositionen anförts vidare att samtidigt som det kan konstateras att tillgången till trafikuppgifter är av stor betydelse för att myndigheterna ska kunna utföra en effektiv brottsbekämpning medför lagringen av trafikuppgifter ett intrång i enskildas personliga integritet. Trafikuppgifter är i många fall uppgifter om enskildas personliga förhållanden och korrespondens. Den absoluta merparten av de uppgifter som enligt förslaget ska

lagras kommer naturligtvis aldrig att begäras utlämnade för brottsutredningar, utan kommer att utplånas efter lagringstidens slut utan att någon har tagit del av dem. Detta skiljer sig inte från vad som i dag gäller i fråga om de trafikuppgifter som nät- och tjänsteleverantörerna lagrar för egna syften och som är tillgängliga för de brottsbekämpande myndigheterna. Regeringen delar emellertid, i likhet med ett stort antal remissinstanser, utredningens bedömning att ett integritetsintrång sker genom att uppgifterna lagras, då detta bidrar till enskildas upplevelse av att få sin privata sfär och frihet att kommunicera inskränkt. Lagringen skulle kunna leda till att enskilda i viss utsträckning avstår från att använda elektroniska kommunikationsmedel i syfte att undvika att uppgifter registreras.

Den bestämmelse i regeringsformen som främst har betydelse för skyddet av den personliga integriteten är enligt propositionen 2 kap. 6 §, som stadgar att var och en är gentemot det allmänna skyddad mot påtvingat kroppsligt ingrepp, kroppsvisitation, husrannsakan och liknande intrång samt mot undersökning av brev och förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Enligt bestämmelsen är det förtroligheten i meddelanden av olika slag som är skyddade. Den föreslagna lagringen av trafikuppgifter omfattar inte innehållet i befordrade meddelanden, vilket enligt propositionen innebär att lagringen inte omfattas av regeringsformen i dess lydelse 2009.

Vidare anges i propositionen att grundlagsskyddet för den personliga integriteten har föreslagits bli förstärkt genom propositionen om en reformerad grundlag (2009/10:80). Där föreslogs bl.a. att en ny bestämmelse införs som anger 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 (2 kap. 6 § andra stycket regeringsformen). Inskränkningar genom lag föreslogs dock vara tillåtna enligt de förutsättningar som anges i dåvarande 2 kap. 12 § regeringsformen. Det innebär bl.a. att en begränsning av den utvidgade rätten till skydd för den personliga integriteten kommer att vara tillåten endast under förutsättning att den tillgodoser ett ändamål som är godtagbart i ett demokratiskt samhälle. Det innebär också att en begränsning inte får gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den eller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen. Riksdagen har genom beslut den 2 juni och 24 november 2010 antagit grundlagsändringarna, som har trätt i kraft den 1 januari 2011.

Det anförs också i propositionen att grundlagsskyddet för den personliga integriteten kompletteras till viss del av det skydd som följer av artikel 8 i den europeiska konventionen av den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). Konventionen gäller sedan 1995 som svensk lag. Enligt artikel 8 har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Rätten till respekt för privat- och familjelivet får endast

inskränkas med stöd av lag i den utsträckning det i ett demokratiskt samhälle är nödvändigt med hänsyn till vissa närmare angivna ändamål, bl.a. bekämpning av brott. Av Europadomstolens praxis följer enligt propositionen att det krävs att det finns ett angeläget samhälleligt behov ("pressing social need") för att en inskränkning ska vara tillåten. Inskränkningen måste vidare framstå som proportionell i förhållande till det syfte som den avser att tillgodose. Enligt 2 kap. 19 § regeringsformen får en lag eller annan föreskrift inte meddelas i strid med Sveriges åtaganden på grund av den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.

I propositionen anges att ett stort antal remissinstanser framhållit vikten av integritetsskyddet. Någon remissinstans har också, med hänvisning till integritetsaspekter, avstyrkt att direktivet genomförs. Vissa anser att utredningen har hittat en bra balans mellan brottsbekämpningsintresset och integritetsskyddet, medan andra anser att brottsbekämpningsintresset fått för stort utrymme på integritetsskyddets bekostnad. I propositionen påpekar regeringen att det redan i direktivet, som ett antal remissinstanser också anfört, görs en avvägning mellan de intressen som nu är aktuella. Direktivet innehåller inte bara en uppräkningslista av vilka trafikuppgifter som ska lagras utan också flera artiklar som ska garantera en rimlig proportion mellan intresset av att allvarliga brott avslöjas, utreds och lagförs respektive skyddet för enskildas integritet. Det gäller t.ex. den längsta acceptabla lagringstiden, att uppgifterna ska utplånas vid slutet av den tiden och att uppgifterna ska skyddas mot olika åtgärder som är skadliga från integritetsskyddssynpunkt.

Sverige är som medlemsstat i Europeiska unionen skyldigt att genomföra direktivet. Sveriges skyldighet att genomföra direktivet hindrar emellertid enligt propositionen inte att integritetsfrågorna vid genomförandet kan beaktas på olika sätt, vilket direktivet också utgår ifrån. En utgångspunkt bör då vara att man vid regleringen av lagringen skapar ett transparent system som gör det möjligt för medborgarna att förutse vilka uppgifter som kommer att lagras och hur de typiskt sett används i brottsbekämpningen. I detta ligger att lagring ska medges endast om det följer av direktivet eller kan motiveras med stöd av artikel 15.1 i direktiv 2002/58/EG om integritet och elektronisk kommunikation. Det anges i propositionen att regeringen, i syfte att öka rättssäkerheten och skyddet för den personliga integriteten, väljer att, i större utsträckning än Trafikuppgiftsutredningen, föreslå att den nya regleringen sker genom ändring i lag. Härigenom ökar enligt propositionen riksdagens kontroll. Integritetsfrågorna ska vidare beaktas vid bedömningen av var lagringen ska ske, av vem uppgifterna ska lagras, hur länge de ska få lagras innan de ska utplånas samt vilka andra villkor som ska gälla för lagringen. För att minimera risken för otillbörliga integritetsintrång mot den enskilde, och för att skapa tillit till systemet, måste enligt propositionen vidare såväl det tekniska som det organisatoriska skyddet för de lagrade uppgifterna vara tillräckligt. De

rättsliga regler som blir tillämpliga om trafikuppgifter ändå skulle komma att spridas i strid mot lagen måste också enligt propositionen verka tillräckligt avhållande och vara reparativa. En säker lagring fordrar vidare en aktiv tillsynsverksamhet.

Sammanfattningsvis anger regeringen i propositionen att såväl en effektiv brottbekämpning som skyddet för enskildas personliga integritet är frågor av stor betydelse. Vid genomförande av direktivet ska därför såväl brottbekämpningens behov av effektiva verktyg som behovet av att skydda enskildas integritet beaktas. Utformningen av lagringskravet ska skapa en balans mellan dessa båda intressen.

Lagring av uppgifter utöver direktivet

Utöver de uppgifter som direktivet kräver föreslås att lagringsskyldigheten ska gälla även vid misslyckad uppringning och för uppgifter om lokalisering av mobil kommunikationsutrustning. I propositionen anför regeringen att en lagringsskyldighet avseende misslyckad uppringning i den mån dessa uppgifter för närvarande inte lagras eller loggas innebär en längre gående skyldighet än vad som följer av direktivet om lagring av trafikuppgifter. En sådan skyldighet kan dock enligt propositionen införas med stöd av artikel 15.1 i direktivet om integritet och elektronisk kommunikation, bl.a. för brottbekämpande syfte. Regeringen instämmer i de brottbekämpande myndigheternas bedömning att det finns ett lika stort behov av uppgifter om misslyckad uppringning som av uppgifter om de samtal som har lyckats.

Beträffande Internetåtkomst och anslutningsform finns det enligt propositionen ett annat lagringskrav i direktivet som innebär att lokaliseringsinformation ska lagras. Av direktivet följer att lokaliseringsinformation för mobil kommunikationsutrustning ska lagras för kommunikationens början. Uppgifter som är nödvändiga för att identifiera den kommunikationsutrustning som använts innebär, när det gäller Internetåtkomst och anslutningsform, att DSL (Digital Subscriber Line) eller en annan slutpunkt för kommunikationsutrustningen ska lagras. Sådana slutpunkter omfattar bl.a. lokaliseringsinformation. Lokaliseringsinformation vid Internetåtkomst och anslutningsform som sker via mobil kommunikationsutrustning ska alltså lagras redan på den grunden. De brottbekämpande myndigheterna har anfört att de också har behov av att få lokaliseringsinformation avseende kommunikationens slut. Direktivet om lagring av trafikuppgifter medför ingen skyldighet att lagra dessa uppgifter. Vidare anför det i propositionen att utifrån samma övervägande som beträffande misslyckade uppringningar kan en skyldighet att lagra sådana uppgifter införas med stöd av artikel 15.1 i direktivet om integritet och elektronisk kommunikation, om det finns ett behov av uppgifterna för brottbekämpningsändamål och lagringsskyldigheten bedöms vara en nödvändig åtgärd.

Det konstateras i propositionen att de brottsbekämpande myndigheterna har behov av vissa uppgifter som inte omfattas av den lagringsskyldighet som direktivet föreskriver. Detta behov ska emellertid enligt propositionen ställas mot andra intressen, dels skyddet för enskildas integritet, dels kostnads- och konkurrensaspekter. Flera remissinstanser har också invänt mot införande av en lagringsskyldighet som går utöver direktivet, bl.a. mot bakgrund av dessa sistnämnda intressen. *Post- och telestyrelsen*, liksom *.SE*, har anfört att den omständigheten att direktivet i sig är en mycket kontroversiell lagstiftning, som föregicks av en omfattande debatt över hela Europa, talar för att genomförandet av direktivet i så stor utsträckning som möjligt bör hålla sig inom dess ramar. *Sveriges advokatsamfund*, *Telia Sonera AB* och *KLYS* har framfört liknande synpunkter.

Vidare anför regeringen i propositionen att som bl.a. *JO* konstaterat är den avvägning som ska göras mellan brottsbekämpning och integritetsskydd i allt väsentligt given i direktivet. *JO* har vidare anfört att det är oundvikligt att lagstiftningen anpassas till de förändrade beteendemönster som är resultatet av att människor utnyttjar nya tekniker som förenklar och effektiviserar deras liv och att användarna i princip är medvetna om att data kring sådana aktiviteter skapas, avsätts och ibland registreras, men att den omständigheten i princip inte avhåller dem från att använda tekniken. Regeringen instämmer i *JO*:s konstaterande att människors allmänna obehag inför att information om dem lagras inte bör underskattas, men att det vore orealistiskt att utesluta detta växande informationsfält från de brottsbekämpande myndigheternas insyn. Det finns enligt propositionen goda skäl att för brottsbekämpande ändamål lagra uppgifter om både misslyckad uppringning och lokaliseringssuppgifter vid kommunikationens slut för mobil kommunikationsutrustning, vilket också bekräftas i remissyttranden från de brottsbekämpande myndigheterna. Sedan skälen för lagring väl bedömts motivera ett intrång i integritetsskyddet bör brottsbekämpningsintresset, som *JO* konstaterat, väga relativt tungt. Regeringen anser alltså, även med beaktande av integritetsskyddet, att det är motiverat att lagringsskyldigheten omfattar misslyckade uppringningar och lokaliseringssuppgifter vid kommunikationens slut för mobil kommunikationsutrustning.

Vem ska ansvara för lagringsskyldigheten?

En ganska självklar utgångspunkt kan enligt propositionen tyckas vara att leverantörerna lagrar de uppgifter som genereras eller behandlas i de tjänster som leverantören tillhandahåller. En annan möjlig modell för lagring av trafikuppgifter skulle kunna vara att leverantörerna skickar de uppgifter som ska lagras till ett centralt lager. Detta skulle innebära att antingen staten eller en utsedd aktör skulle lagra samtliga trafikuppgifter som alla leverantörer genererar eller behandlar.

Regeringen anser att en central lagring skulle vara problematisk, framför allt ur integritetssynpunkt. Den modell som innebär att trafikuppgifterna lagras där de genereras eller behandlas, dvs. hos leverantörerna,

framstår enligt regeringen som ett bättre alternativ. Denna lösning innebär enligt propositionen stora fördelar ur främst integritetssynpunkt, då trafikuppgifterna oftast inte kommer att vara omedelbart läsbara eftersom den enskilda leverantören i många fall bara kommer att ha information som måste ställas samman med trafikuppgifter som lagrats hos någon annan leverantör för att en enskild persons kommunikation ska kunna utläsas.

Skyddet för de lagrade uppgifterna

Enligt propositionen är en grundförutsättning för att syftet med lagringen av trafikuppgifter ska uppnås att uppgifterna lagras med hjälp av en teknik som håller hög kvalitet och säkerhet. Som utgångspunkt för fastställande av den skyddsnivå som bör gälla för trafikuppgifter är det lämpligt att ta det skydd för personuppgifter som gäller enligt personuppgiftslagen. Med denna utgångspunkt bör enligt propositionen kravet på säkerhet för trafikuppgifter formuleras på så sätt att leverantörerna ska vidta de särskilda tekniska och organisatoriska åtgärder som krävs för att säkerställa att behandlade uppgifter skyddas.

Post- och telestyrelsen bör enligt propositionen utöva tillsyn över leverantörernas lagring av trafikuppgifter. Post- och telestyrelsens tillsyn kommer att omfatta exempelvis att leverantörerna lagrar rätt uppgifter, att uppgifterna utplånas efter den föreskrivna tiden samt att leverantörerna vidtar de särskilda tekniska och organisatoriska åtgärder som föreskrivits till skydd för de lagrade uppgifterna.

Överföring av personuppgifter till ett annat land

Enligt propositionen bör trafikuppgifter kunna lagras i ett annat land under förutsättning att den lagringsskyldige lever upp till de krav och skyldigheter som följer av personuppgiftslagen och de föreslagna bestämmelserna om lagring av trafikuppgifter.

I propositionen anför regeringen att det i direktivet om lagring av trafikuppgifter inte finns några uttryckliga regler som stadgar var lagringen av trafikuppgifter får eller inte får ske. Om lagringen sker inom EU eller i ett land som är anslutet till EES tillämpas ett gemensamt regelverk som innebär ett starkt skydd för personuppgifterna. Möjligheterna att lagra trafikuppgifter som också är personuppgifter i ett land utanför denna krets begränsas av bestämmelser i personuppgiftslagen. Även om lagringen förläggs utomlands gäller dock leverantörens alla skyldigheter enligt de bestämmelser som anger hur lagringsskyldigheten ska fullgöras, t.ex. de krav som rör säkerheten för de lagrade trafikuppgifterna. Detta måste särskilt beaktas av leverantörerna om de överväger att lagra trafikuppgifter utomlands. Leverantörernas skyldigheter inkluderar också bestämmelserna om tystnadsplikt. Tystnadsplikten för de uppgifter som ska lagras med stöd av de bestämmelser som genomför direktivet om lagring av trafikuppgifter ska enligt förslaget endast kunna brytas för att uppgifterna under vissa förut-

sättningar ska kunna lämnas ut till enåklagarmyndighet, polismyndighet eller annan myndighet. Med dessa angivna myndigheter åsyftas endast svenska – inte utländska – brottsbekämpande myndigheter.

Det straff- och skadeståndsrättsliga skyddet

Av artikel 13 i datalagringsdirektivet följer att medlemsstaterna ska säkerställa att rättslig prövning, ansvar och sanktioner finns till skydd för uppgifterna.

I propositionen anför regeringen att en leverantör som olovligen bereder sig tillgång till trafikuppgifter eller behandlar dem för ett otillåtet ändamål kan göra sig skyldig till dataintrång enligt 4 kap. 9 c § brottsbalken. Straffskalan är böter eller fängelse i högst två år. Bestämmelsen kan också bli tillämplig om någon utomstående olovligen bereder sig tillgång till de lagrade trafikuppgifterna. Anställda hos en leverantör kan göra sig skyldiga till brott mot tystnadsplikten enligt 20 kap. 3 § brottsbalken. Av personuppgiftslagen följer att det är straffbart att uppsåtligen eller av grov oaktsamhet behandla s.k. känsliga personuppgifter i strid med lagen eller att föra över personuppgifter till ett tredjeland som inte har en adekvat skyddsnivå. Skadeståndsrättslig reglering till skydd för enskilda som lidit skada till följd av felaktig behandling av trafikuppgifter finns i de fall trafikuppgifterna utgör personuppgifter i personuppgiftslagen.

Regeringen gör sammanfattningsvis den bedömningen att det inte finns skäl att förändra befintliga straff- och skadeståndsrättsliga bestämmelser.

Motionerna

I motion 2010/11:Ju5 av Maria Ferm m.fl. (MP) yrkas att riksdagen avslår propositionen. Vidare yrkas bl.a. ett tillkännagivande om att regeringen på EU-nivå bör förhandla om att datalagringsdirektivet ska avskaffas. Motionärerna anför att datalagringsdirektivet är en av flera integritetsinskränkande antiterroristlagar sedan den 11 september 2001. Med den föreslagna lagstiftningen har det skett ett paradigmskifte i svensk rätt när tvångsmedel kan användas mot personer som inte är misstänkta för brott. Alltsedan datalagringsdirektivets tillblivelse har Miljöpartiet kritiserat det, därför att ingreppet inte står i proportion till nyttan. Den information som samlas in kan komma att användas i andra syften än de tänkta. Det finns inga register med integritetskänsliga data som det inte har läckt ut uppgifter från. Motionärerna förstår att Sverige är tvunget att genomföra direktivet men anser att regeringen bör agera för att riva upp eller omförhandla det.

I motion 2010/11:Ju427 av Maria Ferm m.fl. (MP) yrkas bl.a. tillkännagivanden om att regeringen inom EU bör förhandla om att datalagringsdirektivet ska avskaffas och att Sverige ska ställa sig positivt till att EU-domstolen prövar om direktivet strider mot de mänskliga rättigheterna.

I motion 2010/11:Ju6 av Jens Holm m.fl. (V) yrkas att riksdagen avslår propositionen. Motionärerna anför att datalagringen är en del av ett paradigmskifte som äger rum när det gäller statens övervakning av medborgarna. Från att fokus har legat på övervakning av enskilda brottsmisstänkta sker övervakning nu på allt lösare grund. Vidare anför motionärerna att direktivet och regeringens förslag berör och inskränker vissa av de fri- och rättigheter som anges i Europakonventionen och regeringsformen. Det måste beläggas att det finns ett behov av lagändringen och att åtgärderna är effektiva och står i proportion till inskränkningarna. I propositionen finns ingen egentlig analys av hur lagförslagen förhåller sig till bestämmelserna om fri- och rättigheter i regeringsformen. Motionärerna anför att de kommer att använda den möjlighet som finns i 2 kap. 22 § regeringsformen att yrka att ett lagförslag ska vila i ett år innan det kommer upp till prövning.

I motion 2010/11:Ju7 av Kent Ekeröth och Erik Almqvist (båda SD) yrkas bl.a. tillkännagivande om att trafikuppgifter som ska lagras inte ska få lagras utanför Sveriges gränser. Motionärerna anför att säkerheten kan ifrågasättas om trafikuppgifter lagras i ett annat land. En svensk medborgare kan hamna i en situation där han eller hon måste driva en process mot en myndighet eller ett företag i ett annat land. Motionärerna anser att regeringens motivering att det i samtliga medlemsländer finns EU-gemensamma rättsregler inte är tillfredsställande nog med tanke på att rättsäkerheten och korruptionen skiljer sig mellan olika EU-länder.

I motion 2010/11:Ju303 av Betty Malmberg (M) yrkas ett tillkännagivande om att Sverige bör verka aktivt för att stärka den personliga integriteten inom EU.

Gällande rätt

Skyddet för enskildas integritet

Av 2 kap. 6 § första stycket regeringsformen följer att var och en är gentemot det allmänna skyddad mot bl.a. kroppsvisitation, husrannsakan och liknande intrång samt mot undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. I andra stycket stadgas att utöver vad som föreskrivs i första stycket är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

I förarbetena (prop. 2009/10:80 s. 250) anges att bestämmelsen i 2 kap. 6 § andra stycket innebär att enskilda, vid sidan av vad som redan följer av första stycket, är skyddade mot åtgärder från det allmänna sida som innefattar betydande intrång i den personliga integriteten, om intrånget sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Bestämmelsen träffar inte åtgärder som

en enskild vidtar i förhållande till en annan enskild. Avgörande för om en åtgärd ska anses innebära övervakning eller kartläggning är inte dess huvudsakliga syfte utan vilken effekt åtgärden har. Vad som avses med övervakning respektive kartläggning får bedömas med utgångspunkt från vad som enligt normalt språkbruk läggs i dessa begrepp. Uttrycket ”enskilds personliga förhållanden” avses här ha samma innebörd som i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400). Vid bedömning av vilka åtgärder som kan anses utgöra ett ”betydande intrång” ska både åtgärdens omfattning och arten av det intrång åtgärden innebär beaktas. Även åtgärdens ändamål och andra omständigheter kan ha betydelse vid bedömningen. Bestämmelsen 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.

Integritetsskyddskommittén anförde i sitt betänkande (SOU 2008:3 s. 268 f.) att hemlig teleövervakning omfattar två olika moment av intrång i den enskildes privata sfär som därtill sker utan att den enskilde får vetskap om åtgärden: dels lagring av teletrafikuppgifter, dels utlämnande av dessa uppgifter till en brottsutredande myndighet. Övervakningen har i ett integritetsskyddsperspektiv inte ansetts vara lika känslig som hemlig teleavlyssning och hemlig kameraövervakning men utgör likafullt ett ingripande intrång i den enskildes rätt till skydd för sitt privatliv. Hemlig teleövervakning är tillåten för det allmänna endast inom ramen för reglerna om straffprocessuella tvångsmedel i 27 kap. rättegångsbalken. Åtgärder från det allmännas sida i form av lagring av teletrafikuppgifter och utlämnande av dessa för brottsutredande ändamål har vidare en nära anknytning till de intrång i rätten till skydd för en enskilds förtroliga kommunikation som redan omfattas av grundlagsskyddet i 2 kap. regeringsformen. Det fick enligt kommittén därför anses vara motiverat att också denna typ av intrång skulle komma att omfattas av det nya grundlagsskyddet.

Vidare anför kommittén att ett grundlagsskydd av det föreslagna slaget även kommer att omfatta den skyldighet att för det allmännas räkning lagra teletrafikuppgifter för brottsbekämpande ändamål som kommer att införas i Sverige på grund av direktivet (2006/24/EG) om lagring av sådana uppgifter. Det stora flertalet operatörer kommer att vara skyldiga att lagra uppgifter av angivet slag om samtliga abonnenter, såsom det föreslagits, under ett år (SOU 2007:76). Det är alltså frågan om mycket omfattande informationssamlingar som delvis avser ytterst integritetskänsliga uppgifter, nämligen uppgifter om med vem och när man kommunicerar på elektronisk väg via t.ex. telefon, e-post och sms, och vidare uppgifter om uppkoppling på Internet.

Begränsning av fri- och rättigheter

Det anges i 2 kap. 19 § regeringsformen att lag eller annan föreskrift inte får meddelas i strid med Sveriges åtaganden på grund av den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.

I 2 kap. 20 § regeringsformen stadgas att fri- och rättigheterna enligt bl.a. 2 kap. 6 § får begränsas genom lag. En begränsning får enligt 21 § göras endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningen får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen som en av folkstyrelsens grundvalar. Begränsningen får inte göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning.

Enligt 2 kap. 22 § första stycket regeringsformen ska ett förslag till lag som rör begränsning av vissa fri- och rättigheter, om det inte avslås av riksdagen, på yrkande av lägst tio av dess ledamöter vila i minst tolv månader. Riksdagen får dock anta förslaget direkt, om minst fem sjättedelar av de röstande enas om beslutet.

De fri- och rättigheter som omfattas av detta särskilda lagstiftningsförfarande är yttrandefriheten, informationsfriheten, mötesfriheten, demonstrationsfriheten, föreningsfriheten, skyddet för den kroppsliga integriteten och för förtroligt meddelande, skyddet mot intrång som innebär övervakning och kartläggning av den enskildes personliga förhållanden, rörelsefriheten samt rätten till offentlig domstolsförhandling.

Enligt 2 kap. 22 § tredje stycket prövar konstitutionsutskottet för riksdagens del om första stycket är tillämpligt i fråga om ett visst lagförslag.

Underställning av föreskrifter

I 8 kap. 6 § regeringsformen anges att föreskrifter som regeringen meddelat med stöd av ett bemyndigande enligt regeringsformen ska underställas riksdagen för prövning om riksdagen bestämmer det.

Europakonventionen

I artikel 8 i europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) anges att

1. var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens
2. offentlig myndighet inte får inskränka åtnjutande av denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välbefinnande eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.

Direktivet om integritet och elektronisk kommunikation

Genom direktivet om integritet och elektronisk kommunikation ska bl.a. medlemsstaternas bestämmelser för att säkerställa ett likvärdigt skydd av de grundläggande fri- och rättigheterna, i synnerhet rätten till integritet, när det gäller behandling av personuppgifter inom sektorn för elektronisk kommunikation harmoniseras.

I artikel 5 anges att medlemsstaterna genom nationell lagstiftning ska säkerställa konfidentialitet vid kommunikation och därmed förbundna trafikuppgifter via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster. Medlemsstaterna ska förbjuda bl.a. avlyssning och lagring som innebär att kommunikationen och de därmed förbundna trafikuppgifterna kan fångas upp eller övervakas av andra personer än användarna, utom när de har laglig rätt att göra detta i enlighet med artikel 15.1.

Enligt artikel 15.1 får medlemsstaterna genom lagstiftning begränsa vissa angivna rättigheter som följer av direktivet när en sådan begränsning i ett demokratiskt samhälle är nödvändig, lämplig och proportionell för att bl.a. förebygga, undersöka, avslöja och åtala för brott.

Genom datalagringsdirektivet (artikel 11) gäller att artikel 15.1 inte ska tillämpas på uppgifter som specifikt ska lagras enligt datalagringsdirektivet.

Trafikuppgiftsutredningens betänkande

Allmänt om integritetsaspekter

I Trafikuppgiftsutredningens betänkande Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76) framhålls bl.a. att den lagring av trafikuppgifter som ska genomföras till följd av direktivet innebär att mycket stora informationsmängder som rör enskildas kommunikation kommer att lagras under en viss tid. Enligt utredningen kan man utgå från att endast en ytterst begränsad del av de lagrade trafikuppgifterna kommer att begäras utlämnade för att användas vid bekämpningen av allvarlig brottslighet. Merparten av trafikuppgifterna kommer således att vara lagrade utan att de används för de brottsbekämpande syftena. Trafikuppgifter är i många fall uppgifter om enskildas personliga förhållanden och korrespondens, och det är mot bakgrund av uppgifternas integritetskänsliga karaktär som bestämmelserna i rättegångsbalken om hemlig teleövervakning och i lagen om elektronisk kommunikation om tystnadsplikt och undantag från tystnadsplikten har utformats. Att få ut trafikuppgifter för utredning av brott har ansetts vara särskilt känsligt från integritetssynpunkt och förutsättningarna för utlämnande är noggrant reglerade. Enligt kommitténs mening är dock inte frågan om integritetsskyddet vid lagring av trafikuppgifter begränsad till de situationer där trafikuppgifter lämnas ut till de brottsbekämpande myndigheterna. En utgångspunkt för kommitténs resonemang är att en generell lagring av trafikuppgifter i den omfattning som direktivet förutsätter påverkar både enskildas upplevelse av att få sin privata sfär inskränkt och

integritetsskyddet för medborgarna i allmänhet. Intrånget i integriteten sker enligt kommittén redan genom att det allmänna säkrar tillgången till trafikuppgifterna genom lagringen. Redan existensen av ett regelsystem som innebär att uppgifter om människors kommunikation med fast och mobil telefoni eller Internet ska lagras har således en påverkan på enskildas integritetsskydd och upplevelse av integritetsintrång. Det innebär med nödvändighet att den frihet att kommunicera som bör finnas mellan människor som använder kommunikationstjänster upplevs som inskränkt. Lagringen utgör i sig ett intrång i såväl privatliv som korrespondens och kan komma i konflikt såväl med den rätt till skydd för privatlivet som var och en har enligt artikel 8 i Europakonventionen som med det grundlagsskydd som denna rätt har enligt 2 kap. 6 § regeringsformen.

Vidare anför utredningen att lagringen av trafikuppgifter medför ett intrång i den personliga integriteten. En utgångspunkt för utredningens överväganden är att lagringen av trafikuppgifter ska regleras så att systemet blir transparent och gör det möjligt för medborgarna att förutse vilka uppgifter som ska lagras och hur de typiskt sett används i brottsbekämpningen. Detta innebär att regleringen av vilka trafikuppgifter som ska lagras ska vara klar och tydlig och medge lagring endast om det följer av direktivet eller kan motiveras med stöd av artikel 15.1 i direktivet om integritet och elektronisk kommunikation.

Artikel 29-gruppen

I utredningens betänkande anføres att det av artikel 29 i dataskyddsdirektivet framgår att det ska inrättas en arbetsgrupp på gemenskapsnivå för skydd av enskilda personer i samband med behandling av personuppgifter. Vidare anføres att den s.k. artikel 29-gruppen har övervägt integritetsfrågor i anledning av de nationella genomförandena av direktivet om lagring av trafikuppgifter. Gruppen har anført att det är av yttersta vikt att direktivet genomförs på ett sådant sätt att effekterna på privatlivet begränsas och att genomförandet åtföljs av åtgärder som skyddar den personliga integriteten. Gruppen har också understrukit behovet av en harmoniserad tolkning av direktivets bestämmelser och vikten av harmonisering av de nationella genomförandena av direktivet för att säkerställa samma skyddsnivå för alla EU-medborgare. Därför vill gruppen se ett enhetligt genomförande av direktivet i hela EU. För att detta ska kunna ske och för att uppfylla kraven i artikel 8 i Europakonventionen ska medlemsstaterna genomföra lämpliga och specifika skyddsåtgärder. Gruppen föreslår att minst följande skyddsåtgärder ska beaktas:

- Uppgifterna bör endast lagras i särskilda syften, och termen ”allvarliga brott” bör tydligt definieras och avgränsas. All ytterligare behandling bör uteslutas eller strikt begränsas genom särskilda skyddsåtgärder.

- Uppgifterna ska bara vara tillgängliga för särskilt utsedda myndigheter som ansvarar för brottsbekämpning, och de ska överlämnas när det krävs för utredning, avslöjande och lagföring av de brott som anges i direktivet. En förteckning över vilka de särskilt utsedda myndigheterna är bör offentliggöras.
- De uppgifter som ska lagras bör begränsas till ett minimum, och alla ändringar av förteckningen över dessa uppgifter ska omfattas av ett strängt nödvändighetstest.
- Utredning, avslöjande och lagföring av de brott som anges i direktivet får inte medföra någon storskalig datautvinning på basis av lagrade uppgifter om rese- och kommunikationsmönster för personer som de brottsutredande myndigheterna inte misstänker.
- Tillgång till uppgifter bör i princip beviljas av de rättsliga myndigheterna efter en bedömning från fall till fall, utom i de länder där sådan tillgång regleras i lag. I tillämpliga fall bör det i handlingarna om beviljande av tillgång anges vilka typer av uppgifter som behövs i det aktuella fallet.
- Tillhandahållare av allmänna elektroniska kommunikationstjänster eller kommunikationsnätverk bör inte ha rätt att bearbeta data som enbart lagras med hänsyn till den allmänna ordningen, enligt direktivet om lagring av uppgifter, för andra ändamål, särskilt inte för egna syften.
- Särskilt systemen för lagring av data med hänsyn till den allmänna ordningen ska hållas logiskt åtskilda från de system som används för affärsverksamheten.
- Miniminormer ska utformas om de tekniska och organisatoriska säkerhetsåtgärder som tillhandahållarna ska vidta, och de ska hänvisa närmare till de allmänna kraven i direktivet om lagring av uppgifter.

Europeiska datatillsynsmannen

I utredningens betänkande anges också att den europeiska datatillsynsmannen avgav ett yttrande till kommissionen (2005/C 298/01) med anledning av förslaget till direktiv om lagring av trafikuppgifter. Datatillsynsmannen hänförde sig till vikten av att medlemsstaternas brottsbekämpande organ förfogar över alla nödvändiga rättsinstrument, särskilt i kampen mot terrorism och andra allvarliga brott, och menade att en adekvat tillgång till vissa trafikuppgifter kan vara ett avgörande redskap för de brottsbekämpande organen och bidra till människors fysiska säkerhet. Datatillsynsmannen menade också att om man betraktar förslaget endast ur ett uppgiftsskyddsperspektiv bör trafikuppgifter över huvud taget inte bevaras i brottsbekämpande syfte. Därför är det enligt datatillsynsmannen viktigt att direktivet inte leder till att människor berövas sin grundläggande rätt till integritetsskydd. Datatillsynsmannen menade att lagring av trafikuppgifter endast kan motiveras enligt gemenskapsrätten om proportionalitetsprincipen respekteras och lämpliga skyddsåtgärder vidtas. För att förslaget ska vara lämpligt och effektivt krävs enligt datatillsynsmannen att det finns

effektiva sökmotorer så att myndigheterna har riktad och snabb tillgång till de uppgifter som behövs i ett specifikt fall. Av förslaget ska därför enligt datatillsynsmannen framgå att leverantörerna är skyldiga att installera den nödvändiga tekniska strukturen, inklusive sökmotorer. Därutöver bör förslaget för att vara proportionerligt begränsa lagringstiderna och antalet uppgifter som ska lagras, och det måste återspegla styrkta behov från brottsbekämpningens sida. Det måste också säkerställas att det är omöjligt att komma åt uppgifternas innehåll. Slutligen bör förslaget innehålla lämpliga skyddsåtgärder. Som lämpliga skyddsåtgärder angav datatillsynsmannen åtgärder som säkerställer att tillgången till och vidareanvändningen av uppgifterna begränsas enbart till särskilda omständigheter och för ett begränsat antal särskilda ändamål. Vidare ska databaserna skyddas på lämpligt sätt för att motverka ”dumpning” eller utnyttjande av uppgifterna. Det måste också garanteras att uppgifterna utplånas effektivt när bevarandetiden löpt ut, och det ska införas krav på att leverantörerna utplånar uppgifterna automatiskt och minst en gång om dagen.

Lagring av trafikuppgifter som inte omfattas av datalagringsdirektivet

På några punkter har utredningen föreslagit en lagringsskyldighet utöver direktivet om lagring av trafikuppgifter. Det rör lokaliseringsinformation för kommunikationens slut vid mobil telefoni och uppgifter om misslyckad uppringning även om uppgifterna inte lagras eller loggas av leverantören.

En lagringsskyldighet utöver direktivet om lagring av trafikuppgifter kan införas endast om det är motiverat utifrån de överväganden som ska göras enligt artikel 15.1 i direktivet om integritet och elektronisk kommunikation.

Utredningen har funnit det motiverat att föreslå en skyldighet att lagra sådana uppgifter.

Ytterligare upplysningar

Den 24 januari 2010 publicerade Post- och telestyrelsen en rapport med en internationell utblick över trafikdatalagring (Lagring av uppgifter för brottsbekämpning enligt EU-direktiv 2006/24/EG – Internationell utblick m.m., PTS-ER-2011:1).

Som ett led i beredningen av detta ärende har konstitutionsutskottet vid ett sammanträde inhämtat upplysningar från företrädare för Post- och telestyrelsen och därefter från företrädare för Justitiedepartementet.

Utskottets ställningstagande

Inledningsvis vill utskottet framhålla att enligt artikel 15.1 i datalagringsdirektivet ska medlemsstaterna sätta i kraft de bestämmelser i lagar och andra författningar som är nödvändiga för att följa direktivet senast den 15 september 2007. Som medlem i EU är Sverige skyldigt att genomföra

direktivet. EU-domstolen fann den 4 februari 2010 (C-185/09) att Sverige underlåtit att uppfylla sina skyldigheter enligt direktivet. Kommissionen har med anledning av domen inlett nästa steg i överträdelseförfarandet, vilket kan leda till att Sverige åläggs en ekonomisk sanktion. Regeringen har i propositionen anfört att Sveriges skyldighet att genomföra direktivet inte hindrar att integritetsfrågorna kan beaktas på olika sätt. Utskottet delar denna uppfattning. En bedömning av integritetsfrågorna mot bakgrund av de nationella svenska grundlagsreglerna ter sig därvid naturlig. Såvitt gäller de delar av lagförslagen som går längre än vad direktivet kräver ska en sådan bedömning ske.

Enligt 2 kap. 6 § andra stycket regeringsformen är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Utskottet noterar att Integritetsskyddskommittén i sitt slutbetänkande ansåg att bestämmelser om lagrings-skyldighet med anledning av direktivet kunde komma att omfattas av de nya bestämmelser i regeringsformen om skydd för den personliga integriteten som kommittén föreslog.

Trafikuppgifter är i många fall uppgifter om enskildas personliga förhållanden och korrespondens. Det är fråga om mycket omfattande informationssamlingar som delvis avser integritetskänsliga uppgifter, nämligen om vem som kommunicerade med vem, när det skedde, var de som kommunicerade befann sig och vilken typ av kommunikation som användes. Enligt utskottets mening sker ett integritetsintrång redan genom att uppgifterna lagras, även om merparten av de uppgifter som nu föreslås ska lagras troligen aldrig kommer att begäras ut för brottsutredningar. I likhet med regeringen anser därför utskottet att lagringen av trafikuppgifter medför ett intrång i enskildas personliga integritet. Intrånget måste, mot bakgrund av den mängd trafikuppgifter om en enskild som kan komma att lagras, anses vara betydande. Den lagring av trafikuppgifter som föreslås i propositionen omfattas därför enligt utskottets mening av regeringsformens skydd i 2 kap. 6 § andra stycket för den personliga integriteten.

Enligt 2 kap. 20 § regeringsformen får fri- och rättigheterna enligt bl.a. 2 kap. 6 § begränsas genom lag. En begränsning får dock enligt 2 kap. 21 § regeringsformen göras endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningen får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen som en av folkstyrelsens grundvalar, dvs. det ska göras en proportionalitetsprövning. Begränsningen får inte göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning.

Grundlagsskyddet för den personliga integriteten kompletteras av det skydd som följer av artikel 8 i europiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna. Enligt artikel 8 har var och en rätt till respekt för privat- och familjeliv, hem och korre-

spondens. Konventionen gäller sedan 1995 som svensk lag. Denna rättighet får inskränkas endast med stöd av lag i den utsträckning det i ett demokratiskt samhälle nödvändigt med hänsyn till vissa närmare angivna ändamål, bl.a. bekämpning av brott. Enligt 2 kap. 19 § regeringsformen får lag eller annan föreskrift inte meddelas i strid med Sveriges åtaganden på grund av europakonventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.

Utskottet noterar att Lagrådet i sitt yttrande om lagförslagen ansåg att förslagen i allt väsentligt överensstämde med vad som föreskrivits i datalagringsdirektivet och att det i överensstämmande delar fick anses utgöra ett med europeiska ögon försvarligt ingrepp i den personliga integriteten för att få till stånd nödvändiga brottsbekämpande åtgärder.

Regeringens förslag går på två punkter längre än vad datalagringsdirektivet kräver, nämligen så att uppgifter ska lagras om misslyckade upprinningar liksom uppgifter om var en kommunikation med mobil kommunikationsutrustning avslutas. Regeringens förslag i den delen stöder sig på artikel 15.1 i direktivet om integritet och elektronisk kommunikation. I propositionen anges att de brottsbekämpande myndigheterna har anfört att de har behov av trafikuppgifter som gäller misslyckade upprinningar samt av lokaliseringsinformation avseende kommunikationens slut. Utskottet noterar att Lagrådet ansåg att sett i sitt sammanhang fick dessa tilläggsuppgifter anses vara marginella ingrepp i den personliga integriteten som väl motiverades av deras betydelse för att avslöja, utreda och lagföra brott.

En annan fråga som är av betydelse för bedömningen av om lagförslagen innebär en godtagbar begränsning av skyddet för den personliga integriteten, är vilket skydd som finns för de lagrade uppgifterna.

Direktivet innehåller flera bestämmelser som syftar till en säker lagring. I svensk lagstiftning finns regler om teknisk säkerhet i lagen om elektronisk kommunikation. I den lagen finns i dag ett grundskydd för behandlingen av trafikuppgifter. I lagen anges bl.a. (6 kap. 3 §) att den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst ska vidta lämpliga åtgärder för att säkerställa att behandlade uppgifter skyddas. Åtgärderna ska vara ägnade att säkerställa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för åtgärderna, är anpassad till risken för integritetsintrång. I propositionen föreslås det att leverantörerna ska få ansvaret för lagringen av trafikuppgifter. Det blir därmed leverantörernas ansvar att lagringen är förenlig med de krav på kvalitet och säkerhet som direktivet ställer. Regeringen menar att kravet på säkerhet i lagen om elektronisk kommunikation bör höjas och säkerhetsnivån preciseras i lagen. Regeringen menar också att det är lämpligt att ta det skydd för personuppgifter som gäller enligt personuppgiftslagen som utgångspunkt för skyddsnivån för lagrade trafikuppgifter, eftersom trafikuppgifter också ofta är personuppgifter. Med denna utgångspunkt föreslås det i propositionen att kravet på säkerhet för trafikuppgifterna formuleras på så sätt att leverantörerna ska vidta de särskilda tekniska och organisatoriska åtgärder som

behövs för att skydda de lagrade uppgifterna vid behandling. I lagförslagen föreslås det också att regeringen eller den myndighet regeringen bestämmer ska få meddela föreskrifter om skyddsåtgärder.

I propositionen föreslås att lagring ska kunna ske i ett annat land under förutsättning att den lagringsskyldige lever upp till de krav och skyldigheter som följer av personuppgiftslagens regler och de andra krav som föreslås gälla. I propositionen konstateras att det i samtliga medlemsländer inom EU finns rättsregler för dataskydd som grundar sig på dataskyddsdirektivet (95/46/EG) och på direktivet 2002/58/EG om integritet och elektronisk kommunikation. För trafikuppgifter som också är personuppgifter gäller som huvudregel att det är förbjudet enligt personuppgiftslagen att till ett tredjeland föra över personuppgifter som är under behandling eller för behandling i ett sådant land, om landet inte har en adekvat nivå för skyddet för personuppgifter.

De lagändringar som krävs för att genomföra direktivet föreslås bli införda i lagen om elektronisk kommunikation. Det är Post- och telestyrelsen som har tillsyn över efterlevnaden av lagen. Regeringen anser att det är lämpligt att Post- och telestyrelsen utövar denna tillsyn även fortsättningsvis och anser inte att det finns anledning att utse någon annan myndighet till tillsynsmyndighet över efterlevnaden av de bestämmelser som nu föreslås. Det anges i propositionen att Post- och telestyrelsens tillsynsverksamhet kommer att omfatta bl.a. att leverantörerna lagrar rätt uppgifter och att leverantörerna vidtar de särskilda tekniska och organisatoriska åtgärder som föreskrivs till skydd för de lagrade uppgifterna, vilket är angeläget i synnerhet vad gäller lagring som sker utomlands. Enligt förslaget ska trafikuppgifterna lagras under sex månader och vid lagringstidens slut utplånas.

Enligt utskottets mening är de ändamål som avses bli tillgodosedda genom lagförslagen, dvs. att avslöja, utreda och lagföra brott, godtagbara ändamål enligt 2 kap. 21 § regeringsformen.

Som det anförts ovan kommer det att finnas ett skydd för de lagrade uppgifterna, och de lagringsskyldiga leverantörerna kommer att stå under tillsyn. Därtill kommer att lagring av trafikuppgifter sker redan i dag hos företag som driver kommunikationstjänster. Den faktiska skillnad som lagförslagen innebär är endast att de brottsbekämpande myndigheterna kan få tillgång till uppgifterna under strikt reglerade former. Trafikuppgifter används dessutom redan i dag i brottsutredningar. Dessa omständigheter talar enligt utskottets mening för att de föreslagna åtgärderna bör kunna vara godtagbara enligt regeringsformen.

Förslaget överensstämmer i stort sett med direktivet. Utskottet noterar att det redan i direktivet görs en avvägning mellan de intressen som nu är aktuella. Direktivet innehåller sålunda bestämmelser om t.ex. den längsta acceptabla lagringstiden och att uppgifterna ska skyddas mot olika åtgärder som är skadliga från integritetssynpunkt. Avvägningen mellan behovet av tillgång till trafikuppgifter och skyddet för den personliga integriteten är

därför väsentligen given redan i direktivet. Direktivet har dessutom redan varit gällande under flera års tid och tillämpas i andra medlemsstater. Den ytterligare reglering som föreslås med stöd av direktivet om integritet och elektronisk kommunikation innebär enligt utskottets mening ett i sammanhanget godtagbart ingrepp i den personliga integriteten.

Sammanfattningsvis anser utskottet att utformningen av lagringskravet beaktar såväl de brottsbekämpande myndigheternas behov av tillgång till trafikuppgifter som behovet att skydda enskildas integritet. Den begränsning av skyddet för den personliga integriteten som lagförslaget innebär kan enligt utskottets mening inte anses gå utöver vad som är nödvändigt med hänsyn till ändamålet med den föreslagna lagstiftningen. Vid en bedömning mot bakgrund av bestämmelserna i regeringsformen framstår lagförslagen alltså som godtagbara. Det som nu har anförts hindrar inte att utskottet ser det som angeläget att den förutskickade revisionen av datalagringsdirektivet kommer till stånd och att varje möjlighet att förstärka skyddet för den personliga integriteten då tas till vara.

Är det särskilda beslutsförfarandet enligt 2 kap. 22 § regeringsformen tillämpligt?

Som utskottet funnit ovan innebär lagförslagen en begränsning av de fri- och rättigheter som anges i 2 kap. 6 § andra stycket regeringsformen. Konstitutionsutskottet konstaterar därför att regeringens förslag till ändring i lagen (2003:389) om elektronisk kommunikation är ett sådant lagförslag som avses i 2 kap. 22 § första stycket regeringsformen och att det där föreskrivna kvalificerade förfarandet således är tillämpligt på förslaget.

Underställning

I den föreslagna 6 kap. 3 a § lagen om elektronisk kommunikation bemyndigas regeringen att meddela föreskrifter om tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling. Vid sin bedömning av om lagförslaget kan antas har utskottet fäst stort avseende vid skyddet mot spridning av de uppgifter som ska lagras. Utskottet anser därför att det finns anledning för riksdagen att behålla en kontroll över hur reglerna på området utformas även något mera i detalj. Detta kan uppnås genom att det i lagen om elektronisk kommunikation med stöd av 8 kap. 6 § regeringsformen tas in en bestämmelse om att föreskrifter som regeringen meddelat med stöd av bemyndigandet ska underställas riksdagen för prövning. Konstitutionsutskottet förutsätter att så sker. Utskottet utgår från att regeringens eventuella vidarebemyndigande för en myndighet att meddela föreskrifter beslutas i förordningens form. Bestämmelsen om underställning kan enligt utskottets mening lämpligen utformas så att ett nytt stycke av följande lydelse tas in i den föreslagna 6 kap. 3 a §: Föreskrifter som meddelas med stöd av denna paragraf ska snarast underställas riksdagens prövning.

I den föreslagna 6 kap. 16 a § lagen om elektronisk kommunikation anges vidare att regeringen eller den myndighet regeringen bestämmer meddelar närmare föreskrifter om vilka uppgifter som ska lagras. Lagtexten innebär enligt vad som anförs i propositionen en upplysning om att verkställighetsföreskrifter, som preciserar vilka uppgifter som ska lagras, meddelas av regeringen eller den myndighet regeringen bestämmer. Det framstår likväl som om föreskrifterna kommer att få betydelse för omfattningen av lagringsskyldigheten och därmed för mängden av uppgifter som kommer att lagras med stöd av de nya bestämmelserna. Detta innebär att föreskrifterna kan få betydelse för hur stort intrång som kommer att ske i enskildas personliga integritet. Mot denna bakgrund anser utskottet sig kunna utgå från att även föreskrifter som regeringen meddelar i enlighet med 6 kap. 16 a § kommer att underställas riksdagen.

Utskottets sammanfattande ställningstagande

Utskottet föreslår att justitieutskottet tillstyrker propositionen, dock med beaktande av vad konstitutionsutskottet anför ovan om underställning av förordningar, och avstyrker motionerna.

Stockholm den 10 februari 2011

På konstitutionsutskottets vägnar

Peter Eriksson

Följande ledamöter har deltagit i beslutet: Peter Eriksson (MP), Per Bill (M), Peter Hultqvist (S), Andreas Norlén (M), Helene Petersson i Stockaryd (S), Lars Elinderson (M), Billy Gustafsson (S), Karl Sigfrid (M), Phia Andersson (S), Karin Granbom Ellison (FP), Hans Hoff (S), Per-Ingvar Johnsson (C), Hans Ekström (S), Kajsa Lunderquist (M), Tuve Skånberg (KD), Jonas Åkerlund (SD) och Mia Sydow Mölleby (V).

Avvikande meningar

1. Underställning (M, FP, C, KD)

Per Bill (M), Andreas Norlén (M), Lars Elinderson (M), Karl Sigfrid (M), Karin Granbom Ellison (FP), Per-Ingvar Johnsson (C), Kajsa Lunderquist (M) och Tuve Skånberg (KD) anför:

Bestämmelsen i 8 kap 6 § regeringsformen har använts sedan den nu gällande regeringsformens ikraftträdande den 1 januari 1975 i bl.a. ransoneringslagen (1978:268), smittskyddslagen (2004:168) och socialförsäkringsbalken (2010:110) i 117 kap. om socialförsäkringen under krig och krigsfara. I exempelvis ransoneringslagen anges att vissa bestämmelser i den lagen ska träda i kraft om riket kommer i krig. Regeringen får under vissa förutsättningar föreskriva från vilken tidpunkt paragraferna ska tillämpas. Sådana föreskrifter ska underställas riksdagens prövning inom en månad från utfärdandet. I smittskyddslagen anges att, om riksdagens beslut inte kan avvaktas, får regeringen föreskriva att bestämmelserna om allmänfarliga sjukdomar eller samhällsfarliga sjukdomar ska tillämpas från den tidpunkt som regeringen bestämmer på en viss smittsam sjukdom som förekommer eller inom kort kan förekomma här i landet. Föreskrifterna ska snarast underställas riksdagens prövning. Underställning av föreskrifter med stöd av smittskyddslagen har skett bl.a. vid klassificeringen av den mycket smittsamma sjukdomen sars. Det rör sig således om beslut som riksdagen i princip ansett ska förbehållas riksdagen, men som i brådskande fall kan få fattas av regeringen, vars ställningstagande får närmast intermistisk karaktär.

Vi anser att detta visar att bestämmelsen i 8 kap. 6 § regeringsformen är en bestämmelse som bör användas endast i undantagsfall, särskilt vid fara i dröjsmål. Enligt vår bedömning är den nu föreslagna lagstiftningen inte av en sådan karaktär att 8 kap. 6 § regeringsformen ska tillämpas. Det ska därför inte i lagen tas in några bestämmelser om att föreskrifter som regeringen meddelar avseende de föreslagna lagbestämmelserna ska underställas riksdagens prövning.

I övriga frågor i yttrandet delar vi majoritetens ställningstagande.

2. Avslag på propositionen (MP, V)

Peter Eriksson (MP) och Mia Sydow Mölleby (V) anför:

Den s.k. datalagringen är en del av ett paradigmskifte som håller på att ske när det gäller statens övervakning av medborgarna. Från att ha fokuserat på övervakning av enskilda brottsmisstänkta pågår en övergång till övervakning på allt lösare grunder och massövervakning.

Trafikuppgifter innehåller mycket integritetskänsliga uppgifter. Ett exempel på detta är uppgifter om att e-postmeddelanden har sänts till föreningar, politiska organisationer, företag eller vårdinstitutioner. Sådana uppgifter kan ge en ingående bild av en persons privata förhållanden. Samma resonemang gäller vilka telefonnummer en person har ringt eller rings upp från och vilken plats en person har befunnit sig på. I de fallen kan inte ens den medvetna och försiktiga användaren undvika att uppgifterna lagras.

I likhet med majoriteten anser vi att den lagring av trafikuppgifter som föreslås i propositionen bör bedömas mot bakgrund av regeringsformens skydd i 2 kap. 6 § andra stycket för den personliga integriteten.

Skyddet för den personliga integriteten enligt 2 kap. 6 § andra stycket regeringsformen får begränsas genom lag. Av 2 kap. 21 § regeringsformen följer att begränsningar endast får göras för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningen får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen som en av folkstyrelsens grundvalar. Man ska således göra en proportionalitetsbedömning av lagförslagen.

Ett godtagbart ändamål för att inskränka skyddet för den personliga integriteten kan enligt vår mening vara att få till stånd nödvändiga brottsbekämpande åtgärder.

Vid bedömningen av proportionaliteten måste man även beakta skyddet för de trafikuppgifter som ska lagras. Lagförslagen innebär en masslagring av information om enskilda som inte ens är misstänkta för brott. Om trafikuppgifter sprids från någon operatörs databaser kommer många att tvingas ställa sig obehagliga frågor om hur vi använder såväl datorer som telefoner. Risken för att lagrade trafikuppgifter kan komma att användas i andra syften än de som är tänkta är dessutom mycket stor – den senaste tidens avslöjanden genom Wikileaks visar med all önskvärd tydlighet att det inte finns någon absolut säkerhet mot att lagrade uppgifter läcker. I propositionen tas inte riskerna med brister i skyddet för trafikuppgifter på allvar. Regeringens förslag innebär att operatörerna tvingas bygga upp betydligt mer omfattande register än i dag, och detta utan att det presenterats någon övergripande riskanalys.

Vid proportionalitetsbedömningen anser vi att man även måste beakta att det i direktivet enbart anges att det är de trafikuppgifter som den enskilde leverantören genererar eller behandlar som omfattas av lagrings-skyldigheten. Direktivet kan inte tolkas på så sätt att en uppgift måste genereras eller behandlas även om den uppgiften inte behövs för att kunna tillhandahålla det nät eller den tjänst som kan vara aktuell. Direktivet innebär därmed inget hinder mot användande av t.ex. anonyma kontantkort, där några uppgifter om användarens identitet inte finns tillgängliga för lagring. Detta väcker frågor om den masslagring av trafikuppgifter som föreslås verkligen kommer att innebära den nytta för brottsbekämpningen

som är avsedd. En annan fråga är vad direktivet tillför om det leder till att leverantörerna introducerar nya tjänster som innebär att uppgifter inte behandlas eller genereras hos leverantörerna? Detta kan leda till att kriminella använder tjänster som innebär att trafikuppgifter inte lagras, medan sådana uppgifter om andra enskilda lagras.

Mot denna bakgrund anser vi att den begränsning av skyddet för fri- och rättigheter som regeringens lagförslag innebär går utöver vad som är nödvändigt med hänsyn till ändamålet med den föreslagna regleringen. Lagförslagen bör därför inte antas.

Är det särskilda beslutsförfarandet enligt 2 kap. 22 § regeringsformen tillämpligt?

Vi anser i likhet med majoriteten att regeringens förslag till ändring i lagen (2003:389) om elektronisk kommunikation är ett sådant som avses i 2 kap. 22 § första stycket regeringsformen och att det där föreskrivna kvalificerade förfarandet således är tillämpligt på förslaget.

Vårt sammanfattande ställningstagande

Vi föreslår att justitieutskottet avstyrker propositionen och tillstyrker våra motioner.

3. Lagring av trafikuppgifter utomlands (SD)

Jonas Åkerlund (SD) anför:

Det är tvingande för Sverige att införa EU-direktiv, och Sverige kan åläggas en ekonomisk sanktion om Sverige inte genomför datalagringsdirektivet. Det är därför inte möjligt för Sverigedemokraterna att endast ta ställning för eller mot antagandet av lagförslagen. Det är dock viktigt att ta upp frågor som inte direkt omfattas av direktivet eller där Sverige har en valmöjlighet. I detta yttrande tar jag upp den fråga som närmast berör konstitutionsutskottets beredningsområde, nämligen frågan om lagring av trafikuppgifter utomlands.

Att bekämpa brottsligheten är en prioriterad fråga för Sverigedemokraterna. Samtidigt måste det ställas krav på dem som hanterar trafikuppgifter, och man måste ta adekvat hänsyn till den personliga integriteten.

Jag anser att trafikuppgifter inte ska få lagras i andra länder, eftersom säkerheten för uppgifterna då kan ifrågasättas. Enligt min mening är det angeläget att en svensk medborgare, i händelse av t.ex. ett säkerhetsintrång eller ett brott mot hanteringen av trafikuppgifter, ska kunna ställa det företag som hanterar trafikuppgifterna till svars på ett effektivt och smidigt sätt. Om trafikuppgifter lagras utomlands kan en svensk medborgare hamna i en situation där denne måste driva en process mot en myndighet eller ett företag i ett annat land. Detta minskar givetvis rättssäkerheten för personen i fråga, samtidigt som det försvårar för personen att driva den rättsliga processen.

I propositionen anges att det i samtliga medlemsländer inom EU finns rättsregler för dataskydd och om skydd för personuppgifter och att dessa regler grundar sig på direktiv. Detta är dock inte tillräckligt enligt min mening med tanke på att rättssäkerheten och korruptionen skiljer sig markant åt mellan olika EU-länder.

Enligt min mening bör justitieutskottet föreslå att riksdagen lämnar ett tillkännagivande om att regeringen ska återkomma till riksdagen med förslag till lagändringar som tillgodoser det syfte jag angivit. Jag föreslår att justitieutskottet tillstyrker motion 2010/11:Ju7.