

Motion till riksdagen

2010/11:Ju6

av Jens Holm m.fl. (V)

med anledning av prop. 2010/11:46

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

1 Innehållsförteckning

2	Förslag till riksdagsbeslut	2
3	Det växande övervakningssamhället	2
4	Dagens reglering av datalagring	2
5	Är datalagring effektiv brottsbekämpning?	3
6	Regeringens förslag går utöver direktivet	4
6.1	Tunga delar som förordning	4
7	Trafikdata är djupt integritetskänsliga uppgifter	5
7.1	Vem får tillgång till uppgifterna?	5
7.2	Databaser läcker	6
8	Datalagringen bryter mot grundläggande fri- och rättigheter	7
8.1	Europakonventionen	8
8.2	Regeringsformen	9
9	Vad betyder datalagringen på sikt?	12
9.1	Kryptering	12
9.2	Öppna nätverk	13
9.3	Vem måste lagra trafikdata?	13

Fel! Okänt namn på

2 Förslag till riksdagsbeslut

Riksdagen avslår proposition 2010/11:46 Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG.

3 Det växande övervakningssamhället

Den s.k. datalagringen är en del av det paradigmskifte som håller på att ske när det gäller statens övervakning av medborgare. Från att fokusera på övervakning av enskilda brottsmisstänkta håller man på att övergå till övervakning på allt lösare grunder (som i beslutet om preventiva tvångsmedel¹) och ren massövervakning, som när det gäller FRA-lagen och nu förslaget om statligt reglerad lagring av trafikuppgifter.

Ny teknik öppnar ständigt nya möjligheter och vi har på kort tid sett en rad nya former för kommunikation växa fram. Samtidigt har också möjligheterna att kartlägga människors liv ökat och vi har sett hur den grundläggande rätten till förtrolig kommunikation gång på gång begränsas. Vi vill se en utveckling som går åt andra hållet, där tekniken medvetet används för ökad transparens i världens maktcentra och för starkare integritet för den enskildes kommunikation.

4 Dagens reglering av datalagring

Regeringen vill gärna förminska betydelsen av lagen genom att hänvisa till att de trafikdata som diskuteras i debatten redan sparas. Det är ett vilseledande påstående, som bara delvis stämmer.

För det första är lagstiftningen i dag formulerad åt rätt håll: den kräver att operatörerna inte sparar mer data än de behöver. Lagen (2003:389) om elektronisk kommunikation slår fast att trafikuppgifter ”skall utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande” (6 kap. 5 §). Det går att göra undantag på ett par olika väl definierade grunder: en av dem handlar t.ex. om uppgifter ”som krävs för abonnentfakturerings”.

¹ Prop. 2005/06:177.

Propositionen är formulerad tvärtom, så att operatörerna tvingas spara alla användares trafikdata för statens räkning. Regeringen försöker blanda bort korten när de vill jämställa två sorters lagstiftning som egentligen är olika som natt och dag.

För det andra ser vi en positiv utveckling i dag, där nya sorters abonnemang gör att allt färre uppgifter behöver sparas för fakturering, och där många operatörer har svarat på användarnas berättigade krav på minimala register över deras kommunikation. Vänsterpartiet vill se en utveckling som fortsätter åt det hållet. Regeringens proposition syftar till att det integritetsskyddet ska vara omöjligt.

Dagens lagstiftning utgår från trafikdata som ett integritetsproblem som behöver minimeras. Regeringen utgår tvärtom från att problemet är att trafikdata inte samlas på hög, och vill tvinga operatörerna att spara mer och längre. Skillnaden kunde inte vara större.

5 Är datalagring effektiv brottsbekämpning?

Mycket talar för att den här sortens massregistrering av folks vardagsliv är ett djupt ineffektivt sätt för rättsväsendet att arbeta, även om vi bortser från integritetsproblemen.

Det är svårt att uppskatta kostnaden för att bygga upp de registersystem regeringen vill tvinga operatörerna att driva. Branschorganisationen IT & Telekomföretagen har beräknat anpassningskostnaderna till omkring 1 140 miljoner kronor. Ovanpå det skulle det tillkomma årliga driftskostnader på 364 miljoner. Regeringens uppskattning, att driftskostnaderna bara skulle ligga på 20 miljoner kronor om året, verkar orimligt låg.

Regeringen osynliggör kostnaderna dels genom den låga skattningen, dels genom att skjuta över mycket av utgifterna på operatörerna. Resultatet blir i praktiken ett slags bredbandsskatt: varje användare får själv betala kostnaderna för sin ofrivilliga övervakning. Stämmer IT & Telekomföretagens uppskattning motsvarar bara den ökade driftskostnaden omkring 80 kr per hushåll och år. Till det kommer en risk att konkurrensen på marknaden försämras, eftersom kostnadströskeln för att erbjuda nät- och telefonitjänster blir högre.

Motsvaras de här kostnaderna av att polisen kan lösa eller förebygga fler brott än i dag? En utvärdering EU-kommissionen låtit genomföra, som läckte ut våren 2010, visar att det inte finns några kvantitativa data som stöder påståendet att datalagringsdirektivet skulle vara ett effektivt sätt att bekämpa brott. Flera av remissinstanserna hävdar att det inte lett vare sig till att brottsligheten sjunkit eller att andelen uppklarade brott ökat.²

² SvD den 15 maj 2010.

Fel! Okänt namn på

Stämmer IT & Telekomföretagens uppskattning motsvarar datalagringens kostnader en möjlighet att anställa många hundra personer i rättsväsendet. Det ligger på propositionens förespråkare att visa att datalagringen är så mycket effektivare än den sortens satsningar hade varit, att det gör integritetsin-trången försvarliga.

6 Regeringens förslag går utöver direktivet

Regeringen har flera gånger försvarat sin hållning med att Sverige är tvunget att genomföra EU-direktivet, snarare än med sakargument om varför ökad datalagring skulle vara något bra. Den inställningen verkar dock inte ha varit vägledande i arbetet med lagförslagen: propositionen går på flera punkter längre än direktivet kräver.

Ett exempel är att trafikuppgifter ska sparas även när den som blir upp-ringd på telefon inte svarar. Ett annat är att propositionen innebär att lokalise-ringsdata sparas också när kommunikationen avslutas.

6.1 Tunga delar som förordning

Hade regeringen velat genomföra en så försiktig implementering som möjligt, hade propositionen också innehållit en mycket mer utvecklad diskussion om vilka data som ska sparas. Det handlar om politiska beslut som kan få stor betydelse: t.ex. öppnar propositionens formuleringar om vad ett ”elektroniskt meddelande” är för vitt skilda tillämpningar. Ska t.ex. kommunikation via fildelningsprogram eller chattprogram omfattas av en lagringsskyldighet som motsvarar den som är tänkt för e-post? Hur ska formuleringar som ”kommu-nikationens början och slut” tolkas för olika sorters nätanvändning?

Propositionen innebär att ”närmare föreskrifter om vilka uppgifter som ska lagras” ska bestämmas av regeringen eller ansvarig myndighet.³ Det betyder att det finns stora möjligheter för regeringen att utvidga datalagringens om-fattning utan att över huvud taget behöva tillfråga riksdagen. Hur vida de befogenheterna är blir också tydligt i ljuset av teknikutvecklingen. Den kom-mer att ställa datalagringsförespråkarna inför ständigt nya vägskäl, och den här propositionen innebär att regeringen kan avgöra varje sådan situation utan att gå tillbaka till riksdagen.

Det hade naturligtvis inte varit möjligt att genomföra direktivet utan att i någon mån lämna över tillämpningsfrågor till regering och myndigheter. Däremot hade regeringen kunnat erkänna att de tekniska vägvalen innehåller

³ 6 kap. 16 a § i förslaget till förändring av lagen (2003:389) om elektronisk kommunika-tion, s. 8 f.

tunga politiska beslut och resonerat om dem betydligt mer utförligt. Med en sådan implementering skulle det ha varit betydligt svårare att i ett senare skede expandera datalagringen ytterligare.

7 Trafikdata är djupt integritetskänsliga uppgifter

Regeringen skriver att ”det saknas förutsättningar för att göra allmänna kartläggningar av personers agerande på Internet enbart utifrån de IP-adresser som ska lagras med stöd av direktivet” (s. 25). Det är ett sätt att ducka för den verkliga frågan: Hur integritetskänsliga uppgifter kommer operatörerna att lagra över sina användare?

Ett exempel är lagringen av e-postuppgifter. Vilka föreningar, politiska organisationer, företag eller vårdinstitutioner en person skickar e-post till kan ge en ganska ingående bild av privata förhållanden. Det kommer att finnas goda skäl för många användare att gå över till e-posttjänster som inte omfattas av lagringsskyldigheten. Det skyddar å andra sidan inte mer än lagringen på ena sidan av kommunikationen. Databasen hos t.ex. RFSL:s operatör kommer att innehålla högst integritetskänsliga uppgifter, om de inte aktivt gått över till kommunikationsformer som inte omfattas av kravet på datalagring.

Samma resonemang gäller vilka telefonnummer en person har ringt eller ringts upp från, eller vilka platser en person har befunnit sig på. I de fallen kan inte ens den medvetna och försiktiga användaren undvika att uppgifterna lagras. En förening eller en tidningsredaktion kommer t.ex. inte att kunna undvika att det upprättas ett register över alla de samtal som kommer in. En grävande journalist kommer inte att kunna undvika att positioneringsdata från mobiltelefonen samlas utanför hennes kontroll.

Den dag någon av operatörernas databaser läcker eller missbrukas kommer många tvingas ställa sig djupt obehagliga frågor om hur vi använder såväl telefoner som datorer. En del uppgifter från Tyskland tyder på att många började bli försiktiga med att ringa t.ex. sin psykolog efter att datalagringsdirektivet genomfördes.

Regeringen har i det längsta velat undvika en diskussion om det uppenbara: att de register de vill låta bygga upp kommer att vara mycket integritetskänsliga.

7.1 Vem får tillgång till uppgifterna?

Parallellt med regeringens arbete med datalagringspropositionen har den också berett frågan om när de brottsbekämpande myndigheterna ska få tillgång till uppgifter om elektronisk kommunikation. I en lagrådsremiss som presenterades den 16 december i år föreslås att dessa frågor fortsättningsvis ska regleras enbart i rättegångsbalken och inte, som i dag, även i lagen om

Fel! Okänt namn på

elektronisk kommunikation. Regeringen presenterar en lång rad förändringar i villkoren för tillgången till uppgifterna. Självklart måste frågan om lagring av trafikuppgifter ses i ett sammanhang med villkoren för när uppgifterna kan hämtas ut. När nu reglerna är planerade att förändras anser vi att det är helt otillräckligt att riksdagen och allmänheten bara har en vecka på sig att analysera hur de olika ärendena förhåller sig till varandra, innan motionstiden för propositionen om datalagring är slut.

Vi kan dock direkt konstatera att regeringen i lagrådsremissen förbereder en förändring i villkoren för polisens tillgång till abonnemangsuppgifter. Bland annat ska de enligt förslaget kunna få tillgång till information om vilket abonnemang som varit kopplat till ett visst IP-nummer utan dagens krav på att det misstänkta brottet bedöms leda till annan påföljd än böter. Att det i dagsläget finns en gräns på fängelsestraff för att efterforska abonnemangsuppgifter visar på att lagstiftningen hittills utgått från att uppgifterna är integritetskänsliga. Kombinerat med den nya lagringsskyldigheten blir resultatet en ökning av myndigheternas möjligheter att kontrollera medborgarnas förehavanden.

Regeringens försvar av datalagringen har handlat om att det skulle behövas för att bekämpa grov brottslighet. Lagrådsremissen visar dock tydligt att regeringen vill att många register ska kunna öppnas för misstanke om nästan vilka brott som helst. Det märks också i att de gjort skivbolagens organisation Ifpi och Antipiratbyrån till remissinstanser i fråga om själva datalagringens utformning.

I lagrådsremissen föreslås också andra förändringar som vi anser vara problematiska. Vi kommer att återkomma till frågorna om de brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation när de ska behandlas av riksdagen.

7.2 Databaser läcker

En av orsakerna till att det skulle kosta så mycket pengar för operatörerna att bygga registersystemen är att det handlar om uppgifter som kan vara mycket känsliga och att det därför ställs höga säkerhetskrav. Några av de exempel på bristande säkerhet som tagits upp av EU-ländernas dataskyddsmyndigheter är kontrollen över vem som har tillgång till uppgifterna, hur de skickas från operatörer till myndigheter och rutinerna för automatisk radering.⁴

Det här är med all sannolikhet ett problem vi redan har i Sverige, och som skulle behöva åtgärdas med tydligare krav på hur operatörerna hanterar användaruppgifter. Framför allt är det ett starkt skäl att minimera hur mycket uppgifter operatörerna över huvud taget får spara. Wikileaks visar på ett övertygande sätt att det inte finns någon absolut säkerhet.

⁴ DN den 27 oktober 2010.

Propositionen tar inte de här riskerna på allvar, trots att det redan finns gott om erfarenheter av att de är betydelsefulla. För bara ett halvår sedan, i maj 2010, visade sig t.ex. säkerheten undermålig hos ett företag som erbjöd människor lokaliseringsdata över sina egna mobiltelefoner. Under ett par timmar kunde vem som helst med hjälp av ett enkelt program lokalisera vilken svensk mobiltelefon som helst, utan ägarens medgivande. Steget därifrån till scenariot att ett komplett register över tusentals telefoners samlade trafik sprids på nätet är inte särskilt långt.

Regeringens förslag innebär att operatörerna tvingas bygga upp betydligt mer omfattande register än i dag, utan att presentera vare sig någon övergripande riskanalys eller några riktiga resonemang om hur samhället ska hantera de läckor som kommer att uppkomma. Hela frågan om risken för läckage avhandlas på ett par sidor i kapitel 8.1 i propositionen, där en rad remissinstanser som varnar för problem avfärdas med hänvisning till att det kommer att ställas höga krav på operatörerna. I verkligheten är det en tom försäkran. Tvingar vi operatörerna att bygga upp omfattande register, kommer de också med all sannolikhet förr eller senare att spridas.

Förutom att många av uppgifterna är integritetskänsliga, skulle man vid en riskanalys också behöva se över säkerhetsaspekterna av registren. Hur kommer lagringen av t.ex. Regeringskansliets, statsministerns eller Säpos trafikuppgifter att se ut? Ökar risken att stora mängder uppgifter en dag sprids på nätet, eller att ett annat lands underrättelsetjänst får tillgång till dem? Mycket tyder på att det också ur det perspektivet finns stora risker med att operatörerna inte systematiskt raderar trafikdata.

8 Datalagringen bryter mot grundläggande fri- och rättigheter

EU-direktivet och regeringens förslag berör och inskränker vissa av de fri- och rättigheter som anges i Europakonventionen och regeringsformen. Att det är så bör man inte kunna tvista om. Att detta görs är inte otillåtet, men om det ska göras ställs krav på en genomgripande analys och redovisning av varför förslagen ändå ska genomföras på ett sätt som är godtagbart i ett demokratiskt samhälle. Man måste då belägga behovet av lagändringarna samt visa på att det finns en effektivitet i åtgärderna sett till vilket syfte de har samt att förändringarna står i proportion till inskränkningarna i fri- och rättigheter. Dessa frågor har varit aktuella i flera lagstiftningsärenden på senare år, men i väldigt många av dessa fall har underlaget i dessa delar haft stora brister och fått omfattande kritik. Integritetsskyddskommittén, en statlig utredning med representanter för samtliga partier som då var representerade i riksdagen, kon-

Fel! Okänt namn på

staterade för bara några år sedan i total enighet att man på senare tid inte levt upp till dessa principer.⁵

Enligt vår mening har man inte heller denna gång levt upp till dessa krav.

Regeringen hävdar att förslaget om datalagring måste genomföras eftersom Sverige är bundet att implementera EU-direktiv, men vi är också bundna att följa Europakonventionen och regeringsformen och den praxis som följer på dessa. Står dessa förpliktelser i konflikt med varandra måste Europakonventionen och regeringsformen, såsom de demokratiska grundregler de utgör, gå före.

8.1 Europakonventionen

Kritiken att datalagringsdirektivet i alltför stor utsträckning inskränker fri- och rättigheter som anges i Europakonventionen, har följt direktivet från första början. I riksdagen skrev vi tillsammans med ledamöter från Miljöpartiet, Centerpartiet och Moderaterna – däribland nuvarande justitieminister Beatrice Ask – ett särskilt yttrande i justitieutskottets betänkande om polisfrågor från 2005/06:

EU-förslaget om en skyldighet för distributörer av tele- och datatrafik att lagra denna trafik under viss tid har kritiserats hårt av många, bl.a. annat av den s.k. artikel 29-gruppen, som består av alla dataskyddsmyndigheter i EU. Förslaget har enligt dessa ansetts strida mot Europakonventionen. Förslaget innebär att alla som använder sig av elektroniska kommunikationsformer får acceptera att bli registrerade och övervakade. Det är en allvarlig kränkning av den personliga integriteten och de mänskliga rättigheterna.

Det som åsyftas är artikel 8 i Europakonventionen, som har följande lydelse:

1. Var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens.
2. Offentlig myndighet får inte 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.

En lång rad tunga instanser har påpekat att direktivet står i direkt konflikt med de rättigheterna. Den europeiska datatillsynsmannen skrev i ett yttrande 2005 att förslaget till direktiv "har direkt inverkan på det skydd som ges genom artikel 8 i Europakonventionen".⁶ Yttrandet fortsätter med en beskrivning av rättspraxis i Europeiska domstolen för de mänskliga rättigheterna:

⁵ SOU 2008:3, 2007:22.

⁶ Yttrande 2005/C 298/01.

Fel! Okänt namn på

- ? Lagring av information om en person ansågs utgöra ett intrång i privatlivet, trots att den inte innehöll några känsliga uppgifter (Amann [1]).
- ? Detsamma gäller s.k. samtalsmätning som inbegriper användning av utrustning som automatiskt registrerar uppringda nummer på en telefon samt tidpunkt och varaktighet för varje samtal (Malone [2]).

EU-ländernas datatillsynsmyndigheter samlas i artikel 29-gruppen. Deras yttrande angående datalagringsdirektivet är också djupt kritiskt:

Det föreslagna direktivet ställer oss inför ett historiskt beslut. Det avser att för första gången introducera en skyldighet över hela Europa att, för utredningsbehov, spara miljarder data relaterade till hela befolkningens kommunikation.

Trafikdatalagring är ett hinder för (interferes with) den grundläggande rätt till förtrolig kommunikation var och en garanteras av artikel 8 i Europeiska konventionen om skydd för de mänskliga rättigheterna.

Den europeiska domstolen för de mänskliga rättigheterna har också framhållit att hemlig övervakning i syfte att försvara demokratin innebär en fara för att densamma undermineras eller till och med förstörs; dessutom har domstolen bekräftat att stater inte, i namn av kampen mot spioneri eller terrorism, får ta till vilka åtgärder som helst de finner lämpliga. Det är därför varje begränsning av den här grundläggande rättigheten måste baseras på ett trängande behov, bara bör tillåtas i exceptionella fall samt vara underställd fullgoda säkerhetsgarantier.⁷

Ordföranden för gruppen, Jacob Kohnstamm, har uttalat sig för gruppens räkning och sagt att direktivet måste dras tillbaka eller ändras kraftigt. I gruppens rapport framkommer att ”detta enorma ingrepp i folks privatliv inte står i proportion till nyttan man har av denna övervakning”.

Inget av de här exemplen kan förstås sägas entydigt slå fast att direktivet bryter mot Europakonventionen. Den frågan kan i slutändan endast avgöras av Europadomstolen. Men den omfattande kritiken visar att regeringens hållning – att frågan inte kan avvakta prövning – vilar på mycket svag grund. Vi vill påminna om 2 kap. 19 § i den nya regeringsformen:

19 § Lag eller annan föreskrift får inte meddelas i strid med Sveriges åtaganden på grund av den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.

Vidare krävs under alla omständigheter att regeringen själv gör en analys av lagförslagens förhållande till Europakonventionen. I propositionen finns en mycket summarisk redogörelse för artikel 8, dess innebörd och praxis knuten till artikeln. Men en analys av hur dessa förpliktelser påverkar det aktuella lagförslaget, saknas egentligen helt.

⁷ Översatt från 1868/05/EN WP 113.

Fel! Okänt namn

8.2 Regeringsformen

I regeringsformen tillförsäkras människor i Sverige en rad fri- och rättigheter. Vi anser att flera av dessa berörs av lagförslaget, både enligt den lydelse av regeringsformen som gäller fram till årsskiftet och enligt den nya grundlag som börjar gälla från den 1 januari.

Det som framför allt berörs i detta sammanhang är 2 kap. 6 § regeringsformen. Den nu gällande lydelsen är:

6 § Var och en är gentemot det allmänna skyddad mot påtvingat kroppsligt ingrepp även i andra fall än som avses i 4 och 5 §§. Var och en är dessutom skyddad mot 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 den nya grundlagen stärks skyddet för den personliga integriteten i ett andra stycke:

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.

Regeringen redogör för dessa förhållanden i sin proposition. Vad gäller nu gällande lydelse av paragrafen görs bedömningen att det skydd för förtroliga försändelser som finns, inte är aktuellt. Detta för att lagringen av trafikuppgifter inte omfattar innehållet i försändelserna. Vi menar att bedömningen är högst tveksam. Även om det direkta innehållet i försändelser inte registreras torde lagparagrafen också utgöra ett skydd mot en omfattande statlig kartläggning av vilka försändelser vi gör och till vilka personer. I annat fall har vi att göra med en påtaglig brist i vår grundlag.

När det gäller det nya, andra styckets, påverkan på det aktuella ärendet finns dock i propositionen inte någon bedömning av att bestämmelsen inte berörs, utan man hänvisar i stället till att inskränkningar får göras enligt förutsättningar i nuvarande 2 kap. 12 § regeringsformen. Det betraktar vi som ett tyst medgivande av att 2 kap. 6 § andra stycket faktiskt berörs och är aktuellt. För oss är det uppenbart att det faktiskt är så. Att uppgifter om all elektronisk kommunikation ska registreras är ett uppenbart intrång i den personliga integriteten, oavsett om det kan rättfärdigas eller inte.

De bestämmelser som nu finns i 2 kap. 12 § regeringsformen och dess närmast följande paragrafer flyttas i den nya regeringsformen till 20 § och dess närmast följande paragrafer, där det ställs villkor för när fri- och rättigheter får begränsas. Den nya 21 § regeringsformen blir aktuell vid begränsningar i 2 kap. 6 §:

21 § Begränsningar enligt 20 § får 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 såsom en av folkstyrelsens grundvalar. Be-

gränsningen får inte göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning.

Regeringen har alltså redogjort för dessa sakförhållanden i sin proposition. Vad som däremot är saknas är en egentlig analys av hur de aktuella lagförslagen förhåller sig till bestämmelserna. Detta är något som måste finnas på plats och som Integritetsskyddskommittén kritiserat att man inte gjort tillräckligt grundligt vid flera tidigare tillfällen. I detta sammanhang måste man belägga behov, effektivitet och proportionalitet vad gäller de aktuella lagförslagen. Precis som så många gånger tidigare visar man på att brottsbekämpande myndigheter har ett behov av att säkra de uppgifter som man kan få tillgång till genom lagring av trafikuppgifter, men missar att göra en grundlig analys av effektiviteten och proportionaliteten. Regeringen för endast ett resonemang om att integritetsfrågorna får större tyngd om EU-direktivet implementeras i lag, att det ska finnas tillräckliga skyddsåtgärder och att det behövs en aktiv tillsyn. Detta är självklart sant och riktigt om man vill genomföra direktivet, men det utgör ingen analys av om implementeringen är förenlig med regeringsformen.

Vi menar dessutom att datalagringen berör fler av de fri- och rättigheter i regeringsformen än de som regeringen redovisar i propositionen. Det saknas resonemang om förhållandet till de friheter som finns under rubriken Opinionsfriheter i den nya grundlagen. Detta borde bli aktuellt att fundera över, bl.a. för att nätet innehåller en uppsjö av möjligheter till politiska yttringar och annan kommunikation, som har ett skydd enligt grundlagen. Ett exempel som förekommit i medierna är att ett politiskt parti kan göra ett medlemsutskick via e-post till samtliga medlemmar, men även all annan kommunikation och andra opinionsyttringar åtnjuter ett grundlagsskydd. Uppgifter om all sådan kommunikation kommer enligt förslaget om datalagring att registreras efter statligt påbud. Detta borde man resonera om i regeringens lagförslag, vilket man inte gör. Vidare saknas resonemang om exempelvis meddelarfriheten.

Att direktivet verkar svårt att implementera inom ramen för grundlagen är inte något unikt för Sverige. Implementeringen i Tyskland överklagades av 34 000 personer, och författningsdomstolen gav dem rätt i att den var grundlagsvidrig.⁸ Även i Rumänien och Bulgarien finns liknande domstolsbeslut. I Bulgarien har regeringen trots stora protester genomfört en ny implementering. I Tyskland och Rumänien är det fortfarande oklart hur datalagringsdirektivet ska hanteras, vilket är något EU-kommissionen kommer att diskutera i sin utvärdering. Det finns all anledning för Sverige att ta diskussionen om regeringsformen och Europakonventionen på allvar.

Eftersom lagförslagen begränsar fri- och rättigheter i regeringsformen på ett sätt som vi anser dels vara olämpligt i sig, dels inte vara tillräckligt underbyggt, kommer vi att använda den möjlighet som finns i regeringsformen till

⁸ DN den 3 mars 2010, BvR 256/08, BvR 263/08 och BvR 586/08.

Fel! Okänt namn på

att försöka få förslaget att vila i ett år innan det kommer upp till ny prövning. Denna möjlighet finns sedan länge i grundlagen. I den nya grundlagen anges den i 2 kap. 22 § regeringsformen:

22 § Ett förslag till lag enligt 20 § ska, om det inte avslås av riksdagen, på yrkande av lägst tio av dess ledamöter vila i minst tolv månader från det att det första utskottsyttandet över förslaget anmälades i riksdagens kammare. Riksdagen får dock anta förslaget direkt, om minst fem sjätte-delar av de röstande enas om beslutet.

Vi hoppas att ett uppskjutande av beslutet kan leda till en större diskussion i samhället om vart vi egentligen är på väg. De senaste tio årens lagstiftning behöver ses i sin helhet, för då syns det närmast övertydligt att vi håller på att bygga ett övervakningssamhälle. Grundlagens tröskel mot att gå för snabbt fram är till just för att det ska finnas tid att reflektera över sådant. Skjuter vi upp beslutet får vi också tid att se hur debatten utvecklas i resten av EU och vad kommissionens utvärdering kommer fram till.

9 Vad betyder datalagringen på sikt?

Ett av de övergripande problemen med att tvinga fram datalagring är att det pekar ut en riktning. Samma argument som används för att försvara den här lagen, används redan i andra länder för att förespråka ytterligare steg i byggandet av ett övervakningssamhälle. Här tar vi upp tre frågor som står för dörren om tanken att kommunikation måste kunna spåras slår rot i Sverige: kryptering, öppna nätverk och vem som måste lagra data.

9.1 Kryptering

Hur kommer regeringen att svara den dag polisen noterar att en del av de uppgifter de vill åt inte finns lagrade, för att användare krypterar sin kommunikation?

Frågeställningen syns redan i sin allra enklaste form i skillnaden mellan webbmejl och vanlig e-post. För den som e-postar via en webbsida är adressaten en fråga om ”innehåll” i nätanvändandet, för den som e-postar med ett vanligt program är adressaten en del av de trafikdata som ska lagras. Skyldigheten för operatörer att föra register över avsändare och mottagare gäller den ena användaren men inte den andra, trots att funktionen de utför är densamma.

Propositionen ställer upp en skillnad mellan ”innehåll” och andra trafikdata som om det var fråga om en tekniskt given uppdelning. I verkligheten är det inte särskilt komplicerat att packa om stora delar av sin kommunikation så att det mesta blir ”innehåll” och mycket lite meningsfull information återstår att registrera. Om den enda användarinformation polisen kommer åt är att en uppkoppling konstant används för ospecificerad nätkommunikation, hur användbar var lagen då?

Blir den sortens kommunikationshantering utbredd praxis, om så bara bland de lite mer tekniskt medvetna användarna, kommer det förr eller senare att börja stå i vägen för ambitionerna att kunna spåra kommunikation i brottsbekämpande syfte. USA har t.ex. en lång historia av att försöka begränsa spridningen av krypteringsprogram genom djupt problematiska lagar.⁹ Sverige har hittills inte haft den sortens lagstiftning, men i propositionen finns ett par skrivningar som verkar avsedda att tvinga den som tillhandahåller en krypteringstjänst att lämna ut trafikdata om sina användare (s. 25). I sin nuvarande form skulle lagen knappast kunna användas för att på allvar försvåra kryptering, men regeringen verkar inte se några principiella problem med att gå vidare.

9.2 Öppna nätverk

Hur tänker regeringen argumentera den dag polisen konstaterar att öppna nätverk ofta leder till att de användaruppgifter den här lagen går ut på att spara, i praktiken anonymiseras? Redan i samband med Ipredlagen gick chefen för Rikskriminalens Internetspaningsgrupp ut och uppmanade människor att hålla sina trådlösa nätverk låsta.¹⁰ Regeringen hade kunnat ta tillfället i akt att försvara de öppna nätverken, men gjorde det inte.

I Tyskland har en person redan dömts för att inte ha spärrat sitt trådlösa nätverk i hemmet.¹¹ Finland tog ett tydligt steg åt det motsatta hållet när deras motsvarighet till SJ beslutade att införa öppna nätverk på alla tåg.¹² Åt vilket håll ska Sverige gå? Vi har svårt att se hur regeringen skulle kunna motivera en positiv syn på öppna nätverk givet de målsättningar som ställs upp i den här lagen om att kunna spåra enskilda människors kommunikation.

Vänsterpartiet ser det som ett stort framsteg att det har blivit lättare och lättare att hitta ett öppet trådlöst nätverk att ansluta sin dator till i Sverige. Det innebär bl.a. att vi bygger en infrastruktur där ett visst anonymitetsskydd är inbyggt – precis som med brevlådorna.

9.3 Vem måste lagra trafikdata?

Regeringens förslag innebär att lagringsplikten omfattar de leverantörer som är anmälningspliktiga enligt lagen om elektronisk kommunikation, med vissa möjligheter till undantag. I praktiken betyder det att det i nuläget är de stora operatörerna som kommer att behöva bygga register.

⁹ För en översikt av problemen med lagarna, se t.ex. Cindy Cohns artikel "Eight Epic Failures of regulating Cryptography", EFF den 20 oktober 2010.

¹⁰ SvD den 1 april 2009.

¹¹ MSNBC den 12 maj 2010.

¹² Yle den 21 juni 2010.

Fel! Okänt namn på

Tills vidare kommer det att finnas en rad möjligheter att använda nätet utan att trafikdata behöver lagras på det sättet direktivet är tänkt, också om vi bortser från de trådlösa nätverken. Det kan t.ex. handla om vanliga operatörer som är tillräckligt små för att beviljas undantag, eller om kaféer och hotell. Eventuellt kan en operatör också komma förbi delar av lagringskraven genom att minimera hur mycket data som över huvud taget genereras.

Redan i remissvaren har det höjts röster för att vidga omfattningen så att betydligt fler blir skyldiga att lagra användaruppgifter. Regeringens enda invändning mot det är att det ”skulle bli svårt att överblicka och kontrollera”, och skriver också att man ”delar redovisade remissinstansers åsikt att det är mycket viktigt att utvecklingen inte blir sådan att vissa leverantörer, i syfte att locka till sig kunder som bedriver kriminell verksamhet, anpassar sin verksamhet så att de ska medges undantag från lagringsskyldigheten”.

Hur kommer regeringen att reagera på att människor anpassar sina kommunikationsmönster för att undgå en djupt illegitim masslagring av sina trafikdata? De operatörer som erbjuder svar på den utbredda kritiken mot data-lagringen kommer naturligtvis att vinna goodwill, samtidigt som de minskar sina kostnader. Också i samband med tidigare integritetskränkande lagstiftning i Sverige har en rad operatörer lyssnat på sina användare och undvikit att lagra mer uppgifter än nödvändigt.

Allt talar tyvärr för att regeringen förr eller senare föreslår utvidgningar av lagringsskyldigheten, med än större integritetsproblem, kostnader och säkerhetsrisker som följd. Har staten en gång tagit sig an uppgiften att försöka ha kontroll över allas trafikdata, kommer det att vara svårt att hålla tillbaka övervakningssamhällets logik.

Stockholm den 21 december 2010

Jens Holm (V)

Bengt Berg (V)

Amineh Kakabaveh (V)

Lena Olsson (V)

Marianne Berg (V)

Eva Olofsson (V)

Mia Sydow Mölleby (V)