

Stockholm den 24 augusti 2015

ASF_MATTER_ID

Till Justitiedepartementet

Ju2015/03153/Å

Sveriges advokatsamfund har genom remiss den 8 maj 2015 beretts tillfälle att avge yttrande över betänkande Datalagring och integritet (SOU 2015:31).

Inledning

Datalagringsutredningens uppdrag har varit att föreslå de förändringar som bedöms lämpliga för att stärka skyddet för den personliga integriteten i förhållande till reglerna om lagring av trafikdata i lagen (2003:389) om elektronisk kommunikation (LEK). Därtill har utredningen haft uppdraget att kartlägga och utvärdera hur lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (IHL) har tillämpats samt att överväga om den bör förändras för att stärka rättssäkerheten eller skyddet för den personliga integriteten. Dessutom har utredningen haft i uppdrag att analysera Säkerhetspolisens behov av särskild möjlighet att inhämta uppgifter om viss brottslig verksamhet, som inte omfattas av IHL:s huvudregel samt lämna förslag på hur ett sådant behov bör tillgodoses och balanseras mot integritetsintresset.

Datalagringsdirektivet (Europaparlamentets och rådets direktiv 2006/24/EG om lagring av trafikuppgifter, som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG) genomfördes i svensk rätt genom att bestämmelser om trafikdatalagring infördes i LEK.¹ Därefter har EU-domstolen

¹ 6 kap. 16 a–f §§ LEK.

i sin dom den 8 april 2014 i målen C-293/12 och C-594/12, Digital Rights Ireland m.fl., förklarar Datalagringsdirektivet ogiltigt.

Trots att lagringsskyldigheten ansågs utgöra ett omfattande intrång i rättigheterna enligt Rättighetsstadgan, ansåg EU-domstolen att lagringsskyldigheten inte kränker det väsentliga innehållet i rättigheterna och att inskränkningen faktiskt svarar mot ett erkänt allmänt samhällsintresse. Lagringsskyldigheten ansågs därmed i sig tillåten.² Däremot ansågs skyldigheten inte i alla delar uppfylla kraven på proportionalitet, varvid EU-domstolen särskilt reagerade på ett antal brister i Datalagringsdirektivet.

Sammantaget fann EU-domstolen att Datalagringsdirektivet inte uppfyller proportionalitetsprincipen med avseende på flera av rättigheterna i den europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) och Europeiska unionens stadga om de grundläggande rättigheterna av den 7 december 2000, anpassad den 12 december 2007 i Strasbourg (Rättighetsstadgan).³

Sammanfattning av Advokatsamfundets synpunkter

Advokatsamfundet anser att en generell och allomfattande lagring av trafikdata innebär ett omfattande och särskilt allvarligt intrång i rätten till privatliv och skyddet av personuppgifter. Samtidigt finner Advokatsamfundet även att en skyldighet att lagra uppgifter kan vara en ändamålsenlig åtgärd för att uppnå syftet att bekämpa allvarlig brottslighet och upprätthålla allmän säkerhet. Införande av sådana åtgärder måste dock föregås av en ytterst noggrann avvägning mellan dessa båda intressen. Om vi vill behålla ett samhälle som präglas av öppenhet och som även fortsättningsvis ska företräda de demokratiska värdena, måste införandet av detta slags åtgärder ske med yttersta omsorg och vara absolut nödvändiga. Syftet med datalagringsdirektivet var att lagrade uppgifter endast skulle användas vid åtgärder mot särskilt allvarlig brottslighet, t.ex. terrorism. De svenska reglerna möjliggör att uppgifterna används vid åtgärder mot annan brottslighet såsom hemlig övervakning av elektronisk kommunikation avseende brott med lägsta straff om minst sex månader. Advokatsamfundet finner därför att reglerna går längre än vad som angavs i direktivet, vilket strider mot Europakonventionen och Rättighetsstadgan. Datalagringsutredningens avvägningar har enligt Advokatsamfundets uppfattning skett med en så stor tyngdpunkt i intresset att bekämpa brottsligheten och upprätthålla den allmänna säkerheten att utredningen närmast framstår som en partsinlaga för de polisiära intressena.

Advokatsamfundet finner att Datalagringsutredningen endast haft ett begränsat intresse av den personliga integriteten och hur allmänheten upplever övervakningen. Utredningen har inte i tillräcklig utsträckning tagit hänsyn till den personliga integriteten vid sina överväganden. Advokatsamfundet anser även att det inte presenterats något övertygande underlag eller någon argumentation till stöd för att nyttan med en så inträngande och

² EU-domstolens dom den 8 april 2014, p. 44.

³ EU-domstolens dom den 8 april 2014 p. 69.

omfattande datalagring faktiskt är så stor som Datalagringsutredningen gör gällande. Det finns t.ex. inga statistikuppgifter om ökad uppkläring av, eller att brott har kunnat förhindras och där detta är en direkt följd av datalagringen. Avsaknaden av sådant underlag kan ju rentav anses tala emot att datalagringen har den nytta som påstås. Om intresset i att lagra trafikuppgifterna nu är så starkt, är det enligt Advokatsamfundets uppfattning ett rimligt krav att ett sådant underlag presenteras. I stället för att ta fram ett sådant underlag har Datalagringsutredningen nöjt sig med vad som snarare verkar vara myndigheternas blotta påståenden om nyttan med datalagringen. Enligt Advokatsamfundet har bedömningarna skett alltför lättvindigt, vilket inte är acceptabelt i ett demokratiskt samhälle när det är fråga om så väsentliga intrång i den personliga integriteten. Därutöver har Datalagringsutredningen inte i tillräckligt stor utsträckning beaktat frågan om säkerheten och tillförlitligheten hos de uppgifter som genom datalagringen blir tillgängliga från leverantörerna. Dessutom kommer de lagstiftningsåtgärder som Datalagringsutredningen föreslår inte att medföra mer än endast marginella förbättringar för integritetsskyddet i förhållande till föreliggande lagstiftning.

EU-domstolen varnar för att datalagringen kan komma att motverka sitt syfte om de enskilda upplever sig som ständigt övervakade och därigenom tappar förtroendet för myndigheterna. Advokatsamfundet delar denna oro. Reglerna om datalagring ingår i en systematisk lagstiftningstrend som möjliggör övervakning och tillgång till uppgifter i allt högre grad och på allt fler områden. Därför måste Datalagringsutredningen ses i ett sammanhang och inte som en isolerad företeelse. Konsekvenserna kan bli att allmänheten i allt högre grad upplever leverantörerna, näten och tjänsterna som redskap för myndigheternas övervakning, där detta påverkar användandet av näten och tjänsterna på sätt som inte är önskvärt, t.ex. så att enskilda avstår från att använda dem.⁴

Advokatsamfundet finner således att Datalagringsutredningens slutsatser inte fullt ut uppfyller EU-domstolens dom och EU-rätten. Därtill finner Advokatsamfundet att Datalagringsutredningens argumentation inte är övertygande vad gäller behovet och nyttan av de lagrade uppgifterna. Advokatsamfundet anser inte heller att Datalagringsutredningens argumentation för att proportionalitetsprincipen uppfyllts vara tillräckligt övertygande. Därutöver kan Advokatsamfundet inte ställa sig bakom Datalagringsutredningens resonemang för att lagring utanför EU, trots EU-domstolens motsatta uppfattning, ska kunna ske. Advokatsamfundet anser att undantag från lagringsskyldighet bör införas för sådana abonnemang eller andra anslutningar som används för förmedling av uppgifter som omfattas av sekretess, tystnadsplikt eller meddelarskydd. Vidare finner Advokatsamfundet risken vara stor för att säkerheten i näten och tjänsterna jämte de lagrade uppgifternas tillförlitlighet eller bevisvärde överskattas, vilket i sin tur kan leda till felaktiga slutsatser och onödigt lidande för oskyldiga. Dessutom finner Advokatsamfundet det vara angeläget att beslut om inhämtning av uppgifter i underrättelseverksamheten fattas av oberoende organ och inte som nu av myndighetens egen personal. Slutligen anser Advokatsamfundet att ytterligare undantag från leverantörernas tystnadsplikt bör införas, så att de kan rapportera obehörig inhämtning till tillsynsmyndigheten SIN.

⁴ Prop. 2010/11:46 s. 19, 38 och 54, se även SOU 2007:76 s. 19 f. och 111 f.

Förhållandet till EU-domstolens dom

När nu EU-domstolen i sin dom den 8 april 2014 i målen C-293/12 och C-594/12, Digital Rights Ireland m.fl., förklarar Datalagringsdirektivet ogiltigt, innebär inte detta samtidigt att all nationell lagstiftning om datalagring automatiskt är ogiltig. Här instämmer Advokatsamfundet i Datalagringsutredningens bedömning, men får samtidigt framhålla att de nationella reglerna fortfarande måste vara förenliga med Europakonventionen eller Rättighetsstadgan för att gälla.

Den genomgående slutsatsen i Datalagringsutredningens bedömning är att den svenska lagstiftningen i så gott som alla delar undanröjer de brister som EU-domstolen åberopat för att ogiltigförklara Datalagringsdirektivet. I de fåtaliga avseenden där de svenska reglerna inte fullt ut kan anses undanröja bristerna, finner Datalagringsutredningen i stället att EU-domstolens dom inte behöver följas bokstavligen och att bristerna kan undanröjas på annat sätt. Ett exempel är hur Datalagringsutredningen anser att svensk lagstiftning undanröjer den brist på kontroll från oberoende myndighet, som EU-domstolen påtalat beträffande Datalagringsdirektivet.⁵ Datalagringsutredningen anser att kravet på sådan kontroll kan uppfyllas av olika befattningshavare hos den brottsbekämpande myndigheten själv. Advokatsamfundet är starkt kritiskt till ett sådant förhållningssätt och menar att det står i direkt strid mot EU-domstolens uppfattning om behovet av en extern kontrollmyndighet. Oavsett om alla de enskilda handläggarna hos myndigheterna är kapabla att alltid genomföra sina arbetsuppgifter på ett sakligt, objektiva och oberoende sätt, kan det skada allmänhetens förtroende för verksamheten. När myndigheter utövar tillsyn mot sig själv blir detta principiellt tveksamt, även om tillsynen sker genom olika befattningshavare hos myndigheten. Därtill finner Advokatsamfundet inte att kontroll som sker inom den egna myndigheten kan anses vara oberoende. Ett annat exempel gäller den av EU-domstolen påtalade bristen på begränsning av lagringens omfattning till att omfatta endast uppgifter med koppling till brottslig verksamhet.⁶ Datalagringsutredningens slutsats är att detta inte går att uppfylla med mindre än att lagringsskyldigheten uppstår först när någon misstanke riktats mot viss person. Om EU-domstolens dom uppfylls i denna del anser Datalagringsutredningen att det inte kommer att finnas tillräcklig tillgång till sådana uppgifter som behövs i den brottsbekämpande verksamheten, varför slutsatsen helt enkelt dras att det då är godtagbart att trots EU-domstolens dom lagra uppgifter om alla.⁷ Advokatsamfundet får då påminna om att uppgifterna redan finns hos leverantörerna där de lagras för andra ändamål, t.ex. för faktureringsändamål, varför oron är överdriven för att uppgifterna inte skulle finnas att tillgå utan en sådan långtgående lagringsskyldighet som det här är fråga om.⁸ Ett ytterligare exempel gäller kravet på att lagringen av uppgifterna ska ske inom EU. Här kommer Datalagringsutredningen fram till att en lagring utanför EU inte strider mot EU-domstolens krav, eftersom Post- och telestyrelsens tillsyn även omfattar den behandling som sker utanför EU. Advokatsamfundet finner detta resonemang vara alltför långtgående och att det inte är

⁵ EU-domstolens dom p. 61 och 62 och SOU 2015:31, s. 19.

⁶ EU-domstolens dom den 8 april 2014, p. 60.

⁷ SOU 2015:31 s. 120.

⁸ 6 kap. 6 och 8 §§ lagen (2003:389) om elektronisk kommunikation.

möjligt att på detta sätt kringgå kravet på lagring inom EU enligt EU-domstolens dom.⁹ Dessutom var syftet bakom Datalagringsdirektivet att de lagrade uppgifterna endast skulle användas i samband med åtgärder mot särskilt allvarlig brottslighet, t.ex. terrorism. De svenska reglerna möjliggör dock att uppgifterna används i samband med åtgärder mot annan brottslighet, eftersom möjligheten att tillgripa hemlig övervakning av elektronisk kommunikation föreligger redan beträffande brott med lägsta straff som uppgår till minst sex månader. Advokatsamfundet finner därför att de nationella reglerna på detta sätt går längre än vad som angavs i direktivet och att detta strider mot både Europakonventionen och Rättighetsstadgan.

Datalagringsutredningen finner att EU-domstolens dom har tillbakaverkande (retroaktiv) effekt. Domen innebär att rättsläget numera är detsamma som om Datalagringsdirektivet aldrig hade funnits. Detta innebär dock inte att nationella genomförandeåtgärder omedelbart blir ogiltiga, dvs. att de kvarvarande nationella reglerna om lagring fortfarande kan vara giltiga. Datalagringsutredningen anser samtidigt att EU-domstolens dom inte ska anses utgöra en komplett kravlista. I stället ska förenligheten med EU-rätten bedömas sammantaget.¹⁰ Advokatsamfundet vill uppmärksamma om att Sveriges skyldigheter att uppfylla sina åtaganden enligt Europakonventionen och Rättighetsstadgan fortfarande gäller. Därför måste EU-domstolens dom även ses mot denna bakgrund. Advokatsamfundet anser därför inte att Datalagringsutredningen på detta sätt kan välja och vraka vilka av bristerna som ska åtgärdas. I annat fall skulle det kunna anses vara tillåtet att bryta mot de mänskliga fri- och rättigheterna i vissa avseenden bara för att dessa med råge uppfylls i andra delar. Advokatsamfundet anser således att alla de brister som EU-domstolen påtalar, måste uppfyllas i den nationella lagstiftningen och att Datalagringsutredningens slutsatser därför inte fullt ut uppfyller EU-domstolens dom.

Advokatsamfundet anser således inte att Datalagringsutredningen i nämnda avseenden uppfyller Sveriges åtaganden att uppfylla EU-rätten. När Datalagringsutredningen tolkar EU-domstolens dom på ett sådant generöst sätt, förstärks intrycket ytterligare av att Datalagringsutredningen är en partsinlaga för de polisiära intressena.

Behovet och nyttan av datalagringen

Ett genomgående drag i Datalagringsutredningens bedömning är att myndigheternas blotta påståenden om nyttan med datalagringen har ansetts vara tillräckligt för utredningens slutsatser och det anges återkommande att Datalagringsutredningen ”inte finner anledning att ifrågasätta myndighetens uppgifter”.¹¹ Med stöd av dessa påståenden hänvisas återkommande till lagringens och trafikuppgifternas stora och avsevärda betydelse för den brottsbekämpande verksamheten.¹² Någon närmare efterforskning och analys av uppgifternas betydelse för brottsbekämpningen presenteras inte och förefaller inte heller ha gjorts, inte minst mot bakgrund av Datalagringsutredningens uppgifter om att det inte

⁹ SOU 2015:31 s. 15 f.

¹⁰ SOU 2015:31 s. 116 f.

¹¹ SOU 2015:51 s. 163, 167 f., 260 och 264.

¹² SOU 2015:31 s. 15, 18, 21, 84, 118 f, 139, 162, prop. 2010/11:46 s. 17 ff.

finns några rutiner för att redovisa nyttan av åtgärderna och att detta rentav skulle vara onödigt.¹³ I stället verkar Datalagringsutredningen bygga sina slutsatser på intervjuer med handläggare eller uppgifter från olika befattningshavare hos myndigheterna. När Datalagringsutredningen konstaterat att datalagringen utgör ett stort intrång i den personliga integriteten, hade det varit mycket värdefullt att kunna hänvisa till ett underlag som visar hur ofta brottsutredningarna lyckats genom tillgången till trafikuppgifter eller misslyckats till följd av att sådana uppgifter inte funnits tillgängliga och där utredningen verkligen stått och fallit med tillgången till trafikuppgifter. Utan ett sådant underlag anser Advokatsamfundet att Datalagringsutredningen dragit alltför långtgående slutsatser om nyttan av uppgifterna. Den stora tilltro som sätts till myndigheternas påståenden om nyttan med datalagringen, förstärker därför intrycket av Datalagringsutredningen som en partsinlaga för de polisiära intressena. Behovet och nödvändigheten i att lagra uppgifterna har kommit att bli en etablerad sanning som inte ifrågasätts. Advokatsamfundet anser detta vara en farlig utgångspunkt i en demokratisk rättsstat.

Behovet och nyttan av att uppgifterna lagras ska också ses mot en annan bakgrund. Som Datalagringsutredningen själv uppger, blir de personer som är involverade i brottslig verksamhet skickliga på att hemlighålla sina förehavanden. Möjligheterna att hemlighålla sin kommunikation är så stora att det inte behövs någon utvecklad förslagenhet för detta. Kommunikationen kan krypteras, annan adress än den faktiska kan uppges, anonymiseringstjänster finns att tillgå m.m.¹⁴ Eftersom så är fallet, kan det enligt Advokatsamfundets uppfattning antas att de som drabbas av den integritetskränkande lagringen i allt högre grad kommer att bestå av vanliga oskyldiga medborgare och att de som egentligen borde vara föremål för åtgärderna i allt högre grad kommer att kunna hålla sig undan. Detta ger ytterligare anledning att ifrågasätta behovet och nyttan av lagringen.

Förhållandet till proportionalitetsprincipen

Begränsning av skyddet enligt 2 kap. 6 § regeringsformen får endast göras för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle och får inte gå utöver vad som är nödvändigt med hänsyn till det ändamål som föranleder begränsningen.¹⁵

Säkerhetspolisen har framfört att analys av telefontrafik bedöms vara av ovärderlig vikt för arbetet, bland annat för att kartlägga aktörer och nätverk som har en avsikt och förmåga att begå brott som är allvarliga för rikets säkerhet.¹⁶ Advokatsamfundet finner mot denna bakgrund att en sådan kartläggning borde kunna ske efter en begäran om lagring avseende de berörda personernas kommunikation, utan att lagringskravet behöver omfatta i princip all kommunikation mellan alla personer, alla kommunikationsmedel och alla trafikuppgifter¹⁷ och som måste lagras i förväg för ett eventuellt senare behov. Om uppgifter ska lagras om alla blir det ännu viktigare att det kan hänvisas till ett underlag

¹³ SOU 2015:31 s. 194.

¹⁴ SOU 2015:31 s. 234, 247, 269.

¹⁵ Jfr SOU 2013:39 s. 81.

¹⁶ SOU 2015:31 s. 87.

¹⁷ SOU 2015:31 s. 118, 120, jfr EU-domstolens dom den 8 april 2014, p. 57-59.

som påvisar den stora nyttan, men även till att uppgifterna inte är användbara endast i ett förhållandevis fåtal fall. När det nu inte presenteras ett sådant underlag, kan proportionaliteten i ett så allomfattande lagringskrav i än högre grad ifrågasättas.

Därtill är det fråga om uppgifter som redan nu lagras hos leverantörerna och för andra ändamål.¹⁸ Trafikuppgifter får således lagras hos leverantörerna, t.ex. för deras fakturering av användandet av elektroniska kommunikationsnät och kommunikationstjänster. Denna lagring får ske till dess att det inte längre går att invända mot fakturan.¹⁹ Detta innebär att uppgifterna redan lagras hos leverantörerna och sannolikt under längre tid än de sex månader som gäller för lagringsskyldigheten för brottsutredningsändamål.²⁰ Myndigheterna kan därför få tillgång till uppgifterna enligt olika regler om åtkomst utan att det egentligen behövs någon särskild lagringsskyldighet för den brottsbekämpande verksamheten.²¹ Datalagringsutredningen framhåller dessutom själv att lagringen bör ske på ett sådant sätt att man undviker att uppgifter lagras mer än en gång.²² Detta förhållande måste enligt Advokatsamfundet rimligtvis vägas in vid bedömningen om det verkligen föreligger ett sådant behov av en särskild lagringsskyldighet avseende samma uppgifter, särskilt mot bakgrund av att lagringen kan anses mycket integritetskränkande.

När det gäller tillgång till abonnemangsuppgifter, dvs. uppgift om namn, adress, abonnentnummer, IP-adresser eller andra statiska uppgifter om anslutning till näten eller kommunikationstjänsterna, finner Datalagringsutredningen att dessa uppgifter inte är särskilt känsliga ur integritetssynpunkt.²³ Advokatsamfundet anser att denna inställning inte kan accepteras förbehållslöst. Vissa personer kan drabbas särskilt om även sådana slags uppgifter behandlas, t.ex. sådana personer som omfattas av vittnesskyddsprogram eller där abonnemangsuppgifter av andra skäl är skyddade hos leverantörerna. Därför behövs förtydliganden i lagstiftningen, som skyddar sådana lagrade uppgifter.

Antalet abonnemang och abonnenter av anslutningar till elektroniska kommunikationsnät och elektroniska kommunikationstjänster är mycket stort, sannolikt över 30 miljoner.²⁴ Antalet meddelanden som utväxlas via de elektroniska kommunikationsnäten eller tjänsterna och där uppgifter ska lagras om samtliga sådana meddelanden är oerhört mycket större, sannolikt rör det sig om flera hundra miljoner meddelanden varje dag. Med tillgång till sådana enorma mängder information om så många abonnenter, är det självfallet möjligt att kartlägga individer på en utomordentligt detaljerad nivå. Detta ska vägas mot det antal fall där det beslutats om åtgärder för att inhämta informationen enligt berörda lagar, vilket sannolikt inte rör sig om mer än mellan 10 000 – 20 000 fall per år.²⁵ Det vore enligt Advokatsamfundet mycket önskvärt med en redovisning av dessa siffror

¹⁸ SOU 2015:31 s. 88, 107.

¹⁹ 6 kap. 6 och 8 §§ lagen (2003:389) om elektronisk kommunikation.

²⁰ 6 kap. 16 d § lagen (2003:389) om elektronisk kommunikation.

²¹ T.ex. enligt 28 kap. 19 § rättegångsbalken eller lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

²² SOU 2015:31 s. 108.

²³ SOU 2015:31 s. 186.

²⁴ <http://statistik.pts.se/pts1h2013/Marknadsutvecklingabonnemang2.html>.

²⁵ Se t.ex. prop. 2011/12:55 s. 118 f och SOU 2007:76 s. 257.

för att på så sätt bedöma om det verkligen är förenligt med proportionalitetsprincipen att lagra sådana mängder information om medborgarna när informationen kommer till användning i så förhållandevis få fall.

Advokatsamfundet anser mot ovanstående bakgrund att Datalagringsutredningen har tagit alltför lätt på proportionalitetskravet i sina slutsatser och att det därför inte till fullo kan anses uppfylla proportionalitetsprincipen. Advokatsamfundet känner även stor oro för att Sverige i sin lagstiftning och rättstillämpning genomgående tar alltför lätt på proportionaliteten och övervärderar intresset av att kunna övervaka medborgarna.

Kravet på lagring inom EU

Av EU-domstolens dom följer att en oberoende myndighetskontroll inte fullt ut garanteras om lagringen sker utanför EU.²⁶ Datalagringsutredningen anser att lagring utanför EU trots detta kan ske, eftersom det svenska regelverket är utformat så att Post- och telestyrelsen kan bedriva en aktiv och ändamålsenlig tillsynsverksamhet även vid lagring utanför EU.²⁷ Advokatsamfundet anser inte att slutsatserna är förenliga med EU-domstolens dom och att de dessutom är felaktiga. Post- och telestyrelsen har nämligen ingen behörighet att utöva tillsyn i andra länder, samtidigt som uppgifter som lagras där kan komma att lämnas ut till landets myndigheter enligt där gällande regler.²⁸ Vid lagring i annat land har således vare sig leverantörerna eller de svenska myndigheterna någon kontroll över hur uppgifterna där kommer att hanteras eller för vilka ändamål hanteringen sker. Dessutom kommer leverantörerna inte att kunna upprätthålla sin tystnadsplikt för berörda uppgifter mot myndigheterna i annat land. Detta kan rentav innebära att leverantörerna riskerar att åsidosätta sin tystnadsplikt, eftersom ett utlämnande av uppgifterna till andra länders myndigheter inte kan anses behörigt enligt svensk lag.²⁹ Denna osäkerhet tillsammans med EU-domstolens klara uttalande borde enligt Advokatsamfundet leda till slutsatsen att någon lagring av uppgifterna inte får ske utanför EU.

Advokatsekretess, tystnadsplikt och meddelarskydd

Enligt EU-domstolens dom är det en brist att Datalagringsdirektivet inte tar hänsyn till eventuell tystnadsplikt.³⁰ De svenska reglerna tar inte heller någon sådan hänsyn, varför även uppgifter som omfattas av sekretess eller tystnadsplikt måste lagras, t.ex. sådana uppgifter som faller under advokatsekretessen³¹ eller meddelarskyddet.³² Detta är dock inget problem enligt Datalagringsutredningen, eftersom proportionalitetsprincipen hindrar att uppgifterna inhämtas eller används när myndigheterna blir medvetna om tystnadsplikten.³³ Myndigheterna ska få förtroendet att självmant bortse ifrån uppgifterna

²⁶ EU-domstolens dom den 8 april 2014, p. 68.

²⁷ SOU 2015:31 s. 15 f.

²⁸ SOU 2015:31 s. 132 och 172 ff.

²⁹ SOU 2015:31 s. 182, jfr 6 kap. 21 § lagen (2003:389) om elektronisk kommunikation.

³⁰ EU-domstolens dom den 8 april 2014, p. 58.

³¹ 8 kap. 4 § rättegångsbalken.

³² 3 kap. 4 § tryckfrihetsförordningen.

³³ SOU 2015:31 s. 17, 97, 121, 203 och 206 ff.

när det konstaterats att de omfattas av sådan tystnadsplikt.³⁴ Hos advokater gäller särskilda bestämmelser om tystnadsplikt och advokater är i vissa sammanhang även undantagna från vittnesplikten.³⁵ Således tillmäts i lagstiftningen uppgifter hos advokater sådan betydelse att det torde kunna anses som särskilt allvarligt om där förekommande uppgifter hamnar i orätta händer. Därtill torde det ligga i rättsstatens intresse och därmed även utgöra ett viktigt samhällsintresse att advokatsekretessen skyddas.³⁶ Om alla uppgifter lagras, även uppgifter om kontakterna mellan advokaterna och deras klienter, finner Advokatsamfundet att advokatsekretessen riskerar att urholkas och att allmänhetens tilltro till rättsstaten därigenom kan försämrats.

Datalagringsutredningen anser inte att myndigheten överträtt meddelarskyddet eller efterforskningsförbudet när uppgifter om en författare, utgivare eller meddelare blir känd som en bieffekt utan att detta varit syftet.³⁷ Även om de lagrade uppgifterna inte utgörs av själva innehållet i kommunikationen, kan uppgifter om kommunikationen, såsom vem som kommunicerat med vem, varifrån etc., också vara av sådan känslig natur att de kan omfattas av meddelarskyddet. Av de lagrade uppgifterna kan ju t.ex. framgå vem som har lämnat tips till en journalist, vilket är just sådana uppgifter som ska skyddas.³⁸ Jfr Högsta domstolens beslut den 18 augusti 2015 i mål nr Ö 3074-15. (Hänvisningen rättad 2015-09-02 pga. uppenbar felskrivning)

Advokatsamfundet ställer sig ytterst tveksamt till att det ska kunna säkerställas att myndigheterna bortser från sådana uppgifter och inte använder dem i den brottsbekämpande verksamheten. Det är därtill knappast möjligt att kontrollera på vilket sätt en utredning påverkats av sådana uppgifter. Inte minst polisens registrering av uppgifter om romer och misshandlade kvinnor är exempel på att myndighetens iver att lösa sina arbetsuppgifter ibland leder till att integritetsskyddande regler glöms bort. Därför ser Advokatsamfundet en risk för att allmänhetens tilltro till bestämmelserna om advokatsekretess, meddelarskydd eller annan tystnadsplikt kommer att minska om det inte finns ordentliga medel för att säkerställa att uppgifter inte behandlas obehörigen eller för obehöriga ändamål.³⁹ Därför efterlyser Advokatsamfundet regler som undantar detta slags uppgifter från lagringsskyldigheten, lämpligast genom att sådana abonnemang eller andra anslutningar som används för kommunikering av sådana slags uppgifter efter anmälan härom t.ex. till Post- och telestyrelsen undantas från lagringsskyldigheten.

³⁴ SOU 2015:31 s. 207.

³⁵ 8 kap. 4 § och 36 kap. 5 § rättegångsbalken.

³⁶ Artikel 6.3 c) i Europakonventionen, se t.ex. NJA 2010 s. 122.

³⁷ SOU 2015:31 s. 208 f.

³⁸ SOU 2015:31 s. 209 och 326, 3 kap. 4 § tryckfrihetsförordningen.

³⁹ SOU 2015:31 s. 55 och 115.

Säkerhetsfrågorna och uppgifternas bevisvärde

Säkerhetsfrågorna är av mycket stor vikt för förtroendet för rättskipningen, vilket medför att stora krav måste ställas på att de uppgifter som används är skyddade och korrekta.⁴⁰ Det ska gälla samma krav på säkerhet och kvalitet för de lagrade uppgifterna som gäller för operatörerna vid behandling av uppgifter i deras nät för elektronisk kommunikation och elektroniska kommunikationstjänsterna.⁴¹ Advokatsamfundet anser att det i själva verket är fråga om samma uppgifter som lagras för ett annat ändamål. Detta betyder att de uppgifter som kommer att användas för åtgärder i en utredning eller som bevisning i en rättegång, är av samma tillförlitlighet som gäller i övrigt för de uppgifter som behandlas i näten och tjänsterna. Detta medför vidare att även om uppgifterna lagras särskilt, så blir de inte bättre, säkrare eller mer tillförlitliga. Det måste enligt Advokatsamfundet därför ställas stora krav på utredare, tillsynsmyndigheter (såsom Post- och telestyrelsen),⁴² de brottsbekämpande myndigheterna, samt inte minst åklagare, advokater och domstolar att vara väl insatta i hur näten och tjänsterna är uppbyggda och utformade, vilka administrativa, organisatoriska och tekniska säkerhetsåtgärder som vidtagits, vilka särskilda risker som är förknippade med näten och tjänsterna⁴³ och hur detta kan påverka bevisvärdet hos de uppgifter som förekommer. Det är operatörerna själva som har den bästa kunskapen härom.⁴⁴ Om tillförlitligheten hos uppgifterna övervärderas, innebär detta en påtaglig risk för att de uppgifter som inhämtas leder till oriktiga domar och beslut.⁴⁵ Samtidigt kan brister härvidlag leda till minskat förtroende hos allmänheten för myndigheterna och rättstillämpningen.⁴⁶

Uppgifterna kommer aldrig att vara bättre än de ursprungligen var hos leverantörerna och det spelar ingen roll vilka åtgärder som föreskrivs, t.ex. av Post- eller telestyrelsen, eller vilka åtgärder som vidtas avseende uppgifterna när de lagrats för de brottsbekämpande myndigheternas verksamhet.⁴⁷ Förslaget har inte i tillräcklig grad beaktat egenskaperna och förutsättningarna för informationstekniken. Advokatsamfundet är därför oroligt för att rättstillämpningen kan överskatta värdet och tillförlitligheten hos de elektroniska uppgifter som förekommer och som ska åberopas som bevisning, vilket i sin tur kan leda till oriktiga domar och beslut.

Om näten och tjänsterna har ett okänt eller mycket stort antal åtkomstpunkter eller andra accessmöjligheter, om ett stort antal personer har tillgång eller access till näten, systemen och tjänsterna och kan förändra uppgifter däri, om loggning av åtgärder eller uppföljning av sådan loggning är otillräcklig, om det förekommer ett stort antal incidenter där

⁴⁰ Prop. 2010/11:46 s. 54, SOU 2007:76 s. 19 f. och 111 f.

⁴¹ SOU 2015:31 s. 109, 112 f och 170, 6 kap. 3 och 3 a §§ lagen (2003:389) om elektronisk kommunikation, se även SOU 2007:76 s. 189 ff.

⁴² Prop. 2010/11:46 s. 71.

⁴³ Se 6 kap. 3-4 b §§ lagen (2003:389) om elektronisk kommunikation.

⁴⁴ Prop. 2010/11:46 s. 52.

⁴⁵ Jfr t.ex. Svea hovrätts dom, 2006-10-02, mål nr B 8799-05.

⁴⁶ Prop. 2010/11:46 s. 54 och SOU 2007:76 s. 19 f. och 111 f.

⁴⁷ SOU 2015:31 s. 113 och 170, samt 6 kap. 3 a § lagen (2003:389) om elektronisk kommunikation, även prop. 2010/11:46 s. 71.

uppgifter försvunnit eller manipulerats, eller om leverantörerna inte har kontroll över vilka slags incidenter som skett eller kan ske, utgör detta var för sig eller tillsammans sådana omständigheter som i olika hög grad måste medföra att de lagrade uppgifternas bevisvärde minskar. Advokatsamfundet ser med stor oro på att Datalagringsutredningen inte uppmärksammat detta. Advokatsamfundet ser därför en påtaglig risk för att de lagrade uppgifternas robusthet inte kommer att ifrågasättas, i vart fall inte i tillräcklig grad, där våra myndigheter och domstolar tar för givet och utgår ifrån att uppgifter som kommer från leverantörerna av näten för elektronisk kommunikation eller de elektroniska kommunikationstjänsterna alltid är tillförlitliga. Om detta inte uppmärksammas ökar riskerna för felbedömningar och felaktiga beslut, som i sin tur medför onödiga olägenheter eller i vissa fall allvarliga konsekvenser för dem vars uppgifter behandlas.

Inhämtning av uppgifter i underrättelseverksamheten

Trots att EU-domstolen i sin dom påtalat bristen på oberoende beslutsfattare anser Datalagringsutredningen att de brottsbekämpande myndigheterna även i fortsättningen själva ska få besluta om inhämtning.⁴⁸ Advokatsamfundet vill särskilt framhålla att frågan om oberoende dock inte avgörs av om systemet fungerar väl eller inte, utan av vem som faktiskt fattar de aktuella besluten. Att inhämtning ibland måste ske med kort framförhållning och det inte kan garanteras att det finns tillgång till oberoende myndigheter, som omedelbart och dygnet runt kan fatta ett beslut, kan inte utgöra skäl till att i detta avseende frånga EU-domstolens dom.⁴⁹ Därför anser Advokatsamfundet att Datalagringsutredningen på ett alltför lättvindigt sätt bortser från EU-domstolens dom och att slutsatsen rentav strider mot EU-rätten.⁵⁰ Detta trots att Advokatsamfundet tidigare funnit det tveksamt att blanda in utomstående i underrättelseverksamheten.⁵¹ Således finner Advokatsamfundet nu att beslut om inhämtning av uppgifter ska få ske endast efter beslut från en oberoende myndighet och inte av de brottsbekämpande myndigheterna själva.

Datalagringsutredningen framhåller själv att medborgarnas förtroende för myndigheternas verksamhet är viktigt. Det måste finnas tungt vägande allmänna intressen för så pass ingripande åtgärder som insamling av information om och kartläggning av enskilda.⁵² Att beslut om inhämtning ska fattas av en oberoende myndighet och inte av de brottsbekämpande myndigheterna själva, är därför enligt Advokatsamfundet en viktig förutsättning för att medborgarna ska kunna känna förtroende för myndigheterna. Elektronisk kommunikation är av stor betydelse i dagens samhälle, varför tilliten till och förtroendet för leverantörerna och de elektroniska kommunikationstjänsterna är av betydande vikt.⁵³ Därför anser Advokatsamfundet att sådana beslut fortsättningsvis ska fattas av en oberoende myndighet. Även om Säkerhets- och integritetsskyddsnämnden

⁴⁸ SOU 2015:31 s. 19 och 284 f.

⁴⁹ SOU 2015:31 s. 293.

⁵⁰ Jfr Storbritanniens High Court of Justice's dom i målet *Davis, Watson, Bice and Lewis vs The Secretary of State for the Home Department* [2015] EWHC 2092, 17/7 2015.

⁵¹ SOU 2015:31 s. 287.

⁵² SOU 2015:31 s. 55 och 115.

⁵³ SOU 2013:39 s. 300 ff., prop. 2010/11:46 s. 17.

(SIN) i efterhand prövar inhämtningen⁵⁴ skulle denna kontroll bli än mer tillförlitlig om någon annan än den brottsbekämpande myndigheten fattat själva beslutet. Efterhandsprövningen ger nämligen inga garantier för att SIN fått del av beslutet i sin helhet eller att uppgifterna från myndigheterna om beslutet är fullständiga och korrekta.

Datalagringsutredningens arbete har i mycket hög grad utgått från de brottsbekämpande myndigheternas egna uppgifter för sin analys och sina slutsatser. Detta innebär att myndigheterna har fått svara för båda sidorna i den intresseavvägning som ska göras, dvs. att den instans som står för själva integritetsintrånget också bedömer hur allvarligt integritetsintrånget är.⁵⁵ Advokatsamfundet anser att detta bidrar ytterligare till intrycket av att Datalagringsutredningen utgör en partsinlaga för de polisiära intressena. I sin genomgång av de olika ärenden som Säkerhetspolisen haft, har ett begränsat antal ärenden kontrollerats. Advokatsamfundet ifrågasätter därför om en sådan undersökning kan anses tillförlitlig, inte minst om den kan anses statistiskt representativ.⁵⁶

Som Datalagringsutredningen uppger finns det i och för sig tydliga rutiner för hur besluten om inhämtning av uppgifter ska gå till. Bland annat ska tre personer vara involverade i beslutsfattandet och det ska upprättas en särskild detaljerad blankett över beslutet.⁵⁷ Det är alltså endast fråga om personal från den egna myndigheten och beslutet angår samma slags uppgifter som kan åtkommas efter domstolsbeslut om hemlig övervakning av elektronisk kommunikation.⁵⁸ Samtidigt används uppgifterna tillsammans med uppgifter från olika andra håll för att kartlägga personer och skapa ”profiler”.⁵⁹ Inhämtningen kan även leda till beslut om förundersökning och om tvångsmedel, vilket kan innebära att myndigheten genom inhämtningen redan har fått tillgång till sådana uppgifter som annars skulle ha förutsatt ett beslut om hemlig övervakning av elektronisk kommunikation.⁶⁰ Därmed ser Advokatsamfundet en risk för att gränsdragningen mellan vad som är underrättelseverksamhet och vad som är tvångsmedelsanvändning, riskerar att bli alltför otydlig. Informationen kan även användas vid ”byteshandel” för att få tillgång till information från andra myndigheter eller utländska underrättelsetjänster. I sådana fall finns inga eller små möjligheter att kontrollera för vilka ändamål och på vilket sätt uppgifterna kommer att användas hos mottagaren.⁶¹ Datalagringsutredningen hänvisar till uttalanden från en utredare, där det bl.a. sägs att inhämtningens omfattning är en resursfråga, varmed antyds att inhämtning skulle ske i större omfattning om myndigheten fick större resurser.⁶² Är myndighetens resurser avgörande för omfattningen av inhämtningen och inte behovet av uppgifterna vägt mot integritetsintrånget, finns det enligt Advokatsamfundet anledning att vara orolig. Advokatsamfundet finner därför allt detta betänkligt ur rättssäkerhetssynpunkt och att det inte bidrar till allmänhetens

⁵⁴ SOU 2015:31 s. 103 och 284.

⁵⁵ SOU 2015:31 s. 212.

⁵⁶ SOU 2015:31 s. 213 och 215.

⁵⁷ SOU 2015:31 s. 214.

⁵⁸ Se 27 kap. 19 § rättegångsbalken.

⁵⁹ SOU 2015:31 s. 216.

⁶⁰ SOU 2015:31 s. 216, 231, 252 f. och 260.

⁶¹ SOU 2015:31 s. 254 ff., SOU 2007:76 s. 19 f. och 111 f., prop. 2010/11:46 s. 38.

⁶² SOU 2015:31 s. 282.

förtroende för myndigheternas inhämtning av uppgifter. Mot denna bakgrund finner Advokatsamfundet att beslut om inhämtning ska fattas av en oberoende myndighet, i stället för av egen personal hos den brottsbekämpande myndigheten.

När nyttan av inhämtning ska vägas mot integritetsintrånget konstaterar Datalagringsutredningen att detta egentligen inte går att mäta. Det går nämligen inte att avgöra hur stor del av framgången i en utredning som kan tillskrivas inhämtningen.⁶³ Trots detta kommer Datalagringsutredningen fram till att inhämtningen leder till ”beaktansvärd” eller ”avsevärd” nytta och att det inte i något fall kunnat konstateras att inhämtningen varit oproportionerlig.⁶⁴ Advokatsamfundet anser att dessa slutsatser inte är tillfredsställande när det inte finns något underlag som stödjer detta och inte heller att Datalagringsutredningen genomgående väljer att lita blint på myndigheternas egna uppgifter.

Leverantörernas ageranden mot otillåten inhämtning

Datalagringsutredningen konstaterar att leverantörernas tystnadsplikt enligt lagen (2003:389) om elektronisk kommunikation gäller även mot SIN och att någon ändring i detta avseende inte är önskvärd.⁶⁵ Enligt nuvarande regler skulle det t.o.m. vara straffbart för leverantörerna att hos SIN avslöja en otillåten inhämtning av uppgifter.⁶⁶ Advokatsamfundet anser att ett ytterligare undantag från tystnadsplikten borde införas i lagen för att möjliggöra för SIN att inhämta uppgifter från leverantörerna, som behövs för tillsynen mot de brottsbekämpande myndigheterna och för att det tydligt ska framgå att ett röjande av uppgifterna till SIN är tillåtet.⁶⁷ Som det nu ser ut kan SIN endast inhämta uppgifterna från den brottsbekämpande myndigheten, tillsynsobjektet, själv.⁶⁸ En sådan möjlighet skulle enligt Advokatsamfundet åtminstone i någon grad stärka integritetsskyddet vid inhämtningen. Någon skyldighet för leverantörerna att rapportera till SIN bör dock inte införas, eftersom det inte föreligger någon skyldighet för dessa att överpröva lagligheten i myndigheternas begäran om uppgifter.⁶⁹ Motsvarande borde även kunna gälla för postverksamhet.⁷⁰

Föreslagna lagändringar

Advokatsamfundet föreslår att det i lagstiftningen införs bestämmelser, som innebär att lagring inte får ske av sådana uppgifter som myndigheterna inte får inhämta enligt lag. Advokatsamfundet föreslår därtill att det införs bestämmelser, som innehåller undantag från tystnadsplikt för det fall uppgifter om de brottsbekämpande myndigheternas inhämtning till berörd tillsynsmyndighet, t.ex. SIN. Advokatsamfundet föreslår även att

⁶³ SOU 2015:31 s. 273 ff., prop. 2010/11:46 s. 17.

⁶⁴ SOU 2015:31 s. 278, 283 och 290.

⁶⁵ SOU 2015:31 s. 302, 304 och 6 kap. 21 § lagen (2003:389) om elektronisk kommunikation.

⁶⁶ 7 kap. 15 § lagen (2003:389) om elektronisk kommunikation och 20 kap. 3 § brottsbalken.

⁶⁷ Jfr SOU 2015:31 s. 314.

⁶⁸ Jfr SOU 2009:1, s. 16 och 189.

⁶⁹ SOU 2015:31 s. 303, prop. 1992/93:200 s. 141.

⁷⁰ Jfr SOU 2015:31 s. 329.

det i lagstiftningen införs bestämmelser innebärande att beslut om inhämtning ska ske av oberoende myndighet. I övrigt kan Advokatsamfundet ställa sig bakom de lagändringar som föreslås av Datalagringsutredningen med följande reservationer och synpunkter.

*11 § lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott*⁷¹

Advokatsamfundet välkomnar en uttrycklig skyldighet att förstöra sådana uppgifter som framkommer vid hemlig övervakning av elektronisk kommunikation och som på grund av undantagen från vittnesplikten i rättegångsbalken inte skulle kunna inhämtas genom vittnesförhör. Samtidigt är skadan redan skedd i och med att myndigheten fått kännedom om uppgifterna och därmed knappast kommer att kunna bortse från dem i en fortsatt utredning. Advokatsamfundet anser att denna olägenhet endast kan undanröjas genom att undantag från lagringsskyldigheten införs för vissa abonnemang eller andra anslutningar, som används för sådan kommunikation som är undantagen från vittnesplikten.

*Lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*⁷²

Advokatsamfundet får hänvisa till vad som framförts avseende föregående förslag.

Förordningen (2003:396) om elektronisk kommunikation, föreslagen ny paragraf 36 b §

Den föreslagna nya regeln ska uttryckligen ange att den brottsbekämpande myndigheten själv ska få fatta beslut om inhämtande av abonnemangsuppgifter vid brottsmisstanke och närmare om hur sådant beslut får fattas. Advokatsamfundet har inget att erinra rent generellt mot detta, men när det gäller sådana abonnemangsuppgifter som angår personer som omfattas av vittnesskydd eller annat, måste det säkerställas att dessa uppgifter inte hanteras på ett sätt som äventyrar deras personliga säkerhet. Sådana abonnemangsuppgifter måste därför antingen undantas från lagringsskyldigheten eller också måste reglerna förtydligas, så att riskerna för den personliga säkerheten minimeras.⁷³

*5 § lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*⁷⁴

Advokatsamfundet välkomnar förslaget om en uttrycklig skyldighet att lämna själva beslutet om inhämtning av uppgifter till SIN i stället för endast uppgifter därom. Dock uppfyller detta enligt Advokatsamfundets uppfattning inte kravet från EU-domstolen på att beslutet ska fattas av en oberoende instans. Advokatsamfundet efterlyser därför lagregler om att beslut om inhämtande av uppgifter i underrättelseverksamheten inte får fattas av myndigheten själv, utan måste fattas av ett särskilt och oberoende organ.

⁷¹ SOU 2015:31 s. 37.

⁷² SOU 2015:31 s. 43.

⁷³ SOU 2015:31 s. 45 och 332.

⁷⁴ SOU 2015:31 s. 331.

8 § lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet⁷⁵

Advokatsamfundet välkomnar en uttrycklig skyldighet att förstöra sådana uppgifter som framkommer vid inhämtning av uppgifter om elektronisk kommunikation och som på grund av undantagen från vittnesplikten i rättegångsbalken inte skulle kunna inhämtas genom vittnesförhör. Samtidigt är skadan redan skedd i och med att myndigheten fått kännedom om uppgifterna och därmed knappast kommer att kunna bortse från dem i en fortsatt utredning. Advokatsamfundet anser att denna olägenhet endast kan undanröjas om undantag från lagringsskyldigheten införs för vissa abonnemang eller andra anslutningar, som används för sådan kommunikation som är undantagen från vittnesplikten.

Kostnader

Datalagringskyldigheten medför att leverantörerna drabbas av vissa kostnader för åtgärdernas effektuerande, inte minst när de i viss omfattning måste anvisa personal för sådant ändamål. Det torde bli leverantörernas slutkunder, dvs. abonnenterna, som slutligen ska stå för dessa kostnader. Advokatsamfundet ifrågasätter dock rimligheten i att låta leverantörerna bära kostnader för olika åtgärder som ingår i eller senare läggs till grund för brottsutredningar när sådan verksamhet är samhällets ansvar.

Avslutande synpunkter

Det är lätt att ha förståelse för och sympatisera med ambitionerna att förebygga, upptäcka, utreda och ingripa mot den slags grova brottslighet som datalagringen och åtgärderna riktar sig emot, inte minst terrorism. Särskilt gäller detta när ändamålen framstår som ytterst vällovliga – inte minst mot bakgrund av det hot och de hemska konsekvenser för samhället och enskilda, som den aktuella typen av brott kan föra med sig. Samtidigt har datalagringsfrågorna varit mycket debatterade och ifrågasatta,⁷⁶ inte minst mot bakgrund av EU-domstolens dom. Det finns därför enligt Advokatsamfundet särskild anledning att vara noggrann med att skapa förståelse och förtroende bland allmänheten. Således är Advokatsamfundet mycket kritiskt till Datalagringsutredningens slutsatser och att de föreslagna åtgärderna oinskränkt införs i svensk lagstiftning. Rättsutvecklingen har inneburit att myndigheterna i allt större utsträckning kan få tillgång till verktyg för att övervaka medborgarna. Leverantörerna är sedan 1999 skyldiga att välja en teknik och utforma sina nät och tjänster för elektronisk kommunikation, så att hemlig avlyssning eller övervakning av elektronisk kommunikation kan genomföras. I denna skyldighet ingår även att tillhandahålla de brottsbekämpande myndigheterna nätanslutningspunkter där dessa åtgärder kan ske.⁷⁷ Sedan 2012 är operatörer skyldiga att lagra trafikdata i sex månader.⁷⁸ Denna datalagring innefattar väsentliga intrång i enskilda människors rätt till respekt för sitt privatliv och sin korrespondens. Samhällets intresse i och behov av detta långtgående förslag, kan enligt Advokatsamfundet inte rimligen uppväga den olägenhet

⁷⁵ SOU 2015:31 s. 331.

⁷⁶ Prop. 2010/11:46 s. 34.

⁷⁷ 6 kap. 19 § lagen (2003:389) om elektronisk kommunikation, infördes genom lag (1999:578).

⁷⁸ 6 kap. 16 a §§ lagen (2003:389) om elektronisk kommunikation.

som det innebär för en enskild. Myndigheterna borde i tillräckligt hög grad vara garanterade tillgång till information genom operatörernas skyldighet att anpassa nät och tjänster för att möjliggöra verkställande av hemlig avlyssning eller övervakning av elektronisk kommunikation. Datalagringen är mycket ingripande för de enskilda, samtidigt som lagringen utan undantag omfattar allas kommunikation. Med alla dessa verktyg borde myndigheterna ha tillgång till mer än tillräcklig information för att kunna framgångsrikt bedriva brottsutredningarna. Advokatsamfundet anser att Datalagringsutredningen framstår som en partsinlaga för de polisiära intressena och att detta försvårar för samhället att vinna förtroende hos allmänheten för datalagringen och de ändamål som denna avser att uppfylla. På detta sätt kan Datalagringsutredningen rentav motverka dessa ändamål.

Av Datalagringsutredningens beskrivning av sitt uppdrag framgår att ingen representant för Datainspektionen ingått i utredningen.⁷⁹ Advokatsamfundet anser att detta minskar utredningens trovärdighet, eftersom Datainspektionens verksamhet och huvudsakliga arbetsuppgifter är att skydda den personliga integriteten. Det hade därför varit värdefullt att få med Datainspektionens kunskaper och erfarenheter. Motsvarande gäller för operatörerna och tjänsteleverantörerna. Om representanter för dem hade ingått i utredningen hade de kunnat bidra med kunskaper om nätens och tjänsternas uppbyggnad, men även med värdefulla synpunkter vad gäller behandlingen av de lagrade uppgifterna och abonnenternas eller användarnas intressen. Därigenom hade utredningen kunnat få ett underlag vad gäller tekniken och säkerheten, som hade varit värdefullt när det gäller att bedöma tillförlitligheten i de uppgifter som ska lagras. När dessa organisationer inte medverkat i utredningen, har de brottsbekämpande myndigheternas intressen varit dominerande. Advokatsamfundet finner att även detta förhållande förstärker intrycket av utredningen som en partsinlaga för polisiära intressen.

Advokatsamfundet har tidigare uttryckt sin djupa oro över implementeringen av trafikdatalagringsdirektivet och dess konsekvenser.⁸⁰ Datalagringsutredningen stärker Advokatsamfundets uppfattning att rättsutvecklingen på området är mycket oroväckande. Den nytta samhället kan ha av de föreslagna åtgärderna kan inte vara värd priset av det kontroll- och angiverisamhälle med den misstänksamhet mellan medborgare och samhälle som åtgärderna i värsta fall kan komma att leda till. Advokatsamfundet ser nu med ännu större oro på den rådande rättsutvecklingen inom området. Det går enligt Advokatsamfundets uppfattning inte att bedöma utredningens förslag isolerat för sig, utan de föreslagna lagändringarna måste ses i ett större sammanhang. Skyldigheten för operatörerna att anpassa sina nät och tjänster för elektronisk kommunikation för att möjliggöra tvångsmedel för inhämtande av information i utredningarna, har återkommande följts av nya liknande tillskott i lagstiftningen. Som exempel på sådana ytterligare lagstiftningsåtgärder kan nämnas ändringarna i upphovsrättslagen enligt IPRED och nu införandet av trafikdatalagrings-skyldigheten. Operatörer och tjänsteleverantörer har på detta sätt alltmer kommit att bli redskap för myndigheterna för att övervaka och kontrollera medborgarna. Utredningens förslag är i berörda delar

⁷⁹ SOU 2015:31 s. 5 och 345.

⁸⁰ Se Advokatsamfundets remiss den 13 mars 2008, R-2008/0035.

ytterligare steg i denna utveckling, där den enskildes privata sfär och rätt att bli lämnad ifred från myndigheternas insyn krymper alltmer. Det finns ingen anledning att tro att Datalagringsutredningens bidrag blir den sista byggstenen, utan framtiden kommer att innehålla återkommande lagstiftningsinitiativ som fortsätter inskränka den enskildes integritet, så att det till slut inte finns något kvar. Skyddet för den enskildes integritet är ett samhällsintresse, som utgör en av grundvalarna för den demokratiska rättsstaten. Den personliga integriteten är en förutsättning för den enskilde att kunna utföra sina demokratiska rättigheter. Därför är inskränkningar i den personliga integriteten ett allvarligt hot, inte i första hand mot den enskilde, utan mot det demokratiska samhället.

SVERIGES ADVOKATSAMFUND

Anne Ramberg