

Stockholm den 1 november 2023

R-2023/1240

Till Justitiedepartementet

Ju2023/01326

Sveriges advokatsamfund har genom remiss den 7 juli 2023 beretts tillfälle att yttra sig över betänkandet Datalagring och åtkomst till elektronisk kommunikation (SOU 2023:22).

Sammanfattning

Advokatsamfundet har tidigare avgett remissyttrande avseende lagstiftning inom aktuellt område.¹ De synpunkter som tidigare lämnats är i hög grad aktuella även gällande dessa förslag.

Utredningen föreslår nya lagringsskyldigheter för att hantera hot mot Sveriges säkerhet, med möjlighet för Säkerhetspolisen att besluta om generell och odifferentierad lagring. För andra ändamål än nationell säkerhet införs geografiskt riktad lagring och utökad riktad lagring, särskilt relevant för grov brottslighet inom specifika områden. Information om elektronisk kommunikation och uppgifter lagrade utanför Sverige ska också kunna lagras och inhämtas, vilket ökar myndigheternas tillgång till information och möjliggör längre lagringstider. Till detta kommer att det ska vara möjligt att lagra information om uppgifter om elektronisk kommunikation

¹ Se Advokatsamfundets remissyttrande den 24 augusti 2015 över betänkandet Datalagring och integritet (SOU 2015:31).



som uppkommer i samband med användandet av allmänt tillgängliga nummeroberoende interpersonella kommunikationstjänster (OTT, Noik).

Det kommer således generellt sett att bli fler slags uppgifter som enligt utredningens förslag kommer att omfattas av lagringsskyldighet och uppgifterna ska kunna lagras under längre tid. Advokatsamfundet anser att det finns stora risker med sådan ökad övervakning ur ett rättssäkerhets- och integritetsperspektiv. Det kan i slutändan leda till negativa effekter på medborgarnas förtroende för rättssystemet och myndigheter.

Det saknas en djupare analys av förslagets konsekvenser för rättssäkerheten, integriteten och allmänhetens förtroende. Informationsteknikens egenskaper och riskerna med felaktiga tolkningar av elektroniska uppgifter har inte heller beaktats i tillräcklig grad. Eftersom utredningens förslag kan komma att leda till alltför långtgående negativa konsekvenser för rättssäkerheten och den personliga integriteten avstyrker Advokatsamfundet förslagen.

Synpunkter

Inhämtning av elektronisk information som är lagrad utanför Sverige vid användning av straffprocessuella tvångsmedel

Utredningen föreslår en ny lag som ska ge brottsbekämpande myndigheter rätt att genom tillämpliga straffprocessuella tvångsmedel bereda sig tillgång till uppgifter som finns lagrade även utanför Sverige. Detta förutsätter dock att myndigheterna kan få tillgång till uppgifterna utan bistånd från någon utomstående och att åtgärden vidtas i Sverige.

Vidare ska två ytterligare begränsningar gälla, nämligen att en inhämtning inte får innebära mer än ett obetydligt intrång i en annan stats suveränitet och att inhämtningen inte får bedömas orsaka någon skada på det informationssystem som tvångsmedlet avser.

Advokatsamfundet finner härvid inte att utredningen i tillräcklig grad har beaktat huruvida den andra staten kommer att dela uppfattningen att en sådan åtgärd endast utgör ett obetydligt intrång i statens suveränitet. Det har därmed inte gjorts någon mer ingående bedömning av riskerna för att åtgärderna kan komma att få diplomatiska konsekvenser mellan Sverige och staten ifråga (s. 467 ff., där frågan diskuteras). För att säkerställa en internationell acceptans för sådan lagstiftning, åtminstone inom



EU/EES, borde det ha övervägts att ta initiativ till unionsrättslig reglering. Frågan om extraterritoriell inhämtning har länge diskuterats inom EU, men ännu inte lett till något konkret resultat. I utredningen görs en bedömning av hur detta påverkar andra länder men utan att ha undersökt ländernas inställning i frågan, vilket Advokatsamfundet anser otillräckligt eftersom det riskerar att medföra skillnader i olika länders förhållningssätt till extraterritoriell inhämtning.

En annan frågeställning som sannolikt är mer problematisk gäller huruvida bevisvärdet hos den information som inhämtas från system i annan stat kan kontrolleras. Som utredningen konstaterar innebär en inhämtning som medför beaktansvärda risker för informationssäkerheten normalt mer än ett obetydligt intrång. Utredningen framhåller även att informationssäkerhet innefattar att elektroniskt lagrad information ska skyddas så att den alltid finns där när den behövs (tillgänglighet), att man kan lita på att den är korrekt och inte manipulerad eller förstörd (riktighet) och att endast behöriga personer får ta del av den (konfidentialitet). Om informationen finns i system i annan stat kommer informationssäkerheten inte att kunna kontrolleras på samma sätt och i samma utsträckning som är möjligt om systemen i stället finns i Sverige.

Även om information som inhämtats från sådana system får förebringas som bevis i svensk domstol enligt principen om fri bevisprövning, måste bevisvärdet hos informationen bli föremål för särskild bedömning utifrån informationssäkerhetsaspekter och hur informationen behandlats i den andra staten. Möjligheterna för svenska myndigheter och domstolar att undersöka säkerheten i sådana system och därmed bedöma informationens tillförlitlighet är samtidigt starkt begränsade. Detta kan i sin tur öka risken för felaktiga slutsatser, vilket måste föranleda en särskild försiktighet vid bevisvärderingen.

Advokatsamfundet anser inte att utredningen i tillräcklig grad har uppmärksammat detta och att det finns en risk för att tillförlitligheten i informationen inte i tillräcklig grad kommer att ifrågasättas i praktiken. Mot denna bakgrund anser Advokatsamfundet att det finns risk för att sådan information i rättstillämpningen kan komma att ges ett alltför högt bevisvärde och att den kan komma att godtas utan någon närmare prövning av hur informationen har behandlats i systemen och tjänsterna i den andra staten.



Lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet

Enligt utredningens förslag ska Säkerhetspolisen få förelägga den som omfattas av lagringsskyldighet enligt 9 kap. 19 § lagen om elektronisk kommunikation att lagra uppgifter om elektronisk kommunikation. Detta ska enligt förslaget få ske om det föreligger ett allvarligt hot mot Sveriges säkerhet som är verkligt och aktuellt eller förutsebart. Lagringen ska få föreläggas om när detta ska ske i syfte att skydda den nationella säkerheten, samtidigt som föreläggandet tillåts vara generellt och odifferentierat.

Det ska alltså krävas att hotet är allvarligt, verkligt, samt aktuellt eller förutsebart. Därtill finns begränsningar avseende lagringstiden och att lagringen måste vara absolut nödvändig. Säkerhetspolisen kommer självständigt att göra bedömningen av hotets art och karaktär. Dessa omständigheter kan antas komma att omfattas av sekretess och den som föreläggs kommer därmed inte att få veta varför föreläggandet meddelas.

Advokatsamfundet finner att de föreslagna bestämmelserna i denna del syftar till att tillvarata det nationella säkerhetsintresset och att detta intresse är berättigat. Bestämmelserna är utformade på ett sådant sätt och med ett sådant innehåll att Säkerhetspolisens möjligheter att meddela förelägganden om datalagring kommer att vara begränsade. Eftersom föreläggandena ska få meddelas endast när det är fråga om vissa angivna hot eller brott mot den nationella säkerheten och där det dessutom ska ställas särskilt höga krav på behovet av datalagring, torde föreläggandena komma i fråga endast efter en rimlig och proportionerlig avvägning gentemot integritetsintresset.

Advokatsamfundet ser positivt på förslaget att det ska inrättas ett särskilt offentligt ombud för att tillvarata allmänhetens integritetsintresse. Samtidigt måste beaktas att det finns en risk för att de särskilda ombudens möjligheter att agera för att skydda den personliga integriteten i praktiken kommer att bli begränsade. Det framgår av utredningens förslag att kontroll avseende lagringsbeslutet och dess laglighet endast ska omfatta förutsättningarna för att beslutet ska få meddelas. Det ska alltså inte ske någon fortlöpande kontroll avseende hur lagringen fortlöper. Detta är en brist när det nu är fråga om att ge myndigheterna en sådan vidsträckt möjlighet att besluta om lagring som förslaget innebär och när detta utgör ett så allvarligt ingrepp i den personliga integriteten som detta typiskt sett utgör.



Samtidigt kommer allmänheten av sekretesskäl endast att få en ytterst begränsad insyn i hur ombudets eller nämndens arbete bedrivs och vilka slutsatser dessa kommer fram till. Ombuden kommer enligt förslaget nämligen att omfattas av sekretess avseende vad denne iakttar och får därför inte avslöja eventuella felaktigheter eller andra iakttagelser som denne ansett föreligga i samband med besluten. En sådan sekretess är i och för sig nödvändig och adekvat när det gäller underrättelseverksamhet av aktuellt slag, men för allmänheten kommer det fortfarande att vara en synnerligen sluten ordning som kan påverka förtroendet för rättssystemet och myndigheterna.

Följaktligen konstaterar Advokatsamfundet att föreläggandena kommer att meddelas utan att vare sig den som föreläggs eller allmänheten har någon möjlighet att bedöma vilka omständigheter som ligger till grund för bedömningen och kommer därmed inte heller att utifrån detta kunna göra en bedömning av om föreläggandena är motiverade. Även om detta är en rimlig ordning när det är fråga om att skydda den nationella säkerheten finns beaktansvärda risker med detta.

Föreläggandena föreslås kunna vara generella och odifferentierade och kunna meddelas utan att den som föreläggs eller allmänheten kommer att få veta vad som föranlett föreläggandet. Advokatsamfundet har förståelse för de av utredningen påtalade svårigheterna i att kunna mer detaljerat reglera under vilka förutsättningar som ska gälla för lagringsskyldigheten. Samtidigt innebär en sådan ordning typiskt sett att det inte går att förutse när en lagringsskyldighet kommer att bli aktuell. En sådan generell och odifferentierad lagringsskyldighet som föreslås utgör även ett utökat ingrepp i den personliga integriteten som på grund av sin oförutsebara natur blir särskilt känsligt. Detta innebär i sig och typiskt sett en risk för att allmänheten kan komma att uppleva sig som godtyckligt övervakade av samhället, vilket kan leda till att förtroendet för samhället och rättssystemet undergrävs. Det var bland annat sådana förhållanden som föranledde EU-domstolen att ogiltigförklara det tidigare gällande datalagringsdirektivet.² Advokatsamfundet finner inte att det har framkommit något i utredningen som tyder på att allmänheten nu skulle ha ändrat inställning till att bli övervakade, varför denna risk sannolikt kvarstår.

² 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 2002/58/EG och EU-domstolens dom i de förenade målen C-293/12 och C-594/12, Digital Rights Ireland m.fl.



Eftersom de föreslagna bestämmelserna innebär att datalagring ska få ske i fler situationer och för ytterligare ändamål, omfatta fler uppgifter, samt kunna ske under längre tid är det enligt Advokatsamfundets uppfattning ett rimligt antagande att allmänheten kommer att känna sig övervakade i större utsträckning än tidigare. Mot denna bakgrund anser Advokatsamfundet att utredningen inte i tillräcklig utsträckning har bedömt vilka konsekvenser de föreslagna bestämmelserna kan komma att få för allmänhetens upplevelse av att vara övervakade eller för förtroendet för rättssystemet och myndigheterna. Utredningen borde därför ha gjort en mer genomgripande bedömning av hur dessa delar av förslaget kan komma att påverka allmänhetens inställning. En tydlig proportionalitetsavvägning mellan det nationella säkerhetsintresset och integritetsintresset hade varit önskvärd.

Lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet

Enligt utredningens förslag ska uppgifter om elektronisk kommunikation få lagras i vissa kommuner för att bekämpa grov brottslighet, vilket ska kallas *geografiskt riktad lagring*. Denna lagring ska få ske vid förhöjd risk för grov brottslighet inom en viss kommun och där risken är baserad på Sveriges officiella statistik. Den geografiskt riktade lagringen ska dessutom kunna kompletteras med vad som ska kallas en *utökad riktad lagring* och som ska kunna avse ett särskilt område eller en särskild plats, såsom stadsdelar, postområden och vägar.

Det blir därmed fråga om en utökad lagringsskyldighet som ska gälla utöver den skyldighet som redan föreligger enligt nu gällande bestämmelser. Därtill ska lagringen genom beslut om utökad riktad lagring kunna ske under en längre tid än vad som annars gäller. Advokatsamfundet finner mot denna bakgrund att beslut om geografiskt riktad lagring medför ett utökat intrång i den personliga integriteten, särskilt när det kompletteras med ett beslut om utökad riktad lagring och lagringen kommer att kunna pågå under en längre tid. Samtidigt som det på grund av att det aktuella området är särskilt brottsutsatt kan anses befogat att utöka lagringen, kommer ett sådant beslut även att leda till att personer som misstänks för brott eller är föremål för polisiärt underrättelseintresse som är bosatta eller befinner sig inom området kommer att omfattas av den utökade lagringen. För ett sådant utökat ingrepp i de enskildas fri- och rättigheter krävs att det kan anses vara effektivt och nödvändigt samt att det även efter en avvägning ska framstå som proportionerligt (2 kap. 20–21 §§ regeringsformen). Advokatsamfundet anser inte att utredningen ger stöd för en sådan slutsats eller att



dessa utökade möjligheter till datalagring skulle kunna förväntas leda till något påtagligt resultat. Därför framstår de föreslagna bestämmelserna i denna del som ett onödigt ingrepp i den personliga integriteten.

Till detta kommer att begreppet geografiskt riktad lagring antyder att lagringen kommer att vara mer begränsad än vad som i praktiken kommer att bli fallet. Genom att lagringen kommer att omfatta elektroniska meddelande som utväxlas till eller från det aktuella geografiska området, kommer även abonnenter eller användare som befinner sig utanför området att bli föremål för lagringen. Lagringen kommer därmed att kunna omfatta mer än det aktuella geografiska området, vilket inte i tillräcklig grad uppmärksammas av utredningen. Enligt Advokatsamfundet har utredningen underskattat det integritetsintrång som förslagen kan medföra i denna del.

Tillsyn över viss brottsbekämpande verksamhet

Utredningen föreslår att Säkerhets- och integritetsskyddsnämndens tillsynsuppdrag utökas till att omfatta även de brottsbekämpande myndigheternas tillämpning av bestämmelserna i lagen om lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet om utökad riktad lagring. Samtidigt noteras att nämnden inte har någon skyldighet att på begäran av enskild kontrollera om han eller hon har varit föremål för utökad riktad lagring och om detta har varit författningensligt.

Advokatsamfundet anser att det i och för sig är rimligt att nämndens tillsynsuppdrag utökas på detta sätt om de föreslagna bestämmelserna införs i svensk rätt. Samtidigt vore det lämpligt att överväga införandet av en rätt för enskilda att kunna få Säkerhets- och integritetsskyddsnämnden att kontrollera om lagringsåtgärder som företagits varit förenliga med gällande rätt. En sådan kontroll torde bli särskilt angelägen när ingreppet i de enskildas integritet kan komma att öka till följd av de föreslagna bestämmelserna. Utredningen har dock inte förslagit att någon fortlöpande kontroll över lagringen och hur uppgifterna används ska kunna utövas. Prövningen ska i stället begränsas till att endast omfatta förutsättningarna för att lagringen ska få tillåtas.

I avsaknad av en uttrycklig rätt och reell möjlighet för de enskilda att få lagringen av uppgifter kontrollerad kan inte de enskildas personliga integritet anses ha beaktats i tillräcklig grad.



Offentlighets- och sekretesslagen

De ändringar som enligt utredningens förslag ska införas i offentlighets- och sekretesslagen blir nödvändiga om de föreslagna bestämmelserna införs i svensk rätt.

Utredningen förslår att 29 kap. 2 § i offentlighets- och sekretesslagen ändras så att begreppet *annan uppgift som angår ett särskilt elektroniskt meddelande* ersätts med begreppet *trafikuppgift*. Med *trafikuppgift* förstås en uppgift som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande. Med *lokaliseringsuppgift* förstås en uppgift som behandlas i ett allmänt mobilt elektroniskt kommunikationsnät och som anger den geografiska positionen för en slutanvändares terminalutrustning, eller en uppgift i ett allmänt fast elektroniskt kommunikationsnät om nätanslutningspunktens fysiska adress.³

En lokaliseringsuppgift kan följaktligen samtidigt vara en trafikuppgift, men den kan förekomma även utan att det föreligger en befordran av ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller ett meddelande som ska faktureras och då är lokaliseringsuppgiften inte en trafikuppgift.⁴ Lagringsskyldigheten enligt bestämmelserna i lagen om elektronisk kommunikation omfattar även lokaliseringsuppgifter som är trafikuppgifter.⁵ När utredningen nu föreslår att bestämmelsen om sekretess i 29 kap. 2 § offentlighets- och sekretesslagen endast omfattar trafikuppgifter, kan detta uppfattas som att sekretessen inte skyddar uppgifter som endast utgör lokaliseringsuppgifter. Advokatsamfundet ifrågasätter om detta varit avsikten, särskilt eftersom lokaliseringsuppgifter kan användas för att kartlägga personer och därmed vara integritetskänsliga på samma sätt som trafikuppgifter.

Advokatsamfundet kan dock instämma i utredningens bedömning att det är olyckligt att begreppen trafikuppgift och annan uppgift som angår ett särskilt elektroniskt meddelande kan uppfattas avse samma slags uppgift. Samtidigt förefaller utredningen ha förbiset att en lokaliseringsuppgift kan förekomma utan att ha något samband med

³ Begreppen definieras i 1 kap. 7 § lagen om elektronisk kommunikation.

⁴ 9 kap. 7 § lagen om elektronisk kommunikation; jfr SOU 2023:22, s. 174 ff.

⁵ 9 kap. 19 § lagen om elektronisk kommunikation.

ett elektroniskt meddelande.⁶ Därför anser Advokatsamfundet att även lokaliseringssuppgifterna borde omfattas av sekretessbestämmelsen.

Inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet

Utredningen föreslår att en ändring införs i lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, så att uppgifter ska kunna inhämtas från tillhandahållare av nummeroberoende interpersonella kommunikationstjänster med stöd av beslut om inhämtning enligt nämnda lag.

Advokatsamfundet noterar att detta innebär ännu ett utökat ingrepp i den personliga integriteten, eftersom det leder till att ett ännu större antal uppgifter som angår fler personer kan komma att bli föremål för lagring.

Lagen om elektronisk kommunikation

Utredningen föreslår vissa ändringar i lagen om elektronisk kommunikation. Om de föreslagna ändringarna införs i svensk lagstiftning kommer detta att innebära att fler aktörer kommer att omfattas av lagringsskyldigheten, såsom den som tillhandahåller nummeroberoende interpersonella kommunikationstjänster. Eftersom skyldigheten att lagra uppgifter enligt de föreslagna bestämmelserna även kommer att gälla beträffande nationell säkerhetslagring jämte vid geografiskt riktad lagring och utökad riktad lagring kommer lagringens omfattning att öka ytterligare. I och med att utredningen även föreslår längre lagringstider i vissa fall kommer lagringens omfattning att öka ytterligare.

Advokatsamfundet finner därmed att vissa av utredningens föreslagna ändringar i lagen om elektronisk kommunikation innebär ett utökat ingrepp i den personliga integriteten som leder till att ett ännu större antal uppgifter som angår fler personer kan komma att bli föremål för lagring. Därmed föreligger ytterligare utökad lagring av uppgifter som rimligen kan riskera att påverka allmänhetens tillit till rättssystemet och myndigheterna negativt, vilket inte har beaktats i tillräcklig grad.

⁶ Se exempelvis SOU 2005:38, s. 22, 25, 202 ff., 206 ff. och 232.



Förhållandet till de mänskliga fri- och rättigheterna

Vid bedömningen av hur långtgående inskränkningar i enskildas fri- och rättigheter som kan tolereras i ett demokratiskt samhälle för att förebygga och utreda brott är det av vikt att klargöra vilken betydelse en åtgärd som innebär intrång i en skyddad rättighet kan ha för att uppnå målet att förhindra och lagföra brott. En proportionalitetsavvägning måste därefter göras mellan åtgärdens betydelse för det eftersträvande ändamålet (samhällsnyttan) å ena sidan och graden av intrång i enskildas skyddade rättigheter – såsom rätten till yttrande- och informationsfrihet eller rätten till självbestämmande och personlig integritet – som åtgärden innebär å andra sidan.⁷ 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.

Utredningens förslag har föregåtts av en proportionalitetsavvägning som ska balansera intresset i de föreslagna bestämmelserna mot de mänskliga fri- och rättigheterna. Den rådande situationen i Sverige med en eskalerad nivå av gängrelaterat skjutvapenvåld, sprängningar och annan systemhotande kriminalitet medför att kraftfulla åtgärder behövs för att bekämpa sådan kriminalitet. Samtidigt innebär förslaget ökade ingrepp i den personliga integriteten för en långt större krets än vad som krävs för ändamålet att bekämpa kriminaliteten. Lagringen kommer att omfatta alla personer i Sverige trots att de som är delaktiga i den aktuella brottsligheten endast utgör en liten del av befolkningen.

Det kan ifrågasättas om brottsligheten kommer att kunna bekämpas mer effektivt genom att alla övervakas och att deras uppgifter blir föremål för en generell och utökad lagring. Utredningens förslag innehåller inte någon närmare analys som ger något robust stöd för att en ökad övervakning skulle ha en gynnsam effekt och att den skulle minska brottsligheten. Inte heller finns det något som tyder på att allmänheten skulle uppleva större trygghet genom att de blir föremål för övervakning i utökad omfattning. I stället för att ökad övervakningen och lagringen av uppgifter, som i huvudsak kommer att omfatta personer som inte är delaktiga i brottslighet, är en mer effektiv åtgärd att ge de brottsbekämpande myndigheterna ökade resurser och att omprioritera deras

⁷ Se exempelvis departementspromemorian Datalagring, EU-rätten och svensk rätt, Ds 2014:23, s. 33.



verksamhet. Detta innebär att Advokatsamfundet inte anser att de föreslagna bestämmelserna är *nödvändiga* för att uppfylla de ändamål som är avsedda att uppnås, vilket är ett av kraven i den avvägning som ska göras innan en ingripande lagstiftning av aktuellt slag införs.

När det gäller utökad övervakning och lagring av uppgifter om enskilda finner Advokatsamfundet att utredningen inte lagt tillräckligt stor vikt vid risken för att de föreslagna bestämmelserna kommer att leda till att enskilda upplever det som en kränkning av den personliga integriteten, vare sig deras uppgifter är föremål för åtgärder enligt utredningens förslag eller inte. Om allmänheten upplever att samhället ägnar sig åt massövervakning i stället för att åtgärda brottsligheten riskerar utredningens förslag rentav att bli kontraproduktiva genom att allmänheten inte bara känner sig hotade av brottsligheten utan även av lagstiftning som kränker den personliga integriteten.⁸ Advokatsamfundet noterar den översikt av hur utredningens förslag utökar de områden och sammanhang där lagringen ska öka. Av denna framgår att utredningens förslag innebär en väsentligt utökad omfattning av lagringen av uppgifter om enskilda. Därav framgår även att de elektroniska kommunikationsnäten och tjänsterna i allt högre grad används för tvångsmedel.

Advokatsamfundet finner att utredningen inte i tillräcklig grad har beaktat frågorna om hur enskilda kan komma att uppleva den inskränkning i deras friheter och personliga integritet som förslagen innebär. Därmed finns en risk för att allmänhetens förtroende och tillit till rättssystemet och myndigheterna minskar, en risk som blir särskilt påtaglig om de ökade kontrollmöjligheterna inte leder till något påvisbart resultat.

Det hänvisas i utredningen inte till något empiriskt underlag till stöd för att förslaget skulle leda till någon nämnvärd minskning i brottsligheten och säkerhetshoten. Det borde i så fall ha kunnat redovisas fall eller statistik över fall där utredningar varit beroende av tillgången till sådana uppgifter som omfattas av förslagen uppgiftslagring. Det finns enligt Advokatsamfundets uppfattning inget som tyder på att nyttan med förslagen skulle bli mer än marginell och därmed att fördelarna inte väger över de nackdelar som förslagen innebär. Därför kan det enligt Advokatsamfundets uppfattning ifrågasättas om de föreslagna bestämmelserna kommer att vara *effektiva* för att

⁸ Se exempelvis resonemanget i EU-domstolens dom i de förenade målen C-293/12 och C-594/12, Digital Rights Ireland m.fl.

uppfylla ändamålen med utredningens förslag, vilket är ett annat krav i den avvägning som ska göras innan en ingripande lagstiftning av aktuellt slag införs.

Det har i samband med tidigare lagstiftningsarbeten konstaterats att den kategori av personer som är inblandade i sådan brottslighet som åtgärderna är avsedda att riktas mot är medvetna härom och anpassar sin kommunikation därefter. De döljer ofta sina förehavanden för att därigenom försvåra upptäckt och utredningsarbete.⁹ Därför finns det en uppenbar risk för att nyttan med åtgärderna överskattas, eftersom de uppgifter som lagras huvudsakligen angår helt harmlös kommunikation och som därmed inte kommer att vara till någon nytta för polis och säkerhetstjänst. Samtidigt finns det av nämnda skäl en uppenbar risk för att den information som skulle kunna vara intressant inte kommer att kunna upptäckas. Advokatsamfundet anser att en sådan ordning kan orsaka att enskilda upplever sig vara övervakade och kontrollerade.

Informationssäkerheten

En annan omständighet av betydelse är att de uppgifter som ska lagras förekommer i nätverk, system eller tjänster för elektronisk kommunikation där skyddet mot obehörig åtkomst eller andra säkerhetsåtgärder kan variera. Därav följer att säkerheten och tillförlitligheten kommer att vara olika beträffande de uppgifter som lagras hos olika aktörer.

Lagringen av uppgifter kommer att ske för att uppgifterna ska finnas tillgängliga för brottsbekämpande myndigheter och för att de ska användas i deras utredande verksamhet. För myndigheternas brottsbekämpning gäller olika regelverk med krav på åtgärder för informationssäkerheten. Dessa regelverk kommer att gälla även vid behandling av sådana lagrade uppgifter som myndigheterna senare inhämtar.

Viss verksamhet som bedrivs hos de brottsbekämpande myndigheterna och de olika aktörerna kan även omfattas av särskilda krav på informationssäkerhet enligt säkerhetsskyddslagen. Detta innebär att myndigheterna måste se till att de aktörer som omfattas av lagringsskyldigheten uppfyller dessa krav, bland annat genom att särskilda säkerhetsskyddsavtal (SUA-avtal) måste ingås med aktörerna.¹⁰ I avtalen ska det

⁹ Se t.ex. SOU 2015:31, s. 233 ff. och 247.

¹⁰ 4 kap. 1 § säkerhetsskyddslagen.



närmare bestämmas vad som ska gälla för behandlingen av uppgifterna hos aktörerna. Dessa krav kan därför medföra kostnader för berörda parter.

Vissa av de brottsbekämpande myndigheterna och de aktörer som omfattas av lagringsskyldigheten kan även omfattas av lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen). Enligt Europaparlamentets och Rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148 (NIS2-direktivet) kommer den nu gällande lagen att upphävas och ersättas med nya bestämmelser som väsentligt utökar antalet aktörer som kommer att omfattas av bestämmelserna. Enligt NIS2-direktivet kommer samtliga myndigheter att omfattas av de nya bestämmelserna på NIS-området.¹¹ När utredningens förslag träder i kraft kommer sannolikt även den svenska lagstiftningen ha genomfört implementeringen av NIS2-direktivet. Därmed måste NIS2-direktivets och den implementerande nya svenska NIS-lagens krav på lämpliga säkerhetsåtgärder för att skydda informationen beaktas hos de myndigheter och andra aktörer som omfattas av bestämmelserna. Detta medför att det behöver utredas vilka konsekvenser de nya NIS-reglerna får för de brottsutredande myndigheterna och de aktörer som omfattas av lagringsskyldigheten. En myndighet som omfattas av regelverket på NIS-området kommer sannolikt att behöva ställa särskilda krav på hur uppgifterna får behandlas hos den aktör som ska lagra uppgifterna. Detta kan i sin tur leda till ökade kostnader för berörda parter.

Informationssäkerhetsfrågor blir även aktuella med anledning av EU:s cybersäkerhetsakt och kompletterande svensk lagstiftning.¹² Denna lagstiftning kan få betydelse genom att den anvisar olika åtgärder och krav för att åstadkomma hög cybersäkerhet. Detta kan medföra att samhället måste ställa motsvarande krav på informationshanteringen hos de aktörer som ska lagra uppgifterna som gäller hos de brottsbekämpande myndigheterna själva. Utredningen bör beakta och uppmärksamma att reglerna om cybersäkerhet kan medföra att krav måste ställas inte bara på de aktörer som omfattas av lagringsskyldigheten utan även på sådana leverantörer av informationssystem, produkter eller tjänster som dessa aktörer anlitar. De uppgifter

¹¹ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148.

¹² Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten), samt lagen (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt.



som ska lagras och som eventuellt senare ska inhämtas av myndigheterna jämte hur uppgifterna senare behandlas måste även uppfylla de informations- eller cybersäkerhetskrav som gäller. De åtgärder som krävs för att uppfylla kraven kommer att medföra särskilda kostnader för berörda parter.

Advokatsamfundet finner inte att utredningen i tillräcklig grad har beaktat frågorna om vilka krav som de brottsutredande myndigheterna kommer att behöva ställa på informations-, cyber- eller IT-säkerheten hos de aktörer som kommer att omfattas av lagringsskyldigheten. Inte heller har utredningen beaktat omfattningen av de kostnader som dessa krav kan medföra för myndigheterna och dem som lagrar uppgifterna.

Leverantörerna av de elektroniska kommunikationsnät och tjänster som ska bli föremål för den ökade lagringsskyldigheten har ett stort antal anställda och uppdragstagare som har tillgång till sådana system där de lagrade uppgifterna finns. Uppgifterna ska kunna läggas till grund för åtgärder till följd av underrättelseverksamhet och rentav som bevisning i brottmål där höga beviskrav gäller. Detta medför att det är av väsentlig betydelse att uppgifterna inte kan förvanskas, försvinna eller komma exponeras för obehöriga. Ju fler personer hos leverantörerna som har åtkomst till de system som används för lagringen och till de lagrade uppgifterna, desto större torde risken vara för att så blir fallet. Utredningen har inte i tillräcklig grad uppmärksammat denna omständighet och därmed inte resonerat kring hur riskerna kan motverkas, exempelvis genom att föreslå högre krav på leverantörerna och ökade befogenheter för berörda tillsynsmyndigheter. Utredningen förefaller dessutom utgå ifrån att de lagrade uppgifterna kommer att vara pålitliga bara för att de finns och har inte ägnat någon större uppmärksamhet åt risken för att uppgifterna kan vara felaktiga eller bli föremål för obehörig åtkomst hos leverantörerna. Advokatsamfundet finner därför att utredningen överskattar tillförlitligheten i de uppgifter som blir föremål för lagringen och att detta kan leda till felaktiga slutsatser i underrättelseverksamhet eller brottsutredningar.

Kostnader

Det kan antas att utredningens förslag kommer att medföra att enskilda drabbas av vissa kostnader för lagringen, inte minst när de i viss omfattning måste anvisa personal för sådant ändamål. Advokatsamfundet ifrågasätter rimligheten i att låta enskilda



aktörer bära kostnader för olika åtgärder som ingår i eller senare läggs till grund för brottsutredningar när sådan verksamhet är statens ansvar.

Avslutande synpunkter

Advokatsamfundet har tidigare uttryckt kritik över implementeringen av det tidigare trafikdatalagringsdirektivet och dess konsekvenser.¹³ De bestämmelser som utredningen nu föreslår innebär utökade möjligheter till generell övervakning och uppgiftslagring. Det går enligt Advokatsamfundets uppfattning inte att bedöma utredningens förslag isolerat, 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 IPRED¹⁴ och införandet av trafikdatalagringsskyldigheten.

Operatörer och tjänsteleverantörer skulle enligt utredningens förslag involveras mer i utförandet av uppgifter som åvilar statliga myndigheter. Utredningens förslag innebär att den enskildes privata sfär krymper i en utsträckning som är svår att motivera med nyttan av utredningens förslag.

Advokatsamfundet finner att den senaste tidens utveckling, där statens möjligheter till övervakning ökat avsevärt, principiellt sett är oroväckande ur ett integritetsperspektiv. Brottsligheten måste naturligtvis bekämpas men förtroende mellan staten och enskilda är mycket värdefullt och större hänsyn bör tas i det avseendet.

SVERIGES ADVOKATSAMFUND

Mia Edwall Insulander

¹³ Se Advokatsamfundets remissvar den 13 mars 2008 över betänkandet Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76).

¹⁴ Civilrättsliga sanktionsdirektivet[1] (engelska: Intellectual Property Rights Enforcement Directive, Ipred), formellt Europaparlamentets och rådets direktiv 2004/48/EG av den 29 april 2004 om säkerställande av skyddet för immateriella rättigheter.