Kontaktperson RISE
Margaret McNamee
Teknisk Direktör
010-516 52 19
margaret.mcnamee@ri.se

Remissvar från RISE avseende: SOU 2017:75 Datalagring - brottsbekämpning och integritet

Sammanfattning

Research Institutes of Sweden (RISE) AB delar utredningens bedömning att lagringsskyldigheten måste göras mindre omfattande än idag och anpassas till vad som är strängt nödvändigt. Det förslag som lämnats innebär dock fortsatt omfattande och generell lagring av personuppgifter och kan inte anses uppfylla proportionalitetsprincipen som EU-domstolen lyfte fram. Trots att vissa uppgiftskategorier inte längre ska lagras är informationen om individen fortsatt så pass omfattande att det rimligen måste röra sig om generell lagring av individens personliga information.

RISE kritik mot utredningens förslag grundas på att proportionalitetsprincipen inte har efterlevts, att vi anser att förslagens utformning gör att övervakning av individen fortsatt kommer vara huvudregel samt att det i författningsförslagen lämnas utrymme för tolkning av uppgiftskategorierna vilket gör det svårt att förutse egentlig integritetspåverkan av förslagen. Vidare anser RISE i motsats till utredningens övervägande att kryptering av de insamlade uppgifterna är ett måste då det ytterligare stärker individens skydd samtidigt som det inte förhindrar att brottsbekämpande myndigheter får tillgång till uppgifterna Det bör dessutom göras ytterligare utredning kring möjligheten att införa riktad övervakning efter misstanke som huvudregel istället för generell övervakning.

RISE ställer sig också bakom de särskilda yttranden som skrivits av Jonas Agnvall samt Staffan Lindmark i fråga om lagringsskyldighetens utsträckning samt den problematiska användningen av begreppet abonnemangsuppgifter i relation till IP-adresser.

Proportionalitetsprincipen

I remissvar till "Datalagring och integritet" (SOU 2015:31) påpekade RISE SICS AB (då under namnet SICS Swedish ICT) att en proportionalitetsbedömning inte kan anses vara gjord då man i utredningen och dess förslag inte vägde eventuella risker för den personliga integriteten (här förstådd i relation till artikel 7 och 8 i rättighetsstadgan) med den nytta uppgifterna hade för relevanta myndigheter. I SOU 2017:75 är proportionalitetsprincipen återigen central, och tyvärr misslyckas även den föreliggande utredningen att göra en adekvat proportionalitetsbedömning. Bland annat anser RISE att utredningen misslyckas med att ta artikel 7 och 8 i rättighetsstadgan i beaktande i avvägningen mellan riskerna och nyttan med datalagring.

Utredningen förklarar att en proportionalitetsbedömning består av två aspekter. Dels 1) att åtgärderna är ägnade åt att uppnå de mål som eftersträvas, och dels 2) att åtgärderna inte går utöver vad som är lämpligt och nödvändigt för att uppnå de legitima mål som eftersträvas (SOU 2017:75, s. 70). För att kunna avgöra om första aspekten är uppfylld kan det antas att så

länge man upplever att åtgärderna är riktade mot ett visst mål är åtgärden legitim. Det lämnar dock i sig utrymme för extremt vidlyftiga tolkningar om vad som utgör ett legitimt mål och vilka medel som då kan användas. För att avgöra om andra aspekten är uppfylld krävs en bedömning av såväl "lämpligt" som "eftersträvansvärt". För att i sin tur avgöra detta anser RISE att det måste ske en bedömning av dels vilka negativa konsekvenser åtgärderna kan få, och dels vilka positiva effekter åtgärderna kan få. Annars kan man svårligen landa i vare sig vad som är "lämpligt" eller "nödvändigt".

För den första aspekten i proportionalitetsprincipen (att åtgärderna är ägnade att uppnå de mål som eftersträvas) krävs bara ett avgränsat syfte för insamlingen. Där anser RISE att utredningen visserligen lyckas visa ett såväl tydligt som legitimt mål i att bekämpa brottslighet, men att det samtidigt är alltför lättvindigt att hävda att så länge man bara har angett ett mål för en viss åtgärd så är första aspekten att se som uppfylld. Det räcker näppeligen att konstatera att man vill bekämpa brottslighet för att det målet ska anses vara legitimt.

För den andra aspekten i proportionalitetsprincipen (att åtgärderna inte går utöver vad som är lämpligt och nödvändigt) misslyckas dock utredningen att motivera varför föreslagna uppgiftskategorier i sig, och inskränkningen av individers personliga integritet till följd av att lagra dessa uppgiftskategorier är lämpliga eller nödvändiga. Det resonemang utredningen för är att eftersom vissa uppgifter används för att utreda brott så är det strängt nödvändigt att lagra dem och därmed proportionerligt (SOU 2017:75, s. 218-219). Med nytta avser man "helt enkelt att uppgifterna har något värde för brottsutredningen" (SOU 2017:75, s. 119). Med behov menar man att en myndighet får använda tvångsmedel när det föreligger ett påtagligt behov och en mindre ingripande åtgärd inte är tillräckligt för att tillgodose det behovet. (SOU 2017:75, s. 119). Utredningen menar dock att i sammanhanget är det nästan alltid så att om det finns en nytta med uppgifterna finns det också ett behov.

Utredningen konstaterar att det finns teoretiska användningsområden för uppgiftskategorierna som berörs av författningen, och i enskilda fall anekdotiska exempel. Däremot redovisas inte i vilken mån uppgifterna har använts inom ramen för tidigare lagstiftning, vilken vikt de har för lagföring eller avförande av misstänkta gärningsmän, eller om det finns uppgifter som alternativt skulle uppfylla syftet med insamlingen av en specifik uppgiftskategori bättre.

Det kan vara så att nyttan är oomtvistlig och att utredningen fått mer ingående bevis på hur enskilda kategorier av uppgifter har använts än vad som redovisas. Men just på grund av att användningen av de enskilda uppgifterna inte redovisas måste vi komma till slutsatsen att nyttan med de specifika uppgifterna inte är helt klarlagd.

Utredningen menar konsekvent att det är strängt nödvändigt men motiverar inte varför. Att det kan vara bra att ha, eller att det vid tidigare utredning har inhämtats (men inte nödvändigtvis använts med tydlig effekt) kan inte anses vara tillräckligt för att beskriva dessa uppgiftskategoriers insamling "strängt nödvändigt".

Riskerna med lagring

Genomgående i utredningen verkar utredaren bortse från att intrånget i den personliga integriteten sker redan vid insamling och lagring av uppgifterna, något som tar sig uttryck i såväl avfärdandet av nyttan av kryptering som resonemangen kring att hemlig avlyssning är så pass integritetskränkande för individen att generell övervakning för hela befolkningen är att föredra. Intrånget uppkommer alltså inte först när polis eller annan brottsbekämpande myndighet begär ut uppgifter och analyserar dem som utredaren verkar mena. Risken för att det lagrade data missbrukas eller kommer på avvägar kan aldrig uteslutas och således måste även denna risk tas med i proportionalitetsbedömningen. Det finns många exempel på att

känsligt data stulits eller på annat sätt kommit på vift, också från branscher med sedan länge starkt säkerhetsmedvetande, som banker och finans. Därför kan denna risk inte lättvindigt avfärdas med generella fraser att den lagringsskyldige "har en skyldighet att vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda uppgifterna" (SOU 2017:75, sid 288).

En konsekvens av att utredningen inte utgår från att lagringen i sig är ett hot mot integriteten är att man bland annat på sidan 201 resonerar kring att om hemlig övervakning inte fanns tillgängligt som metod för brottsbekämpande myndigheter hade man behövt använda en metod som utgjorde ett allvarligare ingrepp på den enskildes integritet, till exempel hemlig avlyssning.

Det framstår som oerhört märkligt att utredningen framhåller det som alltför integritetskränkande att avlyssna en enskild eller ett fåtal misstänkta individer och samtidigt att en generell och odifferentierad övervakning av i stort sett hela befolkningen är ett mindre känsligt alternativ. Det kan inte nog understrykas att övervakning, och även hemlig sådan, utgör en allvarlig risk för den personliga integriteten för samtliga medborgare, och att detta måste ses som ett allvarligare ingrepp i integriteten än att en enskild eller ett fåtal misstänkta blir utsatta för tydligare riktade åtgärder.

Ett sätt att lindra detta intrång vore att göra kryptering av de datalagrade uppgifterna till huvudregel med möjlighet för exempelvis enbart åklagare att dekryptera uppgifterna vid rest misstanke.

Generell lagring

EU-domstolen vänder sig mot att den svenska lagstiftningen rörande datalagring var generell och odifferentierad. Ett av utredningens mål har varit att formulera nya förslag för fortsatt datalagring som inte är generell eller odifferentierad. RISE anser dock att de förslag som utredningen lämnat innebär en fortsatt omfattande och generell datalagring som inte överensstämmer med vad EU-domstolen uttalat.

Utredningen påpekar mycket riktigt att det finns ett antal uppgiftskategorier som inte längre kommer att lagras eller inte alls har lagrats. Och med avseende på antalet uppgiftskategorier hävdar utredningen att det inte längre är en generell och odifferentierad lagring. Om man däremot ser till spåren till den enskilde individen är det svårt att hävda att lagringen inte är fortsatt generell.

Ett exempel är uppgifterna rörande IP-adress, på- och avloggning samt slutgiltig avskiljning för internetåtkomst. Dessa uppgifter lämnar ett frekvent, tydligt och detaljerat spår av den enskildes rörelser och kommunikationer. Att det samtidigt inte sparas uppgifter om plats som inte är kopplade till internetåtkomsten är enbart en fråga om redundans då kommunikationernas utformning sker med tillräckligt frekvens för att det likväl ska gå att lokalisera individen med hög säkerhet.

Utgår man således från rättighetsstadgans 7:e och 8:e artikel framstår det som att utredningens förslag innebär fortsatt generell och odifferentierad lagring av individens personliga information.

Uppgiftskategorier

På- och avloggning samt avskiljning

Begreppen påloggning, avloggning (förslagna 39§ punkt 3) och avskiljning (föreslagna 40§ punkt 4) är vaga sett till hur nätaccesser idag erbjuds. För fasta nät förekommer (som också påpekas i kap. 12) i de flesta fall inga på- eller avloggningar. För mobila nät är det dock väldigt oklart vad påloggning och avloggning innebär. Det innebär i sin tur att det är svårt att bedöma den faktiska frekvensen med vilken uppgifter kommer att sparas, och därmed hur detaljerad bild av människors vardag som kommer lagras, och som resultat en osäkerhet i hur stor påverkan på artikel 7 och 8 i rättighetsstadgan de förordade förslagen kommer att ha.

Beroende på hur man tolkar begreppen på- och avloggning samt avskiljning får man alltså mycket olika grader av intrång in den personliga integriteten, och det blir därmed i stort sett omöjligt att göra en kvantitativ proportionalitetsbedömning. När det gäller telefonitjänster är samtalets början och avslutning i de flesta fall väl definierade, men många andra internettjänster har ingen tydligt definierad början och slut. Tag som exempel en webb-access, där en mobilt ansluten användare skickar en förfrågan och en server svarar med det data som behövs för att visa upp en webbsida i en visare. Vid vilket tillfälle kan en operatör med säkerhet säga att detta är en avslutad kommunikation? Om användaren därpå klickar på en länk kan man aningen (1) tolka detta som en fortsättning på samma kommunikationsakt, eller (2) inledningen på en ny. I det senare fallet skall man enligt en inte helt orimlig tolkning av den föreslagna förordningen lagra tid och plats för den första kommunikationens "avskiljning", i det förra behöver bara tid och plats för den sista kommunikationen i samma session lagras. Men något sessionsbegrepp definieras inte.

Om man gör den senare tolkningen tvingas man producera extremt detaljerade kartläggningar för alla rörliga användare med anslutning till de mobila näten, då de flesta mobiltelefoner idag kopplar upp sig till näten i stort sett kontinuerligt. För många användare kan detta ge upphov till hundratals positionsbestämmelser per dag. Detta är naturligtvis användbart vid en brottsutredning, men knappast proportionerligt eftersom det görs generellt och urskillningslöst för alla användare.

Gör man, å andra sidan, den första tolkningen måste man separat definiera vad som utgör slutet på en kommunikation t.ex. med en fixerad tidsgräns för pauser inom samma session. Utsträckningen på den sådan tidsgräns påverkar då direkt graden av integritetsintrång, vilket torde underlätta en kvantitativ proportionalitetsbedömning.

Begreppet (slutgiltig) avskiljning låter på ytan som om det bara handlar om när operatören lämnar över ansvaret för uppkomlingen till en annan tjänst, men detta är inte heller nödvändigtvis väldefinierat, då en mobil anslutning inte alls behöver kopplas ner för att en användare kopplar upp sig till t.ex. ett WiFi- eller fast nät. Det enda som händer är att inget data under en period skickas på den mobila anslutningen. Det är också oklart om t.ex. byte av cell i ett mobiltelefonnät skall tolkas som en på- och avloggning och/eller avskiljning, vilket också skulle resultera i tätare spår än om bara t.ex. förändring i adresstilldelning loggas.

Den föreslagna lydelsen för förordningen (2003:396) om elektronisk kommunikation 44§ ger PTS möjlighet att tydligare definiera begreppen i författningsförslagen. Men innan detta är gjort är det alltså svårt att ens veta vilken påverkan på den personliga integriteten som förslagen har. I RISE SICS remissvar för SOU 2015:31 redovisades också att PTS då inte hade en gällande definition av begreppet på- och avloggning, trots att det även då fanns möjlighet för PTS att göra detta.

NAT

I utredningens författningskommentarer till 39§ (SOU 2017:75, s. 310f) kommenteras bl.a. att förslagen kommer ur operatörernas användning av NAT-teknik. Man hävdar bl.a. att förslagen enbart är att se som en redaktionell ändring (SOU 2017:75, s.217) vilket inte stämmer. Ändringarna kommer i grunden påverka såväl integritetsintrånget som användningen av NAT-tekniken.

NAT-tekniken innebär att en koppling mellan användarens privata IP-adress och en publik IP-adress görs per förbindelse. Kopplingen görs mellan användarens privata IP-adress tillsammans med TCP/UDP-portnummer och en publik IP-adress samt TCP/UDP-portnummer. Det betyder att en och samma publika IP-adress kan användas samtidigt av flera användare med olika privata IP-adresser.

Konsekvensen av att kräva lagring av abonnent/användare även i samband med NAT-teknik blir att mycket detaljerade trafikuppgifter kommer att lagras, då tidpunkt för alla användarens data-förbindelser måste lagras. Som exempel så genererar tittande på en vanlig webbsida allt från ett fåtal förbindelser till flera tiotals förbindelser. Denna lagring kommer således att innehålla mycket detaljerad information om användares aktivitetsnivå och således också uppgå till avsevärt större volymer än enbart lagring av kopplingen mellan IP-adress och abonnent/användare.

Utredningen försöker hävda att IP-adresser och uppringda nummer är så kallade "abonnemangsuppgifter". Utan att gå i en diskussion i hur användbara eller känsliga abonnemangsuppgifter är, är det glasklart att lagring av NAT-kopplingar handlar om trafikuppgifter. Det är helt enkelt orimligt att hävda att också denna information är "abonnemangsuppgifter" och därmed faller utanför EU-domstolens utlåtande. Det är också felaktigt att hävda att integritetsintrånget inte ökar som följd av detta krav (2017:75, s. 247).

Detta betyder alltså att en användare vars operatör använder NAT för att leverera en viss tjänst kan behöva lagra många gånger fler observationer av denne, än en operatör som använder fasta IP-adresser. I denna mening är graden av integritetsintrång allt annat än "teknikneutral" och kan också orsaka höga kostnader för de operatörer som med anledning av nya regler kommer vilja byta lösning.

Kryptering bör införas

RISE AB förordar att lagringen tillförs krav på kryptering för att minska risken för den personliga integriteten och stärka rättigheterna i enlighet med artikel 7 och 8 i rättighetsstadgan. I kapitel 12.5.4 framhåller utredningen mycket riktigt att kryptering skulle stärka skyddet för den enskildes personliga integritet men att detta som enskild åtgärd inte kommer leda till att svensk datalagring kommer leva upp till EU-domstolens beslut. Utredningens förslag blir därför att inte föreslå krav på kryptering.

Det är dock viktigt att konstatera att den möjlighet att kryptera som behandlas och sedan avfärdas i kapitel 12.5.4 skulle bidra till en minskad risk för obehörig användning, ett tydligare ansvar för till exempel åklagares formulering av uppgiftsinhämtning och är i sig inget hinder för den föreslagna ordningen för datalagring.

RISE ser således det som en nödvändighet att också ställa krav på att de lagrade uppgifterna krypteras så att de enbart kan avkrypteras vid uttalat och tydligt behov av uppgifterna. Eftersom att utredningen inte heller ser några direkta hinder för en sådan ordning bör det alltså inte råda någon tvekan om att kryptering kommer bidra till en säkrare hantering av uppgifterna. Det skulle radikalt minska riskerna med att de lagrade uppgifterna stjäls eller läcks till obehöriga.

Utred riktad lagring

Det EU-domstolen pekat på när det gäller riktad lagring anser utredningen vara något som ligger vid sidan av själva saken. Utredningen redogör mycket kortfattat för varför olika möjligheter till begränsningar inte skulle fungera och det utreds inte på något djupgående sätt hur man skulle kunna lösa de svagheter som finns. RISE anser att det är viktigt att de brottsbekämpande myndigheterna ska kunna utföra sitt arbete och att det därför skyndsamt bör utredas hur begränsad lagring i enlighet med EU-domstolens uttalande kan ske för att kunna finna en lämplig väg framåt. Detta gäller såväl tydligt riktade åtgärder mot en misstänkt individ eller grupp av individer, som de avfärdade förslagen kring en så kallad "quick freeze"-metod.

Från RISE har följande experter deltagit:

Bengt Ahlgren

Jacob Dexe

Lena Hägglöf

Per Kreuge

RISE Research Institutes of Sweden AB
Strategi och utveckling

Margaret McNamee
Teknisk Direktör