Särskilt yttrande

av experterna Kurt Alavaara och Per Lagerud (Säkerhetspolisen)

Allmänt om förslagen

Inledning

Lagringsskyldigheten och samtliga uppgifter som den omfattar enligt förordningen om elektronisk kommunikation är strängt nödvändiga för brottsbekämpningen. Enligt utredarens förslag ska lagringsskyldigheten minska tämligen kraftigt. Det kommer att få till följd att möjligheterna att förebygga, förhindra och utreda brott försämras avsevärt. I många fall kan konsekvenserna betecknas som mycket allvarliga. Med det särskilda yttrandet vill vi göra tydligt i den fortsatta beredningen vilka effekterna blir om lagringsskyldigheten minskas. Vi vill också framhålla att det är synnerligen angeläget att Sverige inom EU verkar för en lagringsskyldighet som svarar mot de behov som staten har av en både effektiv och rättssäker brottsbekämpning.

Syftet med lagringsskyldigheten

Allvarliga brott orsakar stora skador för enskilda och samhället. Det finns ett stort värde i att brotten kan förhindras eller klaras upp, kanske redan på planeringsstadiet. För samhället i stort, för medborgarna i allmänhet och för brottsoffren är det därför angeläget att förutsättningarna för att klara upp brotten är så goda som möjligt.

Att de brottsbekämpande myndigheterna har tillgång till trafik- och lokaliseringsuppgifter är avgörande för en effektiv bekämpning av grov brottslighet, inklusive sådan som är kopplad till nationell säkerhet. Utredaren anger att om de brottsbekämpande myndigheterna inte

skulle ha tillgång till adekvata utredningsverktyg i den elektroniska miljön så skulle grova brott i vissa fall vara omöjliga att klara upp och brottsoffer i motsvarande omfattning vara skyddslösa. Vissa brott skulle i praktiken bli straffria och många målsägande skulle aldrig kunna få upprättelse. Utredaren konstaterar också att staten har en skyldighet att skydda enskildas privatliv och personliga integritet mot intrång som begås av andra enskilda och, om intrång görs, se till att brotten utreds. Enligt utredaren skulle det inte vara förenligt med Sveriges internationella åtaganden att inte ge de brottsbekämpande myndigheterna möjlighet att effektivt utreda brott i den elektroniska miljön.

Trafik- och lokaliseringsuppgifter har med tiden blivit ett allt viktigare verktyg i brottsbekämpningen. I nuläget, där en stor del av brottsligheten lämnar digitala spår i någon form, är uppgifterna fundamentala. Det gäller i såväl underrättelse- som förundersökningsverksamhet. Uppgifterna används i stort sett i varje utredning av grov brottslighet. Ofta är uppgifterna dessutom den första och enda ingången i utredningarna och ger nyckeln till det vidare arbetet. Utan de nycklarna kommer dörren till framgång många gånger att vara stängd.

Bestämmelserna i bl.a. rättegångsbalken om tillgången till trafik- och lokaliseringsuppgifter syftar till att ge de brottsbekämpande myndigheterna information som kan klarlägga

– *vem* som kommunicerade med vem (dvs. källan och slutmålet). Det framgår av uppgifter om telefonnummer och ip-adresser (vid telefoni), e-postadresser, ip-adresser, SMS-nummer och MMS-nummer (vid meddelandehantering) och ip-adresser (vid internetåtkomst).
– *när* kommunikationen skedde. Det framgår av uppgifter om datum, spårbar tid vid start och slut (vid telefoni och meddelandehantering) och tid för på- och avloggning (vid internetåtkomst).
– *var* kommunikationen skedde. Det framgår främst av uppgifter om lokalisering (vid telefoni, meddelandehantering [indirekt genom ip-adress], internetåtkomst och tillhandahållande av kapacitet för internetåtkomst).
– *hur* kommunikationen skedde. Exempelvis om det är frågan om fast telefoni (inkl. fast ip-telefoni), mobil telefoni (inkl. mobil ip-telefoni), SMS, MMS, e-post eller om tjänsten vidarekoppling har använts.

Lagringsskyldigheten infördes för att säkerställa att uppgifterna kommer brottsbekämpningen till del genom de aktuella tvångsmedlen. I de delar lagringsskyldigheten begränsas kommer den garantin inte att finnas kvar. Resultatet blir att myndigheterna vid bekämpning av den grova brottsligheten får hoppas på turen att operatörerna ändå har sparat uppgifterna, t.ex. för fakturering. Detta kommer i många fall att

få allvarliga följder, inte minst eftersom lagringsskyldigheten redan idag innebär att enbart ett minimum av strängt nödvändiga uppgifter ska lagras.

Lagringsskyldigheten behöver inte begränsas

EU-domstolen bygger sitt avgörande på att den svenska regleringen ”… föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter för samtliga abonnenter och registrerade användare avseende samtliga elektroniska kommunikationsmedel...” (p. 97). Den beskrivningen är felaktig. Som utredaren konstaterar kan EU-domstolens uppfattning härledas från hur kammarrätten formulerade förfrågan till EU-domstolen (p. 51), och man måste därför, som utredaren anger, tolka EU-domstolens slutsatser i ljuset av hur kammarrätten ställde sina frågor.

Många av de kommunikationsmedel som ”den moderna människan” idag använder och många av de trafik- och lokaliseringsuppgifter som operatörerna behandlar omfattas inte av lagringsskyldigheten. Exempelvis omfattas inte

– web-surf (besök på hemsida),
– kommunikation mellan två ip-adresser som inte är telefoni (t.ex. Skype- och Vibersamtal),
– internetbaserad e-post såsom hotmail och g-mail,
– FTP (filöverföring),
– chat (meddelandetjänst),
– iMessage (meddelandetjänst),
– sociala medietjänster (såsom Facebook, Twitter, Viber, Whatsapp m.fl.) och
– informationssamhällestjänster (såsom Blocket, E-bay m.fl.).

Inte heller omfattas följande uppgifter av lagringsskyldigheten.

– position när ett meddelande skickades och när det mottogs,
– position under ett mobilsamtal,
– position vid fast telefoni,
– utrustningsidentitet vid skickade och mottagna meddelanden,
– utrustningsidentitet vid fast telefoni,
– abonnemangsidentitet vid skickade och mottagna meddelanden,
– abonnemangsidentitet vid internetåtkomst,
– uppgifter om samtal med annat än vanligt telefonnummer (däribland uppringande och uppringt nummer, tid och position),

– uppgift om port och lokal ip-adress (dvs. den som används mellan abonnent och internetleverantör) vid internetåtkomst, meddelandehantering och ip-telefoni,
– uppgifter om samtal som inte kopplas fram på grund av tekniskt fel eller dylikt (däribland uppringande och uppringt nummer, tid, utrustning och position) och
– rena lokaliseringsuppgifter (positioner som inte är kopplade till kommunikation eller internetåtkomst).

Det är uppenbart att dagens lagringsskyldighet enbart innefattar en minimilista, som, redan när den kom till, bara uppfyllde de absolut mest grundläggande behoven vid utredning av grov brottslighet. Teknikutvecklingen för dessutom med sig att minimilistan relativt sett blir mindre och mindre i förhållanden till samtliga de trafik- och lokaliseringsuppgifter som operatörerna behandlar och de kommunikationsmedel som finns. Enligt vår uppfattning är lagring redan idag ett undantag och inte en huvudregel.

För oss står det klart att EU-domstolens avgörande bygger på felaktiga antaganden om hur den rättsliga regleringen förhåller sig till den tekniska verkligheten och den snabba utvecklingen på området. Lagringsskyldigheten omfattar inte på långa vägar samtliga uppgifter och kommunikationsmedel. Vi har förståelse för att utredaren valt att tolka avgörandet på det sätt han gjort. Samtidigt menar vi att det finns utrymme för att behålla dagens lagringsskyldighet oförändrad.

Att begränsa lagringsskyldigheten kan få mycket allvarliga konsekvenser

Efter EU-domstolens avgörande har operatörerna i stort slutat att lagra trafik- och lokaliseringsuppgifter för brottsbekämpande ändamål. I stället följer man huvudregeln i lagen om elektronisk kommunikation om att uppgifterna omedelbart ska raderas när de inte längre behövs i den egna verksamheten.

Tillgången till samtliga de uppgifter som lagringsskyldigheten omfattar är idag fundamental och strängt nödvändig för att Sveriges förmåga att bekämpa grov brottslighet och skydda nationella säkerhetsintressen inte ska urholkas. Tillgången fyller de absolut mest grundläggande behoven. Det kan i många fall få mycket allvarliga konsekvenser att begränsa den ytterligare.

Det är inte enbart förmågan att bekämpa brott i Sverige som kommer att påverkas negativt. Grov brottslighet är många gånger internationell till sin karaktär, vilket innebär att även det internationella

brottsbekämpande arbetet påverkas negativt. Gärningsmän reser mellan länder eller har kontakter med, och kanske styrs av, personer i andra länder. Det internationella samarbetet inom brottsbekämpning är mycket omfattande och kommer att försvåras avsevärt när man t.ex. inte längre kan hitta svenska kopplingar till gränsöverskridande grov brottslighet eller, på samma sätt som tidigare, lämna biträde när utländska myndigheter skickar rättshjälpsbegäran till Sverige.

En av orsakerna till den mycket stora betydelse som trafik- och lokaliseringsuppgifter har vid utredningar av grov brottslighet är att den information som uppgifterna ger är unik, dvs. den kan inte ges genom andra metoder. De brottsbekämpande myndigheterna har ingen möjlighet att t.ex. börja arbeta på annat sätt för att kompensera för ett bortfall.

Visst kan fysisk spaning vid något tillfälle användas i stället för att lokaliseringsuppgifter inhämtas från operatörer. Den fysiska spaningen är dock vid jämförelse en mycket begränsad och även resurskrävande metod som knappast kan kallas ett alternativ till information från operatörerna. Snarare är spaningen ibland ett komplement. Utredaren anger också det självklara att det inte går att ersätta inhämtning av historiska trafik- och lokaliseringsuppgifter med fysisk spaning i realtid.

Det sägs också ibland att kriminaltekniska undersökningar av telefoner och datorer skulle vara ett alternativt sätt för de brottsbekämpande myndigheterna att få information. Det är en sanning med modifikation. För det första är beslag ett tvångsmedel som enbart får användas under förundersökning, alltså inte i underrättelseverksamhet. För det andra är det inte alls säkert att de telefoner eller datorer som kan kopplas till brottsligheten påträffas och kan tas i beslag. För det tredje är beslag inte hemligt för den som innehar föremålet. För det fjärde är trafik- och lokaliseringsuppgifter ofta en förutsättning för att över huvud taget rättsligt och praktiskt kunna genomföra husrannsakan, beslag och andra åtgärder med lyckat resultat. För det femte kan det inträffa att informationen i telefonen eller datorn inte är helt identisk med den som ges från operatörerna. För det sjätte kan en telefon eller dator vara krypterad så att det inte går att komma åt informationen.

Kedjan av uppgifter får inte brytas

Tillhandahållandet av elektroniska kommunikationstjänster sker idag på annat sätt än när telefonitjänst tillhandahölls av Televerket som

enda operatör på marknaden. Idag kan många operatörer vara involverade i en och samma kommunikation. Till exempel kan en person ha abonnemang på fiberanslutning från en operatör, internetåtkomsten kan komma från annan och ip-telefonin från en tredje. Operatörerna behandlar enbart uppgifter om sin egen del i kommunikationskedjan. För att de brottsbekämpande myndigheterna ska kunna kartlägga kommunikationen krävs att myndigheterna får uppgifter från respektive operatör som gör det möjligt att gå vidare till nästa operatör i kedjan. Uppgifterna fungerar således som länkar som myndigheterna behöver i arbetet. Om lagringsskyldighet för en typ av uppgift tas bort kan den brygga mellan operatörerna som gör det möjligt att nå framgång försvinna. Detta påtalades också av företrädare för operatörerna i Trafikuppgiftsutredningen som en förutsättning för att kunna spåra deltagare i en kommunikation (SOU 2007:76). Den nuvarande minimilistan bygger också på den förutsättningen att kommunikationskedjan ska kunna följas.

Som exempel innebär utredarens förslag att ip-adresser ska lagras vid internetåtkomst men inte vid telefonitjänst och meddelandehantering. Om myndigheterna t.ex. har tillgång till en ip-adress som används av en viss person för internetåtkomst blir det i stort sett omöjligt att sedan knyta den adressen till telefoni- eller meddelandetjänster hos en annan operatör. Det innebär att vem personen kommunicerat med samt när, var och hur kommunikationen skedde inte kan klarläggas. Det logiska innehåll som minimilistan har bryts alltså om vissa uppgifter inte ska lagras i framtiden. Nackdelarna för brottsbekämpningen kan alltså bli än mer omfattande än man vid en första anblick kan tro när lagringsskyldigheten försvinner för vissa typer av uppgifter. Det är nödvändigt att beakta sådana negativa effekter.

Övrigt om några av förslagen

När det gäller frågan om riktad lagring är det, som utredaren anger, mycket svårt att i förväg veta när, var eller av vem ett allvarligt brott kommer att begås. Det är många gånger inte meningsfullt att i förväg rikta in lagringsskyldigheten mot vissa tider, områden eller personer. Vi instämmer med utredaren att det, vid en jämförelse, inte finns någon större nytta av en möjlighet till riktad lagring. Vi håller också med om att integritetsintrånget för de berörda personerna skulle vara påtagligt med en riktad lagring, och att sekretesskäl i princip skulle hindra att åtgärden genomförs. Orsaken till det sistnämnda är att både enskilda personer och myndigheternas verksamhet med stor sannolikhet

skulle drabbas av skada om uppgifterna behöver lämnas till samtliga omkring 600 operatörer och deras anställda. En riktad lagring, enligt EU-domstolens tanke, skulle alltså föra med sig uppenbara begränsningar i det brottsbekämpande arbetet. Till det kommer att vi instämmer i utredarens tolkning av EU-domstolens yttrande den 26 juli 2017 (1/15) om PNR-uppgifter och möjligheter till generell lagring.

Vi instämmer även i utredarens bedömning att EU-domstolens avgörande inte rör abonnemangsuppgifter utan enbart trafik- och lokaliseringsuppgifter. Vi håller med om att det är åklagare som bör fatta beslut i IHL-ärenden, när beslutsordningen ska ändras. Det är också positivt att de brottsbekämpande myndigheternas tillgång till uppgifterna även fortsättningsvis ska avse uppgifter som operatörerna sparar för egna ändamål och att lagringen inte får ske utanför Sverige.

Vidare är det positivt att utredaren föreslår att operatörernas eget val av teknisk lösning, dvs. användning av NAT-teknik, inte längre ska vara ett hinder för att identifiera vilken ip-adress en användare har tilldelats. Säkerhetspolisen har erfarenhet av att det inte har gått att identifiera målsägande på grund av att deras ip-adresser inte har kunnat knytas till en identifierbar person. Det har varit mycket olyckligt.

Det är ytterst angeläget att bestämmelser om lagringsskyldighet träder ikraft så snart som möjligt; senast den 1 juli 2018.

Ytterligare om konsekvenserna för Säkerhetspolisens verksamhet

Säkerhetspolisen arbetar mot kvalificerade aktörer

I betänkandet nämner utredaren att lagringsskyldigheten redan idag är så pass begränsad att det är möjligt för en person med högt säkerhetsmedvetande att kommunicera på ett sätt som inte lämnar elektroniska spår som omfattas av skyldigheten, och att de begränsningar som föreslås av utredaren därför inte kommer att påverka möjligheterna att utreda brott där dessa personer är inblandade.

En mycket stor del av de utredningar som Säkerhetspolisen genomför, såväl i underrättelsearbetet som i förundersökningar, har en koppling till kvalificerade aktörer som är tränade och styrda av främmande makt eller av större organisationer, exempelvis terrororganisationer. Personerna har många gånger kvalificerad utbildning i att dölja elektroniska spår. Grunden i Säkerhetspolisens arbete i sådana fall är att hitta de mönster som aktörerna har i sin kommunikation och de

avvikelser som finns eller de misstag som faktiskt görs, samt att analysera vilka slutsatser som kan dras av dessa. Sådana mönster, avvikelser och misstag ses ofta och kan bli avgörande för hur Säkerhetspolisen ska agera. Detta är kärnan i arbetet mot aktörer som är tränade och medvetna om att deras brottslighet är under bevakning och påverkas i hög grad av om möjligheten att få del av trafik- och lokaliseringsuppgifter skulle minska. Utredarens slutsats är alltså felaktig. Att begränsa Säkerhetspolisens åtkomst till trafik- och lokaliseringsuppgifter i arbetet mot kvalificerade, resursstarka, uthålliga och systematiska aktörer kan därför få mycket allvarliga konsekvenser för Sveriges säkerhet.

Uppgifterna har avgörande betydelse även i underrättelseverksamheten

En förundersökning har ett bakåtblickande perspektiv, där de brottsutredande myndigheterna försöker klarlägga vad som hände vid ett visst tillfälle. Underrättelseverksamheten har främst ett framåtblickande perspektiv, där myndigheterna ska bedöma vad som kan komma att inträffa i framtiden, allt i syfte att förebygga och förhindra brott men också att upptäcka brott som myndigheterna hittills inte har kunskap om.

Till skillnad mot vad som gäller vid Polismyndigheten får Säkerhetspolisen sällan in anmälningar från allmänheten om redan begångna brott. I stället måste myndigheten själv genom underrättelsearbetet dels ”leta upp” intressanta personer och grupperingar samt företeelser, skeenden och modus som redan är eller som senare kan komma att utvecklas till brottslighet kopplad till nationell säkerhet, dels ta ställning till bl.a. tips och hot som myndigheten får del av. Därför är underrättelseverksamheten tyngdpunkten i Säkerhetspolisens bekämpning av t.ex. spionerи och terrorism. Arbetet innebär att Säkerhetspolisen hämtar in eller får information från många olika håll samt att myndigheten bearbetar och analyserar informationen och gör en bedömning av det som kommit fram. Om det finns skäl delges resultatet utomstående, främst till svenska eller utländska myndigheter. Arbetet syftar till att brottsligheten ska förebyggas, förhindras eller i vart fall upptäckas innan den fullbordas. Ytterst är det fråga om att bedöma hur reellt ett eventuellt hot är, alltså att bekräfta eller avfärda ett misstänkt hot. Inte sällan är den bedömning som ska göras tidskritisk.

För att ge en bild av detta s.k. underrättelseflöde, där trafik- och lokaliseringsuppgifter är fundamentala vid analys och bedömning, lämnas här några verkliga exempel på uppgifter som kommer till Säkerhetspolisen relativt frekvent, både från enskilda och från svenska och utländska myndigheter. I flera fall finns både en namngiven person i informationen och en utpekad plats. Uppgifterna har anonymiserats för att inte avslöja sekretessbelagd information.

– NN var med när en person fick erbjudande om att utföra attentat mot [viss plats i Sverige]
– NN har fått uppdrag att tillverka en bomb och detonera den mot [viss byggnad i Sverige]
– NN har lämnat uppgifter till IS:s attentatsplanerare
– NN planerar att utföra attentat på okänd plats i Sverige och har tillgång till vapen
– NN sympatiserar med IS och letar efter automatvapen
– NN har stridit för IS och bygger nu upp nätverk för att planera attack i Sverige
– NN vill få tag på en bomb och döda människor i Sverige
– NN ska placera ut en bomb i [en svensk stad]
– NN ska hämnas på [vissa personer] på [viss plats i Sverige]
– NN vill använda handgranater mot [vissa personer]
– NN är ansluten till IS, ligger bakom flera attentat och gömmer sig i Sverige
– NN kommer från [visst land] och ska vara redo för ”arbete” i Sverige
– NN har uppdrag från IS att genomföra attentat i Sverige
– NN vill placera ut bomber [på vissa platser i Sverige] och ta bort [vissa personer]

En central del av underrättelsearbetet innebär att personers kontakter och rörelsemönster kartläggs, alltså att aktörer, platser och tidpunkter kopplas samman. I det arbetet har trafik- och lokaliseringsuppgifter en mycket stor och ofta avgörande betydelse. Som Säkerhetspolisen tidigare angett är uppgifterna av ovärderlig vikt för myndighetens arbete (SOU 2015:31 s. 87). Även regeringen har uttryckt att Säkerhetspolisen har ett uppenbart behov av uppgifterna för att bedriva kontraspionageverksamhet och arbete mot terrorism (prop. 2016/17:186 s. 9). Resultatet av analysarbetet kan sedan ligga till grund för strategiska beslut eller operativa åtgärder från Säkerhetspolisens eller andras sida, bl.a. i syfte att reducera ett bekräftat hot eller lagföra begångna brott. Skulle trafik- och lokaliseringsuppgifterna inte längre ges till Säkerhetspolisen kommer förmågan att exempelvis bedöma de attentatshot som ligger i uppgifterna ovan att försämras

avsevärt och i värsta fall leda till att terroristbrott, som hade kunnat förhindras, fullbordas.

Det är mot den bakgrunden av stor vikt att underrättelseverksamheten, vars mål är att förebygga och förhindra att brott över huvud taget kommer att begås i framtiden, får lika stort fokus som förundersökningsverksamheten när omfattningen av lagringsskyldigheten diskuteras. Det gäller inte minst då utredaren själv konstaterar att de försämringar i underrättelseverksamheten som blir följden av en minskad lagringsskyldighet inte kommer att kunna kompenseras med andra åtgärder i någon större utsträckning. Utredaren menar också att förslagens påverkan på underrättelseverksamheten sannolikt kommer att bli större än på förundersökningsverksamheten. För Säkerhetspolisens del är det riktiga slutsatser.

Lagringsskyldigheten och tillgången till samtliga uppgifter är strängt nödvändiga

Säkerhetspolisen har visserligen under utredningsarbetet rangordnat trafik- och lokaliseringsuppgifterna, där vissa typer generellt sett har värderats högre respektive lägre än andra. Det måste dock understrykas att lagringsskyldigheten och samtliga uppgifter som den omfattar är strängt nödvändiga i Säkerhetspolisens arbete. Det gäller inte bara i underrättelseverksamheten utan även i de förundersökningar som bedrivs inom kontraspionaget och kontraterrorismen (inkl. författningsskyddet).

Det är visserligen en självklarhet, men för att undvika missförstånd ska dock sägas att samtliga typer av uppgifter inte samtidigt är strängt nödvändiga i varje utredning. Även om behovet varierar från ärende till ärende beroende bl.a. på vilken brottslighet det är fråga om och vilka personer som är inblandade, är lagringsskyldigheten och samtliga uppgifter den omfattar av avgörande betydelse i Säkerhetspolisens arbete med brottslighet som hotar Sveriges säkerhet.

Som framgick ovan har operatörerna efter EU-domstolens avgörande i stort slutat att lagra trafik- och lokaliseringsuppgifter för brottsbekämpande ändamål. I stället raderas uppgifterna när de inte längre behövs i respektive operatörs verksamhet. Det har lett till stora problem för Säkerhetspolisen i arbetet med att skydda Sveriges säkerhet. Främmande makts illegala verksamhet mot Sverige har blivit svårare att bekämpa. Sverige har inte heller kunnat upprätthålla förmågan att upptäcka terroristnätverk och förhindra terroristattentat.

Nationell säkerhet

Den brottslighet som Säkerhetspolisen hanterar rör Sveriges säkerhet. I regeringens direktiv till utredaren (dir. 2017:16) anges att en särskild fråga är vilken effekt domen har på verksamhet som ligger inom Säkerhetspolisens ansvarsområde. Som utredaren konstaterar öppnar EU-domstolen för något mer tillåtande regler vad gäller nationell säkerhet.

Sedan EU-domstolens avgörande har terroristhotet mot Europa blivit än mer allvarligt, och Sverige har drabbats av ett fullbordat terroristattentat på Drottninggatan i Stockholm i april 2017. Det internationella samarbetet och utbytet av uppgifter mellan brottsbekämpande myndigheter är intensivt och ökar ständigt. I det arbetet är utbyte av information som har sin grund i elektroniska spår, dvs. trafik- och lokaliseringsuppgifter fundamental. Bl.a. genom sådana uppgifter har det gått att klarlägga svenska kopplingar till flera av de storskaliga terrorattacker som genomförts runt om i Europa under senare tid. Till det kommer att främmande makts verksamhet mot Sverige satts i fokus genom att frågor om kontraspionage och bristande säkerhetsskydd hos myndigheter och företag har uppmärksammats. Detta bör beaktas vid bedömningen av vilket utrymme som finns att reglera lagringsskyldigheten. För vår del saknar vi dock ett uttryckligt resonemang från utredarens sida om lagringsskyldighetens omfattning och betydelse när det gäller Sveriges säkerhet.

Närmare om innehållet i förslagen

Vem kommunicerade med vem?

Utredaren föreslår att uppgifter om *vem* som kommunicerade med vem inte längre ska lagras när det gäller fast telefoni (inkl. fast iptelefoni) och meddelandehantering via fast nätanslutningspunkt (t.ex. meddelanden från en ”fast” dator).

Uppgifter om vem som har haft kontakt med vem är fundamentala i de brottsbekämpande myndigheternas arbete med kartläggning av brottslighet, oavsett om det är fråga om förundersökning eller underrättelseverksamhet och oavsett kommunikationsmedel. Saknas de uppgifterna finns en stor risk att omständigheter missas och den vidare analysen och bedömningen får svagheter. Många gånger kommer det inte ens att finnas skäl att begära andra trafik- och lokaliseringsuppgif-

ter från operatörerna, eftersom det fortsatta arbetet med uppgifterna blir meningslöst.

Fast ip-telefoni kommer, till skillnad från den ”vanliga” fasta telefonin, inte att försvinna inom några år. Säkerhetspolisen vill understryka att fast ip-telefoni är en modern tjänst som till stor del kan jämföras med mobil telefoni. Utvecklingen går mot att all telefoni blir ip-baserad och därmed mobil i olika avseenden. Ett och samma ip-telefoniabonnemang kan utnyttjas såväl från en fast telefon som från en mobil.

Sannolikt kommer också gränsen mellan fast och mobil nätanslutningspunkt att suddas ut eller bli diffus och medföra tolkningssvårigheter. Med en utökad anslutning av optofiber till både hem och företag med möjlighet att använda samma ip-telefonitjänst både hemma och på jobbet kan det redan idag konstateras att exempelvis telefonitjänster blir mer frikopplade från både geografisk plats och fysisk utrustning. Det skulle innebära allvarliga förluster av information för brottsbekämpningen om inte lagringsskyldigheten skulle omfatta den mest moderna typen av telefoni.

Det är bl.a. på grund av det sagda förenat med en stor risk för brottsbekämpningen att göra en differentiering mellan fast och mobil telefoni, eller fast och mobil nätanslutningspunkt. Det blir svårt att överblicka följderna framöver av en sådan gränsdragning, i synnerhet på ett område som elektronisk kommunikation där den tekniska utvecklingen går mycket fort.

Det kan vid en första anblick framstå som att, vid en jämförelse med andra uppgifter, borttagandet av lagringsskyldigheten för bl.a. fast telefoni inte skulle ge en särskilt stor skadlig effekt för brottsbekämpningen. Det måste dock framhållas att det inte är ovanligt att man inom spionage- och terrorismverksamhet använder fasta telefoner. Uppgifter kopplade till fast telefoni är fortfarande strängt nödvändiga i utredningarna och om lagringsskyldigheten begränsas kan det få mycket allvarliga konsekvenser. Inte minst kan man utgå från att de kvalificerade aktörer som finns kommer att uppmärksamma en borttagen lagringsskyldighet och utnyttja den begränsningen i Sveriges förmåga att utifrån nationell säkerhet förhindra, försvåra, upptäcka och utreda brott mot Sveriges säkerhet. Att inhämta historiska uppgifter för att t.ex. identifiera de agenter som underrättelseofficerare har kontakt med kommer sannolikt att försvåras betydligt.

Avslutningsvis vill vi framålla att det är positivt att utredaren föreslår att utrustningsidentitet, som är en abonnemangsuppgift, ska lagras även i fortsättningen vid mobil telefoni. IMEI-nummer och MAC-adress är mycket viktiga för att identifiera hårdvaran som används vid

en kommunikation. De uppgifterna ger, på samma sätt som uppringande eller uppringt nummer, information om vem som kommunicerat med vem.

När skedde kommunikationen?

Utredaren föreslår att uppgifter om *när* kommunikationen skedde inte längre ska lagras när det gäller fast telefoni (inkl. fast ip-telefoni) och meddelandehantering via fast nätanslutningspunkt (t.ex. meddelanden från en ”fast” dator).

Att få uppgift om vem som kommunicerat med vem är, som nyss framgick, fundamentalt i brottsbekämpningen. Den kunskapen riskerar att få liten betydelse om inte kontakten kan knytas till en viss tidpunkt genom datum och spårbar tid då kommunikationen påbörjades och avslutades eller ett meddelande skickades och mottogs.

Det är alltså många gånger avgörande att veta tidpunkterna för en kommunikation. Uppgifterna är viktiga pusselbitar i arbetet med att klarlägga personers kontakter, relationer och beteenden, och kan visa ”närheten” mellan personer och deras ageranden vid olika händelser.

Säkerhetspolisen arbetar med att kartlägga personer som ofta är mycket skickliga på att undvika att brottsligheten upptäcks. Som exempel kommunicerar spioner och terrorister ibland genom vissa samtalsmönster. Ett missat (ej besvarat) samtal kan betyda en sak, två uppringningar och ett kort samtal något annat osv. Ett kort eller missat samtal kan vara en kodad signal om att man ska prata på annat kommunikationsmedel, ett långt samtal kan indikera att man har en närmare relation och ett samtal som sker vid en viss tidpunkt kan peka mot att det finns en medgärningsman etc. Avsaknad av denna information skulle försvåra bedömningarna betydligt och riskera att Säkerhetspolisen, även i akuta skeden, tappar förståelsen för spioners och terroristers avsikt och förmåga.

För att på ett effektivt sätt kunna lägga det pussel arbetet med Sveriges säkerhet innebär, krävs alltså tillgång till detaljerade tidsangivelser för kommunikation vid alla kommunikationsmedel. Uppgifterna är strängt nödvändiga i såväl förundersöknings- som underrättelsearbetet, och om lagringsskyldigheten begränsas kan det få mycket allvarliga konsekvenser.

Allmänt ska också nämnas något om ärenden som rör elektroniska angrepp. Där är tidsuppgifter om en aktörs internetanvändning, tillsammans med tider då ”attacker” genomförts, avgörande pusselbitar för att kunna förebygga, förhindra och utreda sådana brott med kopp-

lingar till nationell säkerhet. Cyberhot är ett prioriterat område och uppgifter om bl.a. spårbar tid är strängt nödvändiga för att bekämpa brottsligheten.

Var skedde kommunikationen?

Utredaren föreslår att uppgifter om *var* kommunikationen skedde, dvs. lokaliseringsuppgifter, inte längre ska lagras när det gäller fast telefoni (inkl. fast ip-telefoni) och meddelandehantering via fast nätanslutningspunkt (t.ex. meddelanden från en ”fast” dator). Eftersom utredaren även föreslår att uppringandes och uppringds ip-adress inte längre ska lagras, innebär det att uppgifter om var kommunikationen skedde inte heller kommer fram vid mobil ip-telefoni och vid meddelandehantering (t.ex. sms-, mms- och e-postmeddelanden) via mobil internetåtkomst.

Även uppgifter om var en viss utrustning befann sig när kommunikation skedde är fundamentala uppgifter i brottsbekämpningen. De är ofta avgörande i både förundersökning och underrättelseverksamhet och kan i vissa fall vara av större värde än uppgifter om vilka som har kommunicerat med varandra. Om Säkerhetspolisen inte längre genom lokaliseringsuppgifter kan placera en person på en viss plats vid en given tidpunkt, kan det i många fall få mycket allvarliga effekter i bekämpningen av brott kopplade till nationell säkerhet. Det blir mycket svårare att på olika sätt ingripa mot spioneri och terrorism, t.ex. genom att lokalisera brottsplatser, gärningsmän, ”safehouses”, vapengömmor, provsprängningsplatser m.m. Det kommer inte längre att gå att kartlägga hur en person rört sig över tid för att t.ex. planera, rekognosera, träffa medgärningsmän, utföra brottet, gömma sig etc. Att vara hänvisad till basstationstömningar är inte tillräckligt, bl.a. eftersom det ofta är oklart vilket geografiskt område som är aktuellt.

Inte minst i spioneriutredningar, där kvalificerade aktörer agerar, är rörelsemönster hos underrättelseofficerare och deras agenter avgörande uppgifter. I många fall kan tillgång till lokaliseringsuppgifter vara det enda sättet för Säkerhetspolisen att knyta personer till en viss plats vid en viss tidpunkt. Om uppgifterna inte lagras, skulle det göra Säkerhetspolisen nästan blind i dessa ärenden. Den negativa påverkan på Säkerhetspolisens arbete mot främmande makts underrättelseverksamhet i Sverige skulle bli mycket stor. Inom Säkerhetspolisens kontraspionageverksamhet har effekterna beskrivits som närmast oöverblickbara.

I terrorutredningar händer det mycket ofta att Säkerhetspolisen får information som anger att ett visst telefonnummer eller liknande finns i Sverige och att den som använder adressen har för avsikt att, tillsammans med andra okända aktörer, genomföra attentat i Sverige eller närliggande länder. Skulle Säkerhetspolisen vid sådana tillfällen, ofta i tidskritiska skeden, inte få tillgång till historiska trafik- och lokaliseringsuppgifter för att klarlägga positioner och kontakter kan det finnas stor risk för att misstänkta hot inte kan bedömas och reduceras.

Lokaliseringsuppgifter är alltså strängt nödvändiga i såväl förundersöknings- som underrättelsearbetet. I Ds 2014:23 (s. 52) anges att polisen bedömt att uppgifterna är extremt viktiga. Vi instämmer i det. Om lagringsskyldigheten begränsas kan det få mycket allvarliga konsekvenser.

För tydlighetens skull måste också sägas att lokaliseringsuppgifter för kommunikationens slut oftast är lika viktiga som uppgifter som rör kommunikationens början, vilket utredaren också tagit med i sitt förslag rörande telefoni via mobil nätanslutningspunkt. Om uppgifter rörande kommunikationens slut inte lagras kommer ett modus att bli att spioner och terrorister startar kommunikation med andra gärningsmän för att därefter låta samtalet vara uppkopplat under t.ex. rekognosering, bevakning av tilltänkta brottsoffer, resor, möten eller andra ”konspirativa handlingar”, allt för att undgå att lämna uppgifter om positionen i samband med att brott begås eller vid ageranden som kan kopplas till brottsligheten.

Uppgifter om vilken typ av kapacitet som den enskilde abonnerar på för att få internetåtkomst är också av grundläggande betydelse i sammanhanget (t.ex. fast fiber, xDSL, GPRS eller UMTS). Uppgifterna ger nämligen indirekt tillgång till lokaliseringsinformation. Förmågan att bekämpa brottslighet kommer alltså att påverkas negativt, eftersom utredaren föreslår att dessa uppgifter inte längre ska omfattas av lagringsskyldigheten (se även nedan).

Hur skedde kommunikationen?

Utredaren föreslår att uppgifter om *hur* kommunikationen skedde inte längre ska lagras när det gäller fast telefoni (inkl. fast ip-telefoni) och meddelandehantering via fast nätanslutningspunkt (t.ex. meddelanden från en ”fast” dator). Sådana uppgifter kan röra att det är fråga om talkommunikation, att ett e-postkonto har använts, att vidarekoppling har använts, att flera operatörer har varit inblandade i kommunikationen, att det finns en röstbrevlåda kopplad till abonnemanget eller att

samtal inte har besvarats. Vidare föreslår utredaren att uppgifter om kapacitet för att få internetåtkomst inte längre ska lagras.

Inom den brottslighet som Säkerhetspolisen bekämpar förekommer det ofta att personer vidarekopplar kommunikationen till andra adresser. Det är enkelt att vidarekoppla samtal till en fast telefon till en mobiltelefon eller liknande. En orsak kan vara att man vill dölja ageranden som har med brottsligheten att göra. Den enskilt största förlusten av en borttagen lagringsskyldighet skulle bli att möjligheten att spåra samtal som styrs till mobila telefoner upphör. Samtliga uppgifter om kommunikationen blir ”tvättade” genom de fasta telefonerna. Det skulle innebära stora nackdelar i arbetet med att spåra de nummer som faktiskt används i kommunikationen och skulle öppna en möjlighet att komma undan brottsbekämpningen genom att fasta telefoner används som bryggor som bryter spårbarheten i kommunikationskedjan. Det öppnas med andra ord en enkel möjlighet att dölja vem som är mottagare av ett samtal.

Främmande makt som bedriver olaglig verksamhet i Sverige använder ofta olika samtalsmönster för att kommunicera, i stället för att kommunicera i klartext (se ovan). Att vidarekoppla kommunikation kan vara del av det. Vidarekoppling kan också användas för att dölja positionen vid ett visst tillfälle. Det förekommer dessutom ofta att gärningsmän stänger av sin telefon inför någon aktivitet som kopplas till brottsligheten. Eventuella samtal går då vidare till annan person eller till röstbrevlådan i syfte att dölja det faktiska användandet av mobiltelefonen.

En annan tjänst som är viktig att få uppgifter om är om det finns abonnemang på röstbrevlåda och när den i så fall har varit inkopplad. Innehållet i röstbrevlådan omfattas inte av lagringsskyldigheten, men uppgiften är viktig för att bedöma om man ska gå vidare med bl.a. tillstånd till hemlig avlyssning av elektronisk kommunikation.

För Säkerhetspolisen är behovet av att veta vilken typ av kapacitet som den enskilde abonnerar på för att få internetåtkomst av grundläggande betydelse (t.ex. fast fiber, xDSL, GPRS eller UMTS). Uppgifterna ger information t.ex. om anslutningsformen är fast eller mobil, vilket i sig kan ge lokaliseringsinformation. När utredningen dessutom föreslår att lagringsskyldigheten för lokaliseringsuppgifter ska minska (se ovan), innebär borttagandet av de nu aktuella uppgifterna en dubbel negativ effekt för brottsbekämpningen. Uppgifterna kan också ge information om vem som är abonnent. Därutöver behövs uppgifterna vid verkställighet av hemlig avlyssning av elektronisk kommunikation så att rätt teknik används. Skulle hemlig dataavläsning bli tillåten i framtiden är uppgifter om kapacitet för internetåtkomst av stor bety-

delse för bedömningen av vilken teknik som ska användas i respektive fall.

Om lagringsskyldigheten skulle tas bort kommer det att bli mycket svårare att identifiera utländska hot som verkar i Sverige. Spioner och terrorister skulle få större möjligheter till säker kommunikation. Säkerhetspolisen kan med visshet säga att de möjligheter som öppnas kommer att utnyttjas av spioner och terrorister som är inblandade i brottlighet som rör Sveriges säkerhet. Uppgifterna är alltså strängt nödvändiga i såväl förundersöknings- som underrättelsearbetet. Om lagringsskyldigheten begränsas kan det få mycket allvarliga konsekvenser.

Lagringstiden

Utredarens förslag innebär att lagringstiderna differentieras utifrån hur gamla uppgifter det finns ett påtagligt behov av. Han föreslår att lokaliseringsuppgifter vid samtal ska lagras i 2 månader. Uppgifter om internetåtkomst, förutom uppgifter som identifierar utrustningen där kommunikationen slutligt avskiljs, ska lagras i 10 månader och övriga uppgifter i 6 månader.

Vi har ingen invändning i sig mot principen att lagringstiderna differentieras men kan konstatera att utredaren inte berör Säkerhetspolisen i sina resonemang.

Brott mot nationell säkerhet, som spionerі och terrorism, är speciella till sin karaktär i den meningen att brottsligheten ofta pågår under mycket lång tid.

För främmande makt kan det ta flera år att värva en agent med tillgång till skyddsvärd information. Brottsligheten är utdragen i tiden och sker i flera steg med faser som karaktäriseras av analys, målsökning, kartläggning, närmande, vänskap, värvning och inhämtning av hemlig information.

Även terrorism präglas av att brottsligheten många gånger är utdragen i tiden och att den sker i samverkan mellan flera. En process där en person utvecklas till en ideologiskt motiverad aktör med terroravsikt kan ta lång tid. Dessutom måste personen skaffa sig förmåga att planera och fullborda brott. Det sistnämnda innefattar både kunskap och materiel.

Det är ofta inte möjligt att redan i ett inledningsskede av kartläggningsarbetet förutse vilka trafik- och lokaliseringsuppgifter som bör inhämtas. Utredaren anger att behovet av äldre uppgifter än fem månader inte är särskilt stort i underrättelseverksamhet. Som utredaren

antyder gäller det inte för Säkerhetspolisen. Trafikuppgiftsutredningen nämnde att bl.a. terroristbrott är en typ av brottslighet där mer än två år gamla uppgifter behövs (SOU 2007:76 s. 173 ff.).

Vi ser positivt på att utredaren föreslår att lagringstiden för vissa uppgifter ska förlängas från sex till tio månader. Däremot ser vi, utifrån perspektivet Sveriges säkerhet, allvarligt på att tiden för lokaliseringsuppgifter vid samtal ska minskas från sex till två månader.

Vi beskrev ovan hur grundläggande uppgifter om var kommunikation skedde är i Säkerhetspolisens arbete. Uppgifterna är strängt nödvändiga i såväl förundersöknings- som underrättelsearbetet och om lagringsskyldigheten begränsas kan det få mycket allvarliga konsekvenser. Om utredarens förslag blir verklighet kommer inte enbart lagringsskyldigheten för lokaliseringsuppgifter att minska utan även lagringstiden. Vi är kritiska till detta.