Särskilt yttrande

av experterna Anders Ahlqvist och Anna Olander Selldén (Polismyndigheten), Katarina Bigovic Apitzsch (Tullverket), Carin Ewald Möller (Ekobrottsmyndigheten) samt Hans Harding (Åklagarmyndigheten)

Inledning

Grova brott orsakar stora skador för enskilda och samhället. Samhället ansvarar för medborgarnas trygghet och rättssäkerhet. Både för medborgarna i allmänhet och för brottsoffren är det angeläget att förutsättningarna för att klara upp grova brott och för att kunna förhindra brott redan på planeringsstadiet 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 (avsnitt 12.3). 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. Dessa utgångspunkter bör vara fundamentala för lagstiftarens syn på frågan om datalagring.

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.

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 oumbärliga. 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 denna nyckel kommer dörren till framgång många gånger att förbli stängd.

Lagringsskyldigheten i Sverige är redan begränsad

Utredarens uppdrag har varit att anpassa det svenska regelverket till EU-rätten såsom den uttolkas i EU-domstolens förhandsavgörande den 21 december 2016 i de förenade målen C-203/15 och C-698/15. EU-domstolen har i sin tur tolkat EU-rätten i skenet av den beskrivning av den svenska lagstiftningen som Kammarrätten i Stockholm har presenterat i sin begäran om förhandsavgörande.

Kammarrätten har i sin beskrivning av de svenska bestämmelserna om lagring av uppgifter om elektroniska kommunikation olyckligtvis gett EU-domstolen intrycket att den svenska lagrings-skyldigheten omfattar ”samtliga personer, samtliga kommunikationsmedel och samtliga trafik-uppgifter”. EU-domstolen konstaterar utifrån detta att den svenska lagstiftningen avser samtliga elektroniska kommunikationsmedel och samtliga trafikuppgifter. Den slutsatsen kan dock ifrågasättas. Sanningen är att lagringsskyldigheten omfattar endast en del därav. Det kan inte uteslutas att kammarrättens beskrivning har lett EU-domstolen fel, då domstolen i sina domskäl kommer fram till att

den svenska lagstiftningen har gjort undantaget (från principen att säkerställa konfidentialiteten för kommunikation) till huvudregel (se domskäl 89 och 97–104).

Man måste därför, som utredaren anger (avsnitt 12.4.2), 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 den svenska lagringsskyldigheten.

Exempelvis omfattas inte följande uppgifter av lagringsskyldigheten (se avsnitt 12.4.2):
– 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).

Lagringsskyldigheten omfattar inte heller
– 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,
– VPN-tjänst,
– FTP (filöverföring),
– chat (meddelandetjänst),
– sociala medietjänster (såsom Facebook, Twitter, Viber, Whatsapp m.fl.) och
– informationssamhällestjänster (såsom Blocket, E-bay m.fl.).

Som utredaren konstaterar (avsnitt 12.4.2) är det alltså långt ifrån samtliga trafik- och lokaliserings-uppgifter som omfattas av lagringsskyldigheten. Den är redan idag klart begränsad.

Lagringsskyldigheten innefattar i stället enbart en minimilista, som, redan när den kom till, uppfyllde bara de absolut mest grundläggande behoven vid utredning av grov brottslighet. Teknikutvecklingen för dessutom med sig att minimilistan relativt sett blir mindre och mindre i förhållande till samtliga de trafik- och lokaliseringsuppgifter som operatörerna behandlar och som brottsbekämpande myndigheter skulle kunna ha nytta av i sitt arbete. Sett ur denna synvinkel kan man därför ifrågasätta riktigheten av EU-domstolens beskrivning av den svenska lagstiftningen som att lagringen har gjorts till huvudregel i stället för att vara ett undantag (jfr domskäl 104). Enligt vår uppfattning är lagring redan idag ett undantag och inte en huvudregel.

EU-domstolens bedömning av vad som är en acceptabel omfattning av lagringsskyldigheten hade rimligen kunnat få ett annat utfall, om domstolen hade utgått från det riktiga förhållandet, att den svenska lagringsskyldigheten inte på långa vägar omfattar ”samtliga kommunikationsmedel och samtliga trafikuppgifter”.

Det som nu sagts innebär bl.a. att bedömningsutrymmet är stort i fråga om vad som är en acceptabel omfattning av lagringsskyldigheten. I avvägningen mellan samhällsnyttan och graden av intrång i enskildas skyddade rättigheter är vår uppfattning att det finns större utrymme för en lagringsskyldighet än vad utredarens förslag ger uttryck för.

EU-domstolen kräver en ändring av svensk rätt

Likväl går det nu inte att tolka EU-domstolens dom på ett annat vis än att den fordrar att den svenska lagstiftningen på datalagringsområdet reformeras och lagringen relativt sett begränsas. Utredarens uppdrag har således varit att utifrån tolkning av EU-domstolens dom finna en ny balans mellan tillvaratagandet av den personliga integriteten och en effektiv brottsbekämpning. Även om det förväntade resultatet av utredningen från vårt perspektiv var en försämring av datalagringen, vill vi likväl uttrycka vår uppskattning för utredarens arbete och hans ambition att bevara någon form av datalagring för brottsbekämpningsändamål värd namnet. Utredningen vittnar om ett gediget arbete utfört inom en snävt begränsad tidsram.

Synpunkter på förslagen i utredningen

Vi kommer i det följande att lämna några synpunkter på förslagen i utredningen. Vi vill med detta särskilt belysa att varje form av nedskärning av datalagring för brottsbekämpningsändamål kommer att få allvarliga återverkningar på vår förmåga att förebygga, förhindra och utreda brott.

Minskad effektivitet i brottsbekämpningen

För brottsbekämpningen i Sverige är konsekvensen av EU-domstolens tolkning av EU-rätten att effektiviteten i arbetet minskar. Detta märktes redan kort tid efter EU-domstolens dom, då flera operatörer, som en följd av domen, slutade lagra trafik- och lokaliseringsuppgifter för brottsbekämpande ändamål. Detta har för brottsbekämpningen under innevarande år redan inneburit tillkommande svårigheter att utreda grova brott såsom mord, människorov och grov narkotikasmuggling, för att nämna några konkreta exempel.

Någon enstaka operatör har tolkat EU-domstolens dom som gällande även abonnemangsuppgifter och ip-adresser och har därför slutat att lagra även dessa uppgifter. Detta har fått till följd att vissa brottstyper blivit praktiskt taget omöjliga att utreda. Det har bl.a. lämnat dörren öppen för pedofiler att straffritt ladda ner och sprida övergreppsmaterial, med andra ord att begå grovt barnpornografibrott.

En forskningsstudie som tagits fram av barnrättsorganisationen ECPAT Sverige visar att det finns ett starkt samband mellan barnpornografibrott och sexuella övergrepp på barn. Forskningen omfattade en granskning av drygt 100 avgöranden från tingsrätt och hovrätt, mellan åren 2014 och 2016. Av dessa visade det sig att de personer som dömdes för barnpornografibrott i omkring hälften av fallen (48 %) även dömdes för sexualbrott mot barn. Detta gör det än mer angeläget att säkerställa möjligheter att bekämpa denna brottstyp.

Frågan om vad som ska omfattas av begreppet abonnemangsuppgifter, och särskilt om ip-adresser omfattas av detta, har redan tidigare varit föremål för delade meningar, eftersom lagstiftningen har varit otydlig på den punkten.

Viktigt om abonnemangsuppgifter

Vi instämmer i utredarens bedömning att EU-domstolens avgörande inte rör abonnemangsuppgifter utan enbart trafik- och lokaliseringsuppgifter, och vi delar till fullo hans bedömning av vilka uppgifter som ska anses omfattas av begreppet abonnemangsuppgifter, däribland återfinns IMSI-nummer och ip-adresser. Vi välkomnar särskilt att utredaren på ett tydligt sätt slår fast att ip-adresser är abonnemangsuppgifter. Det är välgörande att utredaren tar tydlig ställning i frågan och inte lämnar fältet öppet för operatörer att tolka sin lagringsskyldighet

på ett sätt som underlättar för deras kunder att ostraffat begå brott på internet. Det är ur principiell synvinkel viktigt att möjligheten för kunderna att komma undan straffansvar inte får bli en konkurrensfördel bland operatörerna.

I detta sammanhang vill vi framhålla utredarens förslag att möjliggöra identifiering av slutanvändare vid internetåtkomst genom s.k. NAT-teknik, dvs. en teknik som låter flera användare dela på en och samma publika ip-adress. Utredaren har här identifierat en betydande inkonsekvens i nuvarande lagstiftning som är en följd av senare teknikutveckling. Enbart en skyldighet för operatörerna att lagra uppgifter för att kunna identifiera användaren av en viss ip-adress är alltså inte tillräcklig vid användning av denna teknik. NAT-tekniken innebär i nuläget att alla slutanvändare (kunder) förblir omöjliga för brottsbekämpande myndigheter att identifiera. Denna inkonsekvens har påtalats i tidigare betänkanden utan att leda fram till lagändring. För att främja teknikneutraliteten beträffande identifiering av slutanvändare vid internetåtkomst har utredaren därför föreslagit att det ska lagras uppgifter för att kunna identifiera en slutanvändare även då operatören använder NAT-teknik (se avsnitt 12.6.4). Vi är eniga med utredaren i denna del. Det är helt nödvändigt att motverka den anonymisering som användandet av NAT-tekniken innebär för slutanvändarna. Operatörens val av teknik bör rimligen inte möjliggöra för dess kunder att i skydd av anonymitet begå brott på internet.

En begränsad lagringsskyldighet är lösningen – alternativ saknas

Vi står bakom utredarens bedömning att det är möjligt att lösa uppdraget genom att föreslå en begränsad lagringsskyldighet i förhållande till idag. Vi har inte funnit något alternativ till sådan lagring som ger möjligheter att förutsättningslöst utreda brott som redan inträffat eller skaffa sig underrättelser om brottslighet som kan vara å färde. Därför har vi avfärdat möjligheten att införa någon form av sådan riktad lagring, som EU-domstolen i ett *obiter dictum* framställt som ett tänkbart alternativ till generell lagring (domskäl 108 och 111 tredje meningen). Anledningen är, som också framgår av utredningen, att en riktad lagring kräver att man redan på förhand vet var eller av vem som brott ska begås, vilket mycket sällan är fallet.

Att, som EU-domstolen föreslår (jfr domskäl 111), på förhand peka ut brottsbenägna personer eller brottsbelastade områden för en riktad lagring skulle enligt vår mening vara förenat med praktiska svårigheter och bl.a. innebära en dubbel diskriminering, där alla personer i vissa områden (dit lagringen riktas) pekas ut som mer brottsbenägna än andra (där lagring inte förekommer) samtidigt som alla personer i områden där lagring inte förekommer skulle nedprioriteras från ett brottsbekämpnings-perspektiv (där skulle grova brott inte kunna utredas lika effektivt).

Enligt vår kännedom tillämpar inte något annat land inom EU riktad lagring i likhet med EU-domstolens förslag. En plausibel anledning till detta är att en sådan form av riktad lagring helt enkelt inte anses utgöra ett effektivt brottsbekämpningsverktyg.

Det av utredaren framförda förslaget innebär, vilket han själv påpekar, att lagringsskyldigheten minskar tämligen kraftigt (avsnitt 13.1.2). Det för med sig att möjligheterna att förebygga, förhindra och utreda brott försämras. Begränsningen kommer enligt vår bedömning att få klart negativa effekter på det brottsbekämpande arbetet i Sverige. I många fall kan konsekvenserna beskrivas som mycket allvarliga.

En av orsakerna till att trafik- och lokaliseringsuppgifter har så stor betydelse vid utredningar av grov brottslighet är att den information som uppgifterna ger är unik, dvs. den kan i praktiken sällan inhämtas 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 i realtid från operatörer, men det är inget alternativ till inhämtning av uppgifter från förfluten tid. Den fysiska spaningen är 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 i avsnitt 7.2 att det i princip inte går att ersätta inhämtning av trafik- och lokaliseringsuppgifter med fysisk spaning.

Det sägs 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 kräver en sådan undersökning att telefonen eller datorn finns tillgänglig för undersökning – att den är i beslag. Beslag är dock 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, ta föremål såsom telefoner och datorer i 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 och således inte är tillförlitlig utan kanske rent missvisande. För det sjätte kan en telefon eller dator vara krypterad så att det inte går att komma åt informationen.

Risker med att bryta kommunikationskedjan

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. Alla operatörerna behandlar enbart uppgifter om sin egen del i kommunikationskedjan. För att de brottsbekämpande myndigheterna ska kunna kartlägga kommunikationen krävs att de 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. Nackdelarna för brottsbekämpningen kan alltså bli 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.

Utredaren föreslår att uppgifter om vem som kommunicerade med vem inte längre ska lagras när det gäller fast telefoni (inklusive fast ip-telefoni) 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 bevisning missas eller att den vidare analysen och bedömningen får stora svagheter. Många gånger kommer det inte ens att finns skäl att begära trafik- och lokaliseringsuppgifter från operatörerna, eftersom det vidare arbetet med uppgifterna bedöms som meningslöst.

Fast ip-telefoni kommer, till skillnad mot den ”vanliga” fasta telefonin, inte att försvinna inom några år. Vi 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.

I detta sammanhang vill vi framhålla 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.

Utredaren föreslår att uppgifter om när kommunikation skett inte längre ska lagras när det gäller fast telefoni (inklusive 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 brotts-bekämpningen. 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.

Utredaren föreslår att uppgifter om var kommunikation skedde, dvs. lokaliseringsuppgifter, inte längre ska lagras när det gäller fast telefoni (inklusive fast ip-telefoni) och meddelandehantering via fast nätanslutningspunkt (t.ex. meddelanden från en ”fast” dator). 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. Utan dessa uppgifter blir det mycket svårare att lokalisera brottsplatser, mötesplatser, gärningsmän, vapen- och narkotikagömmor.

Lokaliseringsuppgifter är alltså strängt nödvändiga i såväl förundersöknings- som underrättelsearbetet.

Som utredaren påpekar omfattar lagringsskyldigheten enligt nuvarande lagstiftning (förordningen om elektronisk kommunikation) inte lokaliseringsuppgifter vid meddelandehantering såsom sms (avsnitt 12.6.3). Detta måste bero på ett förbiseende hos lagstiftaren. Hittills har operatörerna lagrat och lämnat ut dessa uppgifter till brottsbekämpande myndigheter. Dessa uppgifter är lika viktiga som motsvarande uppgifter vid telefonitjänster (telefonsamtal). I många brottsutredningar har det visat sig att kommunikationen mellan gärningsmännen skett nästan uteslutande via sms, och utan tillgång till lokaliseringsuppgifter vid sms-kontakter hade utredningarna inte nått framgång. Vi har förståelse för att utredaren i sitt uppdrag ansett sig förhindrad att föreslå en utökning av lagringsskyldigheten i denna del, även om han anser att denna uppgift är strängt nödvändig. Om operatörerna i framtiden inte lämnar ut denna uppgift kommer dock behovet av en lagringsskyldighet för den att bli akut.

Differentierad lagringstid

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 två månader. Uppgifter om internetåtkomst, förutom uppgifter som identifierar utrustningen där kommunikationen slutligt avskiljs, ska lagras i tio månader och övriga uppgifter i sex månader.

Vi har ingen invändning i sig mot principen att lagringstiderna differentieras men kan konstatera att kortare lagringstider får negativa konsekvenser för tidskrävande utredningar av svårutredda brott.

Vi ser positivt på att utredaren föreslår att lagringstiden för vissa uppgifter ska förlängas från sex till tio månader. Detta kommer att innebära att fler ärenden kommer att kunna knytas till en misstänkt person, inte minst i barnpornografiärenden.

Ny beslutsordning i IHL-ärenden

Vi accepterar utredarens förslag till ny beslutsordning i IHL-ärenden, där åklagare ges behörighet att fatta beslut på ansökan av de brottsbekämpande myndigheterna. Vi är dock, liksom utredaren, bekymrade över att detta bryter mot principen att åklagare endast ska bedriva förundersökning och efterföljande lagföring och inte ska blanda sig i underrättelseverksamheten. Vi vill därför gärna se den föreslagna lösningen som provisorisk.

Övrigt

Vi ser det som mycket positivt att de brottsbekämpande myndigheternas tillgång till lagrade uppgifter även fortsättningsvis ska avse uppgifter som operatörerna sparar för egna ändamål och att lagringen inte får ske utanför Sverige.