Justitiedepartementet
ju.remissvar@regeringskansliet.se
Kopia till: ju.da@regeringskansliet.se
Skickas med e-post

Stockholm den 1 november 2023

Ang. Remissvar över utredningen Datalagring och åtkomst till elektronisk information, SOU 2023:22, ert dnr Ju2023/01326

HI3G Access AB (Tre) har beretts tillfälle att lämna remissvar över utredningen Datalagring och åtkomst till elektronisk information, SOU 2023:22, fortsättningsvis kallad Betänkandet.

I en allt mer digitaliserad värld utgör datalagring en viktig fråga, särskilt med hänsyn till rådande samhällsutmaningar och det ökade behovet av en effektiv brottsbekämpning. Avvägningen mellan å ena sidan brottsbekämpning och å andra sidan användarnas integritet och säkerhet m.m. är svår och bör bestämmas genom lagstiftning och rättstillämpning. Tre är och kommer fortsatt vara behjälplig med datalagring utifrån de regler som beslutas inom ramen för sin befintliga verksamhet.

Det är enligt Tre viktigt att datalagringsreglerna är tydliga och enkla att tillämpa, så att tillhandahållarna kan verkställa beslut om utlämnande av uppgifter på ett snabbt och effektivt sätt. Det är dessutom viktigt att skyldigheterna som åläggs tillhandahållarna ryms inom deras befintliga verksamhet, t.ex. så att krav på att lagra uppgifter i utpekade kommuner beaktar hur infrastrukturen faktiskt är byggd samt att krav på att dekryptera trafik åläggs då rådighet över detta med säkerhet föreligger osv.

Tre kan konstatera att de ändringar som Betänkandet föreslår, jämfört med reglerna idag, kommer göra datalagringen betydligt mer komplex, omfattande och kostsam, vilket är något som åtminstone måste återspeglas i kostnadsfördelningen mellan parterna. Tre anser också att bristande fullgörelse inte ska kunna medföra sanktionsavgift, både med beaktande av reglernas bristande tydlighet och proportionaliteten i en sådan åtgärd i övrigt.

Tre får härmed lämna följande remissvar, över valda avsnitt i Betänkandet som rör teleoperatörer. Det ska klargöras att Tre inte har någon erinran mot att s.k. Noik-tjänster omfattas av regler om datalagring.

1 Allmänna synpunkter

1.1 Invänta harmonisering på EU-nivå

Förslagen om nationell säkerhetslagring och riktad lagring kommer, om det införs, bli en mycket komplex lagstiftning både för tillhandahållare och för brottsbekämpande myndigheter. Förslaget är drivet av en rad avgöranden från EU-domstolen. För att uppnå förutsebarhet och enhetlighet för

tillhandahållarna bör frågan lösas på EU-nivå snarare än att varje medlemsstat försöker finna olika lösningar. Regeringen bör därför avvakta med lagstiftningsförslaget. Detta gör sig särskilt gällande mot bakgrund av att det inrättats en expertgrupp inom EU som ska presentera sina rekommendationer inom området för bl.a. datalagring och brottsbekämpning under år 2024. Som uppmärksammas i Betänkandet ändrades reglerna senast år 2019 på grund av EU-domstolens praxis. Uppdatering av nationella lagar om datalagring har visat sig komplicerat, vilket tydligt syns i Betänkandets förslag. När ett rättsligt ramverk ogiltigförklaras eller måste revideras har företag investerat tid, byggt tekniska system och utvecklat standarder – allt förgäves när lagar och regler revideras eller ogiltigförklaras. Utifrån detta är en EU-harmonisering det bästa sättet att hantera frågor om datalagring inom EU. Det förefaller därför mer samhällsekonomiskt försvarbart att regeringen inväntar expertgruppens rekommendationer innan de lagstiftar om datalagring och tillgång till krypterad data på nationell nivå ytterligare en gång. Tre avstyrker därför förslaget.

För det fall regeringen trots detta ändå väljer att gå vidare med förslaget vill Tre anföra följande.

1.2 Ökade kostnader för tillhandahållarna

Syftet med domarna från EU-domstolen har huvudsakligen varit att begränsa datalagringen. Tre kan dock konstatera att det förslag som lagts fram kommer innebära att det över lag kommer ske lagring av en större mängd data än tidigare, med ökade kostnader för tillhandahållarna som följd. Detta är särskilt sant vad gäller signaleringsuppgifter[1] som utgör en omfattande mängd data. Betänkandet tar upp att mängden signaleringsuppgifter som ska lagras bör preciseras närmare av Post- och telestyrelsen (PTS).[2] Tre vill här understryka att det är av särskild vikt att mer data inte lagras än vad som är absolut nödvändigt, då signaleringsdata kan vara särskilt känslig från integritetssynpunkt samt att nyttan med allt för omfattande mängd signaleringsuppgifter kan ifrågasättas då det kommer vara samma uppgifter som sparas, så är t.ex. fallet när abonnenten ligger och sover. Mobilnätet är konstruerat för att se till, givet den plats som terminalutrustningen befinner sig, att terminalen kan koppla upp sig mot den basstation som ger starkast signal och därmed bästa täckning. Signalerings-uppgifter används för detta syfte och inte för att ge exakta positioner. De kostnader som en lagringsskyldighet av signaleringsuppgifter kommer driva för tillhandahållarna är betydande.

Utöver att mängden data som ska lagras kommer att öka, medför förslaget genomgående en rörlig lagringsmängd, med olika lagringstider som kan komma att bestämmas utifrån flera faktorer så som bl.a. plats, tid, utrustning och vilka uppgifter som ska lagras. Implementeringen av ett systemstöd som klarar av denna nya och komplexa form av lagring kommer innebära omfattande kostnader.

Nationell säkerhetslagring kommer innebära att en stor datamängd kommer att lagras och givet den restriktiva hållning som föreslås kring vilka situationer som ska berättiga ett utlämnande så blir nuvarande ersättningsmodell för kostnadsdelning mellan staten och tillhandahållarna inte rimlig. Förslaget innebär även en ökad administration kring lagringsbesluten, framför allt besluten om

[1] Med signaleringsuppgifter åsyftas enligt Betänkandet ”periodiska uppdateringar, registrering- och bortkoppling från mobilnätet och andra uppgifter som genererats i syfte att initiera, upprätthålla och avsluta sessioner och tjänster under pågående internetåtkomst.” Betänkandet s. 219 f.
[2] Betänkandet s. 220.

utökad riktad lagring. Dessa administrativa kostnader kommer inte heller täckas av den rådande princip där ersättning sker för varje utlämnande.

För det fall att regeringen väljer att gå vidare med förslaget måste det först utredas hur en rimlig fördelning av kostnaderna ska ske mellan staten och tillhandahållarna. Den rådande modellen, dvs. ”ersättning per utlämnande”, skulle bli ohållbar mot bakgrund av att förslaget innebär ökad lagring, mer komplex lagring som kräver systemstöd samt ökad administration.

1.3 Sanktionsavgift vid bristande lagring

I Betänkandet föreslås det att sanktionsavgift ska kunna tas ut vid bristande efterlevnad av de nya lagringsreglerna. Sanktionsavgifter har en straffliknande karaktär.[3] Sanktionsavgift kan endast motiveras när en skyldighet är tydlig vad gäller tolkning och tillämpning, och detta gäller även om skyldigheten som sådan kan betraktas som särskilt angelägen utifrån allmänna intressen. De föreslagna reglerna kring lagring av uppgifter är dock inte alls tydliga på många punkter. Däribland kan nämnas otydligheten i hur den geografiska såväl som den utökade riktade lagringen ska verkställas, mer om detta i avsnitten 4.1 och 4.2 nedan. Tre avstyrker därför förslaget i denna del, och hänvisar i övrigt till TechSveriges remissvar med avseende på sanktionsavgifter.

2 Synpunkter gällande skyldigheten att lagra abonnemangsuppgifter

Utredningen föreslår att uppgifter om abonnemang som genereras och behandlas i tillhandahållarnas verksamhet som behövs för att identifiera en abonnent och registrerad användare ska lagras.

Lagring av abonnemangsuppgifter sker redan idag hos teleoperatörerna dels på frivillig väg, dels p.g.a. dagens lagringsskyldighet. Abonnemangsuppgifter är sådana uppgifter vars syfte är att identifiera en abonnent. Denna kategori av uppgifter har under årens lopp växt till antalet genom bl.a. rättstillämpningen. Vad som kan utgöra en abonnemangsuppgift är således inte helt klarlagt och det finns inte heller någon definition av abonnemangsuppgift i svensk rätt eller EU-rätten. I Betänkandet anges exempel på uppgifter som ska lagras i form av namn, adress, övriga kontaktuppgifter, person- eller organisationsnummer samt IMEI- och IMSI-nummer. Samtidigt anges det att uppräkningen är exempel och att listan inte är uttömmande.[4] Tre anser att förslaget saknar tydlighet i vilka abonnemangsuppgifter som ska lagras för att efterlevnad av lagringsskyldigheten i denna del ska vara möjlig. Det bör därför framgå direkt av författning vad som avses med abonnemangsuppgifter och vilka uppgifter som tillhandahållarna är skyldiga att lagra.

Tre noterar även att avtal och fakturering benämns som abonnemangsuppgifter i Betänkandet, vilket inte har tydligt stöd i varken praxis eller förarbeten. Tre ställer sig frågande till ett sådant synsätt då det snarare är dokument där abonnemangsuppgifter kan förekomma men handlingarna utgör ingen självständig uppgift.

[3] Prop. 2021/22:136 s. 381.
[4] Betänkandet s. 561 f.

3 Synpunkter på förslaget om lagring av och åtkomst till uppgifter om elektronisk kommunikation i syfte att skydda Sveriges säkerhet (”nationell säkerhetslagring”)

Utredningen föreslår regler om nationell säkerhetslagring. En sådan ska vara tillåten, om den bedöms vara absolut nödvändig för att bekämpa ett allvarligt hot mot nationell säkerhet. Säkerhetspolisen ska bedöma hotet mot den nationella säkerheten och får, om ett säkerhetshot finns, besluta om en generell och odifferentierad lagringsskyldighet.

Den lagring som föreslås för nationell säkerhet blir betydligt mer omfattande än dagens datalagring. Behovet av en sådan omfattande lagring måste analyseras noggrant och bör inte, enligt Tres uppfattning, som det huvudsakliga skälet grunda sig på vissa klargöranden i EU-domstolens praxis att EU-rätten tillåter datalagring på området.

De uppgifter som omfattas av den idag gällande regleringen om datalagring används även för ändamålet att bekämpa brott mot Sveriges säkerhet. Eftersom utredaren föreslår att möjligheten till datalagringen ska utvidgas betydligt för detta ändamål måste det också ingå i analysen att det verkligen föreligger ett sådant behov, eller omvänt att nuvarande datalagring är så pass otillräcklig och leder till att brottsbekämpande myndigheterna idag inte effektivt kan utreda dessa brott. Tre efterlyser med andra ord en mer utförligare analys av behovet som motiverar omfattningen. Som jämförelse har lagstiftaren i Danmark bedömt att lagringstiden för nationell säkerhet ska vara ett år jämfört med utredarens förslag på två år.

En väsentlig skillnad och stor brist i förhållande till dagens regler är att det inte kommer att vara förutsebart vem som faktiskt kommer att omfattas av lagringsskyldigheten, hur länge, vilka uppgifter som ska lagras samt villkoren för verkställighet eftersom den bedömningen kommuniceras när, då säkerhetspolisen fattar beslut därom, att lagring ska vidtas.

Nationell säkerhetslagring ska endast vara tillåtet när det är absolut nödvändigt för att skydda Sveriges säkerhet och det är den bedömningen som Säkerhetspolisen ska göra. Å ena sidan kan det göras troligt att lagringen i praktiken blir mer konstant eftersom det finns ett säkerhetshot riktat mot Sverige idag och sedan en viss tid tillbaka men å andra sidan ska lagringsskyldigheten bedömas löpande där det kan infalla perioder då lagringen inte är nödvändig. Om skyldighet växlar över tid är det mycket viktigt i sammanhanget att omställningen följer rimliga ledtider som är nödvändigt för att verkställa lagringsbeslutet. Lagringen kommer att kräva upphandling av tjänster och hårdvara för utökad kapacitet, projektledning, drifttester, formatanpassningar m.m. Det går därför inte som Utredaren föreslår att lagringen ska ske *utan dröjsmål* och med det skyndsamhetskravet avse samma sak som det skyndsamhetskrav som föreskrivs i 9 kap. 29 b § lagen (2022:482) om elektronisk kommunikation (LEK) om utlämnande av uppgifter till brottsbekämpande myndigheter. Innebörden av den bestämmelsen har tolkats av PTS som att kravet utan dröjsmål innebär att beslut ska kunna verkställas dygnet runt årets alla dagar.[5] När det gäller verkställighet av beslut om nationell säkerhetslagring är denna innebörd av uttrycket utan dröjsmål helt orimlig. Verkställigheten måste istället fullt ut ta hänsyn till vad som krävs för att genomföra lagringsbeslutet. Det behöver komma till uttryck i författningstext.

[5] PTS beslut från 2017-09-12 respektive 2020-03-19 med dnr: 16-2818 och 18-3920.

Om regeringen överväger att genomföra förslaget i sin presenterade form anser Tre att lagstiftningen bör vara tidsbestämd för att någon tid efter ikraftträdandet utvärdera proportionalitet, tillämpning och nytta.

4 Synpunkter på förslaget om lagring av uppgifter om elektronisk kommunikation i syfte att bekämpa grov brottslighet (geografiskt riktad lagring och utökad riktad lagring)

4.1 Geografiskt riktad lagring

Utredningen föreslår att geografiskt riktad lagring ska ske i områden där det utifrån objektiva kriterier går att konstatera att det finns en jämförelsevis större sannolikhet för förekomst av grov brottslighet än i andra områden. Geografiskt riktad lagring ska grunda sig på den officiella statistiken över anmälda brott som redovisas av Brå och med kommunerna som geografiska enheter.

Lagringsområdena för geografisk lagring kommer antagligen att vara föränderliga efter det att ny brottsstatistik har tagits fram. Komplexiteten i förslaget ligger framför allt i hur avgränsningen mellan lagringsskyldiga och icke lagringsskyldiga kommuner ska ske. Ett mobilnäts täckningsarealer följer inte kommungränserna. Det innebär att risken för ”överspillningseffekter” uppstår men även att vissa områden inte kommer att täckas upp beroende på hur mobilnätets täckningsareal varierar mot kommungränser. För utökad riktad lagring avseende ett geografiskt område anger utredaren att ”ytterst är det de behöriga myndigheterna som, med exempelvis beaktande av basstationer för telefoni eller knytpunkter för markbunden internettrafik, får avgöra hur avgränsningen ska ske”.[6] Som jämförelse har frågan hur geografisk riktad lagring ska verkställas inte berörts i Betänkandet överhuvudtaget. Tillhandahållarna fyller enbart en verkställande funktion och det måste därför finnas ett mycket tydligt utpekat område inom vilket lagring bör ske.

Om förslaget ska genomföras trots bristerna ovan anser Tre att lagringskravet måste baseras på definierade och entydiga kriterier som är kända för tillhandahållarna. Detta skulle kunna vara fallet om den geografiska riktade lagringen utgår utifrån basstationens belägenhet i en utpekad kommun, dvs. att uppgifter lagras om alla som befinner sig inom hela basstationens täckningsområde, oavsett om täckningsområdet sträcker sig över en kommungräns. Tre ser detta som det enda realistiska alternativet för att någorlunda kunna verkställa den geografiska riktade lagringen. Fortsatt kommer dock problematiken kring att mobilnätets täckningsarealer varierar, som beskrivits ovan, att bestå. Ingen lösning skulle kunna innebära en heltäckande lagring i en hel kommun.

Mot bakgrund av att det dels är otydligt i förslaget hur reglerna kring geografisk riktad lagring är tänkta att verkställas, dels de generella svårigheterna med att verkställa den lagringen som föreslås, är det olämpligt att förena en bristande lagringen med hot om sanktionsavgift. För att kunna ålägga en aktör en sanktionsavgift bör denne rimligen haft en faktisk möjlighet att efterkomma den rättsliga förpliktelsen som sanktionsavgiften grundar sig på. Tre menar att så inte är fallet med den geografiskt riktade lagring. Om lagstiftaren anser att förslaget om geografisk riktad lagring bör genomföras avstyrker Tre att sanktionsavgift ska kunna meddelas.

[6] Betänkandet s. 285 och 290.

4.2 Utökad riktad lagring

Utredningen föreslår att Polismyndigheten, Säkerhetspolisen och Tullverket ska kunna besluta om utökad riktad lagring som ska komplettera den geografiskt riktade lagringen. Utökad riktad lagring kan avse ett begränsat geografiskt område, en skyddsvärd plats, en person som dömts för grova brott, en person som har varit föremål för hemliga tvångsmedel eller en utrustnings- eller abonnemangsidentitet.

Förslaget medför en rörlig lagringsmängd med olika lagringstider som kan komma att bestämmas utifrån flera faktorer så som bl.a. plats, tid, utrustning och vilka uppgifter som ska lagras. I jämförelse med dagens generella och odifferentierade lagring blir detta en ytterst komplex form av lagring där varje beslut medför separata lagringsskyldigheter och lagringstider. Denna ökade komplexitet ökar också risken för att fel uppstår på ett påtagligt sätt.

Mot denna bakgrund kommer förslaget om utökad riktad lagring kräva en hög grad av precision och tydlighet i de beslut som fattas av myndigheterna. Besluten kommer att kunna variera avseende så många olika parametrar att det inte får råda några tveksamheter kring vad som krävs av tillhandahållaren enligt varje enskilt beslut. Det får således inte vara öppet för tolkning av tillhandahållaren vad som ska lagras, särskilt mot bakgrund av risken för sanktionsavgift (jfr ovan). Tre ser vissa risker med, så som utredningen föreslår, att det ska vara upp till myndigheterna själva att genom delegation avgöra vem som ska fatta dessa beslut. Enligt förslaget kommer det även finnas tre olika myndigheter som ska ha möjlighet att fatta beslut om utökad riktad lagring. Om tillhandahållarna ska kunna efterleva en så komplex lagringsmodell som föreslås, måste besluten, inklusive vilka uppgifter som ska lagras och hur dessa uppgifter är definierade, vara utformade på ett enhetligt och mycket tydligt sätt för största möjliga förutsebarhet. De behöriga myndigheterna bör därför åläggas att göra besluten tillgängliga i ett format som gör det enkelt för tillhandahållarna att ta hand om besluten. Tre föreslår att detta ska framgå direkt av författning i likhet med vad som gäller idag för tillhandahållarna enligt 9 kap. 29 b § 2 st. LEK. Det finns annars en överhängande risk att besluten utformas på olika sätt från myndighet till myndighet och från tjänsteman till tjänsteman. Därmed ökar risken för handläggningsfel.

I likhet med vad Tre anfört under avsnitt 4.1 innebär utökad riktad lagring för geografiskt avgränsade platser/områden att tillhandahållarna måste ha tydliga och definierade kriterier att förhålla sig till för att kunna verkställa besluten. Det måste därför tydligt framgå vilket område som avses och att det är de basstationerna inom det området där lagringen ska ske. Av detta följer, likt med geografisk riktad lagring, att området inte kommer täckas i sin helhet av de basstationerna som finns inom området. Mot bakgrund av detta är det även orimligt, av samma skäl som för geografisk riktad lagring, att sanktionsavgift ska kunna tas ut vid bristande efterlevnad vid utökad riktad lagring.

Det framgår av Betänkandet att syftet med utökad riktad lagring är att läka bristerna som uppstår med geografisk riktad lagring. Tres erfarenhet är att en mycket stor andel av de uppgifter som de brottsbekämpande myndigheterna begär avser historiska uppgifter då ett brott har begåtts och inte som ett led i underrättelseverksamheten. Detta får även stöd av Åklagarmyndighetens rapport för

tvångsmedelsanvändningen avseende år 2022.[7] Om polisen behöver kompensera för historiska uppgifter som saknas i vissa kommuner (i den geografiskt riktade lagringen) med utökad lagring skulle polisen således behöva känna till på förhand var den utökade lagringen ska riktas mot, vilket t.ex. är fallet i underrättelseverksamheten. När lagringsskyldigheten för utökad riktad lagring verkställs kommer det inte att finnas någon historisk information att tillgå. Värdet av den utökade riktade lagringen riskerar då att bli högst begränsad i utredningar då brott redan har begåtts och får framför allt ett värde i underrättelseverksamheten. Det kan därför ifrågasättas huruvida utökad riktad lagring, som får anses vara en integritetskränkande åtgärd, är proportionerlig i förhållande till den begränsade nyttan åtgärden kan komma att få.

Tre noterar att författarna av det Särskilda yttrandet till Betänkandet är av uppfattningen att beslut om personbaserad riktad lagring även bör gälla för det fall personen som beslutet rör byter tillhandahållare, under förutsättning att tillhandahållaren omfattas av beslutet.[8] Tre anser att en sådan situation, dvs. att en tillhandahållare bör omfattas av ett beslut om utökad riktad lagring trots att personen som beslutet rör inte är användare av tillhandahållarens tjänster, inte bör förekomma eftersom ett sådant beslut om utökad riktad lagring rimligen bör underkännas vid en proportionalitetsbedömning.[9] Det är nämligen ett stort integritetsintrång för den som berörs av beslutet att en tillhandahållare tar del av beslutet om utökad riktad lagring.[10] Tre anser, för det fall regeringen väljer att gå vidare med förslaget om utökad riktad lagring, att det bör tydliggöras att den som berörs av beslutet om utökad riktad lagring ska vara användare hos en tillhandahållare vid tidpunkten för beslutet för att denna tillhandahållare ska kunna omfattas av beslutet.

5 Synpunkter angående anpassningsskyldigheten

Betänkandet innehåller även en del som rör utformningen av anpassningsskyldigheten, och mera specifikt tillhandahållarnas skyldighet att säkerställa att brottsbekämpande myndigheter får innehåll i och uppgifter om krypterad kommunikation m.m. i ett läsbart format vid verkställighet av hemlig avlyssning och hemlig övervakning. Ett sådant ansvar förutsätter enligt äldre förarbeten[11] följande.

”En förutsättning i det sistnämnda fallet är givetvis att det är teleoperatören som tillhandahåller krypterings-systemet och att teleoperatören har möjlighet att dekryptera meddelandet. Teleoperatörerna bör alltså inte kunna avkrävas telemeddelandena i klartext om abonnenten själv komprimerar eller krypterar sina meddelanden.”

Med andra ord måste operatören tillhandahålla tjänsten och ha rådighet över krypteringslösningen för att anpassningsskyldighet ska kunna åläggas denne. Emellertid blir det allt vanligare att krypteringslösningen tillhandahålls av tredje man. Enligt Betänkandet ska då ansvaret bestämmas

[7] Av rapporten framgår det att antalet tillstånd som meddelats enligt HÖK uppgår till ca 13 000 medan motsvarande tillämpning av inhämtningslagen motsvarar ca 700, Åklagarmyndigheten, 2023, *Redovisning av användningen av vissa hemliga tvångsmedel under 2022*, s. 20, 64.
[8] Betänkandet s. 581.
[9] Jfr Betänkandet s. 284 och 294.
[10] Betänkandet s. 291.
[11] Prop. 1995/96:180 s. 27.

utifrån vilken av parterna, dvs. operatören eller abonnenten, som möjliggjort krypteringen.[12] Två situationer som träffar mobiloperatörer är identifierade som problematiska, dels vid s.k. inbound roaming[13], dels vid totalsträckskryptering i stand alone (SA) 5G. I båda fallen bedömer utredningen att det är mobiloperatören som tillhandahållit eller möjliggjort krypteringen och att denne därmed ska kunna ta bort densamma.[14] Utredningen menar att detta följer av 9 kap. 29 § LEK och föreslår därför ingen ändring av bestämmelsen.

Tre utvecklar sina synpunkter på utredningens bedömningar i avsnitten 5.1 och 5.2, men sammanfattningsvis avstyrker Tre Betänkandets slutsatser i den utsträckning de går längre än vad som följer av förarbetena idag. Tre delar alltså uppfattningen att operatörer ska vara skyldiga att dekryptera kundkommunikation i de fall de tillhandahållit tjänsten och förfogar över krypteringslösningen men vänder sig starkt mot de tolkningarna som Betänkandet tycks lansera, dvs. att mobiloperatörerna alltid råder över tredje mans kryptering i de aktuella fallen, liksom att de råder över kunds kryptering vid 5G SA. Att tala om totalsträckskryptering[15] som del av 5G SA leder dessutom till otydlighet om vilka situationer som avses. Som utvecklas nedan är sådana långtgående tolkningar inte rimliga, och då fullgörelse inte kan säkerställas bör inte heller sanktionsavgifter, som har straffrättslig karaktär, kunna åläggas mobiloperatörer vid bristande fullgörelse.

5.1 Inbound roaming

Tre anser inledningsvis att svenska mobiloperatörer inte är ”tillhandahållare” av den tjänst som avlyssnas m.m. vid inbound roaming, då en avtalsrelation med den utländska besökaren saknas. Tillhandahållandet görs istället av mobiloperatören i hemlandet, den s.k. hemmanätsoperatören, som erbjuder kommunikationstjänster både hemma och i utlandet. Även de tekniska förutsättningarna, såsom krypteringen, bestäms av hemmanätsoperatören.

För att hemmanätsoperatören ska kunna erbjuda tjänster i utlandet måste avtal om roaming, dvs. om nyttjande av utländska nät, träffas med bl.a. svenska mobiloperatörer. Det ska understrykas att för 4G och efterföljande teknologier (5G) innebär den etablerade tekniken som sagt att det är hemmanätsoperatören som kontrollerar krypteringen av kundens kommunikation. Även om roamingavtal ofta innehåller reciproka villkor kan en svensk mobiloperatör aldrig tvinga en roamingpartner att dekryptera kundernas trafik om denne inte vill det. Avsaknaden av rådighet är såväl rättsligt (jämför t.ex. 28 § avtalslagen) som faktiskt, då den svenska marknaden är liten jämfört med länder såsom USA och Kanada m.fl. och det svenska inflytandet i en avtalsförhandling speglar detta. Om en roamingpartner vägrar acceptera villkor om dekryptering finns det risk att inget avtal om 4G- och 5G-roaming träffas, eller att avtalet fördröjs avsevärt, och för svenska kunder vore det förödande att inte kunna kommunicera när de reser utomlands, t.ex. till USA.

[12] Betänkandet s. 412.
[13] Med inbound roaming avses situationen att en utländsk besökare använder ett svenskt mobilnät för sin kommunikation.
[14] Betänkandet s. 412 f.
[15] Totalsträckskryptering är kryptering där bara sändare och mottagare kan läsa meddelandena i klartext.

I tillägg till ovan har mobiloperatörer inom EU-rättsliga skyldigheter som står i direkt konflikt med det krav på dekryptering som nu föreslås, vilket tillgodoser ett i sammanhanget svenskt särintresse. Bl.a. är mobiloperatörerna skyldiga att skydda kommunikationen genom att ha säkerhetsåtgärder såsom bl.a. kryptering[16] på plats, för att skydda konfidentialiteten i kommunikationen och kundernas integritet. Vidare måste de ingå avtal om roaming inom EU, vilket ska ske med den bästa teknologi som erbjuds av mobiloperatören i hemlandet (4G och 5G).[17]

Betänkandet uppmärksammar också ovan nämnda svårigheter för svenska mobiloperatörer, men nämner på ett flertal ställen att ”gemensamma standarder” kan underlätta. Det är oklart vad som avses härmed men Tre tolkar detta som framför allt de avtalsbilagor till roamingavtal, innehållande villkor om dekryptering för nu aktuellt ändamål, som framarbetas inom branschorganisationen GSMA. Dylika bilagor/villkor förändrar emellertid inte svårigheterna eftersom de fortfarande kräver en frivillig överenskommelse mellan parterna.

Således anser Tre att svenska mobiloperatörer kan försöka avtala om dekryptering av utländsk trafik i svenska nät, men accepteras inte detta – vilket kan ske på goda grunder med hänsyn till bl.a. motstående regulatoriska krav – saknar mobiloperatörerna medel att säkerställa kravet på läsbart format för brottsbekämpande myndigheter. Enligt Tre vore det rimligare och mer lämpligt att svenska brottsbekämpande myndigheterna går via sina motsvarigheter i landet där hemmanäts-operatören finns och begär att denne utlämnar uppgifterna i ett läsbart format.

5.2 Totalsträckskryptering m.m.

Frågan som utredningen ska belysa är om introduktionen av 5G och de krypterings- och autentiseringsprocesser som följer därmed gör att anpassningsskyldigheten behöver ändras.[18] En referens till begreppet totalsträckskryptering antyder dock att närmast alla datatjänster som förmedlas via ett mobilt kommunikationsnät ska omfattas av dekrypteringskravet, inte bara de 5G-tjänster som normalt tillhandahålls av mobiloperatörer. Tre anser att Betänkandet har brister, då det utifrån en så bred och mångfacetterad frågeställning inte klargör vilka krypteringssituationer som är de problematiska och analyserar dessa ingående innan en slutsats dras. Istället är beskrivningarna mycket svepande, och följaktligen blir bedömningen av operatörernas rådighet alldeles för kategorisk och i delar felaktig.

Betänkandets resonemang väcker frågor såsom vilka tjänster som avses, var i värdekedjan krypteringen tillhandahålls och av vem. Det är riktigt att 5G-teknologin ökar möjligheterna för mobiloperatörer att kryptera sin egen trafik, men detta är ett extra lager utöver användartjänstens kryptering. Avlyssning av samtal och meddelanden kommer fortsatt kunna ske i ett läsbart format p.g.a. anpassningsskyldigheten. Totalsträckskryptering däremot, som avser användartjänsten ”ovanpå” kommunikationstjänsten, har mobiloperatören inte tillhandahållit och kommer därför inte kunna ta bort. Varför mobiloperatörer plötsligt ska åläggas ett ansvar för oberoende

[16] Se 8 kap. 1 § LEK och 10 kap. i PTS föreskrifter 2022:11 samt artikel 32 i Dataskyddsförordningen (EU) 2016/679.
[17] Art. 3 och 4 i Roamingförordningen (EU) 2022/612.
[18] Kommittédirektiv 2021:58 s. 11.

tredjepartstjänster och deras val av säkerhetslösning, som är ett tydligt avsteg från gällande rätt, motiveras inte i Betänkandet. En sådan radikal förändring kan inte sägas inrymmas i dagens anpassningsskyldighet.

Vidare, även om enbart kryptering i 5G SA beaktas förefaller utredningen ha utgått från ett enkelt grundscenario men berör inte alls det faktum att 5G innehåller ny funktionalitet som medför många nya användningsfall och nya affärsmodeller. Exempelvis innebär 5G att andra aktörer än mobiloperatörer kommer bygga egen infrastruktur baserat på 5G SA, s.k. privata nätverk, inom t.ex. en industri eller ett sjukhus. Ska kommunikation fungera utanför det privata nätverket kan den kopplas samman med ett nationellt mobilnät, i vilket det privata nätverket tilldelas en eller flera dedikerade kanaler (s.k. slicing). Med anledning av utredningens bedömning ska det noteras att den privata aktören då går från att vara en helt fristående tredje part till mobiloperatörens kund. Kopplas näten samman till ett s.k. hybridnät kan det vara den privata aktören som tillhandahåller och förfogar över krypteringslösningen för kommunikationen. I dylika fall är alltså Betänkandets bedömning felaktig, eftersom både vid privata nätverk och hybridnät kan mobiloperatören sakna rådighet över krypteringen av all kommunikation och kan då inte ta bort den.

Betänkandets bedömning i denna del innebär att mobiloperatörer riskerar att få ett närmast allmängiltigt ansvar för kryptering, vilket naturligtvis inte är rimligt. Tre anser att den i lagen gällande uppfattningen om operatörers ansvar måste bestå och avstyrker Betänkandets slutsatser i de avseenden de går bortom detta.

6 Några frågor om hur datalagringen och förslaget till tystnadsplikt ska förhålla sig till dataskyddsförordningens bestämmelser

Tre önskar förtydliganden om hur behandling av trafik- och lokaliseringsuppgifter samt tystnadsplikt i angelägenheter för nationell säkerhetslagring och utökad riktad lagring ska förhålla sig till den enskildes rättigheter enligt dataskyddsförordningen, bl.a. rätt till registerutdrag. I Betänkandet föreslås ytterligare bestämmelser om tystnadsplikt för ärenden om nationell säkerhetslagring och utökad riktad lagring.[19] Tystnadsplikten anges omfatta ärendet i dess helhet.[20] Frågan uppstår då om tystnadsplikten även omfattar de uppgifter som lagras och om tystnadsplikten även gäller mot den registrerade. I förslaget till behandling av trafik- och lokaliseringsuppgifter 9 kap 21 § LEK finns en ändamålsbegränsning som syftar till att tydliggöra att uppgifter som lagras för brottsbekämpande ändamål endast får behandlas för att lämnas ut för brottsbekämpande ändamål.[21] Det huvudsakliga syftet med bestämmelsen torde vara en ändamålsbegränsning och inte en begränsning av den registrerades rätt till information eller registerutdrag. Det får emellertid inte råda några tvivel om bestämmelsernas tillämpning och räckvidd, inte minst av det skälet att brott mot tystnadsplikten är straffsanktionerad (13 kap 2 § LEK).

I det här sammanhanget kan noteras att enligt 5 kap 1 § i dataskyddslagen (2018:218) ska artiklarna 13-15 i dataskyddsförordningen inte gälla sådana uppgifter som den personuppgiftsansvarige inte får

[19] Betänkandet avsnitt 7.3.9 och 8.3.7.
[20] Se Betänkandet s. 239 f.
[21] Betänkandet avsnitt 7.3.8.

lämna ut till den registrerade enligt lag. Om bestämmelser i 9 kap 21 § och eller 32 § LEK utgör en begränsning av artiklarna 13-15 i dataskyddsförordningen bör det på ett tydligare sätt komma till uttryck i författningstext. I tillägg kan nämnas att dataskyddsförordningen artikel 23.2 ställer vissa krav på nationella lagstiftningsåtgärder för dylika begränsningar.[22]

En fråga som inte berörs närmare i utredningen är om förslaget till utökad riktad lagring kan innebära att tillhandahållarna lagrar uppgifter om lagöverträdelser (artikel 10 i dataskyddsförordningen), framför allt när lagringen omfattar personer som har dömts för brott eller varit föremål för tvångsmedelsanvändning. Även om det inte är fråga om att lagra själva brottsuppgifterna så sker lagring mot bakgrund av att person dömts eller varit föremål för tvångsmedelsanvändning. Om datalagringen i det här avseendet innebär att tillhandahållarna behandlar uppgifter om brott behöver lagstödet för denna behandling komma till uttryck på ett tydligare sätt i lag eller motivuttalanden.

Josefine Jonsson Henrik Ringius

Carl-Johan Broman

[22] Se vidare EDPB, 2021, *Guidelines 10/2020 on restrictions under Article 23 GDPR Version 2.1*.