Justitiedepartementet

ju.remissvar@regeringskansliet
ju.da@regeringskansliet.se

Stockholm den 1 november 2023

Telenors svar i remiss av utredning om datalagring Ju2023/01326

Telenor Sverige AB (Telenor) lämnar följande svar i regeringens remiss av utredningen Datalagring och åtkomst till elektronisk information (SOU 2023:22)

Inledning

Telenor har vid upprepade tillfällen tvingats till stora investeringar i system för lagring av data för brottsutredning och förser dagligen brottsutredande myndigheter med tillgång till uppgifter av vikt för förebyggande och utredning av brott. Lagringskraven har ändrats med jämna mellanrum under de senaste 10 åren och varje omtag har varit mycket resurskrävande för Telenor. Föreliggande utredning föreslår stora ändringar i hur data ska lagras som bland annat innebär längre lagringstider och fler uppgiftskategorier, samtidigt som förutsättningarna för när lagring ska ske hur lagringen ska genomföras blir mer komplexa att hantera.

Vid en analys av utredningens förslag är det uppenbart för Telenor att den nya ordningen löper stor risk att underkännas vid en rättslig prövning med utgångspunkt i e-Dataskyddsdirektivet och EU:s stadga om de grundläggande rättigheterna. I förlängningen riskerar detta leda till att kraven även framgent måste ändras och att Telenor och andra lagringsskyldiga på nytt måste bygga om och anpassa relevanta system och processer.

För att skapa en hållbar lösning är det viktigt att denna gång säkerställa en EU-omfattande harmonisering som både tillgodoser de brottsutredande myndigheternas behov och tar tillräcklig höjd för det grundlagsreglerade skyddet för privatlivet och konfidentialiteten i elektroniska kommunikationer. Ett regelverk som ger förutsägbarhet och långsiktiga spelregler för marknaden är också nödvändigt för de aktörer som tvingas att lägga stora resurser på efterlevnad av lagringsskyldigheterna. Det är inte acceptabelt att dessa aktörer ska tvingas bygga om sina system så ofta som nu varit fallet med anledning av att de svenska reglerna vid upprepade tillfällen befarats strida mot grundläggande fri- och rättigheter. EU-harmoniserade bestämmelser skulle också underlätta marknadsinträde, säkerställa effektivitet och undvika snedvridning av konkurrensen.

Närmare om utredningens förslag

Allmänt om proportionaliteten i de föreslagna kraven

Telenor noterar att förslaget innebär att antalet uppgiftskategorier utökas högst väsentligt. Utredningen har inte närmare motiverat varför det är nödvändigt att så många kategorier av uppgifter ska lagras. I stället för att prioritera de uppgifter som är av störst betydelse förefaller i stället så många uppgifter som möjligt inkluderas. Detta står inte i överensstämmelse med kravet på proportionalitet, som snarare bör leda till att antalet uppgiftskategorier ska begränsas till det som kan bedömas vara strikt nödvändigt för att uppnå syftet med lagringen.

Vidare föreslås lagringstider som är väsentligt mycket längre än de som gäller för närvarande. Förslaget innebär därför lagring av extremt stora volymer data. Den stora lagringen driver kostnader, ger ökade inskränkningar i personlig integritet och innebär en berättigad osäkert kring om regelverket klarar en rättslig granskning. Inte heller de långa lagringstiderna eller avsaknaden av differentiering baserat på uppgiftskategorier har motiverats närmare av utredningen. I jämförelse har exempelvis Tyskland krav på lagring av trafikuppgifter i 10 veckor och av positioneringsuppgifter i 4 veckor. Här råder således både en begränsning i lagringstid och en differentiering som får förstås vara grundad på en avvägning mellan intresset för att förebygga och utreda allvarlig brottslighet och intresset att värna enskildas grundläggande rättigheter.

Det är också sammantaget en mycket omfattande lagring som aktualiseras då redan den riktade lagring som ska ske med hänvisning till allvarlig brottslighet är så bred att den träffar minst 70 procent av befolkningen. En så omfattande lagring är i allt väsentligt fortfarande att betrakta som generell och kan svårligen förenas med det höga krav på skydd för privatlivet och konfidentialiteten som EU-domstolen vid upprepade tillfällen hänvisat till.

Nationell säkerhetslagring

Den nationella säkerhetslagring som föreslås i betänkandet ger upphov till osäkerhet kring bl.a. när den kan aktualiseras. Utredningen ger å ena sidan uttryck för att det ska krävas exceptionella omständigheter för att lagringen ska aktiveras, men öppnar samtidigt upp för en godtycklighet som inte utesluter att denna lagring i praktiken blir permanent.

När Säpo funnit skäl för sådan lagring gäller enligt utredningen att lagringen ska kunna verkställas "utan dröjsmål". Telenor ställer sig frågande till att en sådan omfattande lagring går att verkställa utan att föregås av nödvändiga förberedelser och implementationer. Ett mer rimligt krav är att verkställigheten ska ske skyndsamt eller utan onödigt dröjsmål, där hänsyn tas till vad som är rimligt utifrån de lagringsskyldigas förmågor.

När förutsättningarna för nationell säkerhetslagring inte längre finns uppkommer fråga om de lagrade uppgifterna omedelbart ska utplånas. Utredningens förslag är inte tydligt i denna del. Vidare utgör brott mot Sveriges säkerhet sådan allvarlig brottslighet som

omfattas av brottsbalken och som kan bli föremål för hemliga tvångsmedel enligt rättegångsbalken. Det förefaller därför som befogat att inskränka nationell säkerhetslagring och åtkomsten till lagrade uppgifter till åtgärder som syftar till att förebygga, förhindra eller upptäcka hot mot Sveriges säkerhet, medan utredning kring misstanke om sådant brott ska regleras i enlighet med lagringskraven för allvarlig brottslighet.

Riktad lagring

När det gäller utredningens förslag om riktad lagring slår det Telenor hur omfattande lagringen blir. Det gäller både hänvisningen till hela kommuner som det geografiska området och till att det ska gälla kommuner som har högre brottsstatistik per capita än medelvärdet. Det kan jämföras med Danmark där den riktade geografiska lagringen inskränks till område om 3 x 3 km och att det krävs att den relevanta brottsstatistiken är 1,5 gånger högre än medelvärdet. Utredningen anger att förslaget kommer att omfatta 70 procent av Sveriges befolkning, vilket måste anses som en oproportionerligt stor andel givet EU-domstolens uttalande om att en lagring som omfatta hela eller mycket stora delar av befolkningen inte kan accepteras.

Vid en geografiskt riktad lagring kommer det bli svårt för mobiloperatörer att ta ställning till lagringsskyldigheten för abonnemang som används nära kommungränsen, då mobilnätet inte är avgränsat utifrån kommungränser utan i stället har täckning som går över sådana gränser. Inte heller det fasta nätet är uppbyggt efter kommungränser. PTS beslut om vilka områden som ska omfattas måste även ta upp dessa faktorer för att de lagringsskyldiga ska förstå detaljerna.

Såväl riktad geografisk lagring som utökad riktad lagring är komplex för den lagringsskyldige att implementera och det kommer att finnas behov av detaljerad vägledning i förarbeten och myndighetsföreskrifter med stor framförhållning innan kraven träder i kraft.

Den riktade lagringen väcker också många frågor och farhågor hänförliga till mänskliga rättigheter och integritet som bl.a. Integritetsskyddsmyndigheten, lyfter i sitt svar.

Vissa uppgiftskategorier

I avsnitten som behandlar lokaliseringsuppgifter finns otydligheter kring vilka uppgifter som behandlas i ett mobilnät (se exempelvis s. 104). Här vill Telenor understryka att mobiloperatörer inte behandlar uppgift om position som genereras i den använda terminalen. Sådan lokaliseringsuppgift (GNSS) har operatören inte tillgång till och kan följaktligen inte heller förväntas lagra den för brottsutredande eller andra syften. Det är viktigt att det klargörs i propositionen att mobiloperatörerna inte har tillgång till eller i övrig behandlar satellitbaserade lokaliseringsuppgifter som fångas upp av terminalen och inte heller andra typer av uppgifter som genereras av terminal, operativsystem eller installerade appar. Detta för att inte skapa en felaktig bild av vilka uppgifter mobiloperatören har tillgång till.

Det framstår vidare som oklart när en IP-adress ska anses utgöra en uppgift om abonnemang eller när den har karaktär av trafikuppgift. Enligt uttalande från PTS bör det vara avhängigt hur adressen tilldelats och huruvida den genereras vid

trafikfallet eller är bestämd på förhand. En IP-adress kan således omfattas av olika krav utifrån omständigheterna i det enskilda fallet, vilket regeringen gärna får utveckla i propositionen.

Anpassningsskyldighet och kryptering

Utredningen resonerar kring kryptering i samband med att anpassningsskyldigheten beskrivs. Det framstår som att utredningen anser att anpassningsskyldigheten innefattar tillgång i klartext till innehållet i kommunikation som är krypterad, oaktat om det finns rimlig möjlighet att avkryptera eller kringgå krypteringen. Förväntningen att den som omfattas av lagkraven ska bryta, försvaga eller på annat sätt kringgå krypteringen går på tvärs med gällande regulatoriska krav på säkerhet och integritet i tjänsterna och är i många fall inte önskvärt eller proportionerligt. Totalsträckskrypterade tjänster kan dessutom inte avkrypteras då kryptonyckel inte är tillgänglig för den anpassningsskyldige, utan då återstår bara åtgärden att inte tillåta totalsträckskrypterad kommunikation i nätet eller tjänsten. Att generellt neka viss trafik i nätet bara för att den är krypterad utan att det finns ett lagligt grundat beslut i det enskilda fallet, står i strid med tvingade bestämmelser om interoperabilitet, samtrafik och nätneutralitet.

Utredningen resonerar också kortfattat om kryptering i samband med internationell roaming med 4G eller 5G teknik. Utredningen menar att operatören har en långtgående skyldighet att se till att krypteringen är avaktiverad vid trafikutbyte med annan operatör. Här vill Telenor påtala att om exempelvis en mobiloperatör via roamingavtal med utländsk mobiloperatör kräver att krypteringen slås av kommer detta gälla för all inkommande trafik och innehållet exponeras då på ett oacceptabelt sätt för intrång och säkerhetsrisker. Att bara slå av krypteringen för ett enskilt samtal är inte möjligt. Därtill gäller att trafiken som regel går via en tredje part som agerar som transitopertör mellan originerande och terminerande nät. Det är således väldigt sällan fråga om direktförbindelser. En roamingpart kan av intressen för sina egna slutanvändares säkerhet och integritet vägra att slå av krypteringen och då uppstår frågan om anpassningsskyldigheten leder till att allt trafikutbyte ska upphöra. För många länder gäller att det bara finns en roamingpart i det landet och då upphör helt möjligheten att kommunicera mellan Sverige och detta land. Vidare kommer en roamingpart som accepterar att stänga av krypteringen regelmässigt kräva att samma sak ska gälla trafik som kommer från svenskt abonnemang. Då kommer svenska företag och privatpersoner som befinner sig i det landet ha all sin kommunikation exponerad, vilket inkluderar tillgång för underrättelsetjänst i auktoritär stat. Det måste anses oacceptabelt att genom en generellt uttryckt anpassningsskyldighet tvinga svenska operatörer att medverka till sådana risker för Sverige och svenska slutanvändare. En hög säkerhet och integritet i mobiltjänsterna utgör tvingande regulatoriska krav enligt LEK och kryptering är en integrerad säkerhetslösning som följer av gällande industristandarder för mobiltelefoni.

Sanktionsavgifter

Sanktionsavgifter kan på grund av sin straffrättsliga karaktär 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 inte tydliga när det gäller

de uppgiftskategorier som omfattas, de närmare förutsättningar som ska vara för handen för att lagringsskyldighet ska föreligga och hur gallring av uppgifterna ska ske. Vid tillkomsten av nya lagen om elektronisk kommunikation (2022:482) valde lagstiftaren att inte koppla sanktionsavgifter till lagringsskyldigheten och det finns inget som visar att de nu föreslagna reglerna gör skyldigheten tydligare och enklare att efterleva. Tvärtom blir skyldigheten nu ännu svårare att tolka och det kommer att krävas detaljerad vägledning för att bringa klarhet i de olika lagringsfallen och uppgiftskategorierna.

Sanktioner är inte heller motiverade utifrån tidigare erfarenheter av tillämpning av de existerande skyldigheterna för telekomoperatörer. De lagringsskyldiga operatörerna har gjort stora ansträngningar för att på ett effektivt sätt bistå de brottsutredande myndigheterna med lagrade uppgifter. Då skyldigheten nu blir än mer komplex och svår att efterleva är det direkt olämpligt att förena den med hot om sanktionsavgift. Det finns därtill en inte obetydlig risk att de nya svenska kraven på lagring underkänns vid en prövning av EU-domstolen, vilket ytterligare styrker uppfattningen att sanktionsavgifter är olämpliga. Inom ramen för tillsyn kan PTS ge vägledning och ställa upp konkreta krav förenat med hot om vite, vilket måste ses som fullt tillräckligt i de sällsynta fall det kan finnas misstanke om att en lagringsskyldig inte gör helt rätt.

Finansiella konsekvenser

Finansieringen av förslaget och verksamhetsutövarnas rätt till ersättning behöver utredas och omprövas. I dag får verksamhetsutövarna bara ersättning för kostnader som uppstår då uppgifter lämnas ut. Förslaget innebär att stora investeringar i system och processer för lagring måste göras ännu en gång och att kostnaderna för lagring och verkställighet kommer att öka avsevärt.

Skydd för nationell säkerhet och brottsbekämpning är en statlig angelägenhet. Kostnader som uppstår i sådan verksamhet bör därför som utgångspunkt finansieras av det allmänna. Att som nu är fallet de rättsliga kraven ändras flera gånger innebär att befintliga system skrotas eller måste byggas om i grunden. Vi har nu nått en gräns för hur ofta kraven kan ändras utan att staten går in och finansierar de nödvändiga investeringarna. En statlig finansiering skulle också möjliggöra en kravställning som både garanterar funktionalitet och skapar möjligheter för effektivitet baserat på stordriftsfördelar för de aktörer som upphandlar denna typ av system. Statlig finansiering för nödvändiga investeringar i datalagring är huvudregel i många andra EU-länder och det är rimligt att så också blir fallet för Sverige.

Därtill krävs en översyn av den ersättning som lämnas för själva utlämningen av uppgifter. Vad gäller säkerhetslagring så kommer den generera väldigt stora lagringsvolymer när den är aktiv och samtidigt kan antalet verkställigheter förväntas bli relativt lågt, då utredning och underrättelseverksamhet med bäring på Sveriges säkerhet mer sällan leder till utlämning av lagrade uppgifter än utredning av andra allvarliga brott. Att vidhålla dagens modell för ersättning kommer därför inte att vara hållbart för de lagringsskyldiga. I stället krävs en ersättning som reflekterar de faktiska kostnader som verkställigheten driver med hänsyn till hur kraven är utformade.

Övrigt

Telenor står till regeringens förfogande om det finns behov av ytterligare upplysningar. Telenor åberopar inte sekretess för någon uppgift i detta remissvar.

Telenor Sverige AB

Martin Sjöberg
Bolagsjurist