Er referens
Ju2023/01326
Datum
2023-11-01
Vår referens
RL

TechSverige

Justitiedepartementet
ju.remissvar@regeringskansliet.se
kopia till:
ju.da@regeringskansliet.se

Remissyttrande avseende betänkandet Datalagring och åtkomst till elektronisk information (SOU 2023:22)

TechSverige är en bransch- och arbetsgivarorganisation för företag inom techsektorn med drygt 1 400 medlemsföretag – som sammantaget har närmare 100 000 medarbetare i Sverige. TechSverige ingår i förbundsgruppen Almega och i Svenskt Näringsliv.

TechSverige har beretts tillfälle att lämna ett remissyttrande över förslagen och materialet i betänkandet.

Inledning

TechSverige välkomnar möjligheten att lämna synpunkter på utredningsarbetet och det grundliga övervägandet av dessa svåra frågor. Techbranschen ser behoven av en effektiv brottsbekämpning och skydd för nationell säkerhet och vill vara behjälpliga utifrån sina förutsättningar. Samtidigt kräver ett alltmer digitaliserat samhälle att grundläggande rättigheter avseende personlig integritet och säker kommunikation tillgodoses.

Historien gällande datalagring har visat att avvägningen mellan dessa, ibland motstående, intressen är komplicerad vilket skapat en stor osäkerhet på marknaden kring regleringen av datalagring. TechSverige ser en betydande risk att utredningens förslag inte kommer ta bort osäkerheten och skapa den långsiktigt hållbara reglering som branschen efterfrågar. Det finns i stället en uppenbar risk att utredningens förslag inte är förenligt med de avgöranden från EU-domstolen som har föranlett utredningen. I förlängningen riskerar detta leda till att en framtida reglering ogiltigförklaras med konsekvensen att omfattande investeringar och anpassningar av system och processer blir helt eller delvis bortkastade.

TechSverige uppmanar därför regeringen att inte gå vidare enligt utredningens förslag utan i stället arbeta för en lösning på EU-nivå där Sverige under ordförandeskapet drivit frågor kopplat till tillgång till data för en effektiv brottsbekämpning. En lösning på EU-nivå skulle ge en harmonisering och långsiktighet som gagnar både rättsväsendets behov av information och branschens förmåga att vara behjälplig. Ett regelverk som ger förutsägbarhet och långsiktiga spelregler för marknaden är också en viktig grundförutsättning för att bygga ett starkt och konkurrenskraftig digitalt Sverige.

TechSveriges synpunkter i korthet

- Frågan om datalagring bör drivas vidare på EU-nivå för att säkerställa en harmoniserad och långsiktigt hållbar lösning.

- Förslaget om nationell säkerhetslagring riskerar leda till en mycket omfattande lagring men är samtidigt vag och erfarenheter från andra länder visar på en risk att lagringen permanentas.

- Förslaget om riktad lagring är tveksamt avseende grundläggande rättigheter, svårt eller omöjligt att genomföra tekniskt och riskerar leda till ett lagringskrav som omfattar näst intill hela befolkningen vilket inte är förenligt med EU-rätten.

- Samhället är i allt större utsträckning beroende av säkra tekniker för att skydda information. Att som föreslås avseende anpassningsskyldigheten, bryta eller försvaga kryptering är i många fall inte önskvärt eller proportionerligt. Totalsträckskrypterade tjänster kan dessutom inte dekrypteras. Förslaget är vidare oklart avseende vilka krav som ställs kopplat till roaming.

- Offentligrättsliga sanktionsavgifter har en straffrättslig karaktär och bör inte slentrianmässigt kopplas till myndighetsutövning mot enskilda. Sanktionsavgifter kräver tydlighet vad gäller tolkning och tillämpning vilket förslaget avseende lagring inte uppfyller. TechSverige avstyrker därför förslaget om sanktionsavgift kopplat till lagringsskyldigheten

- Finansieringen av förslaget och verksamhetsutövarnas rätt till ersättning måste utredas och omprövas.

EU-harmonisering

TechSverige anser att en datalagringsskyldighet bör införas genom en EU-åtgärd snarare än genom regler på nationell nivå. Det är särskilt viktigt för att säkerställa att användarnas data omfattas av ett enhetligt och starkt skydd, undvika konflikter mellan olika nationella datalagringsbestämmelser och säkerställa effektiviteten på EU:s inre marknad. Det är tydligt att den svenska regeringen ser vinster av en harmonisering med tanke på att man varit drivande för att inrätta EU:s expertgrupp avseende tillgång till data för effektiv brottsbekämpning. Det förefaller därför logiskt att vänta på att gruppen lämnar sina rekommendationer innan medlemsstaterna lagstiftar om datalagring och tillgång till krypterade data på nationell nivå.

Uppdatering av nationella lagar för datalagring har visat sig komplicerat i EU. Ett reviderat ramverk i Tyskland (som försökte genomföra EU-domstolens anvisningar) prövades nyligen av EU-domstolen i fallet Bundesrepublik Deutschland mot SpaceNet AG (C-793/19), Telekom Deutschland GmbH (C-794/19). Det tyska ramverket där allmänna lagringsskyldigheter kräver lagring från 4 till 10 veckor ansågs bryta mot EU-lagstiftningen. På liknande sätt har belgiska lagstiftare försökt tolka EU-domstolens rättspraxis i en ny lagstiftning från 2022. Lagen har ifrågasatts av medborgarrättsgrupper och advokater, med betydande integritetsproblem som tagits upp angående förslagen att koppla skyldigheten att lagra till en användares geografiska plats.

När ett rättsligt ramverk ogiltigförklaras eller måste revideras innebär det att den tid och de pengar som investerats för att uppfylla kraven i den ursprungliga lagstiftningen blir helt eller delvis bortkastade. Detta drabbar marknadsaktörerna och i förlängningen konsumenterna men även de myndigheter som behöver justera sina processer och arbetssätt.

Sverige bör därför, snarare än att försöka individuellt lösa denna mycket svåra fråga, söka och vägleda Europeiska kommissionen för lösningar på EU-nivå. Detta kommer att bidra till en långsiktigt hållbar lösning med en högre nivå av rättssäkerhet och där svenska aktörer inte behöver bära oproportionerliga kostnader för att utveckla nya tekniska lösningar och arbetssätt. Tjänsteleverantörer som är verksamma i EU bör inte åläggas att bygga separata system för att hantera olika skyldigheter i flera jurisdiktioner. Att ha harmoniserade bestämmelser i hela EU skulle underlätta marknadsinträde, säkerställa effektivitet och öka konkurrensen inom den viktiga Techsektorn. Något som i sin tur innebär bättre förutsättningar för den digitala sektorn i Sverige och det politiska målet att vara bäst i världen på att använda digitaliseringens möjligheter.

TechSverige ser teknikneutralitet som en viktig princip och att konkurrerande tjänster i så stor utsträckning som det är lämpligt ska omfattas av samma regelverk Det är dock samtidigt viktigt att lyfta att det finns skillnader mellan telekomoperatöres tjänster och

OTT-tjänster. Det finns även betydande skillnader mellan olika OTT-tjänster. En ny långsiktigt hållbar lagstiftning bör beakta detta och ge utrymme för anpassningar.

Lagringsperiod och volymer

TechSverige anser inte att det är korrekt att såsom utredningen föreslår utöka lagringstiderna och mängden uppgiftskategorier och samtidigt säga att kraven blivit mer proportionerliga.

Utredningen har inte 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 utredningen haft som mål att så många uppgifter som möjligt ska omfattas för att ge största möjliga flexibilitet. Tillvägagångssättet är inte i linje med EU-domstolens uppfattning om att lagringen ska karakteriseras av proportionalitet. Antalet uppgiftskategorier bör därför minskas till det som kan bedömas vara strikt nödvändigt.

Förslaget innebär utökade krav i flera delar som skulle kunna generera extrema volymer när det gäller mängden data som ska lagras. Den stora lagringen driver kostnader, ger ökade inskränkningar i personlig integritet och innebär en ökad osäkert om regelverket klarar en granskning av EU-domstolen. Som tidigare berörts behövs en harmonisering mellan EU-länder vilket även gäller lagringstider för att säkerställa att den digitala inre marknaden blir verklighet. Genom att upprätta harmoniserade lagringskrav inom EU blir det lättare för användare, som rör sig mellan medlemsstater, att förstå hur deras data hanteras. Vidare undviks den betydande uppgiften för leverantörer att behöva utveckla landspecifika lagringsprotokoll baserade på dynamisk information om användarnas lokalisering (vilket inte är genomförbart i många fall).

Nationell säkerhetslagring

Den nationella säkerhetslagring som föreslås i betänkandet riskerar att leda till extremt omfattande lagring.

Det är otydligt när det ska anses föreligga tillräcklig grund för att aktivera lagringen. Erfarenheten från Danmark är att det i praktiken alltid finns ett förhöjt hot mot den nationella säkerheten och att lagringen därför blivit permanent. Samtidigt kan antalet verkställigheter förväntas bli mycket lågt, då utredning och underrättelseverksamhet med bäring på Sveriges säkerhet är mycket mer sällsynt än utredning av andra brott.

Möjligheten att besluta om lagring av många kategorier av uppgifter i kombination med en generell lagringstid på två år skulle skapa en extrem mängd uppgifter för de lagringsskyldiga att hantera. Utredningen har inte visat varför det är nödvändigt att samtliga dessa uppgifter ska lagras i 2 år. Detta är inte i överensstämmelse med EU-domstolens krav på differentierad lagring och hänvisningarna till proportionalitet. En lagringstid på 2 år som tillämpas generellt för alla typer av uppgifter är oproportionerlig, givet de ingrepp i den personliga integriteten som aktualiseras och de kostnader som är förknippade med en så omfattande lagring.

I utredningen lämnas förslag på att lagringen ska kunna verkställas “utan dröjsmål”. Verkställighet av utlämnande och verkställighet av lagring i denna omfattning är väsensskilt från varandra eftersom ett föreläggande om lagring kräver helt andra ledtider (till exempel planering, inköp av kapacitet, bemanning, tester etc.). Ett motsvarande skyndsamhetskrav som vid utlämnande av uppgifter är varken rimligt eller proportionerligt. Detta gäller även beträffande beslut om riktad lagring. Ett mer rimligt och proportionerligt krav är därför att verkställighet av lagring ska ske ”utan onödigt dröjsmål”.

Riktad lagring

I utredningen föreslås så kallad riktad lagring. Detta är något som har kritiserats ur olika perspektiv av medborgarrättsgrupper, integritetsexperter och tjänsteleverantörer. Att exempelvis behålla en användares uppgifter endast när de befinner sig i ett område med hög brottslighet är tekniskt svårt och omöjligt för de som tillhandahåller nummeroberoende kommunikationstjänster. Nedan redogör TechSverige för några av de tekniska utmaningarna och osäkerheterna kopplade till materialet om riktad lagring.

Många tjänsteleverantörer samlar inte in metadata för plats, andra kan samla in viss information som kan indikera plats – till exempel IP-adresser – medan andra samlar in GPS-data men bara när användaren samtycker till att göra det, och endast när användarens enhet är GPS-kompatibel. Även om IP-geolokalisering kan ge en ungefärlig plats som är tillräcklig för att fastställa det land som användaren loggar in ifrån, är dessa data inte tillräckligt exakta för att stödja insamling och lagring för geoinhägnade platser. Vidare försvåras möjligheten att fastställa en användares plats med hjälp av IP-geolokaliseringsdata genom användning av VPN, företagsnätverk och andra metoder för att dölja en användares IP-adress. GPS-data från GPS-kompatibla enheter är helt beroende av att användare möjliggör åtkomst till platsdata, vilket användare rutinmässigt blockerar. Eventuella nya regler bör uttryckligen föreskriva att leverantörer, om det är tekniskt omöjligt att tillämpa geografiskt inriktade lagringsprotokoll, inte är skyldiga att genomföra dessa nya bestämmelser.

När det gäller uppgiftskategorier är det otydligt när en IP-adress ska anses utgöra en uppgift om abonnemang eller när den har karaktär av trafikuppgift. Det förefaller vara avhängigt hur adressen tilldelats och huruvida den genereras vid trafikfallet. En IP-adress kan således omfattas av olika krav utifrån omständigheterna i det enskilda fallet.

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.

Vad gäller utökad lagring begränsat till en plats eller ett geografiskt område så anger utredaren att ”ytterst får lagringen utformas med beaktande av platsens belägenhet och karaktär samt tillhandahållarens infrastruktur. Beslutet bör dock vara tillräckligt preciserat för att tillhandahållarna ska kunna verkställa beslutet” (s. 285 och 290). Frågan är hur bedömningen av avgränsning är tänkt att ske i praktiken. Enligt förslaget om den proportionalitetsbedömning som en brottsbekämpande myndighet ska göra i sitt beslut om utökad riktad lagring finns det inte någon begränsningsregel kopplad till beslutets geografiska räckvidd. Även de tekniska förutsättningarna för lagringen bör uttryckligen beaktas vid ett beslut om utökad riktad lagring.

Anpassningsskyldighet och kryptering

Staten vill med rätta skydda människor från kriminella handlingar, men det är samtidigt viktigt att väga in att det inte går att försvaga krypteringen för en aktör utan att säkerheten riskerar att påverkas för alla. TechSverige anser inte att konsekvenserna av detta har beskrivits tillräckligt i utredningen och vill därför belysa några viktiga aspekter kopplat till utredningsmaterialet om anpassningsskyldigheten och kryptering.

I lagförslaget föreslås bland annat att leverantörer ska vara skyldiga att ge tillgång till innehållet i kommunikation som är totalsträckskrypterad. Att som föreslås bryta eller försvaga kryptering är i många fall inte önskvärt eller proportionerligt. Totalsträckskrypterade tjänster kan dessutom inte dekrypteras. Det kräver att leverantören har en nyckel, vilket skulle göra att det inte längre är totalsträckskryptering.

Att bryta kryptering ger upphov till sårbarheter som äventyrar användares integritet och säkerhet. Vi har sett hur illvilliga aktörer har gjort sitt bästa för att hitta sätt att utnyttja dessa sårbarheter. Experter på området är eniga om att bakdörrar inte bara kan byggas för brottsbekämpning, utan snarare blir det en bakdörr för alla. Det kan också noteras att i det nu antagna NIS2-direktivet (EU 2022/2555, rec 98) så framgår att totalsträckskryptering med avseende på elektroniska kommunikationer är en kritisk teknik för ett effektivt dataskydd, integritet och kommunikationssäkerhet som inte bör försvagas av medlemsstaternas befogenheter när det gäller brottsbekämpning och skydd för nationell säkerhet. I propositionen Hemlig dataavläsning (prop. 2019/20:64) gör regeringen närliggande bedömningar och konstaterar att ”kräva av teknikföretag och tjänstetillhandahållare att de ska kunna gå förbi säkerheten i sina egna system och tjänster för att bistå brottsbekämpningen, t.ex. genom att använda bakdörrar.” inte är ett alternativ då ”riskerna med en sådan lösning är svåra att bedöma men det kan antas att så snart det är möjligt för någon att gå förbi säkerhetslösningar så torde likadana möjligheter öppnas även för andra, också kriminella, vilket kan medföra stora risker för såväl informationssäkerheten som för den personliga integriteten.” Vidare så övervägs om det är ett alternativ att ”systematiskt arbeta med att försvaga krypteringslösningar eller standarder för kryptering.” och konstaterar ”Att generellt eller systematiskt försvaga krypteringslösningar för att komma åt uppgifter kan få stora återverkningar på hela den legitima användningen av den moderna tekniken”

I övervägandena kring anpassningsskyldigheten resonerar utredningen kortfattat om kryptering i samband med internationell roaming och kommunikation via moderna säkra mobilnät med 4G eller 5G. Utredningen menar att operatören redan enligt den befintliga anpassningsskyldigheten har en långtgående skyldighet att se till att krypteringen är avaktiverad vid trafikutbyte med annan operatör, till exempel genom att reglera denna fråga i avtal.

TechSverige menar att frågan inte är utredd på ett tillfredställande sätt och att konsekvenserna för integritet och säkerhet inte beskrivs vilket är en stor brist. Det är inte möjligt för en svensk mobiloperatör att ”säkerställa” dekryptering av en utländsk mobiloperatörs tjänster genom ett avtal, då rättsliga medel att avkräva en sådan ändring saknas. Även de faktiska förutsättningarna kan vara begränsade. 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. 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 ifrån Sverige. Då kommer svenska företag och privatpersoner som befinner sig i det landet ha all sin kommunikation exponerad för bland andra underrättelsetjänsten i det landet. Det måste anses oacceptabelt att genom en generellt uttryckt anpassningsskyldighet tvinga svenska operatörer att medverka till sådana risker för Sverige och svenska slutanvändare.

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 lång lagringstiden ska vara.

Vid tillkomsten av nya lagen om elektronisk kommunikation (LEK) 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 måste därtill anses finnas en överhängande risk att de svenska kraven på lagring underkänns vid en kommande 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. TechSverige avstyrker därför förslaget om sanktionsavgift kopplat till lagringsskyldigheten.

Behov av reform av regler om ersättning

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, beräknad enligt schablon. Förslaget innebär att lagringskostnaderna kommer att öka avsevärt, även de administrativa kostnaderna med att verkställa lagringen.

Skydd för nationell säkerhet och brottsbekämpning är en statlig uppgift. Kostnader som uppstår i sådan verksamhet bör därför som utgångspunkt finansieras av det allmänna. Om nyttan ökar för brottsbekämpande myndigheter med tillgång till fler uppgifter med en effektivare tvångsmedelsanvändning så bör staten vara med och betala för den ökade nyttan som tillgången till uppgifter medför.

Vad gäller säkerhetslagring så kommer det att sannolikt generera väldigt stora lagringsvolymer. Samtidigt kan antalet verkställigheter förväntas bli mycket lågt, då utredning och underrättelseverksamhet med bäring på Sveriges säkerhet är mycket mera sällsynt än utredning av andra brott. Att vidhålla dagens modell för ersättning, dvs. att ersätta kostnad för utlämning men inte investeringar och förvaltningskostnader, blir därmed ohållbart. Detta gäller även vid utökad lagring. Det är inte säkert att uppgifterna begärs ut och då (enligt nuvarande ersättningsmodell) uteblir ersättning helt.

För TechSverige

Christina Ramm-Ericson
näringspolitisk chef

Robert Liljeström
näringspolitisk expert