

2025.01.17

Er referens
Ju2024/02286
Vår referens
RLJustitiedepartementet
ju.remissvar@regeringskansliet.sekopia till
ju.da@regeringskansliet.se

Remissvar avseende Utkast till lagrådsremiss datalagring och tillgång till elektronisk information

TechSverige har beretts tillfälle att lämna ett remissvar avseende rubricerat betänkande (dnr Ju2024/02286). TechSverige är en bransch- och arbetsgivarorganisation för företag inom techsektorn med cirka 1 400 medlemsföretag – som sammantaget har närmare 100 000 medarbetare i Sverige. TechSverige ingår i Svenskt Näringsliv.

TechSverige välkomnar möjligheten att lämna synpunkter på utkast till lagrådsremiss datalagring och tillgång till elektronisk information. Techbranschen ser behoven av en effektiv brottsbekämpning och skydd för nationell säkerhet och vill vara behjälpliga utifrån branschens förutsättningar. Samtidigt kräver ett alltmer digitaliserat samhälle att grundläggande rättigheter avseende personlig integritet och säker kommunikation tillgodoses.

Ett centralt perspektiv att ta hänsyn till vid utformning av ny lagstiftning som påverkar digital infrastruktur och digitala tjänster är att flera rapporter¹ enstämmigt pekar på att Europa står inför stora utmaningar avseende konkurrenskraft beroende på att vi inte håller samma takt i den digitala utvecklingen jämfört med framförallt USA och Asien.

En avgörande faktor som lyfts fram är att komplexa regelverk och bristen på harmonisering inom EU försvårar och fördröjer den digitala utvecklingen. Det är därför av största vikt att utforma regelverk som kan kombinera en effektiv brottsbekämpning med villkor som underlättar för företag att utveckla den digitala infrastruktur som är avgörande för Sverige och Europas långsiktiga konkurrenskraft och ekonomiska utveckling.

Med denna utgångspunkt lämnar TechSverige nedan kommentarer på valda delar av utkastet till lagrådsremiss. Därutöver hänvisas till tidigare inlämnat remissvar på betänkandet Datalagring och åtkomst till elektronisk information (SOU 2023:22).

Riktad lagring

TechSverige välkomnar att utkastet inte innehåller utredningens förslag till så kallad riktad lagring. Tidigare remitterade förslag om riktad lagring skulle innebära stora svårigheter eller vara omöjliga att genomföra rent tekniskt. Förslagen skulle leda till

¹ The future of European competitiveness – A competitiveness strategy for Europe, <https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en#paragraph_47059> och Much more than a market, <<https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf>>.



kraftigt ökad komplexitet och ökade kostnader vilket har en tydlig negativ effekt på sektorns utveckling.

Samtidigt är det dock viktigt att poängtera att utkastet till lagrådsremiss därmed inte behandlar den nuvarande problematiken med en generell lagring för brottsbekämpning. EU-domstolen har i ett antal avgöranden om datalagring på senare år slagit fast att generell och odifferentierad datalagring som huvudregel inte kan accepteras inom EU, med hänvisning till EU:s stadga om de grundläggande rättigheterna och det s.k. ePrivacy-direktivet. Kommer regeringen återkomma med förslag längre fram för att säkerställa att Sveriges datalagring för brottsbekämpning är i linje med EU- domstolens anvisningar?

Otydligheten kring de långsiktiga spelreglerna och kraven gällande datalagring skapar osäkerhet, merkostnader och försvårar möjligheterna att effektivt investera i system som bidrar till utvecklingen av ett säkert digitalt Sverige i framkant.

Vikten av proportionalitet och möjligheten till effektivitet och kostnadstäckning

Skydd för nationell säkerhet är en statlig uppgift och specifika kostnader som uppstår för sådan verksamhet bör finansieras av det allmänna. Säkerhetslagring kommer generera betydande kostnader för att förbereda system som ska stå redo att aktiveras för lagring om behov uppstår. Användningen av systemet kan förväntas bli mycket lågt (om lagringen överhuvudtaget aktiveras), då utredning och underrättelseverksamhet med bäring på Sveriges säkerhet är mera sällsynt än utredning av andra brott. Med dagens ersättningssystem uteblir ersättning helt om systemet inte aktiveras eller inga uppgifter begärs ut. Hela merkostnaden riskerar att hamna på marknadsaktörerna som inte har någon kontroll eller kan påverka möjligheten till kostnadstäckning. Förutom en orimlig börda för marknaden ger det också en stor osäkerhet om möjligheten till kostnadstäckning för tagna investeringar.

Vidare finns det kostnadsmässiga frågor som utkastet inte besvarar. I utkastet finns det bestämmelser som tydliggör när uppgifter som lagras för nationell säkerhet får inhämtas och lämnas ut. Det finns däremot en otydlighet i förslaget kring frågan om hur uppgifterna som lagras för nationell säkerhet ska vara lagrade i förhållande till den ordinarie lagringen. De olika ändamålen och omfattningen av den nationella säkerhetslagringen respektive den ordinarie lagringen ger intrycket av att det skulle finnas ett krav på separerad lagring.

Om avsikten med regleringen är att uppgifterna som lagras för nationell säkerhet ska vara lagrade helt separerade från den ordinarie datalagringen kommer detta innebära åtminstone dubbla kostnader t.ex. i form av lagringsutrymme för tillhandahållarna i jämförelse med dagens kostnader. En sådan begränsning i tillhandahållarnas möjligheter att effektivisera lagringen gör den kostnadsfördelning som föreslås i utkastet än mer orimlig, eftersom kostnadsfördelningen i dag motiveras av att den som kan hålla kostnaderna nere också är den som ska stå för dem.²

Tillåter reglerna däremot att tillhandahållarna kan lagra uppgifterna för den ordinarie datalagringen och den nationella säkerhetslagringen tillsammans men i stället sorterar ut uppgifterna vid utlämnandet, t.ex. med hjälp av behörigheter och filtrering, skulle kostnaderna kunna hållas nere i högre grad. Oavsett bör regeringen uttala sig om hur

² Jfr Utkast till lagrådsremiss Datalagring och tillgång till elektronisk information s. 107



reglerna är avsedda att tolkas i denna del och kostnadsfördelningen mellan aktörerna bör anpassas därefter.

För att undvika att den nationella säkerhetslagringen blir en börda som påverkar utvecklingen av Sveriges digitala infrastruktur negativt krävs en flexibilitet i utformningen i systemen för lagring samt ett nytt ersättningssystem som garanterar kostnadstäckning för tillkommande investeringar och förvaltningskostnader.

Nya krav på datalagring bör vidare vara vederbörligen kalibrerade med leverantörernas rätt till näringsfrihet (som garanteras i artikel 16 i Europeiska unionens stadga om de mänskliga rättigheterna). Det torde innebära undantag för företag som tar emot ett lågt antal dataförfrågningar från brottsbekämpande myndigheter, t.ex. små och medelstora företag eller B2B-leverantörer. Bördan för dessa företag när det gäller deras näringsfrihet skulle sannolikt inte stå i proportion till fördelarna i kampen mot grov brottslighet. I synnerhet för företagskunder får skyldigheten att lagra uppgifter inte gå utöver huvudhyresgästens uppgifter, eftersom den annars oavsiktligt skulle kunna leda till lagring av uppgifter om upp till tusentals enskilda anställda, vilket uppenbarligen inte skulle vara proportionerligt.

Förutsägbarhet och harmonisering för ett konkurrenskraftigt digitalt Sverige

TechSverige har i tidigare remissvar framfört att en datalagringskyldighet bör införas genom en EU-åtgärd snarare än genom regler på nationell nivå. I utkastet till lagrådsremiss konstateras det också att *”det är möjligt att en harmoniserad EU-reglering skulle underlätta bland annat marknadsinträde, säkerställa effektivitet och främja konkurrensen på området”*. Vi delar till fullo denna analys, särskilt för leverantörer som erbjuder tjänster över medlemsstaternas gränser och som för det mesta inte kan implementera olika lagringsskyldigheter i EU, utan att samtidigt bryta mot sina skyldigheter i fråga om uppgiftsminimering enligt GDPR. Utredningen pekar sålunda på flera av de faktorer som är avgörande för utvecklingen av konkurrenskraftigt digitalt EU och Sverige.

Det är vår rekommendation att man fortsätter arbetet med frågorna på EU-nivå för att uppnå både ökad harmonisering mellan länder och teknikneutralitet så att konkurrerande tjänster i så stor utsträckning som det är lämpligt omfattas av samma regelverk. En ny långsiktigt hållbar lagstiftning bör samtidigt beakta att det finns betydande skillnader mellan olika kommunikationstjänster och ge utrymme för anpassningar.

Vi delar inte uppfattningen att en EU-harmonisering i dess helhet inte kan förväntas i närtid. Så sent som den 12 december 2024 godkände Europeiska unionens råd slutrapporten från högnivågruppen för tillgång till uppgifter för en effektiv brottsbekämpning, som tillsattes 2023.³ I rådets [pressmeddelande](#) uppmanas kommissionen att senast under första halvåret 2025 utarbeta en färdplan för genomförandet av konkreta åtgärder för att garantera tillgång till data för en effektiv

³ Concluding report of the High-Level Group on access to data for effective law enforcement, <https://home-affairs.ec.europa.eu/document/download/4802e306-c364-4154-835b-e986a9a49281_en?filename=Concluding%20Report%20of%20the%20HLG%20on%20access%20to%20data%20for%20effective%20law%20enforcement_en.pdf>.



brottsbekämpning, med en tydlig tidsplan och ansvarsområden och som även omfattar resursaspekter.⁴

Etablerandet av ett harmoniserat EU regelverk inom datalagring för brottsbekämpning är en tydlig prioritet från högnivågruppen. Utifrån detta anser TechSverige att regeringen bör undersöka förutsättningarna för ett harmoniserat EU regelverk för datalagring och tillgång till elektronisk information innan man går vidare med ett slutligt förslag. Detta är särskilt viktigt eftersom om varje medlemsland går före EU-kommissionen skulle det skapas ett lapptäcke av datalagringskrav som är tekniskt omöjligt att implementera. Det skulle motverka att vi etablerar en digital inre marknad i EU vilket behövs för tillväxt och konkurrenskraft av digitala tjänster.

Bortsett från potentiellt motstridiga krav på lagring i olika medlemsstater, riskerar Sverige att EU-domstolen underkänner ett nationellt initiativ som går före harmonisering på samma sätt som man gjort med andra medlemsländer. Detta skapar osäkerhet och riskerar leda till merkostnader för de aktörer som ska implementera lösningar för att uppfylla kraven i lagstiftningen men även för de brottsbekämpande myndigheter som ska använda data i sitt arbete.

Risker med att försvaga och bryta kryptering

I tidigare inlämnat remissvar avseende betänkandet Datalagring och åtkomst till elektronisk information (SOU 2023:22) lyfter TechSverige riskerna med att försvaga och bryta kryptering. Vi har sett hur effektiva illvilliga aktörer är på att identifiera och utnyttja sårbarheter i digitala kommunikationssystem. Under senare tid har även experter uppmanat till en ökad användning av totalsträcks-krypterad (end-to-end) kommunikation. TechSverige vill därför trycka på vikten av tydliga skydd för krypterad kommunikation så inte lagstiftningen skapar sårbarheter som kan nyttjas av illvilliga aktörer.

För TechSverige

Christina Ramm-Ericson
näringspolitisk chef

Robert Liljeström
näringspolitisk expert

⁴ Access to data: Council calls for challenges for law enforcement to be addressed, <<https://www.consilium.europa.eu/en/press/press-releases/2024/12/12/access-to-data-council-calls-for-challenges-for-law-enforcement-to-be-addressed/>>.