2023-10-31

Justitiedepartementet

103 33 Stockholm

Yttrande/Remiss över SOU 2023:22 ”Datalagring och åtkomst till elektronisk information”

Ju 2023/01326

Beredda möjlighet därtill lämnar 5 juli-stiftelsen (”Stiftelsen”) följande remissvar:

Stiftelsen konstaterar att utredningen inte håller sådan kvalitet att den kan ligga till grund för lagstiftning. Bland annat bygger delar av betänkandet på missuppfattningar om hur internet- och telekommunikationer fungerar. Vidare konstateras att förslaget är oproportionerligt, strider mot skyddet av privatliv och privata kommunikationer, och med stor sannolikhet strider mot unionsrätten.

Med hänvisning till ovanstående *avstyrker* Stiftelsen förslaget.

Nedan utvecklas grunderna för Stiftelsens ställningstagande.

Om utredningen

Stiftelsen konstaterar inledningsvis att utredningen inte håller en sådan kvalitet att den kan ligga till grund för lagstiftning. Bland annat förefaller erforderlig teknisk kompetens saknas. Flera av de förslag som läggs fram är till sin natur ogenomförbara eller skulle ge oacceptabla konsekvenser för infrastrukturen eller kommunikationernas funktionssätt – detta utan att det senare överhuvudtaget berörs.

Några exempel på när utredaren bortsett ifrån eller inte förstått hur tekniken fungerar ges nedan:

Utredaren föreslår att operatörer på begäran ska spara innehållet i totalsträckskrypterad kommunikation. Detta är inte möjligt då totalsträckskrypterad definitionsmässigt innebär att andra än sändaren och mottagaren inte har tillgång till den. Det är möjligt att utredaren helt vill förbjuda sådana säkra kommunikationer eller tvinga fram bakdörrar. Båda delarna skulle innebära betydande risker för säkerheten på internet och omöjliggöra många av de tjänster som vi i dagens samhälle är beroende av.

Utredaren föreslår att man vid datalagring ska skilja på kommunikation mellan människor och kommunikation mellan maskiner. Sådan trafik emellertid såsom internet fungerar går inte alltid att separera, i synnerhet om kryptering används. Utredarens förslag förutsätter således att det byggs in bakdörrar i kommunikationsprotokollen. Om detta är avsikten borde detta ha nämnts och konsekvenserna av detta beskrivits.

Utredaren föreslår att operatörer ska lämna ut information från användare som använder utländska nät. Standarderna för 4G och 5G är emellertid utformade på ett sådant sätt emellertid inte möjligt utan att slå av krypteringen för samtliga användares inkommande trafik. Det är inte sannolikt att en utländsk operatör skulle gå med på detta – även om denne i teorin skulle vilja medverka till brottsbekämpning i Sverige. Att slå av krypteringen för samtliga användare skulle exponera dem för avlyssning och äventyra deras säkerhet. Den utländska operatören kan också vara buden av nationella regler som förhindrar att krypteringen slås av. Ett sådant krav skulle också sannolikt befinnas strida mot LEK. I det fall en operatör endast har en roamingpartner i ett land skulle även utredarens förslag innebära att trafik till och från det landet skulle stoppas om den utländske operatören inte gick med på de svenska kraven: en konsekvens som skulle vara mycket allvarlig men som utredaren trots detta inte ens nämner.

Utredaren föreslår att operatörer ska lagra positionsdata från telefoner. Här förefaller utredaren inte vara medveten om vilka positionsdata som en operatör har tillgång till. Den position som genereras i telefonen (exempelvis via GPS) lagras lokalt och kan inte inhämtas av operatören, det är endast den position som koppas till basstationen telefonen är uppkopplad mot som operatören har åtkomst till. Det innebär också att en operatör inte kan lagra positioner när en telefon inte är uppkopplad mot deras nät. I och med att utredaren föreslår en skyldighet att lagra positionsdata och att denna ska

vara sanktionerad är detta en viktig distinktion – utredningsförslaget kan som det är utformas tolkas som att operatörer kan straffas för att de inte lagrar uppgifter de inte kan få tillgång till.

Detta är bara axplock ur utredningen. Med tanke på att det som utreds i hög grad rör tekniska frågor är avsaknaden av teknisk kompetens hos utredaren anmärkningsvärd.

Att de tekniska frågorna inte berörs på ett adekvat sätt samtidigt som de är helt avgörande för att kunna bedöma konsekvenserna av förslagen, och därmed också om de är proportionerliga, gör att utredningen skulle behöva göras om.

Förslagen är inte proportionerliga

För att kunna avgöra om ett förslag är proportionerligt är det nödvändigt att korrekt beskriva dess konsekvenser. Detta förutsätter som konstaterats ovan att tekniska möjligheter och begränsningar beaktas. Vidare krävs att nyttor och kostnader beskrivs och utvärderas. Ett förslag som inte kan uppnå det mål som det påstås kan aldrig vara proportionerligt. Stiftelsen menar även att proportionalitetskravet ska tolkas som att den som föreslår något som har bevisbördan när det gäller påstådda kostnader och nyttor.

I det aktuella fallet tas nyttan av förslagen – att datalagring är viktig för brottsbekämpningen – i princip för given. Utredaren skriver att förslagen kommer att ”vara klart positiva för brottsbekämpningen” men det som anförs till stöd för detta är endast hänvisningar till påståenden från Polismyndigheten. Stiftelsen menar att nyttan med ett förslag inte utan vidare kan antas eller enbart baseras på allmänna påståenden om att så är fallet, denna måste beläggas. Det finns emellertid endast begränsad forskning kring datalagringens effektivitet[1], den tillgängliga forskningen och liksom den utredning som Europaparlamentet tog fram visar dock på att datalagring inte är en effektiv brottsbekämpningsmetod. I brist på evidens för motsatsen bör rimligen utredningens proportionalitetsbedömning utgå ifrån att värdet för datalagring för brottsbekämpning är ringa eller obefintligt.

Proportionalitetsbedömningar måste även grundas i adekvat beskrivna kostnader. Även här visar utredningen brister. Utredningen beskriver inte vilka kostnader förslaget skulle föra med sig och dessa kvantifieras inte. När det gäller frågan om integritetskostnaden noteras att utredaren genom en juridisk akrobatikövning lyckas landa i att *utebliven* datalagring skulle kränka integriteten (s 96).

Utredaren menar där att skrivningen i artikel 8 i Europakonventionen om att det finns en skyldighet för det allmänna att tillförsäkra enskilda skydd för privat- och familjeliv innebär att (vissa) integritetsintrång bör kriminaliseras. För att sådana brott ska kunna bekämpas krävs i sin tur att

[1] Se exempelvis Sarre, R (2017). Metadata Retention as a Means of Combatting Terrorism and Organised Crime: A Perspective from Australia. *Asian Criminology* 12, 167–179. Rojszczak, M. (2021). The uncertain future of data retention laws in the EU: Is a legislative reset possible? *Computer Law & Security Review*, *41*, 105572.

staten har tillgång till effektiva utredningsverktyg och eftersom datalagring, enligt utredaren, är ett sådant skulle frånvaro av datalagring innebära ett staten inte levde upp till de enskildas konventionsskyddare rätt till skydd av privatlivet.[2] Därmed kan enligt utredaren inte heller artikel 8 i Europakonventionen i användas för att begränsa datalagring. En begränsning blir i stället ett brott mot artikel 8.

Utifrån detta synsätt skulle förstås inte endast utebliven datalagring hota integriteten utan också *varje* uteblivet intrång i enskildas privata sfär (så länge det motiverades med brottsbekämpning). Att inte kränka människors integritet skulle innebära att man kränkte deras integritet. Orwell hade inte kunnat uttrycka det bättre.

Förslaget strider mot gällande rätt

2014 underkände EU-domstolen (EU-domstolens mål C-293/12 och C-594/12) EU:s datalagringsdirektiv. Domstolen fann att direktivet utgjorde ” synnerligen allvarligt ingrepp i den grundläggande rätten till respekt för privatlivet och skydd för personuppgifter genom att kräva att uppgifter om personers kommunikationer ska lagras och genom att ge behöriga nationella myndigheter tillgång till uppgifterna”.

EU-domstolen pekar på att uppgifter om med vem, varifrån, och hur länge någon kommunicerat kan användas för ett exakt kartlägga en människas privatliv, däribland var personen, tillfälligt eller stadigvarande, vistas, personens dagliga och andra förflyttningar, vilka aktiviteter personen ägnar sig åt, vilka sociala relationer den har och vilka umgängeskretsar personen rör sig i. Detta utgör ett ”omfattande och särskilt allvarligt intrång [i de] aktuella grundläggande rättigheterna”.

Domstolen menar att lagring kan vara tillåtet men måste vara proportionerligt, det innebar också att intrånget måste begränsas till vad som är ”strängt nödvändigt”. Här konstateras att lagring av allas, eller mångas uppgifter, eller alla kommunikationssätt inte är förenligt med unionsrätten. Inte heller kan lagring ske med hänvisning till ”allvarliga brott”.

Sverige valde dock trots domen att fortsätta med datalagring. Den svenska datalagringen underkändes följaktligen 2016 av EU-domstolen (Tele2-domen)[3] som fann att svensk datalagring var alltför omfattande och oförenlig med EU-rätten. EU-domstolen konstaterade även att huvudregeln om konfidialitet vid elektronisk kommunikation i e-privacydirektivet endast får göras undantag från rörande angivna ändamålen i artikel 15.1 i direktivet. Där är brottsbekämpning ett men domstolen menar att 15.1 ska tolkas strikt och lagringsskyldighet kan därför aldrig vara huvudregel utan endast ett undantag. Domstolen menar även att medlemsländerna endast får ha regler om datalagring om de är ”strängt nödvändiga och proportionerliga”.

[2] Utredaren exemplifierar med att det i Finland för ett par decennier sedan inte gick att identifiera en misstänkt för förtal eller sexuellt ofredande eftersom man inte kunde få fram vem som hade en viss IP-adress.
[3] De förenade målen C-203/15 och C-698/15, Tele 2 mot Post- och telestyrelsen m.

Utredningsförslaget innebär odiskutabelt en utökad datalagring, både rörande vilka uppgifter som ska lagras, och hur länge. Vad utredaren kallar geografiskt begränsad datalagring omfattar enligt utredningen minst 70 procent av befolkningen (utredaren föreslår att trafik från och till kommuner med högre brottslighet än genomsnittet ska omfattas). I praktiken rör förslagen ännu fler då flera kategorier kan adderas och lagring skulle bli regel snarare än undantag. Detta torde stå i direkt strid mot unionsrätten.

I domen ges exempel på sådana områden som skulle kunna omfattas av nationell datalagring utan att det stred mot unionsrätten, det rör sig där om flygplatser och järnvägsstationer eller särskilt brottsdrabbade platser. Här kan noteras att exempelvis Danmark som har geografisk lagring har definierad de områden om 3 gånger 3 kilometer där brottsligheten är 50 procent högre än genomsnittet. Om även denna indelning är för grov och omfattande har dock ännu inte prövats. Klart är dock att det i Danmark endast är en begränsad del av territoriet där lagring kan förväntas.

När det kommer till lagringen av IP-adresser står förslaget i betänkandet också i direkt strid med EU-domstolens dom i Space Net-målet. EU-domstolen menar där att en IP-adress inte är en ”uppgift om abonnemang” enligt LEK. Utredaren argumenterar i betänkandet (s 168ff) mot detta utifrån ett resonemang som grundas i att EU-domstolen i Space Net-domen landat fel och missförstått vad en IP-adress är. Det kan emellertid inte utan vidare antas att EU-domstolen skulle ändra sitt tidigare ställningstagande om utredningsförslaget. Stiftelsen konstaterar också att det är utredaren, inte EU-domstolen, som inte förstått vad en IP-adress är.

Utredaren måste således – även om detta inte tas upp i betänkandet – vara medveten om att förslagen om de blev verklighet med mycket stor sannolikhet skulle underkännas av EU-domstolen.

Risker och kostnader beaktas inte

När det kommer till kostnaderna för datalagringen menar utredaren att dessa skulle bli begränsade. Detta är felaktigt. Mängden data som lagras föreslås i betänkandet är betydligt större än tidigare och stora mängder data som inte har relevans för de flesta operatörers verksamhet ska lagras. Att krav på ”nationell säkerhetslagring” ska verkställas utan dröjsmål ökar dessa kostnader ytterligare. Detsamma gäller kravet på att lagringsskyldiga ska kunna särskilja data som de tvingats lagra utifrån olika grunder.

För operatörer kommer detta att kräva stora investeringar i lagringsutrymme och personal och i flera fall ändringar av affärsmodeller. Här bör även noteras att operatörerna vid flera tidigare tillfällen tvingats göra investeringar i anpassningar till tidigare datalagringskrav – krav som sedan underkänts som stridande mot unionsrätten eller mot mänskliga rättigheter. Det finns som ovan nämnts en betydande risk att utredningsförslaget, om det blev verklighet, precis som de tidigare svenska datalagringslagarna, underkännas vid prövning av EU-domstolen. Stiftelsen menar att det är orimligt att ålägga företag att göra investeringar i något som staten måste inse är i strid med EU:s fördrag.

Här bör särskilt nämnas att förslaget om att underminera säkra kommunikationer, genom att ställa krav på bakdörrar till totalsträckskrypterade tjänster för med sig potentiellt mycket stora problem för

alla som använder internet. En mycket stor del av de tjänster som privatpersoner och företag använder bygger idag på att det går att kommunicera säkert.

En bakdörr i en tjänst kan inte begränsas till dem som har laglig tillgång till den. Finns den kan den utnyttjas av alla som känner till den, det inkluderar både organiserad brottslighet som främmande makts underrättelsetjänst. Förekomst av bakdörrar skulle sannolikt också i praktiken användas av kriminella och andra illasinnade aktörer i betydlig större utsträckning än av brottsbekämpande myndigheter. För en kriminell är alla som har den aktuella bakdörren potentiella måltavlor (exempelvis för bedrägerier) medan brottsbekämpande myndigheter normalt är inriktade på en viss misstänkt person eller en grupp misstänkta personer.

Kriminella torde också i större utsträckning än andra vara medvetna om riskerna med osäker kommunikation och kan i större utsträckning än andra väntas skydda sig. Det innebär att de säkerhetsproblem som uppstår kan väntas drabba personer som inte begår brott i betydligt högre utsträckning än de kriminella aktörer man motiverar systemet med.

Många av de tjänster som erbjuder säkra kommunikationer idag är utländska och vänder sig till globala marknader. Det är inte sannolikt att de kommer att avskaffa totaksträckskryptering eller införa bakdörrar på grund av svenska myndighetskrav. Snarare kommer de att sluta erbjuda dessa tjänster i Sverige.

Här kan även emellertid noteras att en svensk operatör torde sakna möjligheter att hindra användare i Sverige från att använda en utländsk totalsträckskrypterad tjänst.

En annan risk är frågan påverkan på exempelvis det journalistiska källskyddet. Denna risk är inte direkt ekonomisk men källskyddet är centralt för medias verksamhet. För att källskyddet ska fungera är det nödvändigt att det finns tillgång till säkra kommunikationskanaler, det är där ju också där uppgifterna om vem som lämnat uppgifter snarare än innehållet som utgör den känsliga informationen. Vad källan sagt kommer ju normalt fram genom den artikel eller det inslag i tv eller radio som blir resultatet av det journalistiska arbetet. Datalagring är därför även när det endast omfattar metadata ett direkt hot mot källskyddet. Utredningen berör inte denna uppenbara invändning alls.

Slutligen innebär datalagring en risk i sig genom de datamängder som lagras. All data som sparas riskerar att läcka – avsiktligt genom exempelvis dataintrång eller genom att någon person som har tillgång till data, hos den lagrande verksamheten oavsiktligt läcker. Det finns också en risk att datalagringsskyldiga infiltreras av organiserad brottslighet eller främmande makts underrättelsetjänst. Ju större datamängder som lagras desto större incitament till intrång eller infiltration finns. Dessa risker berörs inte heller i utredningen, detta trots att denna risk tidigare lyfts fram av EU-domstolen och därmed måste antas vara kända av utredaren.[4]

[4] De förenade målen C-793/19, SpaceNet och Telecom Deutschland, s 62

Att utredaren inte berör risken för läckor innebär också att man helt bortser från att sådana kan få mycket allvarliga konsekvenser för enskilda, inklusive livsfara. Den kommunikation som föreslås lagras omfattar exempelvis hjälpsamtal till sådant som Kvinnofridslinjen, till barnhjälpsorganisationer eller kommunikation mellan patient och läkare eller psykolog.

Förslaget saknar effektiva kontrollmekanismer

Enligt EU-domstolen är ”effektiv kontroll” en förutsättning för att datalagring ska få användas. Det förslag som utredaren lägger fram saknar sådan. Enligt vad utredaren anför ska Säkerhetspolisen kunna besluta om ”nationell säkerhetslagring” (dvs en mer omfattande datalagring än den riktade som föreslås) om det finns ett allvarligt hot mot den ”nationella säkerheten”**.** Samtidigt som utredningen ger uttryck för att exceptionella omständigheter ska föreligga för att lagring ska kunna ske är beskrivningen av de faktiska reglerna sådana att det i praktiken är säkerhetspolisens skönsmässiga bedömning som helt avgör om lagring ska ske. Någon begränsning för hur många som får omfattas finns inte heller i förslaget. Inte heller ger utredningens föreslagna ordning allmänheten någon möjlighet att förutse när lagring ska kunna ske.

Enligt utredarens förslag ska Säkerhetspolisen om den anser att sådan datalagring är motiverad ska kalla ett offentligt ombud till sammanträde. Det offentliga ombudet ska där tillvarata enskildas intressen och ska få möjlighet att yttra sig. Efter detta ska Säkerhetspolisen besluta om lagring. Om ombudet inte är nöjt med beslutet kan det överklagas till en enhet inom Säkerhets och integritetsskyddsnämnden (SIN) – Datalagringsdelegationen.[5] Om denna menar att det inte föreligger ett sådant hot som Säkerhetspolisens påstått kan beslutet upphävas. Utredaren hänvisar emellertid i betänkandet till förarbetena till LEK där det framgår att ”det bara är Säkerhetspolisen och Försvarsmakten som tillsammans har en helhetsbild när det gäller säkerhetsläget och hotbilden mot Sverige”. Detta innebär att för att en begäran från Säkerhetspolisen för att inte ska godkännas att först det offentliga ombudet och sedan Datalagringsdelegationen ska underkänna Säkerhetspolisens bedömning. Det är med utgångspunkt i förarbetsuttalanden om att inga andra än Säkerhetspolisens (och Försvarsmakten) kan göra en sådan bedömning dock närmast uteslutet att de skulle landa i en annan slutsats. För att kunna det måste ombudet i princip ha tillgång till uppgifter som säkerhetspolisens inte har. Utifrån detta menar Stiftelsen att det inte går att säga att det i praktiken finns någon effektiv kontroll. Det får utifrån beskrivningen i betänkandet antas vara uteslutet att ombudet överhuvudtaget kan påverka utfallet. Den föreslagna ordningen kan inte förväntas ge resultat som avviker från en där Säkerhetspolisen, helt på egen hand, avgör när lagring ska ske. Därmed uppfylls inte heller EU-domstolens krav.

Stiftelsen menar att det måste finnas en praktisk möjlighet att underkänna datalagringsbeslut, att genomförandet av beslut måste kunna granskas, och att överträdelser måste följas av sanktioner för

[5] Till detta kan läggas att det offentliga ombudet inte ska få granska det faktiska genomförandet. Man kan tänka sig att om Säkerhetspolisen vill överskrida sina befogenheter och kräva lagring i ett fall där lagen inte tillåter detta kommer myndigheterna inte att säga det när den söker tillstånd.

dem som brutit mot reglerna. Personer som utsatts för lagring utan att det varit befogat måste också få ersättning för det intrång som skett. Även företag som tvingats lagra uppgifter utan att det varit befogat måste kunna få ersättning för detta.

Om 5-juli stiftelsen

5 juli-stiftelsen arbetar för mänskliga rättigheter, integritet och säkerhet på internet. 5 juli-stiftelsen grundades 2013 av ett antal svenska internetveteraner som ville värna mänskliga rättigheter på internet, enligt den FN-resolution som antogs den 5 juli 2012 och som slog fast att mänskliga rättigheter ska gälla även där. 5 juli-stiftelsen tillhandahåller verktyg som hjälper internetanvändare att öka sin frihet, säkerhet och integritet och ägnar sig åt informationsverksamhet och opinionsbildning i dessa frågor.