Stockholm 25 augusti 2015

Yttrande över betänkandet SOU 2015:31 Datalagring och Integritet

SICS Swedish ICT har blivit tillfrågade om yttrande avseende utredningen SOU 2015:31 *Datalagring och Integritet* av Justitiedepartementet.

SICS Swedish ICT är starkt kritiska till utredningen och dess ursprungliga uppdrag baserat på följande:

- Det har inte gjorts någon proportionalitetsbedömning i enlighet med EU-domstolens dom då man inte tagit hänsyn till negativa effekter av integritetsintrånget.
- Det finns ingen redovisning av hur datalagring påverkar den personliga integriteten.
- Det görs ingen kritisk granskning av vilka uppgiftskategorier som ska sparas, trots att de tekniska begreppens innebörd konstant förändras.
- Det tas ingen hänsyn till att lagringen i sig är både integritetskränkande och medför risk för läckor.

Yttrandet är uppdelat i fem sektioner som bedömer utredningen utifrån fem olika perspektiv. De tre första behandlar problem med lagtexten och utredningen där tekniska begrepp används otydligt, det finns ett otydligt ansvar för transparens och säkerhet och det finns en bristande hänsyn till den personliga integriteten. Med anledning av detta består de två sista sektionerna av kritik mot metodval och urval i utredning, vilket skapar dåliga förutsättningar för en god och tydlig lagstiftning.

SICS Swedish ICT ställer sig kritiska till utredningen och förordar en ordentlig omvärdering av datalagringen i Sverige baserat på bättre kunskapsunderlag om dess effektivitet, dess tekniska möjligheter och, framförallt, med ordentlig hänsyn till konsekvenserna för den personliga integriteten.

Betydelsen av tekniska begrepp

Vi måste kunna värdera hur den personliga integriteten för medborgare kränks vid varje givet tillfälle, och avgränsa insamlingen till enbart det strikt nödvändiga. De tekniska begrepp som används i lagtexten har därmed stor betydelse för såväl transparens som effektivitet. Eftersom vi har en ständig teknikutveckling är de tekniska begreppen i lagen rörliga mål; en definition eller specifikation idag behöver inte innebära samma sak om ett eller fem år.

För att ge ett exempel: ett begrepp som används i lagen är ”av- och påloggning” till tjänsten, vid såväl internetkommunikation som övriga kommunikationsformat. Det saknas en entydig definition av vad en ”av- och påloggning” är på internet. Är det när man ansluter till internet? Är det när terminalen tilldelas en IP-adress? Är det när man loggar in på en specifik tjänst? Vad händer om man är ansluten till tjänsten hela tiden? Är det när det specifika datapaketet med ett meddelande skickas? PTS, som

SICS SWEDISH ICT AB
Box 1263
SE-164 29 Kista
ORG NR 556587-0119
WWW.SICS.SE

ansvarig myndighet, kan inte svara på vad som utgör en ”av- och påloggning” i lagens mening[1], vilket skapar osäkerhet. Vi kan vara relativt säkra på att något kommer att sparas, men vi kan inte med säkerhet säga vad.

Tekniska kapaciteter och möjligheter ändras också över tid, och vad som innefattas av ett tekniskt begrepp idag kan vara annorlunda om ett år. Det kommer därför bli än svårare att avgöra vad som kommer att sparas framöver. Ett exempel på detta är geografisk positionering där vi med tidigare användning av telefoner sparade en telefons position ett fåtal gånger per dag, med ganska dålig noggrannhet, men där vi med dagens användning, med samma definitioner, kan spara en telefons position avsevärt mycket oftare och med mycket högre precision. Det får helt andra konsekvenser för hur integritetsintrånget värderas, utan att definitionerna ändras på pappret.

Till det kommer också att vem som kontrollerar data förändras. Det är inte nödvändigtvis alltid internetoperatörerna som sitter på den relevanta tekniska informationen. Det gör det också svårt för konsumenten att förutse vem som är lagringsskyldig. Svårigheterna att, trots stor teknisk kompetens, förstå exakt vad som lagras och av vem, skapar ett transparensproblem. Det gör det omöjligt att göra en relevant bedömning av de integritetskränkningar som lagen leder till.

Säkerhet och ansvar

Vilket ansvar ska den datalagrande organisationen ha för det lagrade datat i de fall då de själva inte har kapacitet att lagra data, hantera frågor från polismyndigheter och motsvarande? Detta är ett problem för bland annat mindre internetoperatörer och stadsnät utan stora personalresurser eller serverhallar för lagringen. Fallet med utvecklingen av ett automatiskt API mellan Säkerhetspolisen och Maintrac, ett företag som datalagrar åt framför allt stadsnät, illustrerade tydligt problemet som kan uppstå när tredje part datalagrar utan direkt relation till de personer vars data blir lagrad. Ny Teknik avslöjade i november 2013 att Säkerhetspolisen ville införa ett sätt att automatiskt hämta ut trafikdata från operatörerna datalagring[2]. Utvecklingen av detta system skedde i samarbete med Maintrac som på rekommendation från Svenska Stadsnätsföreningen datalagrade åt flera stadsnät. Efter Ny Tekniks granskning och efterföljande kritik backade Statsnätsföreningen och Maintrac från samarbetet med Säpo[3]. Att man inte med säkerhet kan veta vem som lagrar ens information och hur de i sin tur hanterar förfrågningar skapar återigen ett transparensproblem i datalagringen, vilket försvårar medborgares möjlighet att förutse de integritetskränkningar som deras användande av elektronisk kommunikation kan leda till.

Datalagring innebär alltid en risk för informationsläckage. Även om man tar höjd för att minska riskerna genom goda säkerhetsstandarder och -kontroller så finns det risk att känslig information kan komma att läcka. Det enda sättet att undvika den risken är att inte lagra information, och det bästa sättet att minska skadan vid en läcka är att spara enbart det som är absolut nödvändigt, och därmed undvika allt för mycket överskottsinformation. Varken utredningen eller utredningens uppdrag tar höjd för detta. Att information kan läcka finns det otaliga exempel på, men ett anmärkningsvärt fall

[1] PTS skrift *Uppgifter som ska lagras för brottsbekämpande ändamål – en vägledning* samt telefonsamtal med Peder Cristvall, jurist på PTS, den 25 juni 2015.
[2] Ny Teknik, 6 november 2013. ”Säpos krav: Flöden från operatörerna”
[3] Ny Teknik, 22 november 2013. ”Stadsnäten stoppar överföringen”

som kan nämnas är den stora läckan från Sony 2011 där känslig information om 77 miljoner användare läckte[4]. Även läckorna från Edward Snowden och Chelsea Manning visar att även system som omgärdas av mycket hög säkerhet ändå är sårbara för läckor.

Polisen begränsar inte sina förfrågningar till det som är strikt nödvändigt för en utredning. Under 2013 uppdagades att Tele2 hade begärt en högre ersättning än andra operatörer för trafikdata relaterat till ett mord. När Polismyndigheten inte ville betala den ersättningen ändrade de så småningom sin förfrågan till att bara omfatta de nödvändigaste uppgifterna, och betalade då en fjärdedel av vad de skulle betalat från början. Det anmärkningsvärda i fallet är inte Tele2s prissättning, utan att polisen kunde minska omfattningen av sin förfrågan med så stor andel utan att det begränsade utredningen.[5] Polisen begärde alltså ut mer uppgifter än vad som var strikt nödvändigt. En undersökning om huruvida detta är normalt tillvägagångssätt har inte gjorts i utredningen, trots att det vore en viktig del i proportionalitetsbedömningen.

Proportionalitetsbedömningar

I kapitel 5 av utredningen diskuteras vilka uppgiftskategorier som ska lagras. Utredaren påpekar att uppdraget för utredningen är att ”föreslå de förändringar som […] bedöms lämpliga för att stärka skyddet för den personliga integriteten”. Detta kräver enligt oss en proportionalitetsbedömning där värdet av det lagrade datat vägs mot den integritetskränkning den innebär, såväl specifikt som sammantaget. Detta stöds av EU-domstolens konstaterande att ”undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt”[6] och att domstolen anser att detta inte är uppnått i direktivet.

Genomgående i kapitlet om uppgiftskategorier är det bara värdet av det lagrade datat som analyseras. Detta värde vägs inte mot den integritetskränkning lagringen innebär. Utredaren utgår ifrån att så länge en typ av data har ett värde för brottsbekämpande myndigheter så innebär det att integritetskränkningen är motiverad. Vi menar att detta är felaktigt. Värdet av datat måste ställas mot graden av integritetskränkning för att en proportionalitetsbedömning ska anses gjord.

Proportionalitetsbedömningarna måste också göras sammantaget. Hur effektivt används det lagrade datat jämfört med hur stor integritetskränkningen är av att all denna data lagras? Det konstateras i utredningen att t.ex. abonnemangsdata inte håller något värde i sig, utan får sitt värde av att sammankopplas med andra uppgifter. Detsamma gäller såklart även andra uppgiftskategorier. Effektiviteten bör därmed bli annorlunda aggregerat än för varje uppgiftskategori för sig. Därmed är utredningens konstaterande ”att lagringsskyldigheten inte omfattar annat än vad som är strikt nödvändigt för att uppnå syftet med regleringen” inte trovärdig, eftersom att en sammanvägd proportionalitetsbedömning ej gjorts.

Under stycket 7.5.3 om parlamentarisk kontroll förs ett resonemang om att om riksdagen skulle behöva kontrollera användningen av datalagring skulle rutinerna för dokumentation och uppföljning behöva ändras. Vi anser, i motsats till utredaren, att detta vore ett välkommet tillskott till den information som finns att tillgå. Att kvantitativt kunna bedöma effektiviteten, snarare än att enbart titta på enskilda fall skulle klargöra nyttan av datalagring och göra den lättare att värdera i relation till integritetsintrånget.

[4] The Telegraph, 26 april 2011. ”Millions of internet users hit by massive Sony PlayStation data theft”
[5] Aftonbladet, 15 oktober 2013. ”Tele2 krävde halv miljon för att hjälpa polisen”
[6] EU-domstolen, 8 april 2014. Dom i de förenade målen C-293/12 och C-594/12.

Metoder

Utredningen lider genomgående av en metodologisk brist på kritiska perspektiv och siffror som kan stödja de slutsatser och bedömningar som utredningen gör. Det är självklart rimligt att tillfråga polis och andra rättskipande myndigheter hur de har använt det lagrade datat, och vilken nytta de upplever med den, men det är minst lika viktigt att verifiera korrektheten i myndigheternas bedömning av nyttan. Det fåtal fallstudier och intervjuer som utredningen genomfört räcker inte för att skapa ett objektivt kunskapsunderlag. Som minst borde en kvantitativ genomgång ha kompletterat utredningen av hur uppgifterna hittills har använts.

Vi är vidare mycket kritiska till att utredningen helt saknar ansatser till att förstå hur integritetskränkningarna uppfattas av de vars data lagras. Bedömningen av integritetsintrången måste utföras med hänsyn till både de datalagrades uppfattning och den forskning som finns på området. Utan sådan hänsyn är det omöjligt att hävda att man bedömt proportionalitet, och inte bara effektivitet. Hur vi än värderar de positiva effekter förslagen har så har de negativa effekterna helt enkelt inte värderats.

Det är också beklagligt att Kommittédirektivet (Dir. 2014:101) som ligger till grund för uppdraget ej har förordat en mer utförlig granskning av just de integritetskränkningar som EU-domstolen väger gentemot allmännyttan av datalagringen. Det framgår ej med önskvärd tydlighet i uppdraget att det finns behov av att på allvar se över proportionalitetsbedömningarna.

Urval

Vidare så går det också att ifrågasätta utredarens urval av experter som kopplats till utredningen. Det framgår av utredningen att utöver Iain Cameron från Uppsala Universitet, och *ett* möte med företrädare för leverantörer av elektroniska kommunikationstjänster, har ingen utanför myndighetsramen tillfrågats om bidrag till utredningen. Inga forskare, ingen särskild expert från branschen ”elektroniska kommunikationstjänster” eller någon annan expertroll. Vi har visserligen full tilltro till att alla medverkande experter har bidragit med stor kunskap och värdefulla insikter, men det står också klart att antalet perspektiv som bidragit till utredningen är högst begränsat, och att viktiga perspektiv därmed har utelämnats. Vi är därför kritiska till att det inte tagits in fler experter med större spridning i kompetenser.

Det framgår ej heller vilka datamängder som de 119 analyserade fallen (60 från Säkerhetspolisen och 59 från Polismyndigheten och Tullverket) omfattar. Detta då Tele2 under våren 2015 avslöjade att de får cirka 10 000 ansökningar per månad[7]. Om Tele2s definition av ”ansökningar” överensstämmer med Säkerhetspolisens, Polismyndighetens och Tullverkets ”inhämtningsbeslut” är det en försvinnande liten del som har granskats. Även om flera ansökningar kan ingå i ett inhämtningsbeslut så har det i utredningen inte tagits hänsyn till den mängd ansökningar som då görs varje månad till varje operatör i Sverige. Vidare saknas en redogörelse för vad som ligger till grund för urvalet (urvalskriterier). Detta är helt nödvändigt för att det ska gå att bedöma relevansen i de slutsatser utredaren drar från de analyserade fallen. Därmed är även urvalet av analyserade fall bristfälligt såväl kvalitativt som kvantitativt.

[7] SvD Näringsliv, 4 maj 2015. ”Tele2 rasar mot polisens övervakning”

Sammanfattning

SICS Swedish ICT kritiserar utredningen för att det inte gjorts någon proportionalitetsbedömning i enlighet med EU-domstolens dom då man inte tagit hänsyn till negativa effekter av integritetsintrånget. För att utredningen saknar en redovisning av hur datalagring påverkar den personliga integriteten. För att utredningen saknar en kritisk granskning av vilka uppgiftskategorier som ska sparas, trots att de tekniska begreppens innebörd konstant förändras. För att utredningen inte tar hänsyn till att lagringen i sig är både integritetskränkande och medför risk för läckor. Sammantaget bör man, om datalagringen ska finnas kvar i Sverige, göra stora förändringar i lagstiftningen för att minska kränkningarna av den personliga integriteten, öka transparensen, och förfina de tekniska begreppen.

För SICS Swedish ICT

Jacob Dexe

SICS Swedish ICTs expertgrupp har bestått av: Bengt Ahlgren, Markus Bylund, Olof Görnerup, Per Kreuger, Olle Olsson

SICS SWEDISH ICT AB
Box 1263
SE-164 29 Kista
ORG NR 556587-0119
WWW.SICS.SE