Stockholm 29 januari 2018

Justitiedepartementet

103 30 Stockholm

Ju.a@regeringskansliet.se

Ju2017/07896/Å

Colts synpunkter på delbetänkandet Datalagring – brottsbekämpning och integritet (SOU 2017:75)

Inledning och sammanfattning

Colt Technology Services AB (Colt) har tagit del av och analyserat delbetänkandet angående datalagring och suttit med i två arbetsgrupper (IT & Telekomföretagen och Business Carrier Coalition (BCC, bestående av AT&T, BT, Colt, Orange Business och Verizon Enterprise Solutions). De två arbetsgrupperna lämnar var sitt remissyttrande, och Colt inkommer även med ett eget remissyttrande för att utveckla synpunkterna angående krav på nationell och teknikneutral lagring samt förslag till selektion av lagringsskyldigheten.

Trots att utredningen försökt att skapa en mer riktad lagringsskyldighet genom att minska antalet olika trafikslag (t.ex. telefoni och meddelandehantering inom fasta nätet är borttagna) som ska lagras och infört differentierade lagringstider för de olika trafikslagen, är det utan tvekan frågan om en generell masslagring som föreslås, vilket EU-domstolen underkände i december 2016, och det finns en uppenbar risk att EU domstolen åter skulle underkänna de nya svenska reglerna i en ny prövning, med förödande konsekvenser. Colt anser därför att liggande delbetänkande skall lämnas utan åtgärd och en ny utredning bör tillsätts för att skapa förutsättningar för långsiktigt hållbara datalagringsregler, viket gynnar både de datalagringsskyldiga och de brottsbekämpande myndigheterna.

Krav på lagring i Sverige

Utredningen föreslår att all datalagring ska ske i Sverige, vilket riskerar att operatörer med verksamhet i flera EU-länder, i förlängningen kan tvingas sätta upp separata datalagringsystem i uppåt 28 länder, och riskerar därmed att skapa ytterligare barriärer mot förverkligandet av en digital inre marknad.

Utredaren anger att ”*Det ska i sammanhanget nämnas att lagring utanför Sverige inte torde förekomma alls eller endast i mycket liten utsträckning.*”[1] Colt vill påpeka att det inom branschen är vanligt att lagring av data sker utanför Sverige, särskilt bland de operatörer som bedriver nationell, nordisk, europeisk och global verksamhet, eftersom det är kostnadseffektivt, och lättare att administrera och skydda data. Det kan därför starkt ifrågasättas om skyddet för de känsliga uppgifter som i enlighet med förslaget ska lagras, verkligen förstärks genom att decentralisera lagringen. Det är tvärtom så att möjligheten att centralisera lagringen inom EU är att föredra, då det finns större möjligheter att ha ett utbyggt skalskydd, bättre säkerhetsrutiner,

[1] SOU 2017:75 s. 292

bättre bemanning och kontroll av verksamheten när lagringen sker centralt för ett flertal länder. Utredaren som själv medger att ”*Det är inte möjligt att inom ramen för detta betänkande göra en tillräckligt djup analys av dataskyddsregleringen för att kunna bedöma om det utifrån ett EU-rättligt perspektiv är möjligt att förbjuda lagring i andra EU-länder.*”[2] Med bakgrund av detta uttalande framstår det som ej underbyggt att lägga ett förslag där endast lagring av data inom Sverige skulle vara tillåtet. Enligt förslaget skulle detta motiveras av att lagring inom Sverige skulle vara av vikt för rikets säkerhet, även om det som är mest skyddsvärt i telekomsektorn enlig utredningen är driftsäkerheten i de allmänna näten, där datalagringen skulle vara en integrerad del av driften. I detta sammanhang kan konstateras av driftsäkerheten av de allmänna näten inte på något sätt kan påverkas av kravet på datalagringen, då de uppgifter som lagras inte används i den dagliga driften. Motiveringen i denna del framstår därför som ett försök att undvika en framtida EU-rättslig prövning av kravet på lagring inom Sveriges gränser, eftersom de centrala intressena för staten enligt utredningen inte omfattas av EU-rätten. Vidare påstår utredaren att kravet på lagring inom Sverige skulle göra PTS tillsyn mer potent. Detta motsägs av den slutsats som redovisas i Heckschers utredning där det framgår att *”det svenska regelverket är utformat på ett sådant sätt att tillsynsmyndigheten, Post- och telestyrelsen, har möjligheter att bedriva en aktiv och ändamålsenlig tillsynsverksamhet även gentemot leverantörer som väljer att lagra uppgifter utanför unionen.*” [3] Under den tid som datalagring varit möjlig i Sverige har PTS kunnat och kommer fortsatt att ha möjligheten att bedriva en ändamålsenlig tillsyn av att regelverket följs av operatörerna även om lagring sker inom EU.

Det föreslagna kravet, att all lagring ska ske i Sverige, strider även mot grundprinciperna i EU-rätten, eftersom det väsentligt skulle hindra etableringsfriheten (artiklarna 49-54 Europeiska unionens funktionssätt - FEUF), fritt tillhandahållande av tjänster (artiklarna 56-52 i EUF-fördraget) och det fria flödet av personuppgifter mellan medlemsstaterna enligt vad som föreskrivs i både den allmänna dataförordningen och dataskyddsdirektivet.

Förslag till selektion av lagringsskyldigheten

Utredningen föreslår vidare att den nuvarande modellen för kostnadsfördelning mellan det allmänna och operatörerna där operatörerna står för kostnaderna för anpassning, drift och underhåll och de brottsbekämpande myndigheterna betalar en ersättning till operatörerna vid varje utlämnande av uppgifter kvarstår.[4] Detta system har klara brister, då den lagringsskyldighet som föreslås, åläggs alla operatörer, även de operatörer som aldrig eller endast vid ett fåtal tillfällen per år får en begäran om utlämnande av uppgifter. Operatörer i denna kategori, är operatörer som huvudsakligen riktar sina tjänster mot företagsmarknaden, eller är så små att de sällan eller aldrig kommer få en sådan begäran. Trots detta förutsätts dessa operatörer skaffa kostsamma lagringssystem och ha personal redo att skyndsamt lämna ut begärda uppgifter. Kostnader som inte kan på något sätt ersätts av det allmänna.
I Finland har den finska lagstiftaren i informationssamhällsbalken löst detta dilemma genom att endast de av inrikesministeriet särskilt utsedda företagen omfattas av lagringsskyldigheten[5], i gengäld står den finska staten för kostnader avseende system och programvaror som anskaffats för att kunna realisera datalagringsskyldigheten.[6] Det finska systemet har den

[2] SOU 2017:75 s. 291
[3] SOU 2015:31 s. 15
[4] SOU 2017:75 s. 75
[5] Informationssamhällsbalk 19 Kap 157 §
[6] Informationssamhällsbalk 37 Kap 299 §

fördelen att den skapar incitament för myndigheter att endast ålägga denna skyldighet på de aktörer där lagringsskyldigheten står i proportion till den nytta skyldigheten ger. Det system som tidigare och nu av utredningen föreslås fortsätta framstår som oproportionerligt och belastar de aktörer i branschen som endast vid ett fåtal tillfällen eller inte alls får någon begäran om utlämnande på ett orimligt sätt. I tillägg föreslår Colt att processen, för att utse de företag som ska ha en datalagringsskyldighet, sekretessbeläggs. Detta skulle öka effektiviteten i brottsbekämpningen, då kriminella aktörer inte skulle kunna välja nät som inte har en datalagringsskyldighet, för sin kommunikation.

IP-adresser genom NAT tekniken

Utredningen föreslår att bestämmelserna om lagringsskyldighet görs **teknikneutrala**, vilket medför att operatörernas användning av NAT-teknik (en teknik för att tillåta att flera abonnenter delar på en och samma publika IP-adress) inte påverkar möjligheterna till identifiering av abonnenten.

Säkerhetspolisen har erfarenhet av att det, inom den tidigare lagstiftningen, inte har gått att identifiera målsägande på grund av att deras ”NAT:ade IP-adresser” inte har kunnat knytas till en identifierbar person. [7]

Colt kan konstatera att förslaget tar sikte på att alla internetanvändare ska kunna identifieras oberoende av teknik, dvs även användare med NAT:ade adresser, där både publik IP-adress och publikt port-nummer samt privat IP-adress och privat port-nummer som varit aktiva under en användares internetsession, ska lagras.

I de fall, när en internetoperatör använder NAT tekniken för att hushålla på publika IPV4 adresser (Carrier Grade NAT eller Large Scale NAT), så bör det finnas en rimligt möjlighet att identifiera en slutanvändare, eftersom internetoperatörens tjänst sträcker sig ända till slut-användaren, och har därmed kontroll på både publik och privat IP-adress och tillhörande port-nummer. Dock torde det bli svårt att identifiera en enskild användare i ett hushåll med mer än en person, då internettjänsten ansluts till en router, som använder sig av NAT tekniken.

När det gäller operatörer som tillhandahåller internetanslutning till företagskunder, så är det som regel så att operatörerna inte har någon kontroll över trafiken på kundsidan, vilket kan indelas i tre olika fall enligt nedan:

Operatören äger och handhar utrustningen på kundsidan:
Här kan det finnas möjlighet att lagra både publik och privat IP-adress och port-nummer. Dock förutsätter detta att:

1. Tillstånd måste inhämtas från företaget för lagring av de anställdas internettrafik, då operatören har avtal med företaget och inte med varje enskild anställd.
2. Det är mycket stora mängder data för måste lagras på användarsidan, typiskt brukar loggfilen på en standardrouter (med NAT funktionen påslagen) tömmas varje timme, i annat fall finns risk för att prestandan allvarligt kan påverkas på routern/firewallen. Detta i sin tur kan medföra att en operatör tvingas köpa in kostsam utrustning som klarar lagringskraven, snarare än för den tjänst, den skall vara dimensionerad för att klara.
3. Att bygga upp lokala funktioner hos en kund är mycket dyrt och betungande för en operatör (speciellt som utredningen föreslår att operatörerna ska stå för dessa

[7] PTS skrivelse till Ekobrottsmyndigheten den 26 februari 2015 (Dnr 15-1185), s. 1

kostnader). Även PTS konstaterar i sin skrivelse[8], att detta är mycket betungande, och inte omfattades av dåvarande lagringsskyldighet.

Operatören äger utrustningen på kundsidan, men handhar den inte
I många fall så placerar operatören en router som har en publik IP-adress hos kunder för att få bättre möjligheter att övervaka sitt nät, men kunden hanterar all kommunikation inom företaget. Typiskt är att företaget ansluter en egen router (med NAT funktion) bakom operatörens router och begär att NAT funktionen deaktiveras på operatörens router.
Här har operatören ingen kontroll över trafik eller trafikdata inom företaget, och data måste begäras från företaget. Operatören kan endast tillhandahålla trafikdata, fram till tjänstens avlämningspunkt med publik IP-adress.

Operatören äger inte utrustningen på kundsidan
Typiskt är att företaget ansluter en egen router, med NAT funktion, till ett, av operatören tillhandahållet, modem. Även här har operatören ingen kontroll över trafik eller trafikdata inom företaget, och data måste begäras från företaget. Operatören kan endast tillhandahålla trafikdata fram till tjänstens avlämningspunkt med publik IP-adress.

IPV6
Utredning konstaterar att man kan förmoda att IPV6-adresser kommer att bli vanligare framöver. IPV6 är en senare version av internetprotokollet, som gör det möjligt att använda 128 bitar långa IP-adresser, vilket möjliggör omkring 340 sextiljoner ($3,4 \times 10^{38}$) unika adresser. Det skulle innebära att användandet av NAT-teknik, utifrån brist på IP-adresser som enda grund, blir obehövligt. Vidare konstaterar man att kan det ändå kan finnas anledning för operatörerna att fortsätta att använda NAT tekniken.[9]

De seriösa aktörerna på marknaden kommer att stödja samexistens av IPV6 och IPV4 under många år framöver, och många kunder kommer att sitta kvar med IPV4-adresser.

Colt kan bekräfta att det finns operatörer och kunder som väljer att utnyttja NAT tekniken även bakom en publik IPV6 adress. Det finns ett antal skäl till detta:

- Motsträvighet att ändra ett bra fungerande koncept.
- Lättare att hantera/administrera IPV4-adresser
- Säkerhet, användaren skall inte exponeras för en publik IP-adress.

Slutsatsen är att vi kan konstatera att IPV4-adresser med NAT teknik kommer att användas många år framöver och även NAT:ade IPV6 adresser.

Slutsats
Ovanstående analys visar på att användande av NAT tekniken är ett mycket komplext område och vi kan konstatera att utredningen inte har analyserat dessa frågor tillräckligt. Enligt utredningen skall PTS få meddela närmare föreskrifter om vilka närmare uppgifter som ska lagras. Men vi kommer inte får någon klarhet, beträffande vilka skyldigheter en lagringsskyldig har innan praxis har etablerats. Även om det är klokt att föreslå en teknikneutral lösning för att kunna hantera den framtida teknikutvecklingen, så måste analysen bygga på det som gäller för stunden.

[8] PTS skrivelse till Ekobrottsmyndigheten den 26 februari 2015 (Dnr 15-1185), s. 4
[9] SOU 2017:75 s. 247

Teknikneutralitet löser inte de faktiska problem som operatörerna står inför, vilket medför stora svårigheter att uppfylla den lagringsskyldighet som föreslås i utredningen.

Detta krav är mycket betungande, eftersom det kräver lagring av enorma mängder data som inte normalt behandlas av operatörerna. Operatörerna hanterar normalt trafik och har kontroll över trafikdata till en kunds anslutningspunkt. De föreslagna skyldigheterna ålägger operatörerna att bygga upp lokala lagringssystem hos kunderna, vilket är mycket kostnadskrävande. Det kan även ifrågasättas om genomförandet av denna nya förpliktelse är oproportionerligt tung, särskilt för de flesta mindre operatör som enbart har företagskunder och inte mottagit en enda begäran om att lämna ut trafikdata.

Med vänlig hälsning

Ulf Wahllöf

Regulatory Specialist

Colt Technology Services AB