CIRIO

Molntjänster, offentlighet och sekretess i offentlig sektor

Utredning om och förslag till lagstiftning rörande offentlig sektors möjligheter att använda publika molntjänster

Cirio Advokatbyrå AB I Box 3294 - 103 65 Stockholm I Mäster Samuelsgatan 20 I 08 527 916 00 I www.cirio.se

INNEHÅLLSFÖRTECKNING

FÖRORD

Cirio Advokatbyrå önskar genom denna skrift lämna ett bidrag till en fråga av stor betydelse för digitaliseringen av Sverige, med fokus på digitaliseringen av offentlig sektor. Det handlar om den sedan flera år diskuterade frågan om möjligheterna enligt offentlighets- och sekretesslagen för myndigheter och andra offentliga aktörer att använda molntjänster. I utredningen redogör vi för frågans och debattens historik i Sverige och för hur vi bedömer att en kommande uppdaterad lagstiftning i frågan bör utformas. Vi redogör också för varför vi bedömer att det nuvarande rättsläget i frågan kanske inte är så oklart som många verkar tro, och att det redan idag finns goda förutsättningar för myndigheter att använda molntjänster.

Det är vår förhoppning att vi genom denna utredning kan få bidra till att skapa bra spelregler för framtidens näringsliv och samhälle i ett digitaliserat Sverige.

Stockholm den 12 maj 2020

David Frydlinger

Partner

Caroline Olstedt Carlström

Partner

David Frydlinger

Managing partner

Cirio Advokatbyrå

david.frydlinger@cirio.se

+46 76 617 09 85

Caroline Olstedt Carlström

Partner

Cirio Advokatbyrå

caroline.olstedt.carlstrom@cirio.se

+46 70 353 90 30

SAMMANFATTNING

Regeringen har i sin digitaliseringsstrategi satt upp ett hållbart digitaliserat Sverige som övergripande vision. Regeringen pekar i strategin också på behovet av ökat reformtempo och anpassningar av lagstiftning som i onödan hindrar digitalisering.

En särskilt aktuell fråga rörande lagstiftning kopplat till digitalisering är offentliga myndigheters möjligheter att köpa molntjänster från privata leverantörer på ett sätt som är förenligt med offentlighets- och sekretesslagen.

Idag råder ett läge där många myndigheter tror, baserat på inte minst uttalanden från eSam, att det är olagligt att köpa molntjänster från privata leverantörer på grund av reglerna i offentlighets- och sekretesslagen. En närmare analys visar dock att eSams tolkningar av denna lag i stora delar verkar vara felaktiga och att offentlighets- och sekretesslagen ofta inte hindrar användning av molntjänster. Vi konstaterar också att inte heller dataskyddsförordningen sätter upp något principiellt hinder mot användning av molntjänster.

Regeringen har under hösten 2019 tillsatt en kommitté som bl.a. har i uppdrag att vid behov lämna förslag till lagändringar i denna fråga. Trots att rättsläget kanske inte är så oklart som det har framställts, ser vi det som viktigt att sådan klargörande lagstiftning antas. I den framtida lagstiftningen anser vi här att det bl.a. finns behov av att skyndsamt

- Förtydliga vad det innebär att röja uppgifter i offentlighets- och sekretesslagens mening,
- Anta Digitaliseringsrättsutredningens förslag till bestämmelser om bl.a. lagreglerad tystnadsplikt, samt
- Anta kompletterande regler om bl.a. informationssäkerhet i staten och hantering av molntjänstleverantörers underleverantörer.

1 De juridiska förutsättningarna för digitalisering

Digitalisering är viktigt, för att inte säga samhällskritiskt. Om det inte var uppenbart tidigare så har det blivit uppenbart genom Covid-19-pandemin, eftersom samhället hade stannat upp ännu mer och ännu fler hade dött om det inte hade varit för möjligheterna att använda digital teknik.

Alla, eller nästan alla, håller med om att digitalisering är viktigt för hela samhället. Regeringen har i sin digitaliseringsstrategi satt upp *ett hållbart digitaliserat Sverige* som övergripande vision. Det handlar enligt regeringen om

> ”ett Sverige där alla i hela landet är en del av och har förtroende för det digitaliserade samhället” och ”ett samhälle som digitaliseras för att det förenklar vardagen, för att det skapar konkurrenskraft och leder till nya jobb och för att det utvecklar Sverige genom att ta till vara Sveriges starka sidor – en väl utbyggd infrastruktur, ett teknikkunnigt och teknikvänligt folk, en väl fungerande offentlig sektor som har stor tillit från befolkningen.”[1]

Digitalisering innebär många saker, inte bara användning av digital teknik utan också förändringar i arbetssätt, processer och beteenden. Digitalisering innebär dessutom i princip alltid att någon form av *mjukvara* används. Denna mjukvara ligger vidare alltid på någon form av infrastruktur, där också den data som genereras i och bearbetas i mjukvaran lagras.

Det idag ofta både effektivaste och säkraste sättet att använda mjukvara är som s.k. molntjänst, där mjukvaran helt eller delvis tillhandahålls över internet. Idag är det ofta också det *enda* sättet att använda mjukvara, som alltmer sällan tillhandahålls i versioner som kan installeras på egen infrastruktur. Många gånger, men inte alltid, är detta också det effektivaste och säkraste sättet att köpa tillgång till IT-infrastruktur. Det finns också många effektiva varianter där delar av en lösning levereras som en molntjänst och andra delar finns installerade hos kund eller där olika mjukvaror, vissa levererade som molntjänst och andra installerade hos kund, samspelar med varandra.

Möjligheten att använda molntjänster är således avgörande för digitalisering. Detta gäller förstås också offentlig sektor och förvaltning. Avseende just digitalisering av offentlig förvaltning ligger sedan länge de av riksdagen beslutade målen om en ”innovativ och samverkande statsförvaltning som är rättssäker och effektiv, har väl utvecklad kvalitet, service och tillgänglighet och som därigenom bidrar till Sveriges utveckling och ett effektivt EU-arbete.”[2]

[1] Regeringskansliet, *För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi*, s. 8.

[2] Ibid., s. 10.

Den samhällsviktiga digitaliseringen av offentlig sektor förutsätter ett juridiskt ramverk. Regeringen betonar i digitaliseringsstrategin att

> I det digitala samhället behöver det finnas långsiktigt hållbar lagstiftning som stödjer utveckling och dess effektiviseringspotential. Lagar och förordningar behöver ge tillräckligt stöd för den digitala utvecklingen och behovet av samverkan mellan aktörer. För att nå strategins mål behöver reformtempot öka och lagstiftning som i onödan hindrar digitalisering anpassas.[3]

När det gäller molntjänster finns idag en spridd uppfattning att lagar och förordningar *inte* ger tillräckligt stöd för den digitala utvecklingen. Som kommer att framgå nedan bedömer många att det helt enkelt är olagligt för offentlig sektor att köpa många typer av molntjänster, eftersom det skulle stå i strid med offentlighets- och sekretesslagen.

Detta omfattar inte bara de stora publika molntjänsterna utan också de tusentals mjukvarutjänster som använder dessa publika molntjänster som sin infrastruktur. På grund av rådande läge tror sig många inom offentlig sektor helt enkelt inte ha möjlig tillgång till dessa molntjänster, vilka annars hade kunnat bidra kraftigt till digitaliseringen av offentlig sektor.

Dagens rättsläge, eller snarare uppfattade rättsläge, utgör ett allvarligt hinder mot digitaliseringen av offentlig sektor, till men för hela samhället. Det var därför mycket välkommet när regeringen i september 2019 antog kommitédirektiv avseende *Säker och kostnadseffektiv it-drift för den offentliga förvaltningen*.[4] I uppdraget ingår att i den mån det behövs föreslå uppdaterade rättsregler.

Det är samhällskritiskt att de juridiska problemen åtgärdas, och vi vill här lämna förslag till hur en uppdaterad lagstiftning skulle kunna utformas. Samtidigt vill vi peka på att rättsläget ingalunda är så oklart som många verkar tro, och att behovet av uppdaterad lagstiftning kanske därför inte är så stort ändå – i alla fall inte för många typer av molntjänster.

[3] Ibid., s. 29.

[4] Dir. 2019:64.

2 Sekretessprövningen enligt offentlighets- och sekretesslagen

Som en bakgrund till vår analys och förslag i denna skrift är det lämpligt att kort redogöra för huvuddragen i hur offentlighets- och sekretesslagen ska tillämpas om en myndighet vill använda tjänster från en molntjänstleverantör.

Enligt 8 kap. 1 § offentlighets- och sekretesslagen får en uppgift för vilken *sekretess* gäller enligt OSL inte *röjas* för enskilda eller för andra myndigheter, *om inte annat anges i OSL*.

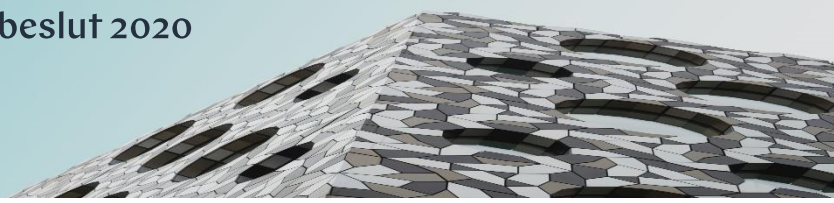
Denna bestämmelse pekar på tre prövningar som måste göras.

1. Först måste prövas om uppgifterna kommer att ”röjas” för molntjänstleverantören. Den nedan refererade debatten och denna skrift handlar primärt om vad just detta begrepp innebär. Om inget röjande sker, så förhindrar inte OSL användning av molntjänstleverantören.
2. Om ett röjande sker måste därefter bedömas om uppgifterna ska anses vara *sekretessbelagda* i förhållande till molntjänstleverantören. Offentlighets- och sekretesslagen innehåller här tre typer av s.k. skaderekvisit – raka, omvända och absoluta. Ett *rakt* skaderekvisit innebär att uppgiften endast är sekretessbelagd om det måste antas att någon form av men uppstår om uppgiften röjs.[5] Ett *omvänt* skaderekvisit innebär att uppgiften är sekretessbelagd om det inte står klart att uppgiften kan röjas utan att men uppstår. Ett *absolut* skaderekvisit är just absolut – om uppgiften röjs så får den helt enkelt inte lämnas ut till molntjänstleverantören.
3. Om uppgiften ska anses vara sekretessbelagd i förhållande till molntjänstleverantören blir den sista frågan om det finns så kallade sekretessbrytande bestämmelser. I vissa fall kan det t.ex., trots sekretess, vara acceptabelt att lämna ut uppgifter till en annan myndighet.

I denna skrift föreslår vi uppdateringar avseende det ovan beskrivna regelverket. För att förstå både våra förslag till lagstiftning och analys av det rådande rättsläget är det dock lämpligt att först redogöra för historiken som har lett fram till dagens olyckliga läge.

[5] Den exakta formuleringen av det raka skaderekvisitet skiljer sig mellan OSLs bestämmelser.

3 Från JO-beslut 2014 till JO-beslut 2020



Den juridiska och i viss mån politiska debatten om det är möjligt för statliga och kommunala myndigheter att använda publika molntjänster och samtidigt handla i förenlighet med offentlighet- och sekretesslagen har pågått sedan åtminstone 2014.

Justitieombudsmannen kritiserar vårdgivare 2014 Frågan hade lyfts redan tidigare men fick förnyad aktualitet när Justitieombudsmannen det året i ett beslut riktade kritik mot vårdgivare som hade ingått avtal om journalföring av patientuppgifter med ett företag – enligt JO i strid med offentlighets- och sekretesslagen.[6] JO, som fattade sitt beslut när personuppgiftslagen gällde, menade att det inte var tillräckligt att företagen endast hade en avtalad sekretesskyldighet för uppgifter som omfattades av omvända skaderekvisit[7], till skillnad från den straffsanktionerade sekretesskyldighet som gäller för personalen hos vårdgivaren.

Slutbetänkande från E-delegationen Efter JO:s beslut uppstod en juridisk debatt om möjligheten för myndigheter att använda molntjänster.[8] I sitt slutbetänkande *En förvaltning som håller ihop* kom E-delegationen dock fram till att det då saknades behov av ytterligare lagstiftning eftersom det enligt delegationens uppfattning var ”mycket få fall av outsourcing som inte kan komma till stånd, pga. av offentlighets- och sekretesslagens utformning.”[9] Åtminstone när det kom till outsourcing fanns inga större problem.

eSam träder in I sitt betänkande påpekade E-delegationen dock att det var ”uppenbart att myndigheterna är betjänta av en vägledning för dessa frågor”.[10] Ett rättsligt uttalande publicerades i december 2015 av det s.k. eSamverkansprogrammet (eSam), som är ett medlemsdrivet program för samverkan mellan 27 myndigheter och Sveriges Regioner och Kommuner.[11] eSam menade att så länge som ”tjänsteleverantören och dennes personal inte får ta del av eller vidarebefordra uppgifterna och omständigheterna i övrigt medför att det är osannolikt att detta ändå sker” skulle ett *röjande* i offentlighets- och sekretesslagens mening inte anses ske. Här ska alltså noteras att frågan rörde om ett röjande sker, och inte frågan om vissa uppgifter är sekretessbelagda i förhållande till leverantören.[12]

Pensionsmyndigheten publicerar en rapport I januari 2016 publicerade Pensionsmyndigheten rapporten ”Molntjänster i staten”, som var resultatet av ett

---

[6] JO:s beslut från den 9 september 2014, dnr 3032-2011.

[7] Se avsnitt 2 ovan för redogörelse för detta begrepp.

[8] Se t.ex. Conny Larsson, *Sekretess utgör därmed ett generellt hinder för myndigheter att använda 'molntjänster' inom IT,* Dagens Juridik 2 oktober 2014, Daniel Westman, *Nej, advokaten – sekretess utgör inget generellt hinder för molntjänster hos myndigheter*, Dagens juridik 12 november 2014 och David Frydlinger, *Offentlighets- och sekretesslagen förhindrar generellt inte användning av molntjänster*, Offentliga Affärer 14 november 2014.

[9] *En förvaltnings som håller ihop*, SOU 2015:66, s. 50.

[10] SOU 2015:66, s. 50.

[11] ”Röjandebegreppet enligt offentlighets- och sekretesslagen”, 17 december 2015.

[12] Se beskrivning i avsnitt 2 ovan.

regeringsuppdrag. Rapporten innehöll en omfattande genomgång av inte minst juridiska aspekter rörande myndigheters användning av molntjänster från privata leverantörer. En viktig aspekt som framhölls var vikten av kontroll och insyn i molntjänstleverantörens användning av underleverantörer.

Digitaliseringsrättsutredningen lämnar slutbetänkande I mars 2018 lämnade Digitaliseringsrättsutredningen sitt slutbetänkande *Juridik som stöd för förvaltningens digitalisering*.[13] I betänkandet föreslog utredningen bl.a. regler om offentlighet och sekretess vid utkontraktering av teknisk bearbetning och lagring. Digitaliseringsrättsutredningens förslag, som också ligger till grund för våra förslag i denna skrift, har än så länge inte lett till några lagstiftningsåtgärder.

CLOUD Act antas Frågan tog en ny vändning under 2018, då USA antog Clarifying Lawful Overseas Use of Data Act – den s.k. CLOUD Act. Lagen var ett tillägg till en redan existerande lagstiftning angående lagrad kommunikation och avsåg att tydliggöra att brottsbekämpande amerikanska myndigheter har rätt att under vissa förutsättningar kräva ut dokument och uppgifter från molntjänstleverantörer under amerikansk jurisdiktion, även om uppgifterna finns på servrar utanför USA.

eSam träder in igen Antagandet av CLOUD Act föranledde två nya rättsliga uttalanden från eSams juridiska expertgrupp, publicerade 2018 respektive 2019, kompletterat med en uppdaterad vägledning rörande sekretess och dataskydd vid outsourcing, publicerad 2019.[14]

eSam menade i uttalandet från 2018 att uppgifter fick anses vara röjda i strid med offentlighets- och sekretesslagen om ”sekretessreglerade uppgifter görs tekniskt tillgängliga för en tjänsteleverantör som till följd av ägarförhållanden eller annars är bunden av regler i ett annat land, enligt vilka tjänsteleverantören kan bli skyldig att överlämna information utan att internationell rättshjälp anlitats eller annan laglig grund föreligger enligt svensk rätt.”[15] Detta och liknande uttalanden från eSam har varit avgörande för dagens spridda uppfattning om svårigheten för offentlig sektor att köpa molntjänster.

Kammarkollegiet publicerar en förstudie I februari 2019 publicerade Kammarkollegiet en förstudie som låg till grund för beslut att inte genomföra en upphandling av webbaserat kontorsstöd. Kammarkollegiet hänvisade här bl.a. till den rättsliga osäkerheten rörande offentlighet- och sekretess samt dataskyddsförordningen.

Regeringen beslutar om ny utredning Digitaliseringsrättsutredningens förslag har som sagt inte lett till någon ny lagstiftning. Regeringen beslutade istället att inleda ytterligare utredning. Vid regeringssammanträde den 26 september 2019 antogs kommittédirektiv avseende *Säker och kostnadseffektiv it-drift för den offentliga förvaltningen*.[16] Enligt direktiven ska en särskild utredare kartlägga och analysera statliga myndigheters behov av säker och kostnadseffektiv it-drift samt hur dessa behov tillgodoses, samt även säkerhetsmässiga och rättsliga förutsättningar för såväl samordnad statlig it-drift som utkontraktering av it-drift till privata leverantörer. Vid behov ska författningsförslag lämnas.

---

[13] SOU 2018:25.

[14] ”Rättsligt uttalande om röjande och molntjänster”, 23 oktober 2018, ”Kompletterande information om molntjänster”, 20 september 2019, ”Outsourcing 2.0 – En vägledning om sekretess och dataskydd”, december 2019.

[15] eSam, ”Rättsligt uttalande om röjande och molntjänster”, 23 oktober 2018.

[16] Dir. 2019:64.

Riksrevisionen kritiserar myndigheters informationssäkerhet I oktober 2019 publicerade Riksrevisionen rapporten *Föråldrade IT-system – hinder för en effektiv digitalisering.*[17] I rapporten konstaterade Riksrevisionen att det förekommer väsentliga effektivitetsbrister hos statliga myndigheter som kan kopplas till föråldrade IT-system samt att dessa även innebär en risk ur ett informationssäkerhetsperspektiv. Ungefär 80 procent av de granskade myndigheterna hade uppgett att man hade svårigheter att upprätthålla eftersträvad nivå av informationssäkerhet för något eller några verksamhetskritiska system.[18]

Försäkringskassan publicerar en vitbok Under hösten 2019 tog saken ytterligare en ny vändning, då Försäkringskassan publicerade en vitbok med titeln *Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt*. I vitboken tyckte sig Försäkringskassan kunna konstatera, bl.a. genom hänvisning till eSams uttalanden, att det finns bestämmelser i såväl svensk rätt som EU-rätt som hindrar svenska myndigheter att använda vissa publika molntjänster i privat regi för att hantera sekretessreglerade uppgifter eller personuppgifter, om molntjänstleverantören träffas av lagstiftning som ger utländska myndigheter rätt att ta del av data och uppgifter som lagras hos leverantören ifråga.[19]

Försäkringskassan debatterar i Dagens Nyheter I samband med utgivandet av sin vitbok gjorde Försäkringskassans generaldirektör ett debattinlägg på DN Debatt med titeln ”Sveriges digitala suveränitet hotas av IT-tjänster i molnet”.[20] Detta inlägg föranledde ett antal repliker på samma debattsida.[21]

Göteborgs Stad anmäls till Justitieombudsmannen I januari 2020 JO-anmäldes Göteborgs Stad för sitt beslut att köpa den publika molntjänsten Office 365, där anmälaren bl.a. menade att detta stod i strid med offentlighets- och sekretesslagen. JO beslutade den 19 mars 2020 att inte ta upp ärendet, med hänvisning till den pågående utredningen enligt ovan.

Den utveckling och debatt som har redogjorts för ovan framstår som både ovanlig och märklig. Försäkringskassans vitbok och den efterföljande debatten i Dagens Nyheter framstår som det kanske märkligaste. Vitboken är i princip ett politiskt dokument, eftersom Försäkringskassan i hög grad baserar sin argumentation på ett påstått behov av att skydda Sveriges ”digitala suveränitet”. Hur många gångar har vi sett en myndighet uttala sig, i en vitbok och på Dagens Nyheters debattsida, i en politisk fråga som ligger långt från myndighetens huvudsakliga uppdrag (socialförsäkringssystemet) i ett läge där regeringen redan har tillsatt en utredning för att eventuellt uppdatera lagstiftningen?

En annan märklig aspekt är avsaknaden av en större debatt kring Riksrevisionens rapport om allvarliga säkerhetsbrister, vilka många gånger förstås skulle kunna övervinnas genom en ökad användning av molntjänster.

---

[17] Rir 2019:28.

[18] Ibid., s. 57.

[19] Försäkringskassan, *Vitbok – Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt*

[20] Dagens Nyheter, 11 november 2019.

[21] Erik Brändt Öfverholm, ”Belägg saknas för tvärsäkra påståenden om amerikanska it-lagen”, 22 november 2019, Peter Dahlen, ”Öbergs slutsatser om it-säkerhet går emot regeringens utredningsdirektiv”, 26 november 2019, Peter Waher, ”Ny teknik kan skydda Sveriges digitala suveränitet”, 27 november 2019, Christian Borggreen, ”Öbergs rekommendation kan hämma Sveriges ledande position”, 29 november 2019 slutreplik Nils Öberg, ”Debatten har inte ändrat vår uppfattning”, 2 december 2019. Samtliga på Dagens Nyheters debattsida.

Det är här lätt att uppfatta debatten som att det finns politiska intressen och rena egenintressen hos viktiga aktörer när det gäller frågan om myndigheters köp av molntjänster.

Oavsett vilket så råder som sagt nu en situation där många myndigheter ser sig juridiskt helt förhindrade att köpa molntjänster från leverantörer som omfattas av CLOUD Act eftersom det skulle stå i strid med offentlighets- och sekretesslagen. Framförallt orsakad av eSams rättsliga uttalanden och vägledningar. Denna uppfattning påverkar förstås inte bara de stora publika molntjänsterna, vilka typiskt sett är amerikanska, utan som sagt också de tusentals molntjänster som använder dessa publika molntjänster som sin infrastruktur. Här finns således ett upplevt och stort juridiskt hinder som försenar digitaliseringen av offentlig sektor.

4 eSams uttalanden och analyser av röjandebegreppet

Att debatten om molntjänster i förhållande till offentlighets- och sekretesslagstiftningen är märklig illustreras kanske bäst genom en närmare analys av eSams olika uttalanden i frågan från år 2015 och framåt. I dagsläget är det som sagt i hög grad dessa uttalanden som ligger till grund för en vad som verkar vara en allmänt spridd uppfattning att det skulle stå i strid med denna lagstiftning att köpa publika molntjänster, åtminstone från leverantörer som omfattas av CLOUD Act eller som använder sådana leverantörer för sin infrastruktur. Detta trots att eSam har svaga argument för en sådan uppfattning. Faktiskt så svaga att man inte förstår varför eSam inte valt att inta motsatt ståndpunkt.

Det som framkommer vid en närmare analys av eSams olika uttalanden är nämligen att eSam, efter antagandet av CLOUD Act, har uppfunnit ett eget juridiskt rekvisit som saknar stöd i lagstiftningen men som, när det tillämpas, försvårar myndigheters användning av sådana publika molntjänster eller mjukvara som använder sådana molntjänster för sin infrastruktur.

4.1 Högsta Domstolen om röjandebegreppet

Den rättsliga bakgrunden är begreppet ”röjande” enligt offentlighets- och sekretesslagen. Enligt lagen får, som beskrivits i avsnitt 2, myndigheter inte ”röja” sekretessbelagda uppgifter, vilket gör det centralt att förstå vad detta röjandebegrepp innebär. Om en myndighet lagrar uppgifter hos en molntjänstleverantör, men där den senares personal inte har tillgång till uppgifterna – är det ett röjande? Vad gäller om leverantörens personal har möjlighet men inte rätt att ta del av uppgifterna? Detta är avgörande frågor vid bedömningen om en molntjänstleverantör får användas.

Det finns få rättskällor att ta till hjälp för att tolka vad begreppet röja ska anses betyda. I ett rättsfall från år 1991 uttalade dock Högsta Domstolen att ett röjande inte kräver att någon faktiskt måste ha tagit del av uppgifter i en allmän handling.[22] Samtidigt krävs inte heller att någon bara har haft en teoretisk möjlighet att ta del av handlingen. Enligt HD måste man *kunna räkna med* att någon kommer att få del av den allmänna handlingen för att den ska anses vara röjd. Genom domen stod det klart att *sannolikhet* – sannolikheten för att någon kommer att ta del av utlämnade uppgifter - har stor betydelse för att bedöma om en uppgift är röjd eller inte. Detta är förstås viktigt för att bedöma om det innebär ett röjande att lagra uppgifter hos en molntjänstleverantör.[23]

En sak som står klart genom domen, vilket eSam också påpekar, är att det inte blir ett röjande per automatik bara för att en uppgift lagras hos en molntjänstleverantör. Man måste göra en bedömning av sannolikheten för att t.ex. molntjänstleverantörens personal ska ta del av uppgifterna, vilket bl.a. kan påverkas av förekomsten av sekretessklausuler i avtalet eller tekniska begränsningar i system.[24] Målet från Högsta

[22] NJA 1991 s. 103

[23] Högsta Domstolens bedömning i NJA 1991 s. 103 har senare tillämpats av Arbetsdomstolen i mål nr 15/19 mål nr A 152/17, dock utan att skapa närmare klarhet i begreppets innebörd. I målet lyckades käranden inte bevisa att kravet på att ”måste kunna räkna med” hade uppfyllts.

[24] eSam ”Outsourcing 2.0 – En vägledning om sekretess och dataskydd”, december 2019, s. 45.

Domstolen rörde dock, vilket eSam helt korrekt påpekar,[25] en tolkning av begreppet röjande *enligt brottsbalken*, och inte enligt offentlighets- och sekretesslagen. Av förarbetena till offentlighets- och sekretesslagen framgår att kravet på röjande behöver vara lägre enligt denna lag än enligt brottsbalken.[26] Det ska alltså krävas en lägre sannolikhetsgrad än att ”kunna räkna med”. Men om det exempelvis är osannolikt att molntjänstleverantörens personal kommer att ta del av uppgifterna så är de inte röjda i offentlighets- och sekretesslagens mening.

Någon annan rättspraxis av större relevans för frågan om offentlighet, sekretess och molntjänster är svår att hitta. Det är med denna praxis som ingångsvärde som eSams uttalanden kan analyseras.

4.2 eSams uppfunna rekvisit – ett krav på rättsliga förpliktelser

I appendix 1 till detta dokument har vi gjort en djupare analys av eSams rättsliga uttalanden och egna analyser rörande framförallt röjandebegreppet. Vi har inte i onödan velat tynga texten för läsaren. Det som dock kan konstateras utifrån vår gjorda analys är att eSam baserar sin uppfattning, att det efter CLOUD Acts ikraftträdande inte är möjligt för myndigheter att köpa molntjänster av leverantörer som omfattas av denna lagstiftning, på en tolkning av röjandebegreppet som är väldigt svår att förstå, för att inte säga helt felaktig..

Mer specifikt verkar eSam helt enkelt ha uppfunnit ett nytt rekvisit för att bedöma om ett röjande ska anses ha skett – ett rekvisit som saknar stöd i såväl lagtext, förarbeten som praxis. Läsaren hänvisas till appendix 1 för den djupare analysen. Här räcker det att konstatera att:

- eSam har, för att ett röjande inte ska anses ha ägt rum, *utöver ett krav på sannolikhet*, också infört ett krav på rättsliga förpliktelser, bestående i att molntjänstleverantören
    - i molntjänstavtalet inte får omfattas av undantag från ett grundförbud mot att vidareförmedla uppgifter till utländska myndighet, och
    - inte heller får omfattas av tvingande regler i utländska rättsordningar på utlämnande av uppgifter,
- detta krav saknar det stöd i förarbetena till offentlighet- och sekretesslagen som eSam menar finns,
- detta krav saknar det stöd i 8 kap. 3 § OSL som eSam menar finns,
- detta krav saknar stöd i den något märkliga analogi med jordabalkens uppdelning av rättsliga och faktiska fel som eSam för fram, samt att
- detta krav inte har stöd i Försäkringskassans vitbok, eftersom Försäkringskassan i denna vitbok ju stödjer sig på eSam i *sin* argumentation i samma fråga vilket således leder till cirkelreferenser.

[25] Se t.ex. eSam ”Outsourcing 2.0 – En vägledning om sekretess och dataskydd”, december 2019, s. 44. Vi noterar att ett antal debattörer som förhåller sig kritiska till eSam i övrigt verkar ha missat det som eSam här helt korrekt har identifierat, och istället tror att det även enligt OSL är kravet ”måste kunna räkna med” som gäller för att ett röjande ska anses ske.

[26] Prop. 1979/80:2 Del A s. 85.

Sammantaget kan vi således inte se att det finns något juridiskt stöd för att i röjandebegreppet, utöver en sannolikhetsbedömning, också tolka in det krav på rättsliga förpliktelser på eSam påstår sig ha funnit stöd för.

4.3 Röjande och sannolikhet

Givet att det inte finns något stöd för eSams nya rekvisit kvarstår endast *en* analys att göra vid bedömningen av om ett röjande ska anses ske i förhållande till en molntjänstleverantör, nämligen en analys av hur *sannolikt* det är att molntjänstleverantören själv kommer att få del av utlämnade uppgifter eller att denne kommer att vidareförmedla uppgifterna till utomstående.

Som framgått ovan är eSam tydliga med att Högsta Domstolens dom i NJA 1991. s. 103 innebär att en uppgift inte per automatik ska anses vara röjd, så fort den lagras hos molntjänstleverantören. Ett antal faktorer måste bedömas, t.ex. kontraktuella eller tekniska begränsningar, för att bedöma sannolikheten om t.ex. leverantörens personal kommer att ta del av uppgifterna. Men detta skulle således inte, enligt eSam, gälla om leverantören omfattas av CLOUD Act. Då verkar eSam istället mena att uppgifterna per automatik ska anses vara röjda. I sitt rättsliga uttalande från 2018 menade eSam ju, som vi har sett, att antagandet av CLOUD Act skulle ha medfört att det inte längre var osannolikt att uppgifter skulle vidareförmedlas till sådana myndigheter.

Denna uppfattning framstår som mycket märklig. Det framstår istället som nästan självklart att det *inte* är sannolikt att en enskild uppgift som en myndighet lagrar hos en molntjänstleverantör ska vidareförmedlas på det sättet, framförallt inte per automatik bara för att en uppgift lagras hos molntjänstleverantören.

Det är utan tvekan så att rättsläget inte är helt klart hur röjandebegreppet ska tolkas. Men det kan nog rätt klart konstateras att den tolkning som eSam har gjort till stora delar är felaktig. Tvärtemot vad eSam anför verkar det mesta tala för att offentlighets- och sekretesslagen *inte* skulle förhindra köp av molntjänster från leverantörer som omfattas av CLOUD Act eller motsvarande lagstiftning.

5 Skyddet för personuppgifter

Vårt fokus i denna skrift och i vårt förslag till framtida regler nedan ligger på möjligheten för offentliga aktörer att använda molntjänster i förenlighet med offentlighets- och sekretesslagen. I den allmänna debatten kring detta har dock också frågan uppkommit om möjligheten att använda molntjänster i förenlighet med även dataskyddsförordningen, där molntjänstleverantören omfattas av CLOUD Act.

Frågan har inte minst uppkommit p.g.a. det grundläggande förbudet enligt t.ex. artikel 44 i dataskyddsförordningen att överföra personuppgifter till tredje land, exempelvis USA, såvida inte något undantag föreligger enligt reglerna i kapitel 5 i förordningen.[27] Vidare får, enligt artikel 28.1 i dataskyddsförordningen, en köpare av en molntjänst endast anlita leverantörer (personuppgiftsbiträden) som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas. Kan en leverantör som omfattas av CLOUD Act anses kunna ge sådana tillräckliga garantier?

Vi kommer här inte att presentera en djupare beskrivning av vilka krav som enligt dataskyddsförordningen måste uppfyllas vid köp av molntjänster. Inte heller av frågan om dataskyddsförordningens förhållande till t.ex. CLOUD Act. I appendix 2 redogör vi övergripande för frågan.

Vi vill dock framhålla att det inte finns något stöd i dataskyddsförordningen för att principiellt påstå att det enligt förordningen skulle vara otillåtet att köpa molntjänster från leverantörer som omfattas av CLOUD Act. Ett sådant påstående vittnar om en bristande förståelse för det riskbaserade synsätt som förordningens vilar på.

[27] Det finns också en fråga där både offentlighets- och sekretesslagen och dataskyddsförordningen aktualiseras samtidigt. Enligt 21 kap. 7 offentlighets- och sekretesslagen gäller nämligen sekretess för personuppgift om det kan antas att uppgiften kommer att behandlas i strid med dataskyddsförordningen. För att denna regel ska bli tillämplig krävs, enligt beskrivningen i avsnitt 2 ovan, att uppgiften först ska anses vara *röjd*. Som framgått av analysen ovan torde själva existensen av CLOUD Act inte, trots eSams påstående om motsatsen, innebära att uppgifter röjs om de lagras hos en molntjänstleverantör som omfattas av det regelverket. Denna bestämmelse i OSL har därför begränsad betydelse i sammanhanget.

6 Framtida lagstiftning

Mot bakgrund av analysen ovan och dess fördjupning i appendix 1 angående offentlighets- och sekretesslagen kan man fråga sig varför en utredning angående bl.a. tydliggörande lagstiftning ska behöva tillsättas. Rättsläget förefaller inte så oklart trots allt. Samtidigt välkomnar vi att förtydliganden sker, inte minst eftersom situationen har blivit rörig mot bakgrund av den historik som beskrivits ovan och de konsekvenser som eSams uttalanden har fått.

I de, i avsnitt 3, nämnda kommitédirektiven till en utredning har förslag till ny eller uppdaterad lagstiftning en underordnad roll. Direktiven handlar först och främst om vad som med inköpsterminologi måste kallas en sourcingstrategi för IT-tjänster inom staten. Tre alternativ – egen drift, samordnad it-drift eller utkontrakterad it-drift – ska utredas, både vad avser myndigheters behov och förmåga och avseende rättsliga och säkerhetsmässiga förutsättningar.

Men även om juridiken här är underordnad så ligger det förstås i kommiténs uppdrag att även se över lagstiftningen. I det följande kommer vi därför att fokusera på de rent rättsliga aspekterna. Vi har här tre rekommendationer för framtida lagstiftning:

6.1 Tydliggör röjandebegreppets innebörd

Utredningen skulle kunna skapa mycket klarhet genom att helt enkelt tydliggöra röjandebegreppets innebörd. Det skulle till och med kunna tänkas att detta är det enda tydliggörande som görs. Att låta detta begrepp vila på något annat än en bedömning av sannolikhet för att t.ex. en molntjänstleverantör får del av uppgifter verkar inte möjligt mot bakgrund av befintlig lagtext, förarbeten och rättspraxis. Tyvärr har dock eSams analyser och uttalanden kraftigt förvirrat situationen, varför ett tydliggörande vore på sin plats. Exempelvis vore det önskvärt med tydligare anvisningar kring vilka typer av faktorer som ska påverka bedömningen av hur sannolikt det är att en molntjänstleverantör tar del av uppgifter, t.ex. genom tekniska eller andra begränsningar.

Vi anser dock att detta inte räcker, av det enkla skälet att uppgifter under vissa förutsättningar kan komma att anses vara röjda för molntjänstleverantören. Exempelvis om avsikten är att leverantören ska ta del av uppgifterna. Men därmed är de inte, vilket behöver understrykas, röjda för brottsbekämpande myndigheter i USA, utan för molntjänstleverantören. Och då uppstår ett antal följdfrågor kopplade till om uppgifterna ska anses vara sekretessbelagda i förhållande till molntjänstleverantören eller inte. Dessa frågor hanteras inte genom att endast fokusera på ett förtydligande av röjandebegreppets innebörd. Dessutom finns det, som kommer att framgå nedan, behov av tydligare regler rörande t.ex. informationssäkerhet inom offentlig sektor, vilka inte heller hanteras genom detta enkla alternativ.

6.2 Anta Digitaliseringsrättsutredningens förslag

För att skapa den klarhet som behövs anser vi vidare att det lämpligaste är att helt enkelt anta Digitaliseringsrättsutredningens redan lagda förslag till uppdatering av offentlighets- och sekretesslagen, som nämndes i avsnitt 3.

Här är det först viktigt att återigen understryka att den här refererade debatten, rent juridiskt, handlar om vad som ska anses vara ett *röjande* i offentlighets- och sekretesslagens mening. Digitaliseringsrättsutredningen hade inte röjandebegreppet i fokus.

Det hindrar dock inte att Digitaliseringsrättsutredningens förslag enligt vår mening bör ligga till grund för en diskussion om framtida lösningar. Men då ska noteras att dessa förslag endast blir aktuella under förutsättning att man först konstaterar att ett röjande i offentlighets- och sekretesslagens mening har ägt rum.

I det av Digitaliseringsrättsutredningen lämnade förslaget till en ny lag föreslogs 4 § att lyda:

> Den som på grund av anställning eller uppdrag hos en privat leverantör tekniskt bearbetar eller tekniskt lagrar uppgifter för en myndighets räkning, får inte obehörigen röja eller utnyttja dessa uppgifter. I det allmännas verksamhet tillämpas i stället bestämmelserna i offentlighets- och sekretesslagen.

Detta förslag till en s.k. lagstadgad tystnadsplikt syftar primärt till att hantera den problematik som JO lyfte i sitt beslut 2014, där JO ansåg att en enbart avtalsreglerad tystnadsplikt inte räcker för att undvika att bestämmelser med ett s.k. omvänt skaderekvisit enligt offentlighets- och sekretesslagen uppfylls. Digitaliseringsutredningen för ett väl utvecklat resonemang kring behovet av och utformningen av denna bestämmelse.[28]

En lagstadgad tystnadsplikt för molntjänstleverantören kommer dock inte att möjliggöra att all typ av information utkontrakteras till en privat molntjänstleverantör. Det finns uppgifter som omfattas av s.k. absolut sekretess. För att sådan information skulle kunna utkontrakteras krävs antingen en definition av röjandebegreppet eller en s.k. sekretessbrytande bestämmelse. Digitaliseringsutredningen valde här det senare alternativet och föreslog en ny 10 kap. 2 a § offentlighets- och sekretesslagen: [29]

> Sekretess hindrar inte att en uppgift lämnas ut till en enskild eller till en annan myndighet som utför uppdrag för enbart teknisk bearbetning eller teknisk lagring för den utlämnande myndighetens räkning, om uppgiften behövs för att utföra uppdraget.
>
> En uppgift ska inte lämnas ut om
>
> 1. övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut, eller
> 2. det av andra skäl är olämpligt.

Om de två nya bestämmelser som utredningen föreslog ska tillämpas, kommer en prövning i tre steg att behöva göras. Först och främst behöver man bedöma om ett röjande alls sker. Om man anser att så är fallet kommer man att behöva bedöma om skaderekvisiten i någon av offentlighets- och sekretesslagens bestämmelser är uppfyllda. Genom 4 § i förslaget till ny lag borde man då komma fram till att den lagreglerade sekretessen gör att vare sig bestämmelser med s.k. raka eller omvända

[28] SOU 2018:24, s. 355 – 372.

[29] SOU 2018:24, s. 374.

skaderekvisit uppfylls. Eftersom överträdelse av den lagstadgade sekretessen, enligt Digitaliseringsrättsutredningens analys, kommer att vara straffsanktionerad för både svenska och utländska medborgare, medför denna sekretess ett mycket starkt incitament att hemlighålla informationen.

Det blir endast om det rör sig om en bestämmelse med s.k. absolut skaderekvisit som man kommer att behöva tillämpa den sekretessbrytande bestämmelsen i den föreslagna 10 kap. 2 a § OSL och då i den intresse- och lämplighetsbedömning som där föreslås. Enligt vår uppfattning uppfattar vi det som lämpligt att, när det gäller uppgifter som skyddas av absolut sekretess, denna typ av intresseavvägning görs.

6.3 Ytterligare tillägg

Även om Digitaliseringsrättsutredningens förslag är bra anser vi dock att de inte är tillräckliga. Vi anser att ytterligare tillägg behövs.

6.3.1 Tydligare regler om informationssäkerhet inom staten

Digitaliseringsrättsutredningen påpekade att förslaget till en uppdaterad 10 kap. 2 § offentlighets och sekretesslagen inte syftade till ”att bli ett frikort för utkontraktering av känslig informationshantering.”[30] I ljuset av Riksrevisionens återkommande och senast hösten 2019 publicerade rapporter om brister i offentliga myndigheters informationssäkerhet är detta förstås viktigt. Digitaliseringsrättsutredningen föreslog också att regeringen skulle låta utreda förutsättningarna för att ta fram en kompletterande reglering om informationssäkerhet, omfattandes hela den offentliga förvaltningen.[31] Vi kan inte annat ställa oss bakom Digitaliseringsrättsutredningens förslag i denna del och hoppas att den nu inrättade kommittén gör verklighet av förslaget.

6.3.2 Klargöranden avseende CLOUD Act och motsvarande lagstiftning

Vidare är det inte säkert hur Digitaliseringsrättsutredningens förslag förhåller sig till utkontraktering till privata molntjänstleverantörer som omfattas av CLOUD Act eller motsvarande lagstiftning. Här finns olika spår som utredningen skulle kunna ta.

Ett spår är att helt enkelt luta sig mot en tydliggörande tolkning av röjandebegreppet. Det blir här, som redan anförts, tyvärr viktigt att åtgärda den förvirring som eSam har skapat, exempelvis genom sitt försök att luta sig mot 8 kap. 3 § offentlighets- och sekretesslagen.[32]

Ett annat spår skulle vara att plocka upp är de rent politiska frågor som Försäkringskassan lyfter i sin vitbok kring lämpligheten att utkontraktera till leverantörer som omfattas av sådan lagstiftning. Att välja detta spår ser vi dock som riskfyllt. Inte för att det är fel i sig, utan för att Försäkringskassan har knutit an sina frågor till det oklara och laddade begreppet ”digital suveränitet”. Suveränitet är i princip ett statsrättsligt begrepp, och skulle kunna avse grad av andra staters inbladning i svenska förhållanden. Men i debatten om detta begrepp handlar det också ofta om det faktum att molntjänstmarknaden domineras av ett antal större aktörer vilka alla är amerikanska. Denna marknadskoncentration har endast begränsat med suveränitet i statsrättslig mening att göra. Vi anser att det finns en tydlig risk att ännu mer oklarhet istället för klarhet skapas genom att basera diskussionen på detta begrepp.

[30] SOU 2018:24, s. 384.

[31] SOU 2018:25, s. 329.

[32] Se analys i appendix 1.

Vår uppfattning är återigen att det är lämpligast att här luta sig mot en kombination av ett förtydligande avseende röjandebegreppet och Digitaliseringsrättsutredningens förslag.

Om en uppgift är röjd eller inte är som sagt primärt en fråga om sannolikheten för att någon får del av utlämnade uppgifter. Som framgått ovan förefaller det åtminstone enligt vår mening vara väldigt osannolikt att en uppgift som lämnas till en privat molntjänstleverantör också skulle delas med en brottsbekämpande myndighet i t.ex. USA.[33] Men ett tydliggörande kring hur röjandebegreppet ska tolkas vore som sagt välkommet.

Vidare kommer, enligt Digitaliseringsrättsutredningens förslag, uppgifter som röjs för en molntjänstleverantör att omfattas av en lagreglerad och därmed också straffsanktionerad tystnadsplikt. Vi har svårt att se att regleringar som CLOUD Act eller liknande skulle ha någon egen betydelse för bedömningen av om s.k. raka eller omvända skaderekvisit är uppfyllda eller inte enligt offentlighets- och sekretesslagens bestämmelser. En lagreglerad tystnadsplikt förefaller vara det bästa sättet att uppnå den grad av informationskontroll som man eftersträvar, oavsett om detta kallas för digital suveränitet eller inte.

Genom tydliggöranden kring röjandebegreppet och införande av en lagstadgad tystnadsplikt enligt Digitaliseringsrättsutredningens förslag kan således alla oklarheter rörande CLOUD Act sannolikt hanteras.

6.3.3 Klargöranden avseende användning av underleverantörer

Vi vill slutligen påpeka att det vore värdefullt att tydliggöra hur de nya reglerna ska tillämpas i förhållande till eventuella underleverantörer till den anlitade molntjänstleverantören. Detta var en fråga som lyftes av Pensionsmyndigheten i dess utredning från år 2016.[34]

För att en myndighet ska kunna göra en bedömning enligt offentlighets- och sekretesslagen vid utkontraktering till en privat molntjänstleverantör är det rimligen nödvändigt att göra denna bedömning i förhållande till hela leverantörskedjan. Är tjänsten upplagd så att personal hos molntjänstleverantören *eller dess underleverantörer* kommer att få del av uppgifterna på ett sådant sätt att de ska anses röjas? Om denna fråga besvaras jakande kommer Digitaliseringsrättsutredningens förslag till en lagreglerad tystnadsplikt i 4 § i en ny lag att omfatta även sådana underleverantörer, som också omfattar den som ”på uppdrag” av en molntjänstleverantör tekniskt bearbetar eller lagrar uppgifter. Men samtidigt vore det önskvärt med ytterligare detaljer i denna del.

---

[33] Här är det viktigt att påpeka att bedömningen av röjande förstås måste ske när uppgiften lämnas ut till molntjänstleverantören. Vad som sedan må ske i ett senare skede påverkar förstås inte röjandebedömningen (utan endast sannolikheten för att något kommer att ske).

[34] Se avsnitt 3 ovan.

APPENDIX 1 - ANALYS AV ESAMS UTTALANDEN KRING RÖJANDEBEGREPPET

I detta appendix beskriver vi närmare eSams uttalanden och vägledningar rörande begreppet röjande. Som framgår av analysen har eSam tolkat in ett nytt rekvisit i bedömning av om röjande ska anses ha skett, utöver det krav på sannolikhet som fastslagits av Högsta Domstolen i NJA 1991 s. 103. Rekvisitet innebär att det krävs en rättslig förpliktelse för molntjänstleverantören att inte ta del av eller vidareförmedla uppgifter för att ett röjande inte ska anses ske samt att leverantören inte får omfattas av skyldigheter till utlämnande enligt utländsk rättsordning.

eSams första vägledning om outsourcing samt uttalande från 2015 eSams nya rekvisit går tillbaka till eSams tidiga analyser i sin första vägledning om outsourcing samt det rättsliga uttalandet från 2015, även om det stod klart först senare hur viktigt detta nya rekvisit skulle bli. När eSam började dessa analyser fanns endast det ovan refererade rättsfallet från Högsta Domstolen att tillgå utöver förarbetena för att tolka röjandebegreppet. Domstolen hade då gjort frågan om röjande till en sannolikhetsfråga, med uttrycker att ”man måste kunna räkna med”.[35]

I sin första vägledning om outsourcing samt sitt rättsliga uttalande från 2015 menade eSam dock att ett röjande enligt offentlighets- och sekretesslagen inte ska anses ske

> om tjänsteleverantören och dennes personal inte *får* ta del av eller vidarebefordra uppgifterna och omständigheterna i övrigt medför att det är *osannolikt* att detta ändå sker. [vår kurs][36]

Detta konstaterande innefattar två element – ett rättighetselement och ett sannolikhetselement. Enligt *rättighetselement* ska molntjänstleverantören inte ha rätt att ta del av eller vidareförmedla uppgifterna. Enligt *sannolikhetselementet* ska omständigheterna i övrigt innebära att det är osannolikt att uppgifterna ändå tas emot eller vidareförmedlas av leverantören.

Det som vi här benämner sannolikhetselementet har eSam förstås hämtat från Högsta Domstolens dom från 1991. Genom en helt korrekt juridisk analys av denna dom och förarbetena till offentlighets- och sekretesslagen kom eSam fram till att kravet på röjande enligt offentlighets- och sekretesslagen måste vara lägre än det för brottsbalken gällande ”måste kunna räkna med”, enligt beskrivningen ovan.

Det är dock oklart hur eSam kommit fram till att det skulle finnas ett, som vi kallar det, rättighetselement i röjandebegreppet. I sin första vägledning om outsourcing refererar eSam till förarbetena och skriver

> I förarbetena till sekretesslagen anges att innebörden av röjandeförbudet är att ”befattningshavaren inte får låta någon ta del av hemlig uppgift vare sig detta sker genom att allmän handling företes eller att någon får ta del av handling som inte är allmän eller att uppgiften meddelas i brev. Också andra former av röjande av en uppgift kan tänkas, t.ex. att någon förevisar ett hemligt föremål för annan.”

[35] Högsta Domstolen uttalade: ”Avgörande för straffansvar bör främst vara om uppgiften har blivit tillgänglig för någon obehörig under sådana omständigheter, att man måste räkna med att den obehörige kommer att ta del av uppgiften.”

[36] eSam, “Röjandebegreppet enligt offentlighets- och sekretesslagen”, 17 december 2015.

> Enligt eSams bedömning *indikerar* denna formulering att ett röjande innebär inte bara att befattningshavaren gör uppgiften tillgänglig för annan, utan också att mottagaren förutsätts ta del av uppgiften i fråga eller åtminstone har *rätt att göra det*. Översatt till en elektronisk kontext skulle man kunna säga att ett röjande innebär inte bara att data görs tekniskt tillgängliga för mottagaren, utan också att denne förutsätts ta del av det faktiska informationsinnehållet eller åtminstone har *rätt att göra det*. [vår kursivering][37]

Detta citat är helt avgörande, för det är i princip här som grunden läggs för det som senare skulle visa sig bli en uppfattning att det inte är möjligt att köpa molntjänster från en leverantör av publika molntjänster som omfattas av CLOUD Act. Det är därför viktigt att konstatera att det räcker att läsa innantill i det av eSam citerade förarbetsuttalandet för att konstatera att det faktiskt *inte finns någonting* i uttalandet som *indikerar* att ett röjande skulle handla om en mottagares rätt att ta del av uppgifterna, framförallt inte om en rätt som skulle gälla som någonting som gäller oberoende av frågan om sannolikheten att mottagaren (molntjänstleverantören) får del av eller vidareförmedlar uppgifter.

Från osannolikt till inte längre osannolikt. I mars 2018 antogs CLOUD Act, vilket som sagt föranledde att nytt rättsligt uttalande från eSam. I detta uttalande figurerade inte de båda elementen från uttalandet 2015 utan istället endast sannolikhetselementet.

I uttalandet skrev eSam att utlämnande till privata aktörer som omfattas av lagstiftning som CLOUD Act ska anses utgöra ett röjande. eSam gjorde härvid det väsentliga uttalandet:

> Anledningen är att det *inte längre är osannolikt* att uppgifterna kan komma att lämnas till utomstående. [vår kurs][38]

eSam avgjorde här således frågan på sannolikhetselementet och det som vi benämner rättighetselementet från uttalandet 2015 nämns inte alls.[39]

Det är i stort sett denna förskjutning från *osannolikt* år 2015 till *inte längre osannolikt* 2018 som förklarar den påverkan som CLOUD Act har fått på offentliga aktörers användning av molntjänster.

Denna förskjutning är intressant, inte minst som den framstår som så uppenbart felaktig. När en framtida händelse inte längre är osannolik är den sannolik. Men det faktum att CLOUD Act trädde ikraft gjorde det självklart inte sannolikt att en viss uppgift som lämnats ut till en privat molntjänstleverantör lämnas ut till brottsbekämpande myndigheter i USA. Av alla miljontals dokument, mail och andra filer som lagras hos en molntjänstleverantör är det tvärtom väldigt osannolikt, något som har påpekats av många. Man behöver fråga sig om det finns vissa kategorier av information där det skulle vara mer sannolikt att de skulle begäras ut av brottsbekämpande myndigheter, men detta torde vara ett undantagsfall.

eSam under 2019 eSam verkar senare ha insett svagheten i sin ändrade ståndpunkt i sannolikhetsfrågan och försökte först i sitt kompletterande rättsliga uttalande i september 2019 och sedan i sin uppdaterade vägledning om outsourcing från december samma år rädda situationen.

---

[37] eSam, ”Outsourcing – en vägledning om sekretess och persondataskydd”, 2015, s. 17.

[38] eSam, ”Rättsligt uttalande om röjande och molntjänster”, 23 oktober 2018, s. 1

[39] Det ska dock noteras eSam synes ha menat att det är själva det faktum att leverantören omfattas av skyldigheter att lämna ut uppgifter enligt utländsk rättsordning som gör att det inte längre är osannolikt att uppgifterna lämnas ut. eSam skriver att ”sekretessreglerade uppgifter [får] anses bli röjda om de lämnas till ett företag som omfattas av en förpliktelse” enligt utländsk rättsordning att lämna ut uppgifter. (eSam, ”Rättsligt uttalande om röjande och molntjänster”, 23 oktober 2018, s. 2.)

I sitt rättsliga uttalande från september 2019 återvände eSam till sitt uttalande från 2015 och återupptog det som vi ovan har kallat rättighetselementet, d.v.s. att mottagarens rätt att ta emot eller vidareförmedla uppgifter är ett eget moment i bedömning av om röjande ska anses ha skett, helt oberoende av sannolikhetsfrågan:

> Det räcker alltså inte att göra en sannolikhetsbedömning. *Först måste den rättsliga regleringen av parternas mellanhavande ha utformats på ett hållbart sätt*. [vår kurs][40]

eSam menade att detta var ett förtydligande av vad man redan hade sagt i uttalandet från 2015. I så måtto att eSam faktiskt antydde det vi har kallat ett rättighetselement i detta uttalande stämmer det, med det problemet att rättighetselementet inte har något stöd i vare sig lagtext, förarbeten eller praxis, som redan framgått ovan.

Det ska emellertid noteras att eSam, i 2019 års uttalande, inte *bara* försökte förtydliga 2015 års uttalande. Man gjorde *dessutom* ett tillägg, vilket inte följer uttalandet från 2015. eSam menade nämligen att det ska anses vara ett röjande, inte bara om avtalet ger leverantören *rätt* att ta del av eller vidareförmedlade uppgifter, utan också om denne är *skyldig* att göra det enligt en annan rättsordning. Även detta nya krav gäller oberoende av en sannolikhetsbedömning:

> Om det följer av den svenska myndighetens rättsliga bedömning att ett utlämnande till en utländsk myndighet får ske enligt det avtal som skulle reglera parternas mellanhavande *eller kan tjänsteleverantören på grund av regler i en främmande rättsordning bli tvungen att lämna ut uppgifter blir en sannolikhetsbedömning inte aktuell*. [vår kurs][41]

Att *enligt avtal* inte ha *rätt* att lämna ut uppgifter är något annat än att *enligt utländsk rättsordning* vara skyldig att lämna ut uppgifter och eSam är föga övertygande i sitt påstående att uttalandet från 2019 endast skulle vara ett förtydligande av vad man skrev redan 2015. Tankarna förs till en efterhandskonstruktion.

Stöd i 8 kap. 3 § 2 st OSL? Tanken kring en efterhandskonstruktion förstärks när man frågar sig vad eSam anser sig ha för stöd för sin tolkning av röjandebegreppet i yttrandet från 2019. eSam försökte nämligen hitta stöd för sitt nya rekvisit i *8 kap. 3 § offentlighets och sekretesslagen*, enligt vilken, som huvudregel, uppgift för vilken sekretess gäller enligt OSL inte får röjas för en utländsk myndighet eller en mellanfolklig organisation. I sin uppdaterade vägledning om outsourcing gjorde eSam en tillbakablick på sina rättsliga uttalanden från 2015 och 2018 och menade att det senare uttalandet, där den viktiga vändningen till ”inte längre osannolikt” gjordes, ska läsas som om det bygger på denna paragraf.

Påståendet är intressant eftersom 8 kap. 3 § OSL *inte nämns någonstans* i uttalandet från 2018, trots att uttalandet alltså skulle bygga på denna paragraf. Vilket alltså förstärker tanken om en efterhandskonstruktion sedan man insett att det kanske inte är så sannolikt att uppgifter vidareförmedlas till brottsbekämpande myndigheter i USA.

eSam gör dessutom, i yttrandet från 2019, en helt felaktig tolkning av 8 kap. 3 § OSL, vilket dock är lätt att missa. eSam skriver:

> Av 8 kap. 3 § 2 offentlighets och sekretesslagen (2009:400; OSL) följer att en myndighet *inte får lämna en uppgift* till en utländsk myndighet utan att den svenska myndigheten först har gjort en prövning av att

[40] ”Kompletterande information om molntjänster”, 20 september 2019, s. 1.

[41] ”Kompletterande information om molntjänster”, 20 september 2019, 2

> uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet. [vårs kurs].[42]

I 8 kap. 3 § OSL står det dock inte att en myndighet ”inte får lämna en uppgift”. I paragrafen står det är att en myndighet inte får *röja* en uppgift, såvida inte något av undantagen i bestämmelsen är uppfyllda. För att tillämpa bestämmelsen måste man därför *först* göra en prövning om uppgiften ska anses vara röjd, och *därefter* undersöka om något av undantagen i bestämmelsen är uppfyllda. Medvetet eller omedvetet så väljer eSam istället uttrycket ”inte får lämna en uppgift”, och tolkar hela bestämmelsen som att så länge inte undantagen i bestämmelsen är uppfyllda är uppfyllda så får uppgiften inte ”lämnas ut”.

Så går det dock förstås inte att resonera. För att kunna tillämpa 8 kap. 3 § OSL måste man först tolka begreppet röja. Om uppgifter som lämnas ut inte ska anses vara röjda behöver man inte ens titta i undantagsbestämmelserna. Och 8 kap. 3 § OSL eller dess förarbeten innehåller ingenting som pekar på att begreppet röjande skulle handla något annat än om sannolikheten för att leverantören tar del av eller vidareförmedlar uppgifter som lämnats ut. Resonemanget är så felaktigt att det helt går att bortse från eSams uttalande från 2019.

Stöd i jordabalken? Kanske har eSam själva insett att argumentationen baserat på 8 kap. 3 § offentlighets- och sekretesslagen är svag. eSam försöker nämligen staga upp sin argumentation i en fotnot till den uppdaterade vägledningen om outsourcing. Tyvärr genom en analogi till jordabalkens uppdelning i *faktiska* och *rättsliga* fel i fastighet. Att lämna ut en uppgift utan en rättslig förpliktelse för leverantören att inte lämna den vidare, eller om den rättsordning som styr avtalet skulle innefatta en skyldighet för leverantören att lämna ut uppgifter, skulle då vara ett ”rättsligt fel” medan ett utlämnande när det är sannolikt att uppgifterna kommer att lämnas ut är ett ”faktiskt” fel. En analogi som tyvärr inte övertygar.[43] Det är i princip omöjligt att förstå hur eSam har kunnat göra denna analogi genom tolkning av den lagstiftning, de förarbeten och den praxis som finns.

Stöd i Försäkringskassans vitbok? Faktum är att eSam verkar ha insett svagheten även i detta fotnotsstödjande argument. Som ett slutligt försök att hitta rättsligt stöd för sin argumentation hänvisar eSam nämligen till Försäkringskassans vitbok.[44] I sin vitbok hänvisade Försäkringskassan dock till eSams rättsliga uttalanden till stöd för *sin* argumentation i samma fråga. Och eSam åberopar å sin sida Försäkringskassan som stöd för *sin* argumentation, som alltså åberopar eSam som stöd för samma argument. Vad blir det av två icke-rättskällor som hänvisar till varandra som stöd för sin argumentation? Denna cirkelreferens påverkar tyvärr allvarligt trovärdigheten i eSams analyser.

Analysen ovan är, det medges, snårig och rätt komplicerad. Vi har dock försökt göra vårt bästa för att i detalj analysera eSams uttalanden och visa på dess brister. eSams argumentation framstår som rimlig därför att man i en kedja av uttalanden och vägledningar till synes håller en konsistent linje. Problemet är dock att eSam inte håller en konsistent linje utan snarare verkar syssla med efterhandskonstruktioner, tydligast visat genom påståendet att uttalandet från 2018 skulle bygga på 8 kap. 3 § OSL, utan att denna paragraf ens nämns i detta uttalande.

Problemet är också att det inte spelar någon roll om eSam hade hållit en konsistent linje. eSam är ingen rättskälla utan måste stödja sig på lagtext, förarbeten och praxis i sin argumentation. Det finns *ingenting* i dessa rättskällor som ger stöd för att det skulle finnas något annat än sannolikhet för att leverantören tar del av eller lämnar ut uppgifterna som ska vägas in i en bedömning av röjande. Hela eSams argumentation vilar ytterst på *två* hänvisningar till några rättskällor,

---

[42] ”Kompletterande information om molntjänster”, 20 september 2019, s. 1f.

[43] eSam, Outsourcing 2.0 – En vägledning om sekretess och dataskydd, december 2019, s. 67.

[44] Ibid., s. 68.

nämligen (i) ett förarbetsuttalande som, tvärtemot vad eSam påstår, inte alls *indikerar* att röjandebedömningen skulle innefatta ett krav på rättsliga förpliktelser, än mindre skyldigheter enligt utländsk lag, samt (ii) 8 kap. 3 § OSL, som eSam alltså tolkar helt felaktigt. Det finns helt enkelt inget stöd för eSams påstående att röjande skulle handla om något annat än *sannolikheten* för att leverantören tar del av eller vidareförmedlar uppgifter.

Mot bakgrund av analysen ovan kan alltså konstateras att:

- eSam har, för att ett röjande inte ska anses ha ägt rum, *utöver ett krav på sannolikhet*, också infört ett krav på rättsliga förpliktelser, bestående i att molntjänstleverantören
    - i molntjänstavtalet inte får omfattas av undantag från ett grundförbud mot att vidareförmedla uppgifter till utländska myndighet, och
    - inte heller får omfattas av tvingande regler i utländska rättsordningar på utlämnande av uppgifter,
- detta krav saknar det stöd i förarbetena till offentlighet- och sekretesslagen som eSam menar finns,
- detta krav saknar det stöd i 8 kap. 3 § OSL som eSam menar finns,
- detta krav saknar stöd i den analogi med jordabalkens uppdelning av rättsliga och faktiska fel som eSam för fram, samt att
- detta krav inte har stöd i Försäkringskassans vitbok, som inte utgör någon rättskälla och som dessutom i sin tur hänvisar till eSam självt som stöd för sin argumentation.

_____

APPENDIX 2 – SKYDDET FÖR PERSONUPPGIFTER

I detta appendix redogör vi kort för varför det inte går att principiellt hävda att det skulle stå i strid med dataskyddsförordningen att använda molntjänster från en leverantör som omfattas av CLOUD Act eller motsvarande lagstiftning.

Artikel 44 och övriga artiklar i kapitel 5 i dataskyddsförordningen handlar om tredjelandsöverföringar. En offentlig aktör som använder en molntjänst från en leverantör som omfattas av CLOUD Act överför inte med automatik personuppgifter till tredje land redan genom sitt användande av molntjänsten. Därför har just reglerna i kapitel 5 begränsad betydelse i sammanhanget.

Den mer relevanta frågan är istället om det är förenligt med artikel 28.1 och kravet på att endast använda personuppgiftsbiträden som kan lämna tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i förordningen och säkerställer att den registrerades rättigheter skyddas.

Det går förstås inte att förneka att det finns en teoretisk risk att en personuppgift som en myndighet lagrar hos en molntjänstleverantör som omfattas av CLOUD Act kommer att bli utlämnad till brottsbekämpande myndigheter i USA. Dataskyddsförordningen uppställer dock inte några absolut krav på åtgärder mot teoretiska risker. Förordningen vilar istället på ett riskbaserat synsätt, där åtgärder som vidtas ska anpassas till graden av risk för intrång i individers integritet. Detta synsätt framkommer t.ex. i kravet enligt artikel 24 att vidta *lämpliga* tekniska och organisatoriska åtgärder för att säkerställa att behandlingen av personuppgifter sker i enlighet med förordningen. I lämplighetsbedömningen ska bl.a. behandlingens art, omfattning samt risker för fysiska personers rättigheter och friheter beaktas, varvid såväl sannolikhet som allvarlighetsgrad ska beaktas i riskbedömningen. Liknande regler ställs upp i artikel 32, vilka mer specifikt handlar om informationssäkerhet.

Dessa regler innebär bl.a. att det inte finns några krav på att se till att IT-system är skyddade mot varje form av externt angrepp. Däremot finns t.ex. ett krav på att ha ökad säkerhetsnivå för personuppgifter som skulle orsaka mycket skada om de hamnar i obehöriga händer eller som av olika skäl skulle kunna vara attraktiva för externa angripare att komma åt.

Detta riskbaserade synsätt gäller förstås även artikel 28.1 i dataskyddsförordningen. Här måste CLOUD Act och risken för att personuppgifter ska lämnas ut till brottsbekämpande myndigheter i USA, och konsekvenserna av ett sådant utlämnande för den enskilde, beaktas på samma sätt som alla andra risker. I denna riskbedömning måste förstås både sannolikhet och allvarlighetsgrad beaktas, på samma sätt som i artiklarna 24 och 32. Det finns ingenting som säger att artikel 28.1 principiellt skulle överträdas bara för att leverantören omfattas av CLOUD Act.

I sannolikhetsbedömningen är det värt att påminna sig om motsvarande bedömning när det gäller frågan om röjande enligt offentlighets- och sekretesslagen. Då offentlighets- och sekretesslagen och dataskyddsförordningen är olika regelverk rör det sig förstås i strikt juridisk mening om olika sannolikhetsbedömningar. Samtidigt framstår det som motsägelsefullt att en uppgift som å ena sidan inte ska anses vara röjd i OSLs mening å andra sidan skulle anses vara föremål för så lågt skydd enligt dataskyddsförordningen att artikel 28.1 ska anses ha överträtts.

Det går dock inte heller att säga principiellt att CLOUD Act aldrig skulle kunna innebära att artikel 28.1 överträds. Vår poäng är att frågan måste bedömas från fall till fall, inte minst med beaktande av vilken information som den offentliga aktören avser att lagra i molntjänsten. Utgångspunkten måste härvid vara en informationsklassning, varefter en riskbedömning behöver göras för var och en av de identifierade informationskategorierna.

_____

Cirio Advokatbyrå AB I Box 3294 - 103 65 Stockholm I Mäster Samuelsgatan 20

08 527 916 00 I **www.cirio.se** | **contact@cirio.se**