Sveriges advokatsamfund

Stockholm den 29 april 2021

R-2021/0188

Till Infrastrukturdepartementet
I2021/00342

Sveriges advokatsamfund har genom remiss den 2 februari 2021 beretts tillfälle att avge yttrande över delbetänkandet Säker och kostnadseffektiv it-drift – rättsliga försättningar för utkontraktering (SOU 2021:1).

Sammanfattning

Advokatsamfundet tillstyrker utredningens förslag till första stycke i 10 kap. 2 a § offentlighets- och sekretesslagen (2009:440), OSL, dock med reservation mot det valda rekvisitet ”teknisk bearbetning eller teknisk lagring”. Advokatsamfundet avstyrker den föreslagna bestämmelsens andra stycke.

Advokatsamfundet är positivt inställt till utredningens förslag att införa en sekretessbrytande bestämmelse i OSL som tar sikte på att främja utkontraktering som ett led i myndigheters digitalisering. Advokatsamfundet gör emellertid andra bedömningar än utredningen i vissa centrala frågor, inbegripet röjandebegreppets innebörd och hur förutsättningarna för svenska myndigheters utkontraktering påverkas av främmande makts lagstiftning.

Advokatsamfundet menar att det är angeläget att regeringen överväger och utreder än kraftfullare lagstiftningsåtgärder för att underlätta och möjliggöra myndigheters utkontraktering av it-drift och användning av molntjänster. Rättsläget är för närvarande, med eller utan utredningens förslag, svåröverskådligt och fragmenterat

Laboratoriegatan 4, Box 27321, 102 54 Stockholm
Tfn 08-459 03 00, advokatsamfundet.se, info@advokatsamfundet.se

vilket försvårar att angelägna frågor om digitalisering, informationssäkerhet och upprätthållande av Sveriges digitala suveränitet drivs framåt. Advokatsamfundet efterlyser därför en bredare utredning med förslag till övergripande strategiska lagstiftningsåtgärder för att offentlig sektor ska kunna digitaliseras snabbare, mera enhetligt och effektivt – naturligtvis utan att göra avkall på viktiga rättsstatliga principer såsom suveränitetsprincipen, offentlighetsprincipen, legalitetsprincipen och skyddet för den enskildes rättssäkerhet och integritet.

Advokatsamfundet har ingen erinran mot utredningens förslag om en inskränkt meddelarfrihet för personer som träffas av lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter.

Synpunkter

Några allmänna synpunkter och reflektioner angående utredningen

Samhällets digitalisering förändrar tillvaron för alla myndigheter, företag, organisationer och medborgare. Utredningen reser allvarliga frågetecken kring hur den offentliga digitaliseringen har hanterats – och alltjämt hanteras – inom svensk offentlig förvaltning.

Utredningen visar bl.a. att endast hälften av Sveriges myndigheter har utfört grundläggande arbete kring informationssäkerhet (informationsklassning).[1] Vidare påstås, med hänvisning till en tidigare undersökning utförd av Myndigheten för Samhällsskydd och Beredskap (MSB), att 80 % av Sveriges kommuner idag har utkontrakterat sin it-drift.[2] Båda dessa siffror är anmärkningsvärda med beaktande av att, om utredningens tolkning av röjandebegreppet är riktig (jfr nedan), har all sådan utkontraktering skett i strid med gällande rätt, i vart fall när sekretessen är absolut eller där den prövning som annars krävs inte är möjlig att göra på hela materialet.

Advokatsamfundet befarar att de brister som utredningen påvisar vad gäller myndigheters informationssäkerhetsarbete kan innebära risker för såväl nationella säkerhetsintressen som för medborgarnas rättssäkerhet. Advokatsamfundet efterlyser därför mer omfattande insatser från regeringen för att säkerställa att myndigheters, regioners och kommuners digitalisering sker i enlighet med svensk lag och unionsrätt,

[1] Utredningen, s. 71 och 113.
[2] Utredningen, s. 54.

med användning av ändamålsenlig och kostnadseffektiv teknologi och utan betydande negativ inverkan på skyddet för den enskildes rättssäkerhet, privatliv och integritet.

Advokatsamfundet menar också att utredningens omvärldsanalys visar att såväl våra nordiska grannländer som Nederländerna och Storbritannien har kommit längre när det gäller styrning, samordning och upprättande av enhetliga ramverk för offentlig digitalisering.

Advokatsamfundet ser i denna del fram emot utredningens slutbetänkande, med förhoppning om att utredningens förslag kommer att innefatta både strategi och metod för att möjliggöra snabb förbättring och ökade samordningsvinster för den offentliga förvaltningens digitalisering.

Om utredningens begreppsanvändning (avsnitt 2.2.3 m.fl.)

En rimlig utgångspunkt för ny lagstiftning är att den i möjligaste mån utformas på ett teknikneutralt sätt utan onödiga kopplingar eller utgångspunkter i befintlig teknologi, produkt-/tjänstepaketeringar, trender eller branschspecifika begrepp. Denna utgångspunkt är särskilt motiverad i frågor om it och digitalisering, eftersom teknikutvecklingen sker i snabb takt vilket inte sällan leder till osäkerhet om hur befintliga författningar ska tillämpas på ny teknik. Advokatsamfundet menar mot den bakgrunden att äldre begrepp i lagstiftningen kritiskt bör utvärderas innan de förs vidare till ny lagstiftning, för att säkerställa att sådana begrepp inte har förlorat sin relevans i en modern kontext. En modernisering av lagstiftningen måste naturligtvis vägas mot den osäkerhet som kan skapas av nya och oprövade begrepp. Advokatsamfundet menar dock att det finns ett omfattande och generellt behov av att se över och, om det bedöms lämpligt, modernisera tillämplig lagstiftning kring offentlig digitalisering, men inte begränsat till bestämmelserna i OSL.

Begreppet ”it-drift” är omvittnat otydligt och utredningen ägnar stort utrymme åt att försöka definiera och avgränsa detta begrepp.[3] Liknande – och kanske ännu större – otydlighet finns i begreppet ”teknisk bearbetning eller lagring” som utredningen väljer som rekvisit för sitt förslag till sekretessbrytande bestämmelse (se vidare nedan).

Utredningen hade haft mycket att vinna på att – i stället för de relativt invecklade och svårbegripliga redogörelser som nu görs avseende t.ex. ”teknisk bearbetning”, ”it-drift”,

[3] Se bl.a. avsnitt 2.2.3 och 2.2.4 i utredningen.

”molntjänster”, ”samlokalisering”, ”arbetsplatstjänster”, ”applikationsdrift”, ”IaaS”, ”PaaS” och ”SaaS” – identifiera en minsta gemensam och rättsligt relevant nämnare för de tjänster som berörs av utredningen. Advokatsamfundet menar att vad som – från tekniskt perspektiv – utmärker alla de typer av it-tjänster som är relevanta för utredningen är att en myndighet uppdrar åt ett företag eller annan att hantera och ansvara för (åtminstone) de lägre ”lagren” i en systemarkitektur eller IT-miljö, dvs. den infrastruktur och de servrar som myndigheten använder för sin informationshantering och för myndighetens nätkommunikation för använda tjänster. Samma leverantör kan även ha ansvar för högre ”lager” – vilket innebär att tjänsten typiskt sett kallas något annat – men detta saknar rättslig betydelse i sammanhanget.

Advokatsamfundet inser att utredningen i viss mån varit bunden av hur dess uppdrag har formulerats men det hade, exempelvis, varit bättre att använda begreppet ”infrastrukturtjänster” på samma sätt som t.ex. IT-och telekomföretagen inom Almega gjort sedan 2014 i sina s.k. Allmänna bestämmelser. Ytterligare ett annat sätt att beskriva de it-tjänster som utredningen omfattar hade kunnat vara ”uppdrag som innebär att en myndighets information i digital form befinner sig i någon annans besittning, står under annans förfogande och/eller kontroll”.[4] Även andra formuleringar eller minsta gemensamma nämnare hade naturligtvis varit möjliga.

Utredningens tolkning av GDPR (avsnitt 7)

Advokatsamfundet menar att utredningen på ett olyckligt sätt gjort egna omfattande analyser och tolkningar av EU:s allmänna dataskyddsförordning (”GDPR”).[5] Merparten av bestämmelserna i GDPR är förbehållna unionsrättslig kompetens och uttolkning, inbegripet de delar som utredningen analyserar (kapitel V GDPR).

Utredningen konstaterar mycket riktigt att det inte är möjligt att ”*vidta några författningsåtgärder på nationell nivå i fråga om tredjelandsöverföringar vid utkontraktering av it-drift till privata leverantörer eftersom dataskyddsförordningens regler inte lämnar något utrymme för nationell*

[4] Uttryckssättet ”besittning, förfogande eller kontroll” är en direktöversättning av ”possession, custody or control” som bl.a. används i US CLOUD Act och som på ett adekvat sätt beskriver den rättsliga dimensionen och utmaningen med molntjänster och andra komplexa it-tjänster (inklusive ”it-drift”). Ett motsvarande kriterium i svensk rätt hade skapat högre förutsebarhet och rättssäkerhet än alla de begrepp som utredningen försöker tolka och tillämpa, såsom ”röja”, ”ta del av”, ”lämna ut”, ”tillgänglig för”, ”tekniskt bearbeta”, ”tekniskt lagra” osv.
[5] Avsnitt 7 i utredningen.

lagstiftning i dessa situationer"[6]. Märkligt nog har detta uttalande inte hindrat utredningen från att dra egna långtgående slutsatser som i vissa fall är svårförenliga med såväl EU-domstolens dom av den 16 juli 2020 dom i mål C-311/1 (”Schrems II”) som Europeiska Dataskyddsstyrelsens (”EDPB”) rekommendation om s.k. kompletterande skyddsåtgärder.[7]

Exempelvis förefaller utredningen, till skillnad från EDPB, mena att det alltid är omöjligt att läka brister i tredje lands lagstiftning genom s.k. standardavtalsklausuler och kompletterande skyddsåtgärder – oavsett vilka skyddsåtgärder som tillämpas.[8] Denna slutsats är framförallt onödig i sammanhanget, men även högst tveksam utifrån EU-domstolens domskäl i Schrems II.

Även i andra avseenden gör utredningen bedömningar och sammanfattningar i dataskyddsfrågor, vilket enligt Advokatsamfundets uppfattning alltså helt borde ha undvikits. Advokatsamfundet inser vikten av rättslig vägledning kring dataskyddsfrågor i ljuset av Schrems II och EDPB:s rekommendation, men anser att sådan vägledning bör lämnas av Integritetsskyddsmyndigheten (”IMY”) inom ramen för IMY:s formaliserade och lagreglerade samverkan med EDPB.

Utredningens tolkning av röjandebegreppet (avsnitt 8.9)

Den för utredningen centrala rättsfrågan avser tolkningen av det s.k. röjandebegreppet i OSL. Advokatsamfundet finner skäl att ifrågasätta flera av de bedömningar som utredningen gjort i denna del.

Av 1 kap. 1 § andra stycket och 3 kap. 1 § OSL framgår att sekretess betyder ”*[e]tt förbud att röja uppgift, vare sig detta sker muntligen, genom utlämnande av allmän handling eller på något annat sätt*”. Utredningen menar att denna lydelse innebär att varje utlämnande av sekretessreglerad uppgift per definition utgör ett röjande. En uppgift som lämnats ut av myndigheten måste alltså, enligt utredningen, därmed vara ”röjd”.[9] Utlämnande och röjande äger rum så fort en uppgift passerat något som utredningen kallar ”sekretessgränsen” (se vidare nedan om detta begrepp).

[6] Utredningen, s. 211.
[7] EDPB: *”Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data”.*
[8] Utredningen, s. 221.
[9] Utredningen s. 238.

Advokatsamfundet konstaterar att utredningens tolkning förefaller stå i strid med såväl rättspraxis[10] och tidigare förarbetsuttalanden[11] kring röjande i it-miljö. Utredningens analys av gällande rätt hänför sig i stället till rättsfall och motivuttalanden som tar sikte på pappersmiljö, samt till semantiska analyser. De tolkningar som gjorts i lagmotiv och praxis av vad som anses bli tillgängligt för utomstående i it-miljö och därmed ett röjande tas inte upp i betänkandet, trots att dessa uttalanden föranleder en annan bedömning.

Utredningen förklarar – å ena sidan – att det är ”logiskt och följdriktigt” att varje åtgärd som leder till att någon obehörig tillgängliggörs uppgifter i en pappershandling *inte* leder till att uppgifterna i pappershandlingen röjs.[12] Utredningen gör – å andra sidan – rakt motsatt bedömning för uppgifter i it-miljö. De uppgifter som digitala data bär skulle, enligt utredningen, vara röjda så snart digitala data har lämnats ut till en leverantör av it-drift oavsett om omständigheterna när uppgifterna tillgängliggjordes för tjänsteleverantören var sådana att man – t.ex. med hjälp av kryptering eller annan teknisk säkerhetsåtgärd – inte måste ha räknat med att tjänsteleverantören eller någon annan utomstående skulle komma att ta del av uppgifterna. I it-miljö innebär alltså, enligt utredningen, varje åtgärd som innebär ett utlämnande av digitala data till en driftleverantör att uppgifterna röjs för driftleverantören, helt oberoende av om leverantören haft faktisk möjlighet att ta del av uppgifterna.[13] Utredningens slutsatser stämmer inte heller överens med regleringen på säkerhetsskyddets område, där funktioner för kryptering är särskilt reglerat för att säkerställa att uppgifter inte röjs även när de befinner sig utanför verksamhetsutövarens omedelbara kontroll.[14]

Advokatsamfundet konstaterar att OSL:s definition av sekretess föreskriver att ett röjande kan ske genom ”utlämnande av allmän handling”. Samtidigt föreskrivs i 1 kap. 1 § tredje stycket OSL att vad som är en ”handling” framgår av 2 kap. TF. Av 2 kap. 3 § TF framgår att med handling avses, utöver en framställning i skrift eller bild ”*en upptagning som endast med tekniska hjälpmedel kan läsas eller avlyssnas eller uppfattas på annat sätt*”. Avgörande för handlingsbegreppet i it-miljö är således att innehållet i en upptagning kan ”uppfattas”. Enligt Advokatsamfundets bedömning är

[10] NJA 1991 s. 103 och AD:s dom nr 15/19, mål nr AD 152/17, meddelad den 6 mars 2019.
[11] Se bl.a. prop. 2007/08:160 s. 71 och 164.
[12] Utredningen, s. 274.
[13] Utredningen, s. 282.
[14] Jfr t.ex. PMFS 2019:2 3 kap. 21 § andra stycket.

det lagtexten i OSL med dess hänvisning till 2 kap. 3 § TF som torde vara avgörande för bedömningen av om uppgifter röjs.[15] Med andra ord, en uppgift bör anses vara röjd i OSL:s mening om uppgiften kan ”uppfattas” av myndighetens drift- eller tjänsteleverantör. Ett sådant resonemang är också i linje med EDPB:s rekommendation om kompletterande skyddsåtgärder, där det avgörande kriteriet är om information (personuppgifter, i det fallet) är tillgängliga ”i klartext”.[16]

Mot ovanstående bakgrund menar Advokatsamfundet att det finns starka skäl att ifrågasätta utredningens rättsliga analys och tolkning av röjandebegreppet i it-miljö. Advokatsamfundet menar dessutom att det principiellt är olämpligt att tillämpa olika röjandebegrepp för pappersmiljö respektive it-miljö. En sådan uppdelning är svårförenlig med lagstiftarens allmänna strävan att utforma teknikneutral lagstiftning.

Advokatsamfundet menar vidare att utredningens tolkning av röjandebegreppet innebär att information inte bara ”röjs” för driftleverantören, utan även för andra leverantörer som i samband med utkontraktering tillhandahåller tjänster till myndigheten, t.ex. leverantörer för nätverks- eller kommunikationstjänster. Eftersom den föreslagna sekretessbrytande bestämmelsen inte omfattar sådana leverantörer (kommunikationstjänster utgör knappast ”teknisk bearbetning” eller ”lagring” [17], se nedan), torde detta innebära att myndigheten i praktiken skulle röja uppgifter i strid med OSL för kommunikations-/nätverksleverantören varje gång myndigheten via allmänt kommunikationsnät överför uppgifter till it-system eller databaser som lagras hos driftleverantören.[18] Detta är en *allvarlig* brist i utredningen som kan medföra långtgående rättsliga och praktiska konsekvenser, vilka utredningen inte alls har analyserat.

OSL och extraterritoriell lagstiftning (avsnitt 10.1.5 m.fl.)

Det föreligger idag en normkonflikt mellan, å ena sidan, unionsrätt i form av GDPR och EU-stadgan respektive, å andra sidan, andra länders lagstiftning med extraterritoriell

[15] I lagmotiven tydliggörs att det är uppgifterna i betydelsen *informationsinnehållet* som är ”upptagningen”, se t.ex. om så kallade potentiella handlingar i SOU 2019:12 s. 60 ff. och prop. 2007/08:38.
[16] EDPB: *”Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data”,* s. 22, 26–27.
[17] Kommunikations-/nätverkstjänster är närmast att betrakta som en tjänst ”endast för befordran” (jfr 2 kap. 14 § första stycket, första punkten TF).
[18] Sådana situationer skulle i så fall kunna uppstå såväl vid överföringar mellan myndigheter som inom myndigheten vid överföring mellan olika verksamhetsställen, samt vid distansarbete.

effekt, bl.a. amerikansk lagstiftning såsom Foreign Intelligence Surveillance Act sektion 702 (”FISA 702”), Clarifying Lawful Overseas Use of Data Act (”US CLOUD Act”) och andra länders underrättelsetjänstlagstiftning (t.ex. den kinesiska lagen NIL). Denna normkonflikt är svårlöslig och i skrivande stund är det sannolikt att konflikten kommer att bestå under överskådlig tid.

Av särskilt intresse i sammanhanget är FISA 702, vilken är en amerikansk lagstiftning som den amerikanska underrättelsemyndigheten NSA tillämpar för att begära och få tillgång till information som hanteras av amerikanska leverantörer av t.ex. telekommunikation och molntjänster. Av lagtexten till FISA 702 framgår att NSA, både med och utan domstolsbeslut, kan inhämta underrättelseinformation om andra länder via en amerikansk leverantör utan att röja för kunden att inhämtning pågår. Inhämtad information kan därefter lagras på obestämd tid. Berörda leverantörer är skyldiga att hjälpa NSA att inhämta underrättelseinformation om t.ex. Sverige. Inhämtad information kan sedan delas med andra, såsom FBI eller CIA.[19]

Utredningen innehåller vissa uttalanden och bedömningar kring förhållandet mellan OSL och US CLOUD Act, men inte i relation till FISA 702 (denna lagstiftning analyseras, märkligt nog, endast utifrån GDPR). Detta är en generell brist i utredningen. FISA 702 och annan liknande lagstiftning innebär att en svensk myndighet inte, oaktat om utredningens förslag till sekretessbrytande regel införs i OSL, kan veta eller bedöma om sekretessreglerade uppgifter kommer att röjas för amerikanska myndigheter eller inte.

En naturlig utgångspunkt är att utkontraktering aldrig kan frånta eller befria en myndighet från ansvaret för sina allmänna handlingar, arbetsmaterial eller liknande. Detta kan sägas följa redan av grundlag i form av legalitetsprincipen (1 kap. 1 § tredje stycket RF). När en främmande makts rättsordning som driftleverantören lyder under föreskriver eller i praktiken leder till att *driftleverantören*, i stället för den myndighet som utkontrakterat sin it-drift, bedömer om sekretessreglerad information som är tillgänglig för driftleverantören de facto ska lämnas ut till myndighet i det främmande landet (och driftleverantören inte genom avtal eller på annat sätt kan undandra sig att

[19] Detta framgår bl.a. av Schrems II-domen (punkt 61) och av följande uttalande i CIA:s publikation FISA Dissemination Report från 2017 (s. 5): *”CIA is, however, authorized to receive, review, and appropriately disseminate a subset of data acquired pursuant to Section 702 or Titles I/III that have been initially collected by FBI or NSA”.*

följa dessa utländska rättsregler) leder en utkontraktering till att den svenska myndigheten i praktiken förlorar kontrollen över sekretessreglerad information och huruvida denna information röjs för utländska myndigheter.

Det har i olika sammanhang argumenterats för att myndigheten på så vis har berövats möjligheten att uppfylla sin skyldighet enligt lag och författning att göra sin sekretessprövning.[20] En myndighet kan inte utan stöd i lag eller förordning överlåta sekretessprövning till någon annan[21] utan måste själv pröva om en uppgift får lämnas ut.[22] Eftersom handläggningen av frågor om utlämnande av allmänna handlingar innefattar myndighetsutövning får sådana förvaltningsuppgifter inte heller enligt grundlag (12 kap. 4 § andra stycket RF) överlämnas till enskild utan stöd i lag. Mot ett sådant resonemang kan dock möjligen anföras att det i formell mening inte är fråga om att myndigheten medvetet överlåter ansvaret för sin sekretessprövning, detta ingår sannolikt inte i det utkontrakterade uppdraget.

Det intressanta i sammanhanget är dock, enligt Advokatsamfundets mening, att myndigheten på grund av utkontraktering och extraterritoriell lagstiftning *de facto* förlorar kontroll och bestämmanderätt över sekretessreglerad information och att sådan information kan överföras till utländsk myndighet utan föregående prövning av myndigheten – till och med utan att myndigheten överhuvudtaget får reda på sådant röjande. Detta är naturligtvis allvarligt och borde ha analyserats betydligt mer ingående av utredningen.

Av 8 kap. 3 § OSL följer att en svensk myndighet inte får lämna en uppgift till en utländsk myndighet utan att den svenska myndigheten (1) gjort en prövning av att uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet, och dessutom (2) vid sin prövning funnit att det står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten. De bedömningar som krävs enligt 8 kap. 3 § OSL måste ske i varje enskilt fall och kan inte ske på förhand.[23]

---

[20] Se bl.a. Furberg och Westberg: *”Måste myndigheterna följa lagen – om utkontraktering och legalitet i digital miljö”* i JT 2020/21 nr 2, s. 406–418.
[21] Se 2 kap. 17 § andra stycket TF, JO 2016/17 s. 351 och JO 2019/20 s 279.
[22] Om inte beslutsrätten är delegerad tillkommer sådan behörighet normalt en statlig myndighets chef, se 5 § myndighetsförordningen (2007:515) och för kommunala förvaltningar vederbörande nämnd, se 6 kap. 37 och 38 §§ samt 7 kap. 5 § kommunallagen (2017:725).
[23] Det är en annan sak om sekretessprövningen och utlämnandet sker till den utländska myndigheten i enlighet med särskild föreskrift i lag eller förordning (8 kap. 3 § 1 OSL). Som exempel på sådana fall nämns i förarbetena de socialförsäkringskonventioner som Sverige har ingått med främmande länder. Dessa konventioner innehåller

Utredningen menar att en utkontrakterande myndighet inte ska anses handla i strid med 8 kap. 3 § OSL när myndigheten anlitar en tjänsteleverantör som lyder under utländsk rätt med extraterritoriell lagstiftning. Utredningen menar att inte heller leverantörens senare faktiska utlämnande utgör ett otillåtet röjande i strid med 8 kap. 3 § OSL, eftersom OSL inte är tillämplig på leverantören. Advokatsamfundet menar att utredningen gör dessa bedömningar alltför lättvindigt och att i synnerhet FISA 702 har avgörande betydelse för frågan om röjande enligt OSL.

Här bör också noteras att EDPB – till skillnad från utredningen – gjort bedömningen att *”T[t]he mere fact that the data are comprised within the scope of a third country legislation that allows access to data by public authorities without specific essential guarantees (as recalled in the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures) would amount, per se, to considering that such access will possibly take place, without the need to rely on any practical experience in this regard or absence of requests for disclosure from public authorities received by the data importer.”*[24]

Det ovan angivna citatet ger stöd för att en myndighet i en sådan situation bör *utgå från* att utlämnande kommer att äga rum, om tjänsteleverantören står under jurisdiktion av extraterritoriell lagstiftning. Ett antal myndigheter har också inom ramen för eSamverkansprogrammet gemensamt uttalat att 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 om tjänsteleverantören på grund av regler i en främmande rättsordning kan bli tvungen att lämna ut uppgifter, blir en sannolikhetsbedömning inte särskilt relevant eftersom uppgifterna får anses bli röjda i OSL:s mening. Vad som däremot är mer relevant för myndigheten är att inom ramen för en riskbedömning bedöma konsekvenserna av att uppgifterna röjs, om en sådan bedömning i praktiken är möjlig (se vidare nedan om behovet av regler).

Med hänvisning till föregående avsnitt om röjandebegreppet bör nämnas att ett röjandebegrepp som utgår från vad myndigheten ”har att räkna med” avseende risken

åtaganden att lämna uppgifter i olika hänseenden. Eftersom konventionernas bestämmelser genom förordning har införlivats med svensk rätt innefattas dessa bestämmelser av det nämnda undantaget. Sveriges suveränitet upprätthålls därmed.

[24] EDPB – EDPS Joint Opinion 2/2021, s. 19 p. 87.

för att någon tar del av uppgifterna, i detta avseende passar bättre för prövningen avseende om leverantör som lyder under främmande makts rättsordning kan bli skyldig att lämna ut uppgifterna enligt utländsk rätt, än den innebörd av röjandebegreppet som utredningen föreslår (jfr föregående avsnitt).

Advokatsamfundet menar att en myndighet inför en utkontraktering, för det första, bör bedöma om det finns anledning att räkna med att någon obehörigen tar del av de sekretessreglerade uppgifterna. Om svaret är jakande bör myndigheten, i andra hand, utreda om det finns något undantag i OSL som är tillämpligt – t.ex. en sekretessbrytande bestämmelse såsom den som utredningen föreslår. Om det inte heller finns någon sekretessbrytande bestämmelse att tillämpa får myndigheten, i sista hand, utföra en sekretessprövning vilken i vissa fall kan göras översiktligt vid massuttag (s.k. schabloniserad sekretessprövning).

Vid sekretessprövning inför utlämnande av uppgifter till en *amerikansk* tjänsteleverantör, har myndigheten, på grund av bl.a. FISA 702, att *utgå från* att tjänsteleverantören kan komma att lämna ut uppgifter till amerikansk myndighet utan föregående sekretessprövning eller bedömning av den utkontrakterande myndigheten. Risken för utlämnande till utländsk myndighet och konsekvenserna av sådant utlämnande måste därför noggrant analyseras av myndigheten för att säkerställa att myndigheten kan eliminera eller åtminstone starkt begränsa denna risk. Det bör understrykas att det *inte* främst är sannolikheten för ett utlämnande som bör bedömas, utan i stället hur myndigheten kan hindra utländsk myndighet från att ta del av uppgifterna (dvs. ”uppfatta” uppgiften, jfr Advokatsamfundets bedömning av röjandebegreppet ovan). Vad som krävs för att denna risk ska kunna elimineras eller begränsas på ett effektivt sätt beror på omständigheterna i det enskilda fallet.

Om risken för att utländsk myndighet ”uppfattar” uppgifter, efter att denne med stöd av extraterritoriell lagstiftning mottagit uppgifter från driftleverantören, inte kan elimineras eller i vart fall minimeras till en acceptabel nivå, så torde tjänsten inte kunna användas av myndigheten utan överträdelse mot OSL och i förlängningen svensk grundlag.

Av ovanstående skäl ifrågasätter Advokatsamfundet utredningens rättsliga slutsatser kring extraterritoriell lagstiftning såsom FISA 702 och dessa slutsatsers lämplighet för Sveriges säkerhet och digitala suveränitet. Advokatsamfundet efterlyser fördjupad

analys av hur extraterritoriell lagstiftning ska påverka myndigheters utkontraktering och möjligheterna att upprätthålla svensk jurisdiktion över sekretessreglerad information.

Utformningen till ny sekretessbrytande bestämmelse är oklar (avsnitt 10.3)

Vad gäller utredningens förslag till ny sekretessbrytande bestämmelse för utkontraktering, delar Advokatsamfundet utredningens bedömning att det är lämpligt att införa en sådan bestämmelse i OSL. Advokatsamfundet har dock invändningar när det gäller utredningens förslag till utformning av bestämmelsen. Dessa invändningar rör dels begreppet ”teknisk bearbetning eller lagring”, dels förslaget att införa en intresseavvägning i bestämmelsens andra stycke.

Advokatsamfundet menar att begreppet teknisk bearbetning/lagring i detta sammanhang är förenat med flera frågetecken, vilka inte rätas ut av utredningen. Ytterligare gränsdragningsproblem skapas av att utredningen vill klargöra att *enbart* teknisk bearbetning eller lagring som sker *för myndighetens räkning* ska omfattas.

Advokatsamfundet vill särskilt lyfta fram följande omständigheter och frågor som exempel på de gränsdragningsproblem som uppkommer med utredningens förslag:

- Nätverks- och kommunikationstjänster förefaller inte utgöra vare sig ”lagring” eller ”bearbetning”, vilket leder till en märklig rättslig situation (jfr ovan).
- Omfattas momentan behandling (i klartext) i arbetsminnet utan beständig lagring (dvs. utan nedskrivning till disk eller lagringsminne) hos leverantören?
- Omfattas it-tjänster på de övre lagren av en systemarkitektur (applikationsrelaterade tjänster), såsom applikationsdrift eller systemleveransåtaganden?
- Omfattas it-tjänster som innebär komplexa beräkningar, analyser eller annan avancerad behandling av myndighetens information i leverantörens mjukvara (SaaS)? Är detta ”enbart teknisk bearbetning”?
- Hur ska s.k. potentiella handlingar bedömas vid denna hantering?
- Omfattar rekvisitet ”enbart teknisk bearbetning/lagring” sådana tjänster där leverantören samlar information om hur myndigheten använder tjänsten, sedan

jämför detta med andra kunder och därefter redovisar statistik eller analyser till myndigheten?[25]

Utredningen konstaterar att begreppen ”teknisk bearbetning eller lagring” härrör från 2 kap. 9 § TF och är ”inarbetat”. Utredningen tillstår att *”uttrycket inte kan sägas vara alldeles entydigt”* men menar att det ändå är *”mer tydligt än uttrycket it-drift”*.[26] Att något är mer tydligt än något annat innebär knappast att det första alternativet därmed också skulle vara det mest lämpliga alternativet. Som framgått inledningsvis i detta yttrande, menar Advokatsamfundet också att det finns betydligt bättre begrepp och rekvisit att använda i detta sammanhang. Det är olyckligt att utredningen inte närmare analyserat och övervägt om det varit lämpligt att använda modernare och mer träffsäkra rekvisit, som har en tydlig innebörd i här aktuella miljöer.

När det sedan gäller utredningens förslag om intresseavvägning i den föreslagna bestämmelsens andra stycke, menar Advokatsamfundet att detta riskerar att leda till godtyckliga bedömningar och (fortsatt) osäkerhet kring om och under vilka förutsättningar en myndighet kan utkontraktera sin it-drift. Den omständigheten att det aktuella intresset i detta fall handlar om myndighetens eget intresse av en kostnadseffektiv IT-användning genom egeninitierat utlämnande – och *inte* om allmänhetens rätt till insyn till följd av en utomståendes begäran – bidrar ytterligare till att bestämmelsen blir svårtillämpad och något apart utifrån OSL:s systematik och skyddsintresse. Av bl.a. rättssäkerhetsskäl förordar Advokatsamfundet därför ett mer objektivt rekvisit.[27] Under alla omständigheter krävs ytterligare vägledning kring hur en eventuell intresseavvägning i denna situation ska gå till. Det kan också konstateras att utredningens förslag ställer mycket höga krav på kompetens,

---

[25] Exempel på sådana tjänster är SaaS där det ofta finns tilläggstjänster där kunden kan jämföra sin användning av molntjänsten med andra kunder eller branschen i stort. Det kan också vara fråga om s.k. prediktivt underhåll eller andra ”datadrivna” tjänster, vilka kännetecknas av att leverantören samlar (och, med olika grader av noggrannhet, avidentifierar) data från många kunder för att skapa nya insikter/erbjudanden.

[26] Utredningen, s. 295.

[27] Ett sådant mer objektivt kriterium kan exempelvis utformas med ledning i eSams rättsliga uttalande 2018-10-23 (VER 2018:57) om röjande och molntjänster: *”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, får uppgifterna anses vara röjda. Anledningen är att det inte längre är osannolikt att uppgifterna kan komma att lämnas till utomstående. Detsamma får anses gälla om redan ägarförhållanden eller geografisk placering av en tjänsteleverantörs tekniska hjälpmedel ger anledning att befara att mänskliga rättigheter (till exempel skyddet för privatlivet) eller det allmännas intressen (t.ex. rikets säkerhet) inte skulle säkerställas om svenska myndigheters data hade tillgängliggjorts.”*. Även utredningens bedömningskriterier för intresseavvägning (s. 338) är relevanta i ett sådant sammanhang och skulle kunna ingå i ett lagstadgat kriterium.

informationsinhämtning och omvärldsbevakning hos enskilda myndigheter för att genomföra en dylik intresseavvägning. Detta kan, i sin tur, föranleda både sänkt digitaliseringstakt och ökade kostnader för myndigheten.

Advokatsamfundet vill också understryka att mycket talar för att den ”avvägning” och övergripande bedömning som myndigheten bör göra inför en utkontraktering inte bör begränsas till enbart sekretesshänsyn och OSL, utan att den relevanta bedömningen snarare borde omfatta den generella *lämpligheten* i en viss utkontraktering. Advokatsamfundet återkommer till detta i det avslutande avsnittet.

Det saknas utredning av alternativa åtgärder

Utredningen framhåller att det behövs ny reglering som medger utkontraktering i offentlig sektor, och att detta behov kan tillgodoses med en sekretessbrytande bestämmelse i OSL.[28] Advokatsamfundet är, som ovan nämnts, positivt inställd till en sådan bestämmelse men utesluter inte att det kan finnas andra alternativ för att nå detta behov. Advokatsamfundet ställer sig frågande till om och i så fall hur utredningen övervägt även andra metoder som komplement eller som alternativ till den sekretessbrytande bestämmelse som utredningen föreslagit.

OSL är långt ifrån den enda reglering som påverkar myndigheters utkontraktering av it-drift. Myndigheter omfattas bl.a. av säkerhetsskyddslagen, GDPR, arkivlagen och i vissa fall olika registerförfattningar. En jämförelse kan även göras med reglerad verksamhet i privat sektor, såsom bank och försäkring, där det finns uttryckliga specifika regelverk kring just utkontraktering. Flera av dessa regelverk tar – från olika perspektiv – sikte på hur den utkontrakterande kunden ska kunna bibehålla kontroll och bestämmanderätt över den information eller verksamhet som är föremål för utkontraktering och som därmed befinner sig utanför den utkontrakterande kundens besittning, förfogande eller direkta kontroll. Frågeställningen hanteras i dessa regelverk på snarlikt sätt, nämligen genom att ålägga den utkontrakterande organisationen att ingå ett särskilt avtal med visst obligatoriskt innehåll som anses nödvändigt för att upprätthålla sådan fortsatt kontroll även efter utkontrakteringen. Sådana avtal har olika benämningar, såsom säkerhetsskyddsavtal,

[28] Utredningen, s. 293.

personuppgiftsbiträdesavtal respektive uppdragsavtal, men fyller principiellt samma syfte.

Gemensamt för dessa avtalstyper är att de ska möjliggöra för kunden att uppdra till någon annan att hantera kundens information eller verksamhet, utan att säkerhetsskyddet, skyddet för personuppgifter eller kundens kontroll över den utkontrakterade verksamheten försämras. Annorlunda uttryckt, syftet med dessa avtal är att flytta gränsen för när uppgifter ska anses ha lämnat kundens kontrollsfär samtidigt som kunden ska kunna fullgöra sina skyldigheter och bära sitt ansvar enligt författning för hanteringen av uppgifter i tjänsten.

I OSL finns varken idag eller med utredningens förslag någon motsvarande mekanism för att utvidga kundens kontrollsfär, annat än s.k. utlämnandeförbehåll enligt 10 kap. 14 § OSL (vilket inte har någon större relevans från digitaliseringsperspektiv). Utredningen hänvisar till en ”sekretessgräns” som måste passeras för att en uppgift ska anses utlämnad och exemplifierar med en myndighetsanställd som lämnar en uppgift till sin kollega utan att uppgiften därmed anses utlämnad. Detta är en rimlig slutsats. Det kan dock ifrågasättas om det nödvändigtvis ska ha avgörande betydelse om uppgiften lämnas till en myndighetsanställd kollega och inte till en person anställd av myndighetens driftleverantör som omfattas av tystnadsplikt enligt lagen (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter.

Advokatsamfundet utesluter inte att det finns avgörande skäl till varför det från sekretesshänsyn och OSL inte skulle vara lämpligt att använda avtalsinstrumentet för att kunna flytta myndighetens kontrollsfär. Eftersom en sådan metod används i varje annan reglering för utkontraktering (inklusive för säkerhetsskydd) menar Advokatsamfundet att utredningen åtminstone borde ha utrett och analyserat möjligheterna till en sådan mekanism. Det torde enligt Advokatsamfundets uppfattning finnas visst sådant utrymme under vissa angivna och lagstadgade förutsättningar, såsom att det finns en juridiskt bindande och betryggande sanktionerad avtalssekretess som har utformats på ett hållbart sätt, att tjänsteleverantören inte är juridiskt eller praktiskt förhindrad att upprätthålla sekretessen och omständigheterna även i övrigt medför att myndigheten inte har att utgå från att tjänsteleverantören eller dennes personal, som inte får ta del av eller vidarebefordra uppgifterna, i praktiken ändå kommer att befatta sig med dem på ett otillåtet sätt.

Ny lagstiftning om digitalisering och utkontraktering bör utredas

Det kan avslutningsvis konstateras att tillämpliga regler om utkontraktering, digitalisering, sekretess, dataskydd och informationssäkerhet idag finns utspridda i många olika författningar. En myndighet som önskar utkontraktera sin it-drift måste analysera detta utifrån en mängd olika lagar och regler, såväl unionsrättsliga som nationella. I många fall är det inte heller givet hur lagstiftningen ska förstås och tolkas i en digital kontext. Detta är i sig ett hinder mot effektiv digitalisering av offentlig verksamhet.

Utkontraktering är i stor utsträckning nödvändigt för att dra nytta av digitaliseringens positiva effekter. Samtidigt är det avgörande att Sveriges digitala suveränitet upprätthålls, och att nationella digitaliseringsstrategier fastställs utan otillbörlig påverkan från främmande makt eller utländska tjänsteleverantörer. Detta förutsätter i praktiken djup teknisk och juridisk kunskap i offentlig sektor, strategiska regeringsbeslut och – inte minst – ändamålsenlig lagstiftning.

Advokatsamfundet menar att strukturella förändringar i svensk lagstiftning kan vara nödvändiga för att stärka en effektiv och säker digitalisering i offentlig sektor. Exempelvis kan det vara lämpligt att samla övergripande regler och principer för säker utkontraktering i offentlig sektor i en ny fristående lagstiftning, vilken mera precist och ändamålsenligt kan reglera de rättsliga förutsättningar som är specifika och relevanta just för utkontraktering – oavsett om utkontrakteringen avser ”it-drift”, ”teknisk bearbetning”, ”befordran av ett meddelande” eller någon annan del av myndighetens verksamhet eller behov av tjänster. Mycket talar även för att en sådan framtida lagstiftning bör inkludera ett generellt lämplighetsrekvisit för utkontraktering av it-drift och andra viktiga it-funktioner.[29]

Regeringen bör således enligt Advokatsamfundets uppfattning ytterligare överväga och utreda möjligheten till förbättrad och mer ändamålsenlig lagstiftning kring utkontraktering och digitalisering av svensk förvaltning.

[29] Jfr s. 300–301 i utredningen, Digitaliseringsrättsutredningen (SOU 2018:25) och Försäkringskassan ”Vitbok, Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt”. Notera dock att det följer av Advokatsamfundets resonemang ovan att en sådan framtida lag endast undantagsvis kan innehålla bestämmelser förbehållet unionsrättslig kompetens, såsom GDPR.

SVERIGES ADVOKATSAMFUND

Mia Edwall Insulander