Datum
2021-05-06

Diarienummer
2021-3052-2

Mottagare
Infrastrukturdepartementet
103 33 Stockholm

Er referens
I2021/00342

Säker och kostnadseffektiv it-drift - rättsliga förutsättningar för utkontraktering (SOU 2021:1)

Säkerhetspolisen har tagit del av utredningens bedömningar och förslag och har följande synpunkter.

Synpunkterna avser i huvudsak utredningens bedömning av röjande och kryptering samt utformningen av den sekretessbrytande bestämmelse som utredningen föreslår. Enligt Säkerhetspolisens uppfattning är bedömningarna som avser kryptering och röjande inte tillräckligt utredda för att kunna läggas till grund för lagstiftning.

Allmänt om utkontraktering och säkerhetsskydd

En ökad utkontraktering av it-drift kan ställa mycket höga krav vad gäller säkerhetsskyddsåtgärder. Ett stort antal myndigheters uppgifter kan komma att samlas hos en eller ett fåtal leverantörer och de samlade uppgifterna kan ha ett stort skyddsvärde. Vid utkontraktering av it-drift är det därför viktigt att myndigheter och leverantörer har kompetens och kunskap avseende gällande krav på säkerhetsskydd och att kraven sedan följs.

6.2.12 Särskilt om aggregerad och ackumulerad information

Som framhålls i utredningen är det enligt säkerhetsskyddslagstiftningen tjänsteleverantören, dvs. den som sköter it-driften, som ska ställning till det samlade skyddsvärdet i sin verksamhet. Säkerhetspolisen vill dock i sammanhanget framhålla att det i praktiken är en bedömning som är svår att genomföra. Det kräver ingående kunskap om de skyddsvärden som finns hos kunderna, dvs. myndigheterna. Bedömningen kan vara särskilt svår i en situation där myndigheternas information, var för sig inte utgör säkerhetsskyddsklassificerade uppgifter. Detta kan komma att utgöra en risk i samband med utkontraktering.

8.9 Röjandebegreppet

Inledningsvis kan det konstateras att det råder oenighet om hur röjandebegreppet ska tolkas. Säkerhetspolisen ifrågasätter om den tolkning som utredningen landar i, där de likställer utlämnande med röjande, är

Postadress
Box 12312
102 28 Stockholm

Besöksadress
Bolstomtavägen 2
171 69 Solna

Telefon
010-568 70 00
+46-10-568 70 00

Telefax
010-568 70 10
+46-10-568 70 10

E-post/Internet
sakerhetspolisen@sakerhetspolisen.se
www.sakerhetspolisen.se

rimlig. Särskilt eftersom den leder utredningen till slutsatsen att uppgifter som lämnas till tjänsteleverantören är röjda oavsett om de är krypterade eller inte. Vissa av de avgöranden och förarbetsuttalanden som utredningen grundar sina ställningstaganden på är skrivna långt tillbaka i tiden och har exempelvis inte tagit ställning till dagens kryptografiska funktioner. Det kan därför vara vanskligt att utifrån dessa dra slutsatsen att sådana funktioner saknar betydelse för röjandefrågan idag (se vidare under avsnitt 10.1 Utkontraktering och röjande).

Säkerhetspolisen anser att följande måste vägas in i tolkningen av röjandebegreppet.

Av 3 kap. 1 § andra stycket offentlighets- och sekretesslagen (2009:400), OSL, framgår att sekretess innebär ett förbud att röja uppgifter, oavsett om det sker muntligen, genom utlämnande av allmän handling eller på annat sätt. Ordalydelsen innebär att röjande *kan* ske genom utlämnande. Den innebär däremot inte nödvändigtvis att utlämnande *alltid* är ett röjande.

Vid utkontraktering av it-drift behöver leverantören i regel ha tillgång till de faktiska uppgifterna för att kunna utföra sitt uppdrag och för att bearbeta och strukturera uppgifterna. Vid sådana fall är det naturligt att en uppgift är att betrakta som röjd när den lämnas över i samband med utkontrakteringen. Det finns dock situationer då en leverantör endast lagrar uppgifter och uppdraget kan utföras fastän uppgifterna är krypterade för leverantören. Att i den situationen komma fram till att uppgifterna alltid ska anses som röjda följer inte av formuleringarna i OSL. I en sådan situation är det istället rimligt att göra en bedömning av om mottagaren har haft möjlighet att ta del av uppgiften.

Utredningen anger att den avgränsat analysen av röjandebegreppet så att den endast avser utkontraktering av it-drift till privata tjänsteleverantörer. En sådan avgränsning är svår att göra i praktiken och utredningens bedömning kan få konsekvenser för andra situationer där röjandebegreppet ska tillämpas. Till följd av avgränsningen har utredningen t.ex. inte analyserat vad ställningstagandet skulle kunna få för konsekvenser för annan lagstiftning där röjandebegreppet aktualiseras, t.ex. i 19 och 20 kap. brottsbalken. Behovet av en djupare analys blir särskilt tydligt eftersom utredningen även gör bedömningen att uppgifter som lämnas ut i förhållande till it-tjänsteleverantörer är röjda oavsett om uppgifterna är krypterade eller inte (se vidare avsnitt 10.1 Utkontraktering och röjande).

10.1 Utkontraktering och röjande

Säkerhetspolisen delar inte utredningens bedömning att det vid utkontraktering av it-drift saknar betydelse för röjandefrågan om uppgifterna är krypterade eller inte. En sådan tolkning får konsekvenser som skulle riskera att omöjliggöra myndigheters elektroniska kommunikation.

Utredningens uppfattning är att uppgifter som omfattas av utkontraktering av it-drift är röjda enligt OSL så snart de är utlämnande, oavsett om omständigheterna när uppgifterna tillgängliggjorts var sådana att man – t.ex. på grund av kryptering eller annan teknisk säkerhetsåtgärd – inte måste ha räknat med att tjänsteleverantören eller någon annan utomstående skulle komma att ta del av uppgifterna.

Skälet till att kryptering används är att obehöriga inte ska kunna ta del av uppgifterna. En säker kryptering ger ett gott skydd mot obehörig åtkomst. Därtill finns även signalskydd, dvs. kryptografiska funktioner som har godkänts av Försvarsmakten enligt 3 kap. 5 § säkerhetsskyddsförordningen (2018:658), och som används när säkerhetsskyddsklassificerade uppgifter ska kommuniceras utanför verksamhetsutövarens kontroll.

Den som är behörig mottagare av uppgifterna är avsedd att kunna ta del av uppgifterna och har i regel tillgång till en giltig krypteringsnyckel. I dessa fall är det naturligt att uppgifterna anses röjda för mottagaren. Uppgifterna kan dock inte alltid anses röjda i förhållande till någon annan utomstående eller för det fall att uppgifterna mot förmodan är krypterade i förhållande till mottagaren. Vid en sådan situation måste man bedöma sannolikheten för att uppgifterna faktiskt blivit röjda.

Om man som utredningen menar att det saknar betydelse om uppgiften är krypterad i förhållande till mottagaren betyder det rimligtvis att den är röjd för alla andra som också får tillgång till den krypterade uppgiften. Det skulle i många fall innebära att uppgifter som skickas krypterat röjs enligt OSL för alla utomstående som kan inhämta meddelandet, även för den som förmedlar uppgiften. Det är en brist att utredningen inte har analyserat vilka konsekvenser ställningstagandet skulle kunna få för andra bestämmelser där röjandebegreppet aktualiseras, t.ex. i brottsbalken, eller vilka konsekvenser det kan få för regelverk som anger att viss kryptering krävs för att skydda uppgifterna. Utredningens bedömning att uppgifter ska anses vara röjda trots kryptering kan få mycket långtgående konsekvenser för myndigheters möjlighet att kommunicera elektroniskt.

10.3 Den sekretessbrytande bestämmelsens utformning

Säkerhetspolisen delar utredningens bedömning att det finns ett behov av en sekretessbrytande bestämmelse för att kunna utkontraktera it-drift. Säkerhetspolisen har dock vissa synpunkter på bestämmelsens utformning.

Intresseavvägning

Den intresseavvägning som utredningen föreslår kommer vara mycket svår för myndigheterna att utföra i praktiken. Det finns en uppenbar risk att tillämpningen av regeln blir godtycklig och varierande. Riskerna kan bestå i att sekretessintresset inte ges tillräcklig betydelse i förhållande till intresset att utkontraktera och att känsliga uppgifter därmed lämnas ut felaktigt. Det

kan även leda till att myndigheter inte förstår hur bestämmelsen ska tillämpas och inte använder den alls på grund av osäkerhet. Det finns enligt Säkerhetspolisen ett behov av att utforma bestämmelsen med tydligare kriterier för hur intresseavvägningen ska utföras.

Även om det finns flera andra regelverk som är till för att skydda uppgifterna bör särskilda kriterier ställas upp i den sekretessbrytande bestämmelsen som tar sikte på skyddet av uppgifterna. I bedömningen bör det enligt Säkerhetspolisen t.ex. vägas in hur leverantören skyddar uppgifterna och hur skyddet för vidarespridning av uppgifterna ser ut.

Utöver vad som anges ovan är det viktigt att myndigheterna tar hänsyn till alla regelverk som aktualiseras vid utkontraktering. En utkontraktering kan, trots att det inte finns sekretesshinder, stå i konflikt med exempelvis säkerhetsskyddsregleringen. Detta bör förtydligas i kommentaren till den sekretessbrytande bestämmelsen.

Detta remissyttrande har beslutats av biträdande säkerhetspolischefen Charlotte von Essen. Verksjuristen Fredrik Sjöberg har varit föredragande.