Sveriges advokatsamfund

Stockholm den 10 januari 2022

R-2021/2008

Till Försvarsdepartementet
Fö2021/00796

Sveriges advokatsamfund har genom remiss den 22 september 2021 beretts tillfälle att avge yttrande över betänkandet Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63).

Betänkandet är ett resultat av utredningens uppdrag att bedöma om det finns anledning att på motsvarande sätt som gäller enligt EU:s cybersäkerhetsakt[1] införa nationella särskilda certifieringskrav för IKT-produkter, -tjänster och -processer i sådana nätverks- och informationssystem som ska användas i säkerhetskänslig verksamhet. Det kan även bli aktuellt med krav på godkännande från en myndighet för att sådana IKT-produkter, -tjänster och -processer ska få tas i drift i säkerhetskänslig verksamhet. Regeringen har utsett Försvarets materielverk (FMV) till nationell myndighet för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt. Samtidigt faller åtgärder som rör försvar och nationell säkerhet utanför EU:s kompetensområde, vilket betyder att detta egentligen inte omfattas av EU:s cybersäkerhetsakt (art. 4.2 EU-fördraget).

[1] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

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

Sammanfattning

Advokatsamfundet anser att betänkandet i många delar är väl genomtänkt och att författningsförslagen i stort är rimliga och balanserade. Samtidigt finns det vissa inslag i förslagen och vissa förhållanden som behöver bli föremål för ytterligare överväganden, vilket utvecklas nedan.

Synpunkter

Allmänna synpunkter

Det är allt viktigare att cyber- och informationssäkerhetsfrågor tas på största allvar. Under den senaste tiden har ett flertal incidenter förekommit som visat att nätverk och informationssystem är mycket sårbara och att de lätt kan slås ut eller allvarligt störas.[2] Denna problematik omfattar inte bara sådan verksamhet som angår Sveriges säkerhet och som träffas av säkerhetsskyddslagstiftningen. Även annan verksamhet måste engagera sig i säkerhetsfrågorna, inte minst sådan verksamhet som omfattar samhällsviktiga tjänster och som omfattas av särskilda krav på informationssäkerhet.[3] Advokatsamfundet har mot denna bakgrund full förståelse för att frågor om cyber- och informationssäkerheten ges ett allt större utrymme också på området för Sveriges säkerhet.

Det har under senare tid tillkommit en rad olika lagstiftningsinitiativ, på EU-nivå och nationell nivå, som direkt eller indirekt handlar om cyber- eller informationssäkerhet. Förutom EU:s cybersäkerhetsakt och NIS-direktivet med olika nationella regler som kompletterar eller implementerar dessa, innehåller den svenska säkerhetsskyddslagen (2018:585) flera bestämmelser som tar sikte på informationssäkerhet. Även i EU:s dataskyddsförordning (GDPR) finns ett antal artiklar som aktualiserar olika slags åtgärder på informationssäkerhetsområdet. När det nu förekommer flera lagstiftningsprodukter som gäller för en rad olika verksamheter och verksamhetsområden anser Advokatsamfundet det särskilt viktigt att regelverken är samordnade och harmoniserade. Detta gäller inte minst terminologin i regelverken, där begrepp och definitioner inte alltid har samma innebörd, och där nya begrepp och definitioner tillkommer i takt med den snabba teknikutvecklingen. Begrepp och

[2] Exempelvis ransomwareattackerna mot Kalix kommun den 15 december 2021 (https://www.svt.se/nyheter/lokalt/norrbotten/it-attacken-mot-kalix-kommun-detta-har-hant) och den 2 juli 2021 som drabbade Coop (https://www.svt.se/nyheter/inrikes/it-attacken-mot-coop-detta-har-hant).
[3] Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

definitioner bör därför så långt som möjligt vara gemensamma för de olika regelverken. En sådan samordning är viktig för att undvika förvirring eller missförstånd och för att underlätta rättstillämpningen.

En annan problematik som Advokatsamfundet vill framhålla särskilt är att gränsdragningen mellan olika regelverk riskerar att bli otydlig för de verksamheter som berörs. Avgränsningarna avseende regelverkens tillämpningsområde är inte alls självklara och beskrivs ofta på ett sådant sätt att det blir fråga om en specifik bedömning av om en viss verksamhet faller under något av regelverken. Bedömningen handlar ofta – och inte minst i säkerhetsskyddslagstiftningen – om huruvida en risk, skada eller någon annan omständighet kan anses vara av visst slag, viss omfattning eller viss storlek. De bedömningskriterier som förekommer lämnar ett påtagligt utrymme för skönsmässighet. Det kan medföra att viss information får en felaktig klassificering eller att värderingen av en risk inte motsvarar det potentiella hot som risken egentligen utgör. Samtidigt riskerar verksamheten att drabbas av olika slags sanktioner vid felaktiga eller inadekvata bedömningar. Advokatsamfundet vill därför framhålla att tillsynsarbetet i första hand måste vara inriktat på att ge de verksamheter som träffas av lagstiftningen råd, stöd, utbildning och anvisningar. Sanktionsavgifter bör tillgripas först när inget annat visat sig effektivt. I annat fall kan sanktionsavgifterna komma att uppfattas som onödiga eller överdrivna. Det finns därutöver även en risk för att verksamheterna hellre väljer att avstå från att använda och tillvarata fördelarna med tekniken när det inte kan förutses på vilka grunder en sanktionsavgift kan komma att bli aktuell.

En ytterligare problematik ligger i den mycket snabba utvecklingen som är typisk för informationstekniken, samtidigt som framtagandet av regelverken är föremål för ganska långsamma processer. Ett sätt att bemöta problematiken är att fortsätta låta lagstiftningen på cyber- och informationssäkerhetsområdet vara mer generell till sin natur och snarare innehålla målsättningar än detaljerade krav. Därefter får de mer detaljerade föreskrifterna ges längre ned i normhierarkin. På så sätt kan regelverken snabbare och lättare anpassas till teknikutvecklingen och meddelas av sådana aktörer som har särskild kompetens på det aktuella verksamhetsområdet, exempelvis de behöriga tillsynsmyndigheterna. Advokatsamfundet anser det därför angeläget med ett ökat arbete från myndigheternas sida med att ta fram föreskrifter, råd och anvisningar på cyber- och informationssäkerhetsområdet.

Advokatsamfundet anser att utredningen inte i tillräcklig grad har beaktat den särskilda problematik som uppmärksammas ovan.

Författningsförslagens tillämpningsområde

De föreslagna bestämmelserna utgör kompletteringar eller ändringar i den gällande säkerhetsskyddslagen och innebär ytterligare krav på de aktörer och verksamheter som redan omfattas av lagens tillämpningsområde. Några nya subjekt kommer således inte omfattas av reglerna.

Den tidigare gällande säkerhetsskyddslagen tillkom redan 1996.[4] När den nya och nu gällande säkerhetsskyddslagen trädde ikraft den 1 april 2019 hade det redan innan ikraftträdandet tillsatts en utredning med förslag om kompletteringar i lagen.[5] Den 1 januari 2021 infördes en första del av kompletteringarna bestående i bestämmelser med särskilda krav vid överlåtelse av säkerhetskänslig verksamhet.[6] Därefter infördes fler kompletterande bestämmelser med ytterligare krav, vilka trädde ikraft den 1 december 2021.[7] Nu föreslås återigen kompletteringar. Advokatsamfundet känner mot angiven bakgrund viss oro för att lagstiftningen kan uppfattas som osäker och framstå som oförutsebar.

Vissa regler bör ges i lag i stället för i förordning

Advokatsamfundet anser principiellt att en ordning där det överlämnas åt specifika myndigheter att ålägga enskilda olika slags skyldigheter är tveksam ur rättssäkerhetssynpunkt.

Samtidigt följer av informationsteknikens natur att införandet av olika regelverk måste vara snabbfotat för att hänga med i teknikutvecklingen. De processer som kännetecknar framtagandet av EU-förordningar och direktiv, men även det nationella lagstiftningsarbetet och införandet av kompletterande regeringsförordningar, är i detta sammanhang mycket långsamma. När ett regelverk slutligen har antagits och trätt ikraft kan det informationstekniska område som avses ha förändrats i sådan omfattning att regelverket redan har hunnit bli obsolet. Advokatsamfundet har förståelse för att detta medför att detaljerna i hög grad måste överlåtas åt olika

[4] Säkerhetsskyddslagen (1996:627).
[5] SOU 2018:82, Kompletteringar till den nya säkerhetsskyddslagen.
[6] Prop. 2020/21:13, Åtgärder till skydd för Sveriges säkerhet vid överlåtelser av säkerhetskänslig verksamhet.
[7] Prop. 2020/21:194, Ett starkare skydd för Sveriges säkerhet.

myndigheters föreskrifter. Men när lagstiftningen överlåter sådan normgivning till olika myndigheter, och normerna innebär skyldigheter och andra ingrepp i enskilda subjekts verksamheter, måste detta ske med stor försiktighet.

Digitalisering, informations- och cybersäkerhet, utvecklingen av hot, sårbarheter samt risker

Enligt utredningen är ett övergripande mål för Sverige att vara bäst i världen på att använda digitaliseringens möjligheter.[8] Utredningen uppmärksammar även den hastighet med vilken tekniken på området utvecklas.[9] De fördelar och möjligheter som utvecklingen medför är naturligtvis av stort värde för samhället och även för rättssystemet, vilket Advokatsamfundet givetvis välkomnar. Advokatsamfundet vill emellertid varna för att ambitionerna att tillvarata tekniken och de möjligheter som denna erbjuder kan medföra att säkerhetsfrågorna kan hamna på undantag. Utredningen synes instämma i denna farhåga.[10]

Advokatsamfundet anser att säkerhetsfrågorna ännu inte har fått den uppmärksamhet de rätteligen förtjänar. Detta kan möjligen tillskrivas ett visst mått av naivitet och överdriven tilltro till de tekniska lösningarnas robusthet hos olika aktörer och verksamheter. Om vi inte kan lita på tekniken och de system eller tjänster som denna erbjuder, blir den omedelbara konsekvensen därav att vi inte heller kan lita på den information som hanteras eller genereras. Informationen ska i sin tur leda till olika slags beslut eller åtgärder som kan vara mycket väsentliga för samhället och medborgarna. Detta gäller inte minst sådan verksamhet som omfattas av säkerhetsskyddslagstiftningen och som kan vara särskilt sårbar för yttre hot eller angrepp. Därför vill Advokatsamfundet framhålla betydelsen i att säkerhetsfrågorna kommer in som en naturlig del redan i ett inledande skede när ny teknik utvecklas och sätts i drift. Samtidigt måste även juridiken beaktas i detta tidiga skede så att tekniken även utvecklas i enlighet med tillämpliga regelverk, exempelvis så att den uppfyller sådana krav som gäller enligt GDPR eller andra regelverk som gäller för personuppgiftsbehandling.

Utkontraktering och användandet av molntjänster leder till att informationen inte längre finns i verksamhetens omedelbara närhet och direkta kontroll. I praktiken

[8] SOU 2021:63 s. 94.
[9] SOU 2021:63 s. 95.
[10] SOU 2021:63 s. 99 f.

medför sådana tjänster att den information som ska hanteras i verksamheten kommer att finnas hos någon annan och där blir tekniskt åtkomlig för denne. Ett talande exempel på detta är Transportstyrelsen utkontraktering av sina körkorts- och fordonsregister, där informationen blev tillgänglig hos olika anlitade leverantörer, varav en rentav fanns utanför EU.[11] Exemplet visar att det finns en risk för att förväntningarna på och tilltron till tekniken medför att vi glömmer bort att bedöma om den aktuella lösningen inte bara är bra utan även om den är laglig, säker eller lämplig för den slags information som ska hanteras.

Enligt Advokatsamfundets bedömning är synen på cyber- och informationssäkerheten i mångt och mycket en attitydfråga. Utredningens förslag och slutsatser är ett steg i rätt riktning, men mycket återstår innan cyber- och informationssäkerhetsfrågorna ges nödvändig prioritering bland samhällets olika aktörer.

Den säkerhetsskyddsklassning som ska göras enligt säkerhetsskyddslagstiftningen syftar bland annat till att bedöma om hantering av ett visst slags information är lämplig ur säkerhetsskyddsaspekt. En sådan slags bedömning torde behöva göras beträffade all slags informationshantering i olika slags verksamheter och bör utmynna i en informationsklassning avseende den aktuella informationen.[12] Detta medför att olika slags information kommer att få olika informationsklasser beroende på vilka hot och risker som förekommer samt den skada som kan uppstå om informationen obehörigen röjs, används, förstörs, försvinner eller förvanskas. I undantagsfall kan detta innebära att viss information inte överhuvudtaget bör förekomma i informationstekniska system och då särskilt sådana system som tillhandahålls eller drivs av utomstående aktörer. Advokatsamfundet anser att betänkandets förslag inte i tillräcklig grad behandlar denna problematik.

Säkerhetskänslig verksamhet

I GDPR framgår att förordningens regler inte gäller beträffande nationell säkerhet och att säkerhetsskyddslagstiftningen därmed gäller i stället för GDPR.[13] Enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster är lagen

[11] Se https://www.svt.se/nyheter/inrikes/transportstyrelsens-sakerhetsskandal-detta-har-hant.
[12] Jfr. art. 32 och 35 GDPR, även 12 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.
[13] Art. 2 GDPR.

tillämplig på verksamhet som omfattas av säkerhetsskyddslagstiftningen.[14] I praktiken är det dock inte lika självklart och enkelt att avgöra vilken lagstiftning som är tillämplig på verksamheten. De begrepp som används lämnar ett stort utrymme för självständig bedömning som kan göra det svårt att förutse vad som avses. Exempelvis framgår inte när en verksamhet ska anses vara ”av betydelse” för Sveriges säkerhet och inte heller när en sådan verksamhet till ”någon del ”ska anses säkerhetskänslig.[15] Det är även svårt att förutse när verksamheten eller däri förekommande information innehåller säkerhetskänsliga uppgifter som är av sådan art att säkerhetsskyddslagens bestämmelser blir tillämpliga. När det gäller placering i säkerhetsklass för den som tar del av säkerhetskänsliga uppgifter bestäms säkerhetsklassen av mängden uppgifter och känslighetsgraden hos de uppgifter som vederbörande kan få tillgång till. Även uppgifternas omfattning och känslighet får ett stort utrymme för självständig bedömning.[16] På detta sätt kommer verksamhetsutövaren att själv få ta ställning i dessa frågor, samtidigt som bedömningen sker med risken att påföras sanktionsavgifter eller andra påföljder om den är felaktig. Även när det är fråga om ett sådant system eller sådan förändring av ett system som ska omfattas av de nya bestämmelserna jämte vilka säkerhetskrav som är ”motiverade” eller om driftsättningen är ”lämplig” kommer i praktiken dessa prövningar bli föremål för en självständig bedömning.[17] Utredningens förslag innebär därtill att sanktionsavgift ska kunna tas ut av den samrådsmyndighet som utövar tillsyn.[18]

Advokatsamfundet vill mot den bakgrunden framhålla att det är viktigt att sanktionsavgifter eller andra påföljder tillgrips med stor restriktivitet och att sådana påföljder blir aktuella först när verksamhetsutövaren fått rimliga förutsättningar att känna till vad som förväntas av denne eller när det är fråga om särskilt allvarliga åsidosättanden. Som utgångspunkt måste det enligt Advokatsamfundets uppfattning i första hand bli fråga om råd och anvisningar för att åstadkomma det säkerhetsskydd som krävs. Det är önskvärt att detta kommer till tydligt uttryck i bestämmelserna, exempelvis genom att det anges i lagtexten att myndigheten i första hand ska försöka åstadkomma rättelse genom råd och anvisningar.

[14] 8 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.
[15] 1 kap. 1 § säkerhetsskyddslagen (2018:585).
[16] 3 kap. 5-8 §§ säkerhetsskyddslagen (2018:585).
[17] Se förslaget till nytt 3 a kap. 1 § st. 1-2 i säkerhetsskyddslagen (2018:585), SOU 2021:63 s. 47.
[18] Se förslaget till ny 7 kap. 2 a § i säkerhetsskyddslagen (2018:585), SOU 2021:63 s. 49 och 445 ff.

Informationssäkerhet och åtgärder för stärkt säkerhet i nätverks- och informationssystem

Advokatsamfundet anser att utredningen generellt sett har gjort en gedigen genomgång av olika slags hot och risker samt att utredningen uppmärksammat behovet av olika slags informationssäkerhetsåtgärder.[19] Advokatsamfundet ställer sig därför bakom utredningens bedömningar i dessa delar, men vill även framhålla följande.

Informationssäkerheten hos en verksamhet är som utgångspunkt ett beställarproblem. Det är beställaren som ska känna till vilket slags information som ska behandlas och vilka konsekvenserna kan bli om informationen förvanskas, försvinner eller kommer i orätta händer. Att det samtidigt införs ett certifieringssystem som syftar till att säkerställa att vissa IKT-tjänster, -produkter eller -processer är tillförlitliga, och att den leverantör som erbjuder dessa också är tillförlitlig, ändrar inte på detta.

Advokatsamfundet vill därför uppmärksamma att säkerhetsskyddslagen, och de föreslagna bestämmelserna i densamma, utgör krav på beställaren att beakta säkerhetsfrågorna och välja lämplig leverantör. EU:s cybersäkerhetsakt innehåller bland annat bestämmelser om certifiering av leverantörer som ska tillhandahålla IKT-produkter, -tjänster och processer. Detta innebär att cybersäkerhetsakten riktar sig mot leverantörssidan. Enligt Advokatsamfundets bedömning finns en viss risk för att förhållandet mellan dessa båda regelverk kan missuppfattas. Gränsdragningsfrågorna blir därför viktiga, så att tillämpningsområdet för regelverken inte blandas ihop.

De uppmärksammade ransomwareattackerna under 2021, först mot Coop och senare mot Kalix kommun, utgör varnande exempel på vilka konsekvenser som kan uppkomma vid bristande cybersäkerhet. Den tekniska utvecklingen innebär även utökade möjligheter att begå intrång och attacker av olika slag som riktas mot informationen. Det finns även risk för att information förvanskas eller försvinner till följd av tekniska fel och brister. Advokatsamfundet vill därför särskilt framhålla nödvändigheten i att ha beredskap för sådana eventualiteter. Detta blir särskilt påtagligt när det är fråga om säkerhetskänslig verksamhet där tillgången till informationen är en nödvändig förutsättning för att verksamheten ska kunna bedrivas. För att undvika att en incident eller en attack helt lamslår en verksamhet måste det finnas redundanta lösningar. Advokatsamfundet efterlyser en strategi där de olika verksamheterna har tillgång till alternativa system som snabbt kan sättas i drift utan att

[19] Se t.ex. SOU 2021:63 s. 103 f. och 149 ff.

vara anslutna till det system som har drabbats. Därtill måste det finnas en löpande säkerhetskopiering eller backuptagning som innebär att informationen snabbt kan införas i det ersättande systemet.

Certifiering av nätverks- och informationssystem

Ett av utredningens uppdrag har varit att se till att säkerhetsskyddslagstiftningen korresponderar med det europeiska ramverket för cybersäkerhetscertifiering, dvs. EU:s cybersäkerhetsakt och de genomförandeakter som utfärdas med stöd av cybersäkerhetsakten.[20] I detta sammanhang får Advokatsamfundet inledningsvis hänvisa till att åtgärder som rör försvar och nationell säkerhet inte ingår i EU:s kompetensområde och att verksamhet som omfattas av säkerhetssyddslagstiftningen därmed inte omfattas av EU:s cybersäkerhetsakt.[21] Därefter får Advokatsamfundet framhålla att sådan verksamhet är särskilt känslig och att de krav som gäller för leverantörer som certifierats enligt cybersäkerhetsakten inte automatiskt medför att aktuella IKT-produkter, -tjänster eller -processer är tillräckliga för att uppfylla de krav som följer av säkerhetsskyddslagstiftningen.

Advokatsamfundet anser det därför angeläget att utredningens förslag inte låser fast verksamheter som omfattas av säkerhetsskyddslagstiftningen vid att endast använda sig av sådana certifierade produkter, tjänster eller processer. Det måste således finnas utrymme för verksamheterna att välja andra lösningar när behovet av säkerhetsskydd föranleder detta.

Samtidigt finns det skäl att sätta större tillit till sådana lösningar som är certifierade av olika ackrediterade certifieringsorgan. Det torde enligt Advokatsamfundets uppfattning kunna förutsättas att certifierade produkter, tjänster och processer genomgått en viss säkerhetsgranskning som säkerställer en viss miniminivå gällande informationssäkerhet. Olika slags ISO-certifieringar är exempel på detta. Dock gäller för verksamhet som hanterar särskilt känslig information, vilket är fallet inte minst när det är fråga om sådan som omfattas av säkerhetsskyddslagstiftningen, att inte blint förlita sig på olika slags certifieringar. Det finns en risk för övertro på certifieringar,

[20] Se SOU 2021:63 s. 19.
[21] Se SOU 2021:63 s. 20 och art. 4.2 EU-fördraget.

framförallt inom områden där den tekniska utvecklingen är mycket snabb och där det finns en uppsjö av tekniska lösningar.

Advokatsamfundet konstaterar att utredningen i och för sig har uppmärksammat att en certifiering inte lämnar några garantier för en tillförlitlig säkerhet.[22] Mot bakgrund därav, och med hänvisning till vad som anförts ovan, borde det enligt Advokatsamfundets mening särskilt tydligt framgå att de verksamheter som omfattas av säkerhetsskyddslagstiftningen inte ska ha någon *skyldighet* att anlita endast certifierade leverantörer eller att endast använda certifierade produkter, tjänster eller processer.

Krav på godkännande och utvidgat samrådsförfarande för informationssystem

Advokatsamfundet konstaterar att utredningen föreslår ett samrådsförfarande som liknar det krav på förhandsamråd som gäller enligt GDPR vid behandling av särskilda kategorier av personuppgifter.[23]

Enligt förslaget ska samrådsmyndigheten, dvs. Säkerhetspolisen eller Försvarsmakten[24], kunna förbjuda ett driftsättande av ett informationssystem[25] och även kunna besluta om olika förelägganden eller ta ut sanktionsavgift.[26] Eftersom detta utgör mycket ingripande åtgärder är det viktigt att de krav som samrådsmyndigheten uppställer för godkännande av en driftsättning, eller de skäl som ligger bakom ett förbud eller andra beslut från samrådsmyndigheten, framstår som motiverade och proportionerliga. Advokatsamfundet saknar sådana begränsningar avseende samrådsmyndighetens åtgärder eller beslut och anser att det behövs klargöranden i dessa avseenden under det fortsatta lagstiftningsarbetet.

Tillgång till informationssystem vid tillsyn

Enligt förslaget ska tillsynsmyndigheten ha rätt att få tillgång till de informationssystem som används i den verksamhet som omfattas av tillsynen.[27]

---

[22] SOU 2021:63 s. 266 och 469.
[23] Se förslaget till nytt 3 a kap. 2 § i säkerhetsskyddslagen (2018:585), SOU 2021:63 s. 48, jfr. art. 35 GDPR.
[24] Se förslaget till ändring i säkerhetsskyddsförordningen (2018:658) 3 kap. 1 §, SOU 2021:63 s. 51.
[25] Se förslaget till ny 3 a kap. 5 § i säkerhetsskyddslagen (2018:585), SOU 2021:63 s. 48.
[26] Förslaget till nytt 3 a kap. 2 och 5 §§ och ny 7 kap. 2 a § i säkerhetsskyddslagen (2018:585), SOU 2021:63 s. 48 f.
[27] Se förslaget till ändring i 6 kap. 3 § i säkerhetsskyddslagen (2018:585), SOU 2021:63 s. 48 f. och 472 ff.

Tillgången till systemen ska vägas mot integritetsintresset hos den enskilde som blir föremål för tillsynen.[28]

Advokatsamfundet får i detta sammanhang uppmärksamma att tillsynsmyndigheten därigenom kommer att få tillgång till information som omfattas av sekretess eller tystnadsplikt enligt lag eller annan författning. Den som tillsynen gäller kommer att behöva bistå tillsynsmyndigheten med att få tillgång till informationssystemen och därmed även till den information som ingår i dessa. I en sådan situation kan den som tillsynen gäller potentiellt anses ha röjt informationen för tillsynsmyndigheten. Även om tillsynsmyndigheten själv omfattas av sekretess för den information man på detta sätt får tillgång till, bör det enligt Advokatsamfundet förtydligas att det röjande som därvid blir aktuellt inte ska anses strida mot någon bestämmelse om sekretess eller tystnadsplikt.[29]

Handläggning och överklagande

Bestämmelserna om handläggning och överklagande följer samma ordning som gäller i liknande sammanhang. Advokatsamfundet har ingen erinran mot detta.

Offentlighet och sekretess

Utredningen har konstaterat att det kan förekomma mycket känsliga uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) hos verksamhetsutövaren. I första hand kan informationen omfattas av försvarssekretess, utrikessekretess eller underrättelsesekretess.[30] Sådan sekretess gäller oavsett hos vilken myndighet uppgifterna finns och samma sekretesskydd kommer därför att gälla hos samrådsmyndigheten som hos verksamhetsutövaren. Därför finner utredningen att inga ändringar behövs vad gäller sekretess för allmänna intressen, vilket Advokatsamfundet instämmer i.[31]

När det gäller sekretesskyddet för enskilda verksamhetsutövares intressen för utredningen ett resonemang kring om särskilda bestämmelser kan behöva införas i offentlighets- och sekretessförordningen (2009:641) till skydd för sådana uppgifter

[28] SOU 2021:63 s. 473.
[29] Sådana sekretessregler finns i offentlighets- och sekretesslagen (2009:400) men regler om tystnadsplikt kan även ingå i bestämmelser i viss specialförfattning som gäller för den aktuella verksamheten.
[30] 15 kap. 1-2 §§ och 18 kap. 2 § offentlighets- och sekretesslagen (2009:400).
[31] SOU 2021:63 s. 479.

som samrådsmyndighetsmyndigheten får tillgång till.[32] Advokatsamfundet ifrågasätter om inte samma sekretessbestämmelser, dvs. försvars-, utrikes-, eller underrättelsesekretessen, kan vara tillämpliga även i dessa fall eftersom det är samma slags uppgifter som förekommer hos de enskilda verksamhetsutövarna och som angår Sveriges säkerhet. Annars skulle dessa aktörer inte omfattas av säkerhetsskyddslagstiftningen. Advokatsamfundet ställer sig därmed tveksamt till om det egentligen finns något behov av särskilda sekretessbestämmelser i offentlighets- och sekretessförordningen (2009:641).

Det finns dock en annan problematik som föreligger när tillsyns- eller samrådsmyndigheter ska få tillgång till informationssystem och den information som förekommer i systemen som bör uppmärksammas.

När myndigheterna får tillgång till sådan information är det svårt att se att detta kan ske utan att de aktuella uppgifterna anses utlämnade till myndigheten, vilket innebär att tillämpliga sekretessbestämmelser måste beaktas innan någon annan anlitas för behandlingen.[33]

När en myndighet som omfattas av säkerhetsskyddslagen lämnar ut uppgifter till samråds- eller tillsynsmyndigheten genom att någon av dessa får tillgång till information i berörda informationssystem, kan denna anses utlämnad eller röjd för myndigheten med stöd av någon sekretessbrytande grund.[34] Tillgängliggörandet, utlämnandet eller röjandet skulle därmed i denna situation vara behörigt och tillåtet.

För en enskild verksamhetsutövare som omfattas av säkerhetsskyddslagstiftningen är situationen dock annorlunda. Dennes verksamhet omfattas nämligen av en särskild tystnadsplikt som innebär att den som på grund av anställning eller på annat sätt deltar eller har deltagit i säkerhetskänslig verksamhet hos verksamhetsutövaren inte obehörigen får röja eller utnyttja säkerhetsskyddsklassificerade uppgifter.[35] Svårigheten ligger här i begreppet *obehörigen* och att offentlighets- och sekretesslagens bestämmelser med bland annat sekretessbrytande grunder inte gäller för enskilda verksamhetsutövare. Det innebär att det måste kunna anses vara fråga om ett *behörigt* utlämnande eller röjande när samråds- eller tillsynsmyndigheten ges tillgång till

[32] SOU 2021:63 s. 479.
[33] SOU 2018:25 s. 348 ff. och SOU 2021:1 s. 270.
[34] Exempelvis 10 kap. 17 § offentlighets- och sekretesslagen (2009:400).
[35] 8 kap. 2 § säkerhetsskyddslagen (2018:585).

informationssystemen och informationen däri. Frågeställningarna diskuterades bland annat i förarbetena till nuvarande säkerhetsskyddslagen, men utan att något egentligt svar gavs vad gäller i vilka situationer ett röjande ska anses vara ”behörigt”.[36]

Advokatsamfundet anser det logiskt att det är fråga om ett ”behörigt” röjande när information i informationssystem blir tillgänglig för en tillsyns- eller samrådsmyndighet i enlighet med lag. Men eftersom bestämmelser om sekretess eller tystnadsplikt ska tolkas restriktivt till skydd för det bakomliggande intresset, måste det på något sätt framgå när en skyddad uppgift får lämnas ut.

Enligt Advokatsamfundet är det angeläget att denna problematik uppmärksammas och att det uttryckligen framgår i vilka slags situationer en enskild utövare av säkerhetsskyddad verksamhet behörigen kan lämna ut uppgifter. Detta bör framgå antingen direkt i lagtexten eller åtminstone genom uttalanden i förarbetena.

Säkerhetsskyddsanalys och särskild säkerhetsskyddsbedömning

Av säkerhetsskyddslagen följer att behovet av säkerhetsskydd ska utredas och dokumenteras i en *säkerhetsskyddsanalys*. Analysen ska utgöra utgångspunkt för den planering och de åtgärder som behövs för säkerhetsskyddet. Analysen ska ske med hänsyn till den aktuella verksamhetens art och omfattning, förekomsten av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter.[37] I förarbetena framhålls säkerhetsskyddsanalysens centrala betydelse för att åstadkomma ett väl anpassat säkerhetsskydd, för identifiering av skyddsvärde, hot och sårbarheter i den aktuella säkerhetskänsliga verksamheten. Bedömningarna i analysen, motiveringen och grunden för de säkerhetsskyddsåtgärder som ska vidtas ska säkerställa att åtgärderna hänger ihop i ett väl fungerande säkerhetsskyddssystem. I analysen ska tydliggöras olika slags hot och sårbarheter som åtgärderna ska skydda mot, men även vilka negativa konsekvenser som kan bli följden av ett angrepp. Säkerhetsskyddsanalysen bör identifiera vilka säkerhetsskyddsklassificerade uppgifter som finns och vad som i övrigt behöver skyddas i verksamheten. Det bör därefter göras en bedömning av säkerhetshot, potentiella konsekvenser och sårbarheter. Analysen ska dokumenteras och mynna ut i en bedömning av behovet av säkerhetsskyddsåtgärder. Förarbetena

[36] Se bl.a. prop. 2017/18:89 s. 119 ff.
[37] 2 kap. 1 § säkerhetsskyddslagen (2018:585).

framhåller dessutom att arbetet med säkerhetsskyddsanalysen bör vara en kontinuerligt pågående process och analysen bör hållas uppdaterad.[38]

När det ska göras en *särskild säkerhetsskyddsbedömning*[39] för bedömning av behovet av säkerhetsskydd i samband med driftsättning av informationssystem, kan förekomsten av dessa båda olika begrepp verka förvirrande. Skillnaden mellan en *säkerhetsskyddsanalys* och en *säkerhetsskyddsbedömning* framgår nämligen inte i lagtexten. Avsikten synes vara att säkerhetsskyddsanalysen ska vara inriktad mot en bedömning av de konsekvenser som olika hot eller risker kan medföra för verksamheten, medan säkerhetsskyddsbedömningen snarare ska ta sikte på att bedöma vilka dessa hot eller risker är. Det är möjligt att skillnaden mellan begreppen är känd hos de aktörer som normalt omfattas av säkerhetsskyddslagstiftningen, men Advokatsamfundet hade trots detta gärna sett att en definition av dessa båda begrepp ingått i de föreslagna bestämmelserna. Som förslaget är utformat kan det uppfattas som att en särskild säkerhetsskyddsbedömning ska göras vid driftsättning av informationssystem men att någon säkerhetsskyddsanalys inte ska göras i dessa fall, vilket inte torde vara avsikten. Exempelvis skulle de båda begreppen definieras enligt följande och införas i 2 kap. 1 § säkerhetsskyddslagen (2018:585).

Säkerhetsskyddsanalys: Med säkerhetsskyddsanalys avses den dokumenterade utredning av behovet av säkerhetsskydd som anges i punkt 1 och som bland annat omfattar vilka olika slags hot eller risker som kan förekomma i verksamheten. Säkerhetsskyddsanalysen ska beskriva de konsekvenser som kan uppkomma till följd av att hoten eller riskerna förverkligas.

Säkerhetsskyddsbedömning: Med säkerhetsskyddsbedömning avses en dokumenterad utredning avseende vilka säkerhetskrav som ska uppställas och som bland annat omfattar vilka olika slags hot eller risker som kan förekomma i verksamheten. Säkerhetsskyddsbedömningen ska innehålla en bedömning av sannolikheten för att hoten eller riskerna förverkligas.

[38] Prop. 2017/18:89 s. 56, även SOU 2021:63 s. 129.
[39] Se förslaget till nytt 3 a kap. 1 § i säkerhetsskyddslagen (2018:585), SOU 2021:63 s. 47 och 160 ff.

SVERIGES ADVOKATSAMFUND

Mia Edwall Insulander