Stockholm den 14 augusti 2017

R-2017/0948

Till Justitiedepartementet

Ju2017/03997/L4

Sveriges advokatsamfund har genom remiss den 23 maj 2017 beretts tillfälle att avge yttrande över betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36).

Advokatsamfundet anser att flera av förslagen i betänkandet behöver genomlysas ytterligare.

I remissvar över betänkandena Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten (SOU 2015:23) och En ny säkerhetsskyddslag (SOU 2015:25) har Advokatsamfundet noterat att informationssäkerhetsarbetet bedrivs utifrån olika utgångspunkter med stöd i olika författningar som tillkommit vid olika tidpunkter, utifrån olikartad terminologi och utan strukturerat inbördes samband samt att ny teknik och eskalerande hot och risker drivit fram nya regler, vilket lett till överlappande bestämmelser som inte alltid är lätta att tillämpa. Sammantaget har detta gett bilden av ett växande, svåröverblickbart och fragmenterat rättsområde, vilket skapar osäkerhet i den praktiska hanteringen och riskerar innebära rättsosäkerhet vid rättstillämpningen (en jämförelse kan göras med de komplikationer som de s.k. registerförfattningarna har fört med sig). Advokatsamfundet noterade samtidigt att en omfattande överlappning mellan olika organs tillsynsansvar skulle bli följden av den då föreslagna regleringen. Mot bakgrund härav avstyrkte Advokatsamfundet förslagen i dess dåvarande utformning.

De förslag som nu läggs fram av utredningen om genomförande av NIS-direktivet, utgör ett angeläget steg i arbetet med att stärka informationssäkerheten. Arbetet måste dessutom

ske skyndsamt med hänsyn till att Sverige är bundet av ett direktiv med kort genomförandetid. Advokatsamfundet konstaterar emellertid att de farhågor som samfundet tidigare gett uttryck för stärks genom de framlagda förslagen. För tydlighetens skull väljer samfundet denna gång att ta sin utgångspunkt i konkreta exempel.

En explosiv utveckling sker mot molntjänster, som tillhandahålls av privata aktörer. En sådan leverantör kan komma att ha kunder från många av de sektorer, som tas upp i bilaga 2 till direktivet. I några delar kan det dessutom bli fråga om t.ex. betrodda tjänster enligt eIDAS-förordningen, verksamhet av betydelse för Sveriges säkerhet eller elektronisk kommunikation för vilken särskilda regler gäller. För dessa fall ska andra regler än nu föreslagen lag och förordning tillämpas. I andra fall där föreslagen lag och förordning alltjämt skulle bli tillämplig, tilldelas olika myndigheter uppgiften att utöva tillsyn, beroende på inom vilken sektor en viss tjänst hör hemma. Den digitala infrastruktur som leverantören använder för att leverera tjänsterna kan dock, med beaktande av hur de tekniska lösningarna normalt har utformats, knappast separeras så att ett it-angrepp naturligt kan hänföras till en av dessa sektorer. På motsvarande sätt är det en grannlaga uppgift att tolka t.ex. eIDAS-förordningen, så att det kan bedömas vad som ska vara undantaget från den nu föreslagna regleringens tillämpningsområde. En omfattande överlappning synes därmed uppkomma mellan olika organs tillsynsansvar och svårigheter att veta enligt vilken eller vilka författningar incidentrapporter ska lämnas.

Advokatsamfundet inser att tiden för ett genomförande av NIS-direktivet är kort. Samfundets synpunkter tar emellertid främst sikte på sådant som föreslås bli reglerat i förordning och myndighetsföreskrifter. Leverantören i exemplet med flera kunder från olika verksamhetsområden måste inte bara beakta vad som föreskrivs i lag och förordning. Det kommer dessutom att kunna finnas relevanta myndighetsföreskrifter utfärdade av inte bara Myndigheten för samhällsskydd och beredskap (MSB), utan också av var och en av sektorsmyndigheterna. Advokatsamfundet ifrågasätter, dels att så många olika myndigheter ska bygga upp kompetens för att reglera informationssäkerhetsfrågor av likartat slag, dels om det ens finns förutsättningar att rekrytera it-säkerhetsspecialister till alla dessa myndigheter för att separat inom vart och ett av dessa områden utföra erforderlig granskning av informationssäkerheten.

Mycket talar i stället för att samla specialistkompetensen hos en myndighet. Utvecklingen pekar tydligt bland leverantörerna mot ökad specialisering, så att det inte är möjligt att hos var och en av dem bygga upp hela den kompetens som behövs; jfr t.ex. de komplikationer som redan finns när det gäller att ha en helhetsbild över skyddsbehovet vid e-legitimering, e-underskrifter och intrångsdetektering och liknande. När det redan för tillhandahållandet av sådana funktioner i många fall krävs expertis på nationell nivå, är det inte enkelt att förstå hur tillsynen över informationssäkerheten skulle kunna spridas ut på många olika tillsynsmyndigheter. Det som är sammanhållande och gemensamt är de komplexa säkerhetsfrågorna, inte i första hand skillnader inom olika sakområden – så länge siktet ska vara inställt på samhällets informationssäkerhet.

Rättssäkerheten skulle öka om t.ex. privata företag, som omfattas av regleringen utan närmare undersökning, kan veta vilken myndighet de ska vända sig till och vem som kan utfärda myndighetsföreskrifter inom området. Risker skulle inte heller uppkomma för att olika tillsynsmyndigheter gör motstående bedömningar eller utfärdar föreskrifter som pekar i olika riktning.

Advokatsamfundet ser samtidigt ett behov av att närmare genomlysa konsekvenserna av att EU:s dataskyddsförordning kommer att gälla parallellt med den nu föreslagna regleringen. Båda dessa regelverk innehåller regler om sanktionsavgifter, som med avseende på bl.a. avgifternas storlek framstår som nya påtagliga affärsrisker. Utredningen om genomförande av NIS-direktivet synes utgå från att dessa frågor enkelt kan lösas i samverkan med Datainspektionen. Vid remiss av promemorian Tillhandahållande av tekniska sensorsystem – ett sätt att förbättra samhällets informationssäkerhet, har emellertid framkommit att bl.a. MSB och Datainspektionen har helt olika syn på frågor av central betydelse för informationssäkerheten, och därmed i vissa fall möjligen även på vad som ska drabbas av en sanktion.

Advokatsamfundet ställer sig också frågande till varför berörd information endast ska omfattas av svag sekretess. Utgångspunkten för ett rakt skaderekvisit är att uppgifterna är offentliga och att sekretess gäller endast om det kan antas att viss skada uppstår om uppgiften lämnas ut samt att skadebedömningen i huvudsak ska kunna göras med utgångspunkt i själva uppgiften. Vid svag sekretess ska frågan inte i första hand behöva knytas till en skadebedömning i det enskilda fallet. Vid ett omvänt skaderekvisit har befattningshavare vid den myndighet där t.ex. en incidentrapport blivit allmän däremot ett begränsat utrymme för sin bedömning. – För incidentrapporter och liknande, får generellt antas gälla att en skadebedömning inte kan ta sin utgångspunkt endast i själva uppgiften, utan förutsätter kringliggande detaljinformation och en grannlaga bedömning. Begås ett misstag kan informationssäkerheten sättas i fara i en samhällsviktig tjänst. Att sådana misstag hittills inte synes ha förekommit, utgör enligt Advokatsamfundet inte tillräckliga skäl för att bibehålla ett skaderekvisit som får anses vara ämnat för en lägre nivå av risk. En förtroendefull samverkan mellan berörda myndigheter och företag, torde också förutsätta att själva sekretessregleringen ger uttryck för det starka behovet av skydd.

Sammanfattningsvis vill Advokatsamfundet anföra att det är av stor betydelse för samhällets informationssäkerhet att NIS-direktivet genomförs, men att dessa angelägna behov riskerar att motverkas av en fragmenterad reglering och ett delvis överlappande tillsynsansvar samt att det blir en utmaning att inom så många myndigheter inte bara rekrytera, utan även behålla expertkunskap på informationssäkerhetsområdet.

Med hänvisning till det ovan anförda avstyrker Advokatsamfundet de berörda förslagen i dess nuvarande utformning.

SVERIGES ADVOKATSAMFUND

Anne Ramberg/

genom Maria Billing