Sveriges advokatsamfund

Stockholm den 28 maj 2024

R-2024/0702

Till Försvarsdepartementet
Fö2024/00496

Sveriges advokatsamfund har inte tagits upp som remissinstans, men avger härmed på eget initiativ yttrande över delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18).

Sammanfattning

Advokatsamfundet bedömer att förslaget, om det genomförs i sin nuvarande form, skulle leda till ett ineffektivt utnyttjande av statens resurser. Resurserna skulle fördelas mellan myndigheter på ett sätt som motverkar lagens syfte, samtidigt som enskilda verksamhetsutövare åsamkas onödiga kostnader och betydande regulatoriska utmaningar. Advokatsamfundet har flera invändningar mot innehållet i betänkandet, vilka redovisas nedan.

Synpunkter

Direktivets tillämpningsområde m.m. (avsnitt 5 och 7 i betänkandet)

Enligt Advokatsamfundet är det, oaktat att NIS2-direktivet (nedan direktivet) innehåller en klassificering av de sektorer som omfattas av direktivet, i många fall inte tydligt vilka verksamheter som omfattas. Vissa begrepp är svårtolkade, inte minst mot bakgrund av att hänvisningar i stor utsträckning görs till definitioner i annan EU-reglering.

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

Till detta kommer att hänvisningar i vissa fall enbart görs till direktivet, trots att samma begrepp definieras i annan EU-lagstiftning. Ett sådant exempel är begreppet ”laddningsoperatör” som även definieras i förordningen EU 2013/1804, i vilken definitionen är bredare. Detta medför tolkningsproblem och svårigheter för verksamhetsutövarna att förutse hur reglerna kommer att träffa dem. Sådana slags otydligheter måste vägas in vid en bedömning av om en verksamhetsutövare eventuellt åsidosatt reglerna och påverka dennes ansvar.

Utredningen har föreslagit att ansvariga tillsynsmyndigheter ska få i uppdrag att klargöra vilka verksamheter som omfattas av de aktuella verksamhetsdefinitionerna. Tills dess att sådana klargöranden publicerats och berörda verksamhetsutövare fått erforderlig tid att anpassa sin verksamhet till den nya lagens krav bör de föreslagna sanktionsmöjligheterna i lagen inte tillämpas.

Advokatsamfundet noterar att utredningen valt att inte införa alla delar av artikel 21 i direktivet i förslaget till lagen om cybersäkerhet (nedan cybersäkerhetslagen) och även har valt att i vissa fall använda andra begrepp än de som direktivet har. Detta skapar problem dels för verksamhetsutövare som bedriver verksamhet i flera länder, dels för att Sverige inte fullt ut genomfört direktivet. Om direktivet implementeras med olika innehåll i olika medlemsländer, samtidigt som en av ambitionerna bakom direktivet är att åstadkomma en harmonisering, medför detta ytterligare en komplikation för verksamhetsutövarna och påverkar rättssäkerheten för dessa.

Ett exempel på detta är utredningens slutsats att det är onödigt att ha ett krav på grundläggande praxis för cyberhygien. Att skapa cybersäkerhet genom bland annat cyberhygien är centralt i direktivet. Cyberhygien finns tydligt med i listan över åtgärder i artikel 21 i direktivet. Att inte ha med hela listan i cybersäkerhetslagen bör inte godtas eftersom det försvårar för verksamhetsutövare som ska efterleva kraven. Eftersom dessa dessutom finns i en särskild artikel i direktivet har medlemsstaterna varit överens om att kravet har en egen innebörd och i kommande praxis från EU-domstolen kan kravet komma att preciseras. Denna typ av lagstiftningsteknik kan skapa en stor osäkerhet och leda till att rättssäkerheten för verksamhetsutövarna undergrävs.

Utredningens slutsatser kring ledningens ansvar bedöms inte heller ligga i linje med direktivkraven. Av artikel 20.1 i direktivet följer att medlemsstaterna ska säkerställa att verksamhetsutövarens ledningsorgan godkänner och övervakar genomförandet av

riskhanteringsåtgärderna. Utredningen menar att detta inte behöver regleras rättsligt eftersom ansvar redan följer av aktiebolagslagens regler. Denna slutsats delas inte av Advokatsamfundet. Det noteras därtill att inte enbart aktiebolags ledningsorgan kommer att omfattas av skyldigheterna. Det finns inte någon tydlig reglering som motsvarar direktivets krav i aktiebolagslagen, i annan associationsrättslig lagstiftning eller i lagstiftning för andra utpekade verksamhetsutövare. Förtydliganden kring detta bör övervägas i den fortsatta beredningen.

Definitioner (avsnitt 7 i betänkandet)

Utredningens utgångspunkt är som följer av avsnitt 5.2.1 att direktivet inte ska införlivas direktivnära utan att förslagen ska utformas utifrån den systematik och terminologi som används i svensk rätt och att ett normalt språkbruk ska eftersträvas.

Advokatsamfundet konstaterar att många av de begrepp som definieras i NIS2-regelverket används i olika sammanhang och definieras på olika sätt i olika EU-rättsakter m.m. Det riskerar att leda till begreppsförvirring. Det är viktigt utifrån ett rättssäkerhetsperspektiv att lagstiftaren i största möjliga mån tillser att verksamhetsutövare har ett så tydligt regelverk som möjligt att efterleva. I annat fall får verksamhetsutövarna svårigheter att bedöma vilka verksamheter som omfattas och vilka åtgärder som bör vidtas.

Det är inte rimligt att låta verksamhetsutövarna riskera att få ansvara för otydligheter i lagstiftningen. En sådan ordning skulle strida mot rättsstatliga principer. Enligt legalitetsprincipen måste allmänheten kunna förutse och förstå vad som krävs av dem för att de ska kunna hållas ansvariga och det måste därför ankomma på lagstiftaren att utforma och formulera tydliga krav.

Advokatsamfundet inser att utredningen inte har haft möjlighet att hantera alla sådana frågor inom ramen för sitt uppdrag. Dock anser Advokatsamfundet att formuleringen ”systematiskt och riskbaserat informationssäkerhetsarbete” bör kompletteras med ”cybersäkerhet”. En definition av cybersäkerhet finns i cybersäkerhetsakten och dessutom använder utredningen begreppet cybersäkerhet i övriga delar av betänkandet. Enligt vad Advokatsamfundet har erfarit använder verksamhetsutövare begreppet IT-säkerhet ofta för tekniska frågor och med cybersäkerhet omfattas hot, risker och attacker utifrån via nätverk och tjänster. Informationssäkerhet kan synas vara ett övergripande samlingsbegrepp där de två förstnämnda ingår men definitionen

blir tydligare genom att även cybersäkerhet ingår i definitionen. Till det kommer att skäl 4 i direktivet anger att det är viktigt att höja cybersäkerhetsnivån i hela EU. I andra länder kommer man rimligen att använda cybersäkerhet som en del av definitionen. Det kan leda till problem för koncerner att man använder olika begrepp nationellt och på EU-nivå. Det framstår dessutom som tveksamt att inte inkludera cybersäkerhet i definitionen då lagen föreslås benämnas lagen om cybersäkerhet.

Utredningen har även föreslagit att begreppet ”riskhanteringsåtgärder” ska ersättas med ”säkerhetsåtgärder” för att ansluta till etablerat språkbruk på området. Advokatsamfundet förordar att denna ändring inte genomförs. Säkerhetsåtgärder är ett väl etablerat begrepp för åtgärder som används för att skydda nätverk och informationssystem. Riskhantering innefattar arbete med att förhindra eller minska sannolikheten för att en incident eller ett hot uppstår. Säkerhetsåtgärder är inte endast detta, utan kan även vara åtgärder som ska vidtas när något redan har inträffat. Säkerhetsåtgärder kan dessutom vara åtgärder för att minska skadeverkningar av en incident.

Kommuner (avsnitt 5.2.10 i betänkandet)

Utredningen har föreslagit att cybersäkerhetslagen ska omfatta all kommunal verksamhet och menar att detta är det sätt man måste tolka direktivet. Advokatsamfundet delar inte den bedömningen.

Inledningsvis bör noteras att offentliga förvaltningsentiteter ingår i bilaga I till direktivet. I artikel 2.5 anges dock att medlemsstaterna får föreskriva att direktivet ska tillämpas av offentliga förvaltningsentiteter på lokal nivå. Det är alltså inte ett absolut krav att kommuner ska ingå. Bedömningen ska göras av de enskilda medlemsstaterna. Direktivet lämnar med andra ord utrymme för att endast låta vissa delar av kommunal verksamhet omfattas. Kommuner bedriver många olika verksamheter av mycket skilda slag. Verksamheterna har därmed inte samma behov av säkerhet. Viss kommunal verksamhet ställer till och med särskilt höga krav på säkerhet och faller rentav under säkerhetsskyddslagen där NIS2-direktivet inte är tillämpligt och inte uppfyller de krav som ställs där. Annan kommunal verksamhet är typiskt sett okänslig och borde inte i onödan behöva omfattas av sådana särskilda säkerhetskrav som lagförslaget innebär.

För att bedöma om kommuner alls ska ingå är det rimligt att först titta på den grundläggande tanken med direktivet, nämligen att förhindra att cyberhot leder till

allvarliga incidenter som skadar samhället. En av de risker som lyfts i direktivet är vikten av att säkra städer och dess funktion. I skäl 53 till NIS-direktivet talas om sårbarheten när allt fler allmännyttiga tjänster är uppkopplade mot digitala tjänster. Bestämmelserna i direktivet nämner hur städer är sårbara för cyberattacker och att detta kan orsaka medborgarna stor skada. I Sverige har vi sett den här typen av sårbarheter flera gånger, till exempel i IT-attacken mot Kalix kommun 2021 som ledde till stora problem för kommunen. Det är därför rimligt att kommuner ingår i den krets som ska tillämpa NIS2.

Däremot ifrågasätter Advokatsamfundet om det är rimligt att all kommunal verksamhet måste ingå. För att förebygga att cyberhot leder till incidenter som allvarligt skadar kommunal verksamhet är det i stället viktigt att kommunerna fokuserar sina resurser på de områden där det finns störst risk för sådan påverkan.

Kommunerna bör dessutom överväga att hålla känslig verksamhet och känsliga system separerade från andra, så att dessa inte riskerar att ”smitta” varandra om något inträffar. Därigenom kan det undvikas att kommunerna vidtar onödiga åtgärder där de egentligen inte behövs, samtidigt som en inträffad incident därmed inte behöver drabba kommunens hela verksamhet.

Självklart ska generella system som kommunen använder i all sin verksamhet omfattas av kraven, men en annan fråga gäller de lokala system som en viss förvaltning är den enda användaren av. Här borde lagstiftaren i stället för att kräva att all verksamhet ska omfattas utgå ifrån en riskbaserad ansats. En sådan ansats bör resultera i slutsatsen att verksamhet som snabbt kan få samhällskritiska effekter omfattas, såsom socialtjänst, barnomsorg och skolverksamhet (föräldrar behöver denna verksamhet för att själva exempelvis kunna arbeta i känsliga verksamheter som omfattas av direktivet och cybersäkerhetslagen), tillsynsverksamhet och liknande ingår.

Lagtekniskt borde denna lösning inte vara allt för svår att åstadkomma eftersom man redan idag enligt exempelvis dataskyddsregleringen/GDPR utgår ifrån att det är kommunala nämnder och inte hela kommunen som är personuppgiftsansvarig enligt GDPR.

Risken att låta hela den kommunala verksamheten ingå blir att cybersäkerhetsåtgärder blir lika viktiga avseende kommunala badhus och bibliotek som i den tidigare nämnda

verksamheten. Detta riskerar att splittra kommunens fokus och försvåra ett effektivt införande av cybersäkerhetslagen.

Advokatsamfundet delar inte heller utredningens slutsats att det inte finns några andra alternativ än att låta hela verksamheten ingå. Förutom tidigare nämnda artikel 2.5 i direktivet bör man även beakta de kriterier som finns i artikel 2.2. I denna bestämmelse anges att verksamheter som inte når upp till storlekskraven ändå kan omfattas om verksamheten kan ha en betydande påverkan på skyddet av människors liv och hälsa eller där störningar kan medföra betydande systemrisker.

Direktivet har lämnat till medlemsstaterna att själva avgöra vad som krävs för den lokala nivån av den offentliga sektorn för att den ser olika ut i olika medlemsstater. Som tidigare nämnts godtar redan svensk rätt att kommunala nämnder kan ha eget ansvar trots att de ingår i den juridiska personen kommunen. Som redan nämnts är det nämnderna som är personuppgiftsansvariga och nämnder kan även genomföra offentliga upphandlingar.

Advokatsamfundet förordar att lösa frågan lagtekniskt genom att ange att kommunala nämnder som bedriver viss verksamhet, till exempel socialtjänst, ska omfattas av den nya lagen, men att andra inte behöver omfattas.

Tillsynsmyndigheter (avsnitt 8 i betänkandet)

I 1 kap. 1 § i författningsförslaget till cybersäkerhetslagen anges att syftet med lagen är att uppnå en hög cybersäkerhetsnivå. Enligt Advokatsamfundets uppfattning kan detta syfte inte uppnås, om ansvaret för att bedriva tillsyn m.m. sprids på många myndigheter på det sätt utredningen har föreslagit. Huvuddelen av dessa myndigheter ansvarar för ett stort antal andra verksamhetsområden och risken är uppenbar att myndigheterna inte kommer att ha det fokus eller de resurser som krävs för att tillse att lagens syfte uppnås.

För en enskild verksamhetsutövare innebär förslaget att verksamhetsutövaren kan komma att stå under tillsyn av ett flertal myndigheter. Detta kan i sin tur leda till att tillsynsmyndigheterna kommer till olika eller motstridiga slutsatser, vilket i sin tur kan medföra att verksamhetsutövaren ställs inför omöjliga val och tvingas att rätta sig efter endast en av dem.

Utredningen har även föreslagit att en verksamhetsutövares anmälan om att den omfattas av NIS2-regleringen ska göras till respektive tillsynsmyndighet. Detta innebär att varje tillsynsmyndighet inom sitt tillsynsområde ska upprätta ett register över väsentliga och viktiga verksamhetsutövare. Detta innebär att en rad olika myndigheter ska lägga ner resurser på att ta fram nya egna system som kan hantera verksamhetsutövarnas anmälningar med tillräcklig säkerhet. För verksamhetsutövare som står under tillsyn av flera krävs att dessa får lägga ner betydande resurser för att tillse att rapportering görs inte bara till en myndighet utan till flera – avseende samma information. Samtliga verksamhetsutövare ska även skicka in incidentrapporter till MSB/CSIRT-enheten. Förslaget kan därför ifrågasättas både ur effektivitets- och kostnadssynpunkt.

När det gäller incidentrapportering vill Advokatsamfundet även uppmärksamma det sekretesskydd som gäller för sådan rapportering. Denna typ av rapporter kan innehålla uppgifter om en inträffad incident som kan användas för att underlätta obehörig åtkomst eller för att skada eller störa berörda informationssystem. Det är avgörande för säkerhetsarbetet att uppgifter om svagheter och brister i berörda system inte avslöjas för aktörer med onda avsikter. För närvarande innehåller den tillämpliga sekretessbestämmelsen i 18 kap. 8 § offentlighets- och sekretesslagen endast ett rakt skaderekvisit, vilket innebär att utgångspunkten är att rapporterna ska lämnas ut till allmänheten på begäran. Därtill kommer att berörd myndighet självständigt ska pröva om sekretess ska gälla – oberoende av vad verksamhetsutövaren begär avseende sekretess. Detta kan medföra att verksamhetsutövarna känner oro inför att lämna in rapporterna eller väljer att utelämna olika uppgifter för att undvika att sådana slags uppgifter kommer i orätta händer.

Av dessa skäl finner Advokatsamfundet det vara angeläget att den tillämpliga sekretessbestämmelsen ändras så att det i stället ska gälla absolut sekretess för sådana uppgifter i rapporterna. Under alla förhållanden bör sekretessbestämmelsen ändras så att uppgifterna omfattas av sekretess med ett omvänt skaderekvisit, och att de därmed endast får röjas när det står klart att detta kan ske utan att det kan medföra skada för de intressen som sekretessen avser att skydda. Advokatsamfundet har noterat att i det kommande slutbetänkandet ska även sekretessfrågorna behandlas av utredaren. Det är då lämpligt att göra en översyn av bestämmelserna.

Vidare ifrågasätts om de myndigheter som pekas ut som tillsynsmyndigheter kommer att kunna hantera uppdraget. Frågan har, som berörts ovan, inte alltid ett nära samband med grunduppdraget. Det finns risk för att det innebär att det inte kommer finnas en gedigen kompetens att tillgå. Till det kommer att erfarenheterna av tillsynen enligt NIS-lagen inte är särskilt goda, vilket framgår av de uppgifter utredningen hämtat in. Som exempel kan nämnas att Riksrevisionen granskat Transportstyrelsens tillsynsverksamhet, som har bedrivits i mycket liten skala. Skälet tycks vara att Transportstyrelsen haft problem att rekrytera personal. Det skälet kommer att kvarstå även efter att Transportstyrelsen föreslås få ett utökat uppdrag. Rekryteringsproblemen kommer sannolikt att öka, eftersom många fler verksamheter och tillsynsmyndigheter kommer att omfattas av cybersäkerhetslagen. Lagförslaget måste därför åtföljas av möjligheter till utbildning för att stänga kompetensglappet som uppstår.

Ett särskilt problem är att länsstyrelserna anges bli tillsynsmyndigheter och att vissa länsstyrelser ska stå under tillsyn av andra länsstyrelser. Eftersom länsstyrelserna har gått samman i sitt IT-arbete och samlat detta kommer länsstyrelsernas tillsyn över andra länsstyrelsers cybersäkerhet belastas av ett jäv: Då de har samma IT-struktur kommer granskningen att lika mycket avse den egna verksamhetens IT vilket inte är särskilt trovärdigt.

Det kommer även att finnas särskilda problem för IKT-leverantörer som kommer att stå under tillsyn. Leverantörerna ska enligt förslaget till förordning stå under tillsyn av Post- och telestyrelsen. Kunderna till IKT-leverantörer kan dock vara från alla sektorer som omfattas av förordningen och alltså stå under annan tillsyn. Dessa kunder kommer att ställa krav på leverantörerna utifrån de krav deras tillsynsmyndigheter har. Om kraven inte är jämförbara kommer det uppstå spänningar i relationen. Frågan är vilka krav som då ska tillämpas. IT-system kan inte alltid byggas olika för olika kunder. Detta kan även leda till rättssäkerhetsproblem för IKT-leverantörerna och dess kunder.

Ska lagstiftningen bli effektiv bör därför ansvaret åläggas en myndighet, vilket i förekommande fall bör vara MSB. Mot bakgrund av myndighetens uppgift att verka för samordning av det civila försvaret men även som CSIRT-enhet och expertmyndighet avseende de områden som omfattas av NIS2-regleringen framstår det som ändamålsenligt att tilldela MSB uppdraget. MSB har även i flera år arbetat med uppdrag kopplade till informationssäkerhet.

Självfallet bör det åligga MSB att samverka med andra berörda myndigheter med särskild kompetens inom ett verksamhetsamhetsområde, exempelvis innan MSB meddelar föreskrifter eller vid utredningar.

Ingripanden (avsnitt 9 i betänkandet)

Enligt Advokatsamfundet är syftet med direktivet och de föreslagna bestämmelserna inte i första hand att reagera på inträffade fel eller brister, utan att det så långt som det är möjligt ska försöka undvikas att de ens uppkommer. Detta uppnås inte effektivt genom olika slags ingripanden i efterhand mot verksamhetsutövarna, när incidenten redan inträffat och skadan redan är för handen. Den försvinner inte heller genom att verksamhetsutövaren åläggs att t.ex. betala en sanktionsavgift.

En tillsynsmyndighet som vill kritisera en verksamhetsutövare bör därför endast göra detta i en situation där myndigheten dessförinnan kommit med råd, anvisningar, uppmaningar eller föreläggande. Myndigheternas tillsyn inom ramen för cybersäkerhetslagen bör, mot bakgrund av lagens syfte, fokusera på att ingripa först när en verksamhetsutövare uppvisat tydliga brister i sitt systematiska och riskbaserade informations- och cybersäkerhetsarbete.

Mot denna bakgrund bör det övervägas att ge tillsynsmyndigheter möjligheter att ingripa mot verksamhetsutövares brister i sitt systematiska och riskbaserade informations- och cybersäkerhetsarbete samt fokusera tillsynen på detta område, genom att detta tydliggörs i 5 kap. 1 § cybersäkerhetslagen.

Vid bedömningen om ett ingripande bör aktualiseras bör även beaktas vad Advokatsamfundet anfört ovan avseende tolkningsproblem och svårigheter för verksamhetsutövarna att förutse hur reglerna kommer att träffa dem.

Övrigt (avsnitt 9 i betänkandet)

Det kan noteras att utredningen inte tydligt genomfört alla befogenheter som tillsynsmyndigheter ska ha enligt direktivtexten. Denna sorts lagstiftningsteknik kan skapa rättsosäkerhet och leda till problem både för verksamhetsutövare och domstol. Ett exempel på detta är att det inte finns en reglering kring direktivets befogenhet att tillsätta en övervakningsansvarig. Utredningen har tolkat direktivet som att den övervakningsansvarige ska finnas hos tillsynsmyndigheterna, medan direktivtexten även kan tolkas som att denne ska finnas hos verksamhetsutövarna.

Utredningen har inte heller klarlagt vilka krav som bör ställas på en övervakningsansvarig, exempelvis om denne ska vara certifierad.

SVERIGES ADVOKATSAMFUND

Mia Edwall Insulander