Säkerhetspolisen

REMISSVAR

Datum: 2024-05-28
Diarienummer: 2024-6501-2
Enhet: Rättsenheten

Mottagare:
Försvarsdepartementet
103 33 STOCKHOLM
Referens: Fö2024/00496

Delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18)

Säkerhetspolisen har, utöver vad som anges nedan, inget att erinra mot utredningens förslag.

5 Cybersäkerhetslagens tillämpningsområde

Som framgår av utredningen följer av artikel 4.2 i fördraget om Europeiska unionen att den nationella säkerheten ska vara varje medlemsstats eget ansvar. Att EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet) inte påverkar medlemsstaternas ansvar för att skydda nationell säkerhet förtydligas genom artikel 2.6 i direktivet. Av artikel 2.7-9 framgår vilka begränsningar i direktivets tillämpningsområde som följer av detta. Utredningen föreslår bland annat mot bakgrund av dessa begränsningar de undantag från den föreslagna lagen om cybersäkerhets tillämpningsområde som följer av 1 kap. 11-13 §§ i lagförslaget.

Det är viktigt att medlemsstaternas ansvar för att skydda nationell säkerhet säkerställs. Från det perspektivet bidrar utredningens förslag till en önskvärd tydlighet. Samtidigt innebär utredningens förslag att verksamhet som omfattas av säkerhetsskyddslagen inte kommer att omfattas av kraven på ett systematiskt och riskbaserat informationssäkerhetsarbete. De riskhanteringsåtgärder som följer av den föreslagna lagen om cybersäkerhet har enbart delvis sin motsvarighet i säkerhetsskyddslagstiftningen. Mot den bakgrunden har Säkerhetspolisen tidigare framfört förslag om att NIS-direktivets krav på riskhanteringsåtgärder skulle kunna utgöra en lämplig bottenplatta även för verksamhetsutövare enligt säkerhetsskyddslagen. Sådan verksamhet skulle samtidigt kunna undantas från krav om incidentrapportering samt från tillsyn och sanktioner. Säkerhetspolisen anser alltjämt att det finns betydande fördelar med en enhetlig reglering av åtgärder för informations- och cybersäkerhet. Hur en sådan reglering kan utformas bör vara föremål för vidare utredningsåtgärder.

5.5.3 Undantag för säkerhetsskyddsklassificerade uppgifter

Det omfattande informationsutbyte mellan verksamhetsutövare, myndigheter och EU-institutioner som följer av NIS2-direktivet innebär att känslig information om bland annat sårbarheter kommer att hanteras av och delas mellan många aktörer. Förslaget att uppgiftsskyldighet enligt lagen om cybersäkerhet inte ska gälla uppgifter som är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagen (2018:585) är ur det perspektivet av särskild betydelse. Även med en sådan begränsning finns det dock anledning att ytterligare analysera huruvida det föreslagna informationsutbytet riskerar att leda till att uppgifter vars röjande kan medföra skada för Sveriges säkerhet kommer obehöriga till del. Utredningen berör exempelvis inte närmare de särskilda svårigheter som är förenade med att bedöma vilka säkerhetsskyddsklassificerade uppgifter som går att härleda ur stora informationsmängder med känslig information och hur skyddsvärd den samlade bild som framgår av överskottsinformation från flera parallella incidenter är. Den föreslagna möjligheten att förelägga en verksamhetsutövare att offentliggöra information om överträdelser av den föreslagna lagen och föreskrifter som har meddelats med stöd av den (se avsnitt 9.5.3) är ytterligare ett exempel på en sådan situation i vilken dessa bedömningar kommer att vara både viktiga och komplicerade. Det bör framgå av förarbetena till bestämmelsen att hänsyn behöver tas till lämpligheten av att uppgifterna offentliggörs. Det kan vidare inte uteslutas att regelverkets komplexitet medför en risk att uppgifter som omfattas av sekretess lämnas till fel mottagare.

8.4.5 Föreskrifter

Säkerhetspolisen avstyrker delvis förslaget om att tillsynsmyndigheterna inom sitt tillsynsområde ska få meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning. Det finns en stor risk att en sådan ordning skulle leda till osäkerhet kring vilka föreskrifter som gäller för en viss verksamhet samtidigt som avgränsningen till säkerhetskänslig verksamhet enligt säkerhetsskyddslagen skulle kompliceras. Säkerhetspolisen förordar mot den bakgrunden som utgångspunkt en lösning med ett samlat regelverk med gemensamma krav som vid behov kompletteras av ytterligare och mer sektorsspecifika föreskrifter från respektive tillsynsmyndighet.

12 Konsekvensanalys

Utredningens förslag riskerar att leda till flera komplicerade gränsdragningar i förhållande till verksamhet som omfattas av säkerhetsskyddslagen och Säkerhetspolisen bedömer mot den bakgrunden att antalet frågor till tillsynsmyndigheterna enligt säkerhetsskyddslagen kommer att öka. Det finns sannolikt behov av såväl vägledning som samordning myndigheterna emellan vilket därutöver kommer att ställa krav på insatser från samordningsmyndigheterna. Det bör mot den bakgrunden övervägas vilka ytterligare resurser som behövs för att svara upp mot dessa behov.

Övrigt pågående lagstiftningsarbete

Säkerhetspolisen noterar att ett antal betänkanden, promemorior och andra förslag som på olika sätt berör cybersäkerhetsområdet är under beredning i skrivande stund. Förslagen är i vissa fall motstridiga vilket innebär att vägval i en viss fråga kommer att påverka även de övriga förslagen. Även i de fall förslagen inte är motstridiga påverkar de varandra och därmed styrningen och regleringen av cybersäkerhetsområdet. Enligt Säkerhetspolisens mening är det viktigt med ett helhetsgrepp och att samordning sker i den fortsatta beredningen av förslagen så att styrningen inom området blir konsekvent och effektiv.

Detta yttrande har beslutats av chefsjuristen Per Lagerud. Verksjuristen Hannes Beckman har varit föredragande.