Sveriges advokatsamfund

Stockholm den 9 november 2026

R-2026/1641

Till Justitiedepartementet
Ju2026/01670

Sveriges advokatsamfund har genom remiss den 9 juli 2026 beretts tillfälle att yttra sig över betänkandet Effektiva ingripanden i cybermiljö (SOU 2026:45).

Sammanfattning

Advokatsamfundet delar utredningens bedömning att de brottsbekämpande myndigheterna behöver bättre möjligheter att ingripa mot allvarlig brottslighet i cybermiljö. Behovet är särskilt tydligt vid angrepp mot Sveriges säkerhet och samhällsviktig verksamhet. Lagförslaget har emellertid ett alltför brett tillämpningsområde och saknar tillräckliga rättssäkerhetsgarantier i förhållande till de föreslagna befogenheterna. Advokatsamfundet avstyrker därför förslaget i dess nuvarande utformning.

De huvudsakliga invändningarna gäller gränsen mot hemlig dataavläsning, formerna för oberoende kontroll och raderingens oåterkalleliga verkningar. Advokatsamfundet ansluter sig i dessa delar till den huvudkritik som framförs i de särskilda yttrandena (s. 427–432).

Synpunkter

Tillämpningsområdet

De föreslagna befogenheterna kan medföra betydande intrång i enskildas informationssystem. Tillämpningsområdet måste därför avgränsas med hänsyn till

vilka ingripanden som behövs för att bekämpa den brottslighet som myndigheterna har beskrivit. Enligt 6 § i den föreslagna lagen om polisiära ingripanden i cybermiljö är det tillräckligt att ett års fängelse ingår i brottets straffskala; varken ett minimistraff eller ett konkret straffvärde på ett år krävs (s. 260). Behovet av att möta statsanknutna cyberangrepp motiverar inte utan vidare motsvarande befogenheter vid betydligt mindre allvarlig brottslighet. Tillämpningsområdet bör därför, utifrån proportionalitetshänsyn, begränsas efter dokumenterade behov, med olika krav beroende på hotets allvar och åtgärdens verkningar.

Förutsättningarna för ingripanden enligt bestämmelserna i 3 och 5 §§ i den föreslagna lagen behöver också preciseras när det gäller informationssystemets koppling till brottsligheten. Till skillnad från 4 § innehåller dessa bestämmelser inget uttryckligt misstanke- eller riskrekvisit. Kraven på särskild respektive synnerlig vikt klargör inte i sig hur starkt underlaget för systemets brottsliga användning måste vara. Advokatsamfundet delar i denna del invändningen i det särskilda yttrandet (s. 430).

Gränsen mot hemlig dataavläsning

Utredningen bedömer att skillnader i syfte och varaktighet undanröjer risken för att de föreslagna befogenheterna används som ersättning för befintliga tvångsmedel (s. 345–347). Advokatsamfundet anser inte att denna avgränsning är tillräcklig. Som framhålls i det särskilda yttrandet kan ingripandena ske utan den enskildes vetskap och innebära integritetsintrång jämförbara med hemlig dataavläsning (s. 427–429). Även ett kortvarigt intrång kan ge tillgång till omfattande historisk kommunikation. Skillnaden i syfte är därför inte tillräcklig för att säkerställa en tydlig gräns i den praktiska tillämpningen.

Granskning och kopiering bör uttryckligen avgränsas till vad som behövs för att utöva de föreslagna befogenheterna. Informationsinhämtning som går därutöver måste ha självständigt lagstöd och prövas enligt tillämpliga tvångsmedelsregler. Ett ingripande för att stoppa skadlig trafik får exempelvis inte samtidigt ge en allmän rätt att söka igenom användarens meddelanden efter annan brottslighet. För att gränsen ska kunna kontrolleras behövs loggning av åtkomst och sökningar samt tydliga regler om vilka uppgifter som får sparas och hur de får användas för andra ändamål än det ursprungliga ingripandet.

Proportionalitet och domstolsprövning

Advokatsamfundet välkomnar den föreslagna proportionalitetsregeln i 7 § och aktsamhetskravet i 18 §. För att bestämmelserna ska få erforderligt genomslag behöver det emellertid redovisas varför mindre ingripande alternativ inte räcker och hur konsekvenserna för utomstående och bevisning ska begränsas. Även vid ingripanden mot främmande makt måste påverkan på enskilda vars system utnyttjas beaktas. För kortvariga ingripanden bör tyngdpunkten ligga på noggrann dokumentation och oberoende efterhandskontroll av både beslutet och genomförandet.

Radering bör däremot som huvudregel föregås av domstolsprövning, eftersom information som väl har förstörts inte kan återställas genom en senare kontroll. Vid konkret fara för allvarlig skada måste ett brådskande beslut kunna fattas utan att domstolens avgörande avvaktas, men beslutet bör då obligatoriskt underställas skyndsam domstolsprövning även om det redan har verkställts. Reglerna i 14–17 §§ lagen om hemlig dataavläsning visar att snabbhet kan förenas med en sådan kontroll. Även hemligt bostadstillträde och andra åtgärder som innebär betydande integritetsintrång bör omfattas av en särskild bedömning av behovet av domstolsprövning.

Efterhandskontrollen bör ge möjlighet att upptäcka felaktigheter och pröva lagligheten av genomförda ingripanden. För blockeringar vars verkningar består under längre tid bör den berörde dessutom kunna få det fortsatta behovet och proportionaliteten prövade. En begäran om prövning bör inte i sig hindra verkställigheten. Detta ligger i linje med experternas invändning att den enskilde saknar en generell möjlighet att invända mot ett ingripande och verka för att en blockering hävs (s. 431). För att möjligheterna till kontroll och prövning ska kunna användas i praktiken, bör efterhandsunderrättelse till identifierbara berörda vara huvudregel, med tydligt reglerade och kontrollerade undantag.

SVERIGES ADVOKATSAMFUND

Mia Edwall Insulander