Stockholms universitet

Rektor

BESLUT

2026-10-29

Dnr SU FV-2446-26

Handläggare:
Rikard Skårfors
FD, Utbildningsledare
Rektors kansli,
Ledningssekretariatet

Yttrande över betänkandet Effektiva ingripanden mot brott i cybermiljö (SOU 2026:45)

Stockholms universitet har anmodats av Regeringskansliet (Justitiedepartementet) att inkomma med synpunkter på betänkandet *Effektiva ingripanden mot brott i cybermiljö* (SOU 2026:45).

Stockholms universitets yttrande över betänkandet utgörs av två bilagda yttranden från Juridiska fakultetsnämnden respektive Kriminologiska institutionen.

Detta beslut är fattat av rektor, professor Hans Adolfsson, i närvaro av prorektor, professor Jane Reichel, och universitetsdirektör Åsa Borin. Studeranderepresentanter har informerats och haft tillfälle att yttra sig. Övrig närvarande har varit Jacob Färnert, Ledningssekretariatet (protokollförare). Ärendet har beretts av Områdesnämnden för humanvetenskap. Föredragande i ärendet har varit utbildningsledare Rikard Skårfors.

Stockholms universitet

Juridiska fakultetskansliet

Områdesnämnden för humanvetenskap

Remissvar – Effektiva ingripanden mot brott i cybermiljö (SOU 2026:45)

Juridiska fakultetsnämnden vid Stockholms universitet avstyrker förslaget i sin nuvarande form och anser mot bakgrund av nedan angivna synpunkter att förslaget bör omarbetas och kompletteras.

Utredningens uppdrag har varit omfattande, bl.a. att kartlägga rättsliga möjligheter, analysera behovet av åtgärder för att förhindra, störa och förhindra brott och brottslig verksamhet i cybermiljöer och lämna nödvändiga författningsförslag.

Uppdraget har motiverats av: att nästan alla brott i dag har en digital komponent, att befintlig lagstiftning rörande hemliga tvångsmedel endast avser fysiska åtgärder och att andra åtgärder behövs för att också kunna ingripa i digital miljö. Detta för att bereda sig tillgång till informationssystem för att ändra, blockera eller radera uppgifter. Syftet är vällovligt och ansatsen speglar en övergång till ett mer proaktivt synsätt för att hantera konkreta problem på ett tidigare stadium. Förslaget väcker dock kritiska frågor.

1. *Systematik och bakgrund:* Problemet bör ses i ett större sammanhang och andra rättsliga och proaktiva insatser bör beaktas. Flera av dessa är initierade, omfattande och även internationella. Utredningen sammanfattar detta arbete översiktligt (s. 119-129) men helhetsbild saknas.

2. *Klarhet.* Förslaget inkluderar all slags befintlig och framtida teknisk utrustning som kan användas för att kommunicera elektroniskt, t.ex. datorer, mobiltelefoner, läsplattor, servrar, smarta klockor, och liknande utrustning, inkluderande sladdar, tangentbord, minnen, datormus och andra elektroniska tillbehör. I utredningens tolkning av informationssystem ingår också uppkopplade fordon, kameror och produkter som kan förekomma i stort sett i alla sammanhang. Konsekvenser är att egentligen vad som helst och nära nog hela befolkningen, tillika företag och organisationer kan komma att bli föremål för ingripanden och i vissa fall hemliga åtgärder.

   Vissa känsliga verksamheter är undantagna med hänvisning till tystnadsplikt, yttrandefrihet och integritetsskydd, men att överblicka konsekvenserna av så generella bestämmelser som nu föreslås är enligt Fakultetsnämndens mening ogörligt. Analysen försvåras av att alla brott som har minst ett år i straffskalan

omfattas samt att framtiden kan innebära att fler sådana brott tillkommer. Anmärkningsvärt är också att lagen inte endast avses försvåra brott. Även det vagt definierade begreppet ”brottslig verksamhet” omfattas.[1] Utredningen anger att detta är ett inarbetat begrepp eftersom det med varierande betydelser förekommer i andra sammanhang, ofta som en samlingsbeteckning för olika brott. Skillnaden är emellertid att begreppet, som i detta sammanhang är opreciserat, kan komma att läggas till grund för att motivera mycket ingripande åtgärder.
Fakultetsnämnden ställer sig i detta även bakom argumenten om oklarheter som framförts i de särskilda expertyttranden som bifogats utredningen.

3. *Konsekvensanalys*. För att hantera osäkerhet om lagens effekter föreslår utredningen att lagen ska vara tidsbegränsad och att den efter fem år ska utvärderas. Fakultetsnämnden ser detta som positivt, och har i olika sammanhang förordat att uppföljning rörande ny lagstiftning, på samma sätt som konsekvensutredningar bör vara obligatorisk. En utvärdering över tid förutsätter emellertid att relevanta kriterier och ingångsvärden finns tillgängliga initialt. De myndigheter som omfattas av lagen har beskrivit och uppskattat behoven, men problemets omfattning redovisas inte på ett kvantifierbart sätt, t.ex. genom statistik om nedlagda undersökningar p.g.a. lagtekniska problem, anmälda eller misstänkta brott av det slag som nu är aktuella. Fakultetsnämnden ifrågasätter inte de behov som redovisas men avsaknad av initiala kontrolldata är en brist som utesluter möjligheterna till verifierbar framtida utvärdering.

4. *Proportionalitet*. Problemets omfattning och möjligheterna till utvärdering ska också relateras till frågan om insatsens proportionalitet. Detta kan även ske på generell nivå. I konsekvensutredningen anges (sid 337) uppskattningsvis att antalet ärenden inte kommer att understiga 500 per år. Kostnaderna för att under fem år bygga upp detta system beräknas till 1 562 900 000 kr. Under antagande att teknik, personal, utbildning m.m. är så pass etablerad att systemet efter fyra år kan tas i full drift har detta under alla förhållanden skett till en betydande kostnad. Berörda myndigheter anger därtill att om lagen därefter permanentas behövs nya genomlysningar av kostnaderna. Huruvida detta är proportionerligt är svårt att bedöma, speciellt mot bakgrund av anteckningen om avsaknad av helhetsbild under punkt 1 ovan.

5. *Beslutsordning*. Fakultetsnämnden menar att beslut om insatser som omfattas av lagförslaget bör fattas av åklagare och/eller domstol. Detta är upparbetade rutiner för handläggning av jämförbara ärenden och motiveras av rättssäkerhet och konsekvens. Att myndigheterna, som förslaget anger, var för sig ska utse

1 Utredningen s. 29 ” Ett annat viktigt ändamål för ingripande är att störa eller avbryta brottslig verksamhet även om det ännu inte går att identifiera konkreta brott.”

speciella befattningshavare för att hantera dessa beslut ökar risken för uppkomsten av rättsosäkerhet i form av oenhetlig och svåråtkomlig praxis. Polismyndigheten har exempelvis angett (s. 378) att ”myndigheten i ett första skede kommer att fokusera på en nationell tillämpning av lagen, för att därefter successivt låta lagen och det arbete som följer med den steg för steg etableras regionalt”.

6. *Lagens benämning*. I utredningen anges som skäl till att i lagens rubrik utesluta tullverket och i stället använda begreppet ”polisiära ingripanden” att det är en fördel om en benämning på en lag är kort. Fakultetsnämnden menar att en lags rubrik företrädesvis ska vara innehållsbeskrivande, vilket inte hindrar att rubriker samtidigt kan vara korta, och föreslår att ett reviderat förslag betitlas med det mer rättvisande *Lag om ingripanden i cybermiljö.*

Remissvaret har på fakultetsnämndens uppdrag beslutats av dekanus, professor Pernilla Leviner. Yttrandet har beretts av professor Peter Wahlgren Föredragande har varit Karolina Alveryd. Yttrandet har expedierats av Juridiska fakultetskansliet.

Pernilla Leviner

Karolina Alveryd

Stockholms universitet

Kriminologiska institutionen,
Samhällsvetenskapliga fakulteten

BESLUT

Tove Pettersson
Kriminologiska institutionen

Protokollförare
Erika Gilbertsson
Administrativ chef

Stockholms universitet

2026-10-02
Dnr SU FV-2446-26

Yttrande över remiss: SOU 2026:45, Effektiva ingripanden mot brott i cybermiljö.

Synpunkter från Kriminologiska institutionens forskare och experter har inkommit till institutionsstyrelsen och redovisas i bifogad bilaga 1, som utgör Kriminologiska institutionens svar.

BESLUT

Kriminologiska institutionens institutionsstyrelse godkänner bifogat remissvar på SOU 2026:45, Effektiva ingripanden mot brott i cybermiljö.

Delges:

Kriminologiska institutionen
Samhällsvetenskapliga fakulteten
Juridiska fakultetskansliet

Stockholms universitet

Kriminologiska institutionens remissvar på SOU 2026:45 Bilaga 1. Effektiva ingripanden mot brott i cybermiljö.

Sammanfattning av yttrandet

Kriminologiska institutionen avstyrker utredningens förslag och vill särskilt framhålla följande:

- Utredningens utgångspunkt är att ingripandena ska vara systemcentrerade (riktade mot informationssystem) men underlaget för att identifiera ett ingripande är potentiellt personbundet.
- Begreppen informationssystem och brottslig verksamhet behöver avgränsas tydligare. Det gäller särskilt eftersom lagen ska kunna tillämpas redan på underrättelsestadiet, vilket ökar risken för felaktiga ingripanden och för att exempelvis, laglig politisk aktivitet drabbas.
- Gränsen mellan informationssystem som verktyg och kanal är svår att upprätthålla och medför en risk för att laglig kommunikation och aktivitet drabbas
- Utredningen visar inte att bristen på rättslig befogenhet är det huvudsakliga hindret för effektiva ingripanden i cybermiljö. Tekniska hinder, som att identifiera, lokalisera och nå den relevanta infrastrukturen, kan vara lika viktiga och riskerar att göra verktygen verkningslösa.
- Det är oklart om de föreslagna ingripandena leder till minskad brottslighet eller om brottsligheten i stället flyttas eller tar en annan form.
- De mest ingripande och oåterkalleliga åtgärderna, såsom radering och tillträde till platser som är skyddade mot intrång, bör prövas av åklagare eller domstol och inte beslutas inom den myndighet som själv ska verkställa ingripandet.
- Den enskilde bör kunna få kännedom om ett felaktigt ingripande.
- Valet av myndigheter samt konsekvenserna för privata leverantörer och för informationssystem utomlands behöver motiveras och belysas tydligare.
- Det finns en risk att en tidsbegränsad befogenhet med tiden normaliseras och permanentas, samt en risk för ändamålsglidning.

Utredningens direktiv

Utgångspunkten för utredningen är att den ökade digitaliseringen och den tekniska utvecklingen har skapat nya möjligheter för kriminella aktörer och att brottsbekämpande myndigheter idag saknar tillräckliga möjligheter att aktivt ingripa mot vissa former av brottslighet i cybermiljö. Utredningens övergripande uppdrag har varit att ”analysera behovet och nyttan av samt föreslå en möjlighet att störa och avbryta pågående brott eller brottslig verksamhet i cybermiljö, eller vidta andra jämförbara åtgärder i sådan miljö, i syfte att förbättra de brottsbekämpande myndigheternas samlade förmåga att ingripa mot sådan brottslighet, och lämna nödvändiga författningsförslag och vid behov förslag på andra åtgärder” (dir. 2025: 12).

Utredningen har inom ramen för detta uppdrag bland annat behandlat frågor om ingripanden mot informationssystem, tillträde till platser skyddade mot intrång, vilka myndigheter som bör omfattas, beslutsordningen samt konsekvenserna för den personliga integriteten och andra grundläggande fri- och rättigheter.

Utredningens förslag

Utredningen föreslår en ny lag om polisiära ingripanden i cybermiljö. Regleringen ska ge Polismyndigheten, Säkerhetspolisen och Tullverket möjlighet att aktivt ingripa mot informationssystem som används vid brott eller brottslig verksamhet. De föreslagna befogenheterna omfattar bland annat möjligheten att bereda sig tillgång till informationssystem, kringgå systemskydd och utnyttja tekniska sårbarheter. Myndigheterna ska under vissa förutsättningar kunna ändra eller blockera uppgifter och i särskilda fall även radera dem. Vidare föreslås en möjlighet att tillfälligt bereda sig tillgång till trafikdata i syfte att kartlägga hur informationssystem kommunicerar med andra informationssystem. En sådan kartläggning kan bland annat användas för att identifiera hur ett angrepp är uppbyggt eller vilken annan digital infrastruktur ett informationssystem kommunicerar med. För att genomföra ett ingripande föreslås myndigheterna även kunna bereda sig tillträde till en plats som är skyddad mot intrång i syfte att installera tekniska hjälpmedel som behövs för åtgärden. Regleringen föreslås inte bygga på en uttömmande uppräkning av särskilda brott. I stället föreslås mer generella kriterier för när befogenheterna får användas. Regleringen ska dessutom kunna tillämpas inte endast när ett konkret brott har identifierats utan även i förhållande till brottslig verksamhet.

Kriminologiska institutionens bedömning

Den tekniska utvecklingen har förändrat vissa former av brottslighet samt förutsättningar för brottsbekämpning. Att nya befogenheter kan underlätta polisens eller andra myndigheters arbete innebär dock inte i sig att de kommer att minska brottsligheten. Utredningen visar tydligt vilka nya rättsliga och tekniska möjligheter myndigheterna efterfrågar, men det är oklart vilka av dessa ingripanden som förväntas leda till färre brott eller minskad utsatthet för brott. Enligt utredningen kan ett framgångsrikt tekniskt ingripande innebära att en server görs otillgänglig, att information blockeras eller raderas eller att en digital tjänst tillfälligt slutar fungera. Detta innebär inte nödvändigtvis att den bakomliggande brottsligheten upphör. Gärningspersoner kan byta plattform, skapa ny infrastruktur, förändra sina kommunikationsvägar eller flytta verksamheten till en annan jurisdiktion. Det är därför centralt att skilja mellan möjligheten att tekniskt ingripa mot en viss digital infrastruktur och den faktiska eller potentiella effekten av ingripandet. Utredningen gör själv gällande att lagen kommer att få en avhållande effekt och att vissa brottsfenomen förväntas minska avsevärt.

Begreppen informationssystem, brottslighet och brottslig verksamhet

Begreppet informationssystem är centralt för den föreslagna regleringen eftersom det är sådana system som myndigheterna ska kunna bereda sig tillgång till och påverka genom exempelvis kartläggning, blockering, ändring, eller radering av uppgifter. Utredningen väljer samtidigt att inte ge begreppet en närmare legal definition. Detta motiveras av behovet av teknisk flexibilitet och av att en snäv definition riskerar att snabbt bli föråldrad. Institutionen anser dock att detta väcker frågor om regleringens förutsägbarhet och avgränsning. Ett informationssystem kan i praktiken avse många olika typer av digitala miljöer, exempelvis större digitala plattformar. Detta är särskilt problematiskt i blandade miljöer där brottslig och legitim användning förekommer parallellt. Ju bredare begreppet informationssystem förstås, desto viktigare blir det att tydligt ange hur ett ingripande ska avgränsas till den del av systemet som faktiskt är relevant för den misstänkta brottsligheten.

På sida 204 (SOU 2026) konstaterar utredningen att vad som avses med begreppet brott inte behöver diskuteras närmare. Däremot framhålls att innebörden av begreppen brottslighet och brottslig verksamhet inte är lika självklar. Detta är enligt institutionens mening en central fråga för regleringens avgränsning. Utredningen beskriver brottslig verksamhet som en inte närmare preciserad verksamhet som innefattar flera kriminaliserade handlingar. De enskilda handlingarna behöver inte tillsammans eller var för sig uppfylla rekvisiten för ett visst konkret brott, utan kan utgöra tecken på en identifierbar form av brottslighet. Regleringen är därmed avsedd att kunna användas redan på underrättelsestadiet, när det ännu inte har kunnat fastställas vilket konkret brott som har begåtts eller kommer att begås. Detta aktualiserar en välkänd och återkommande problematik vid användning av ingripande statliga åtgärder i tidiga skeden, nämligen att osäkerheten kring huruvida den aktuella verksamheten faktiskt är brottslig är som störst i just dessa skeden. Ju tidigare i en möjlig brottsprocess staten ges möjlighet att ingripa desto större är osäkerheten kring vilka aktiviteter som faktiskt är kopplade till brott och vilka som senare visar sig vara legitima. Risken för falska positiva bedömningar ökar därmed, det vill säga att legitima aktiviteter felaktigt bedöms som brottsrelaterade.

Denna problematik är särskilt relevant i digitala miljöer där legitim och brottslig aktivitet kan förekomma parallellt. Kommunikationsplattformar, forum och andra digitala communities kan innehålla ett stort antal personer där endast en mindre del har anknytning till den brottsliga verksamhet som myndigheten söker kartlägga. Digital kommunikation är dessutom ofta kontextberoende. Diskussioner om exempelvis brott, politiska system, våld eller andra kontroversiella frågor kan innefatta ironi, mörk humor, hypotetiska resonemang eller andra uttryck som inte innebär någon faktisk brottslig intention. Det är därför inte tillräckligt att konstatera att ett ingripande måste vila på objektivt verifierbara omständigheter. Utredningen analyserar inte vilken risk för felaktiga bedömningar den föreslagna regleringen innebär och vilka konsekvenser ingripanden kan få för personer och digitala miljöer som senare visar sig sakna koppling till den brottslighet som initialt antogs föreligga. Det finns även en mer generell risk för att en bred definition av brottslig verksamhet över tid leder till ett utvidgat användningsområde. När nästan all brottslighet i någon utsträckning kan ha en digital komponent, såsom det tillskrivs i utredningen, blir avgränsningen av vilka situationer som faktiskt bör omfattas av de nya befogenheterna särskilt viktig.

Utredningen anger att gränsen för lagens tillämpningsområde går vid frågan om ett informationssystem används som medel för brottet eller enbart fungerar som en kommunikationskanal mellan inblandade aktörer. Denna distinktion är enligt institutionens mening svårare att upprätthålla vid brottslig verksamhet än vid ett konkret brott. Vid ett konkret brott kan gärningen analyseras för att avgöra om informationssystemet utgjort ett medel. Vid brottslig verksamhet saknas per definition ett sådant fastställt brott att pröva informationssystemets funktion mot. Bedömningen av om ett utbyte av information ska anses utgöra medel eller ren kommunikation riskerar därmed att göras utifrån något som inte är fastställt, vilket ökar snarare än minskar osäkerheten.

Den öppna definitionen av såväl informationssystem som brottslig verksamhet ger de brottsbekämpande myndigheterna ett stort handlingsutrymme att själva avgöra vad som faller innanför tillämpningsområdet. Då verkligheten sällan låter sig fogas in i fasta kategorier kan en viss öppenhet vara befogad, men denna flexibilitet kan samtidigt flytta en del av gränsdragningen för befogenheten från lagstiftaren till den tillämpande myndigheten. Det uppstår då en risk att myndigheten i sin praktik efter hand vidgar tillämpningen bortom lagstiftarens intentioner och att en sådan expanderad praktik i efterhand legaliseras (så kallad ex-post legalisering) snarare än att prövas mot lagstiftarens ursprungliga avsikt.

Utredningen framhåller att den nya lagen, till skillnad från exempelvis tvångsmedel, ”förutsätter inte att det finns någon identifierad gärningsman utan endast ett identifierat informationssystem”. Ingripandet är alltså i utredningens framställning systemcentrerat snarare än personcentrerat. En risk finns här i själva utgångspunkten för ett ingripande. Enligt förslaget krävs det ”någon faktisk omständighet” för att ett ingripande ska riktas mot ett visst informationssystem. Kravet bör enligt utredningen ”vara lågt ställt” – det räcker med att det kan antas att informationssystemet utnyttjas i brott eller brottslig verksamhet (SOU 2026, s.250). Samtidigt beskriver utredningen ett antal typsituationer där en sådan omständighet uppkommer: brottsanmälan från målsägande, tips från allmänheten, uppgifter som framkommer vid husrannsakan, information som inhämtats genom hemligt tvångsmedel

eller information från utländsk brottsbekämpande myndighet. Gemensamt för flera av dessa exempel är att de när de specificeras potentiellt blir knutna till person(er) snarare än till informationssystemet som sådant. Även om tillämpningsvillkor är knutna till informationssystemet tycks det praktiska underlaget för att kunna identifiera vilket system och vilken del av ett system som ska bli föremål för ett ingripande bygga på information om person snarare än om ett specifikt informationssystem. En återkommande fråga blir därmed: i vilken utsträckning skiljer sig den systemcentrerade logiken sig från personbunden brottsbekämpning och prevention och hur riskerar denna otydlighet att underminera rättssäkerhet som annars är kopplad till en viss misstankegrad?

Institutionen vill betona att regleringens skyddsmekanismer, såsom straffvärdesgränsen, kravet på att informationssystemet ska utgöra medel och inte enbart kanal, proportionalitetskravet och skyddet för fri åsiktsbildning, måste vara tillräckligt starka för att lagstiftningen inte ska riskera att kränka, inskränka eller på annat sätt påverka yttrande- eller tryckfriheten negativt. Eftersom flera av dessa skyddsmekanismer definieras i förhållande till brottets allvar, kan förändringar i angränsande straffrättslig reglering indirekt påverka den föreslagna regleringens faktiska räckvidd, utan att detta kräver någon ändring av lagen som sådan. Flera delar av förslaget innebär en påtaglig risk för normalisering, permanentering och därmed ändamålsglidning i praktisk tillämpning. Det är mot denna bakgrund särskilt viktigt att tydligt hålla isär brottslig verksamhet och laglig politisk aktivitet, såsom demonstrationer och annat politiskt engagemang, eftersom en reglering som inte gör det riskerar att drabba den fria åsiktsbildningen som sådan. Ett exempel är förslaget om nya möjligheter för Säkerhetspolisen att registrera stora mängder personuppgifter i särskilda uppgiftssamlingar (SOU 2025, s.49). Tillsammans med befogenheterna i denna utredning kan sådana förändringar öka risken för att lagliga politiska miljöer träffas av kartläggning och ingripanden. Institutionen vill därför uppmärksamma att två till synes orelaterade lagstiftningsprocesser kan få sammanlagda effekter som inte fångas upp av separata analyser och granskningar av utredningarna.

Från dataintrång till polisiär praktik

En viktig aspekt av förslaget är att brottsbekämpande myndigheter ges rätt att utföra handlingar som tekniskt motsvarar flera av de handlingar som annars kan omfattas av straffbestämmelsen om dataintrång (4 kap. 9 c § brottsbalken). Myndigheterna ska kunna bereda sig tillgång till informationssystem, kringgå säkerhetsmekanismer samt ändra, blockera och i vissa fall radera information. Genom den föreslagna lagen ges dessa handlingar rättsligt stöd och utförs därmed inte olovligen. Utredningen behandlar dock inte hur detta rättsliga stöd förhåller sig till att informationssystem ofta drivs av privata aktörer med egna användarvillkor, i vissa fall utomlands. Lagen begränsas till situationer med anknytning till Sverige (SOU 2026, ss.222–226), men anknytningsfaktorerna är alternativa och kan omfatta system som finns utomlands, exempelvis när brottet riktas mot någon eller något i Sverige. I utredningen konstateras att det kan utgöra en överträdelse av en annan statssuveränitet att ändra och störa data (SOU 2026, s.227), men bedömer att förslaget ändå är förenligt med folkrätten, utan krav på samtycke från den stat där systemet finns (SOU 2026, s.229). Därför behöver konsekvenserna för leverantörer och användare av sådana system belysas tydligare. Detta är inte i sig ett argument

mot att sådana befogenheter införs. Det innebär emellertid en principiellt viktig förändring. Staten ges rätt att aktivt ingripa i samma intressen, informationens konfidentialitet, integritet och tillgänglighet, som straffbestämmelsen om dataintrång annars syftar till att skydda. Utredningen konstaterar dessutom själv att den typ av ingripanden som kan bli aktuell oundvikligen kommer att påverka enskildas integritet. Den framhåller vidare att myndigheters tillgång till informationssystem i vissa fall kan innebära intrång som för den enskilde har likheter med det intrång som användning av hemliga tvångsmedel medför.

När staten ges rätt att bereda sig tillgång till, ändra, blockera eller radera uppgifter bör det därför ställas särskilt höga krav på tydliga rekvisit, proportionalitet och oberoende kontroll. Det gäller särskilt åtgärder av oåterkallelig karaktär. Radering är det tydligaste exemplet. I brådskande situationer kan ett beslut om radering ha verkställts innan åklagarens efterhandsprövning. Om åklagaren därefter kommer fram till att det saknades tillräckliga förutsättningar för åtgärden kan den ursprungliga situationen inte nödvändigtvis återställas. Att en kopia av uppgifterna i vissa situationer kan bevaras innebär inte nödvändigtvis att den ursprungliga digitala miljön, sammanhanget eller funktionaliteten kan återställas. Enligt förslaget ska sådana kopior dessutom förstöras senast sex månader efter åklagarens prövning. Detta aktualiserar frågan om vilket skydd som finns för den enskilde när en åtgärd har fått oåterkalleliga konsekvenser och det i efterhand konstateras att tillräckliga skäl för ingripandet saknades. Vid jämförbara ingrepp i Danmark, såsom dataavläsning (*dataaflæsning*), ska den som har rådighet över informationssystemet underrättas när ingreppet har avslutats, och det är domstolen som avgör om underrättelsen får underlåtas eller skjutas upp (retsplejeloven §§791 b och 788). Enligt utredningens förslag ansvarar i stället den myndigheten som har beslutat om ingripande både för underrättelsen och för tillämpningen av undantagen samtidigt som det framstår tydligt att den enskilde som märker en åtgärd inte får veta vem som ligger bakom den, och att en underrättelse är det som gör det möjligt att begära skadestånd (SOU 2026, ss.321–322). Detta väcker följande fråga: på vilket sätt ska den enskilde få kännedom om ett felaktigt ingripande i praktiken, inte minst eftersom kopior av raderade uppgifter förstörs efter sex månader?

Beslutsordningen mellan myndighet och åklagare

Utredningen framhåller att en effektiv förmåga att ingripa i cybermiljö kan kräva beslut som fattas på sekunder eller minuter. Polismyndigheten betonar att en effektiv förmåga att ingripa i cybermiljö kräver sekunder eller minuter för att fatta beslut (SOU 2026, s.179), och utredningen utgår från att mycket snabba beslut kan behövas och att beslut därför bör fattas av de brottsbekämpande myndigheterna själva (SOU 2026, ss.279–282). Detta behov är dock myndigheternas egen bedömning och utredningen redovisar inte hur ofta sådan snabbhet faktiskt har varit avgörande i praktiken. Erfarenheter från tidigare tvångsmedel signalerar försiktighet. Forskningen har visat att myndigheters påståenden om behov ofta är svagt underbyggda och att hemliga tvångsmedel som förts som betydelsefulla i en majoritet av fallen inte haft avgörande betydelse för utredningen (Flyghed 2007, ss.62–63). Det bör därför tydligare analyseras i vilka situationer detta faktiskt gäller och om behovet av snabbhet motiverar den föreslagna beslutsordningen för samtliga berörda åtgärder. Flera centrala beslut föreslås kunna fattas av särskilt utsedda befattningshavare inom Polismyndigheten,

Säkerhetspolisen eller Tullverket. Detta kan även omfatta beslut som möjliggör tillträde till platser som är skyddade mot intrång för installation av teknisk utrustning.

Mot denna bakgrund behöver utredningen tydligare motivera varför de mest ingripande åtgärderna inte ska omfattas av en starkare oberoende förhandskontroll. Det behöver också framgå i vilken omfattning krav på åklagar- eller domstolsprövning faktiskt skulle förhindra effektiva ingripanden. Att vissa situationer kräver sekund- eller minutoperativa beslut innebär inte nödvändigtvis att samma beslutsmodell behöver tillämpas vid alla former av ingripanden. Ett alternativ skulle kunna vara en differentierad beslutsordning där mindre ingripande och lätt återställbara åtgärder kan beslutas inom myndigheten, medan åtgärder som innebär större integritetsintrång, fysisk tillgång till skyddade platser eller risk för irreversibel påverkan underställs åklagarprövning eller, vid de mest ingripande åtgärderna, domstolsprövning.

Myndighetskretsen och organiserad ekonomisk brottslighet

Den nya regleringen föreslås kunna användas av Polismyndigheten, Säkerhetspolisen och Tullverket. Samtidigt används ekonomisk brottslighet som ett exempel när utredningen beskriver innebörden av brottslig verksamhet. Det väcker frågor om vad som anses vara organiserad brottslighet och hur kretsen av myndigheter har avgränsats. Skatteverket behandlas i utredningen men bedöms ha mer begränsade brottsbekämpande befogenheter än de myndigheter som föreslås omfattas av regleringen.

Ekonomisk och organiserad brottslighet kan i dag involvera omfattande digital infrastruktur, digitala identiteter, betalningslösningar och kommunikationssystem. Om regleringen är avsedd att vara generell och om ekonomisk brottslighet uttryckligen omfattas av resonemanget kring brottslig verksamhet bör valet av vilka myndigheter som omfattas av lagen motiveras mer utförligt. Det är exempelvis oklart om begreppet brottslig verksamhet i praktiken främst tar sikte på mer traditionellt polisiärt orienterad organiserad brottslighet, såsom narkotikahandel, eller om även ekonomisk brottslighet såsom penningtvätt, systematiska skattebrott och andra upplägg inom organiserad ekonomisk brottslighet avses omfattas på motsvarande sätt. Om det senare är fallet aktualiseras frågan om varför myndigheter med särskild kompetens och ansvar, såsom Skatteverket och Ekobrottsmyndigheten, exempelvis, inte omfattas av den föreslagna regleringen. Därmed inte sagt att ytterligare myndigheter nödvändigtvis bör ges samma befogenheter. Frågan är snarare vilken brottsproblematik regleringen faktiskt är avsedd att lösa och varför just de föreslagna myndigheterna bedöms ha behov av en så omfattande befogenhet.

Hur ska ingripandena aktualiseras i praktiken?

Utredningen beskriver relativt utförligt vilka befogenheter myndigheterna ska ha när ett relevant informationssystem väl har identifierats. Det framgår däremot mindre tydligt hur myndigheterna i praktiken ska gå från en första underrättelse, misstanke eller annan indikation på brottslighet till att identifiera den person, det konto eller det informationssystem som ska bli föremål för ingripande. Denna fråga är central för bedömningen av regleringens praktiska och preventiva betydelse. Om misstänkt brottslighet först måste identifieras genom befintlig underrättelseverksamhet, tips, tidigare utredningar eller annan informationsinhämtning bör det

tydligare framgå vilken del av den operativa processen den nya regleringen faktiskt förändrar. Problemet blir särskilt tydligt när personer använder VPN-tjänster, anonymiseringsnätverk som Tor, alias, krypterade kommunikationstjänster eller informationssystem placerade utanför Sverige. I sådana situationer är det inte endast den rättsliga befogenheten som är avgörande, utan även möjligheten att identifiera, attribuera, lokalisera och tekniskt nå den relevanta infrastrukturen.

Institutionen anser därför att det krävs en tydligare beskrivning av den operativa kedjan från upptäckt av misstänkt aktivitet till identifiering av ett relevant informationssystem och därefter till själva ingripandet. Utan en sådan analys är det svårt att bedöma vilken praktisk betydelse de föreslagna befogenheterna faktiskt kommer att få och i vilken utsträckning de stärker den preventiva förmågan snarare än endast möjligheten att ingripa när ett relevant system redan har identifierats.

Rättslig befogenhet eller tekniskt hinder?

Utredningen behandlar bristen på rättslig befogenhet som ett centralt hinder för aktiva ingripanden i cybermiljö. För vissa typer av informationssystem kan denna bedömning vara korrekt. Om en myndighet redan har identifierat relevant digital infrastruktur och har faktisk teknisk möjlighet att ingripa mot den, men saknar rättsligt stöd för att genomföra åtgärden, kan den föreslagna regleringen undanröja ett konkret hinder. Det är däremot inte visat att detta är det huvudsakliga hindret i alla de situationer som används för att motivera lagstiftningen. För exempelvis Darknet-marknadsplatser kan det huvudsakliga hindret i praktiken vara att identifiera och lokalisera den bakomliggande infrastrukturen, avgöra var denna befinner sig och få faktisk teknisk tillgång till den.

Anonymiseringsteknik innebär inte att den fysiska infrastrukturen upphör att existera, men kan göra det mycket svårt att identifiera var den finns. Informationssystem kan dessutom vara distribuerade mellan flera servrar, länder och jurisdiktioner. Information kan vara kopierad eller säkerhetskopierad på flera platser och tjänster kan snabbt återuppstå efter ett ingripande. En ny rättslig befogenhet undanröjer inte dessa tekniska och praktiska hinder. Utredningen borde därför tydligare ha redovisat i vilken andel och i vilken typ av ärenden den rättsliga begränsningen, snarare än bristande teknisk åtkomst, lokalisering, attribution eller internationell behörighet, faktiskt utgör det huvudsakliga hindret för ingripande. Utan en sådan analys är det svårt att bedöma hur stor praktisk betydelse den föreslagna regleringen kommer att få.

Förslagens brottspreventiva effekter

En central fråga är vilken effekt de föreslagna ingripandena faktiskt kommer att få på brottsligheten. Utredningen fokuserar i stor utsträckning på myndigheternas förmåga att genomföra ett ingripande. Ett sådant ingripande kan emellertid vara tekniskt framgångsrikt utan att den underliggande brottsligheten minskar. En marknadsplats kan stängas ned, ett informationssystem blockeras eller en server göras otillgänglig samtidigt som användarna flyttar till en annan tjänst eller skapar ny infrastruktur.

Kriminologisk forskning har länge uppmärksammat att brottsförebyggande och brottsbekämpande åtgärder i vissa fall kan leda till förskjutning eller anpassning snarare än att den bakomliggande verksamheten helt upphör. Detta är särskilt relevant i digitala miljöer, där studier av nedstängningar av Darknet-marknadsplatser visar att vissa användare snabbt flyttar sin aktivitet till andra existerande marknadsplatser och att handelsaktiviteten kan återhämta sig relativt snabbt (ElBahrawy et al., 2020). Ett ingripande mot en viss digital infrastruktur behöver därför inte nödvändigtvis innebära att den bakomliggande verksamhet upphör, utan kan i vissa fall leda till att den förskjuts eller omorganiseras. Mot denna bakgrund bör utredningen tydligare beskriva den kausala kedja genom vilken respektive ingripande förväntas minska brottsligheten: från ingripande mot ett informationssystem, till minskade möjligheter att genomföra brott, begränsade möjligheter till anpassning eller förflyttning av verksamheten och slutligen minskad brottslighet och utsatthet. Här är det också viktigt att skilja mellan olika former av brottslighet.

Vid cyberberoende brottslighet kan den digitala infrastrukturen utgöra en nödvändig del av själva brottet, vilket innebär att ett ingripande direkt kan påverka gärningspersonens möjligheter att genomföra det. Vid annan brottslighet kan digitala plattformar främst fungera som kommunikations-, rekryterings-, eller försäljningskanaler, vilket innebär att ett ingripande mot plattformen inte nödvändigtvis påverkar den underliggande verksamheten i samma utsträckning. Effekten bör därför inte primärt bedömas utifrån hur många servrar, konton, marknadsplatser eller informationssystem som myndigheterna har lyckats påverka. Det centrala bör i stället vara om utsattheten för brott faktiskt minskar, hur varaktig effekten är och i vilken utsträckning brottsligheten anpassas, flyttas eller tar annan form.

Tidsbegränsning och risken för normalisering

Utredningen föreslår att lagen tidsbegränsas till fem år och att en särskild utvärdering ska ligga till grund för ett framtida ställningstagande om permanent lagstiftning. Institutionen vill dock uppmärksamma att jämförbar tidsbegränsad lagstiftning historiskt sett ofta har permanentats genom upprepade förlängningar snarare än genom en självständig prövning av behovet, ett mönster inom tvångsmedel (Flyghed, 2002). Ett närliggande exempel är hur terroristlagstiftningen successivt fått ett alltmer omfattande tillämpningsområde . Risken är således att en inledningsvis avgränsad och tidsbegränsad befogenhet successivt normaliseras och institutionaliseras, utan att det motsvaras av en granskning som hade krävts vid införandet av permanent reglering. Institutionen vill i sammanhanget peka på risken för ändamålsglidning – att en befogenhet som införs för ett visst, avgränsat syfte över tid kommer att tillämpas på situationer som ligger vid sidan av eller bortom detta ursprungliga syfte.

Kriminologiska institutionens slutsats

Den tekniska utvecklingen har förändrat brottsbekämpningens förutsättningar, men utredningens motivering präglas av otydligheter kring regleringens praktiska tillämpning, avgränsningen av centrala begrepp, de faktiska hinder som lagen är avsedd att undanröja och de brottspreventiva effekterna. Utredningen visar inte att bristen på rättslig befogenhet är det huvudsakliga hindret, och inte hur ingripandena ska leda till varaktigt minskad brottslighet snarare än till exempel förskjutning. Utredningen bör därför tydligare redovisa hur ofta den rättsliga begränsningen är det avgörande hindret, hur ofta tekniska och internationella hinder i stället är avgörande, vilken risk som finns för att legitima användare påverkas och hur ofta ett framgångsrikt ingripande leder till en minskning av brottsligheten. Eftersom förslaget är en generell reglering och inte begränsat till ett mindre antal särskilt allvarliga brott eller särskilda typer av digital infrastruktur, bör större krav ställas på empiriskt stöd för dess behov, effektivitet och konsekvenser. Den öppna definitionen av brottslig verksamhet, möjligheten att ingripa redan på underrättelsestadiet och beslutsordningen inom de verkställande myndigheterna ökar risken för felaktiga ingripanden och för att laglig politisk aktivitet drabbas. De mest ingripande och oåterkalleliga åtgärderna bör därför prövas av åklagare eller domstol, och den enskilde bör kunna få kännedom om ett felaktigt ingripande. Därutöver behöver avgränsningen av begreppet informationssystem, valet av myndigheter samt konsekvenserna för privata leverantörer och system utomlands belysas tydligare.

Stockholms universitet

Beredning och beslut

Remissvaret på SOU 2026:45, Effektiva ingripanden mot brott i cybermiljö, har beretts av doktorand Evagelia Milona och docent Katarina Winter och beslutades den 2 oktober 2026 per capsulam av Kriminologiska institutionens styrelse under ledning av ordförande, professor Tove Pettersson.

Protokollförare var Erika Gilbertsson, administrativ chef.

Yttrandet har expedierats av Kriminologiska institutionen.

Referenser

Dir. 2025:12. Hemliga och preventiva tvångsmedel – en effektiv och tydlig reglering.

ElBahrawy, A., Alessandretti, L., Rusnac, L., Goldsmith, D., Teytelboym, A., & Baronchelli, A. (2020). Collective dynamics of dark web marketplaces. *Scientific Reports*, *10*(1), 18827. https://doi.org/10.1038/s41598-020-74416-y

Flyghed, J. (2007). Kriminalitetskontroll: baserad på tro eller vetande? Svensk Juristtidning, 92(1), 59–68. https://svjt.se/svjt/2007/59

Flyghed, J. (2002). Normalising the exceptional: The case of political violence. Policing and Society, 13(1), 23–41. https://doi.org/10.1080/1043946022000005608

SOU 2025:49. Säkerhetspolisens behandling av personuppgifter.

SOU 2026:45. Effektiva ingripanden mot brott i cybermiljö.