Datum 2026-11-06

Informationsklass Öppen

Diarienr (åberopas) A438.617/2026 Saknr 000

Polismyndigheten

Justitiedepartementet

ju.remissvar@regeringskansliet.se
ju.L4@regeringskansliet.se

Er referens Ju2026/01670

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

Sammanfattning

Polismyndigheten är i huvudsak mycket positiv till utredningens förslag och bedömningar.

Den ökade digitaliseringen samt utvecklingen av ny teknik har förändrat brottsligheten och de flesta brott har i dag en digital beståndsdel. De befogenheter som Polismyndigheten förfogar över avser dock framför allt den fysiska miljön och myndigheten saknar de författningsstöd som krävs för att på ett effektivt sätt utföra sina uppgifter i den digitala miljön. För att kunna fullgöra sitt samhällsuppdrag samt upprätthålla förtroendet som brottsbekämpande myndighet är det därmed både brådskande och nödvändigt att Polismyndigheten ges förmåga att förhindra, störa eller avbryta brott och brottslig verksamhet även i cybermiljö.

Cybermiljön utmärks av att gärningspersoner, brottsoffer och informationssystem ofta befinner sig på olika geografiska platser vilket försvårar möjligheterna för brottsbekämpande myndigheter att vidta åtgärder. Användningen av molntjänster, proxyservrar och anonymiseringsverktyg gör det därutöver utmanande för myndigheterna att klarlägga omständigheterna i ett visst fall, vilka dessutom snabbt kan förändras. För att den föreslagna lagen om polisiära ingripanden i cybermiljö ska kunna användas i praktiken är det därför avgörande att dess tillämpningsområde inte begränsas ytterligare i det fortsatta lagstiftningsarbetet. Risken är annars att omständigheterna i den snabbt föränderliga cybermiljön medför att lagen sällan, eller endast i undantagsfall, kan tillämpas och att de förväntade positiva effekterna därmed uteblir.

Polismyndigheten lämnar följande synpunkter.

Postadress Polismyndigheten 106 75 Stockholm
Besöksadress Polhemsgatan 30 Stockholm
Telefon 114 14
Webbplats polisen.se
E-post registrator.kansli@polisen.se

Polismyndighetens synpunkter

Det behövs ny lagstiftning (avsnitt 12.5)

Polisens arbete syftar till att upprätthålla allmän ordning och säkerhet samt att tillförsäkra allmänheten skydd och annan hjälp. För Polismyndighetens del innebär det bl.a. att utreda begångna brott samt förebygga, förhindra och upptäcka brottslig verksamhet och andra störningar av den allmänna ordningen eller säkerheten samt ingripa när störningar har inträffat. Uppdraget omfattar hela samhället och därmed såväl den fysiska som den digitala miljön. De befogenheter som Polismyndigheten tilldelats för att utföra detta uppdrag avser dock framför allt den fysiska miljön vilket innebär att myndigheten i dag saknar de författningsstöd som krävs för att på ett effektivt sätt utföra sina uppgifter i cybermiljö.

Som utredningen beskriver (se avsnitt 9.2) uppger Europol i sin rapport IOCTA 2026[1] att cyberbrottsligheten utvecklas mycket snabbt och att avståndet till de brottsbekämpande myndigheternas förmåga att utföra sitt uppdrag ökar. Europol framhåller att teknikutvecklingen inom AI gör det möjligt för kriminella att skala upp och industrialisera brottsligheten samtidigt som anonymiseringsverktyg och andra krypteringstjänster försvårar brottsbekämpande myndigheters utredningsverksamhet och deras möjligheter att vidta effektiva förebyggande åtgärder.

Med hänsyn till samhällsutvecklingen är det brådskande att Polismyndigheten ges förmåga att utföra sitt uppdrag effektivt även i cybermiljön. Om utredningens förslag genomförs innebär det enligt Polismyndighetens uppfattning inte så mycket en utvidgning av myndighetens befogenheter som en anpassning av dessa utifrån förutsättningarna i det moderna samhället. Med den föreslagna lagen om polisiära ingripanden i cybermiljö skulle myndigheten t.ex. kunna ingripa och avbryta brott så som omfattande narkotikaförsäljning över internet, onlinerekrytering av barn och unga till grov organiserad brottslighet eller förmedling av fotografier eller filmer som visar sexuella övergrepp. Om dessa brott hade begåtts i den fysiska miljön hade allmänheten betraktat det som en självklarhet att Polismyndigheten skyndsamt skulle ingripa och avbryta brotten.

Polismyndigheten delar uppfattningen att ingripanden i cybermiljö i många fall kommer att innebära integritetsintrång för enskilda men vill påpeka att

[1] Se Europol, The evolving threat landscape. How encryption, proxies and AI are expanding cybercrime – Internet Organised Crime Threat Assessment (IOCTA) 2026, Publications Office of the European Union, Luxembourg, 2026.

även polisingripanden i den fysiska miljön ofta utgör betydande ingrepp i fri- och rättigheter. De avvägningar som integritetskänsliga ingripanden föranleder har Polismyndigheten därmed etablerade rutiner för och stor vana att hantera. Det bör understrykas att förslagen i betänkandet också innebär betydande positiva effekter för enskildas personliga integritet. Den som har blivit utsatt för ett inspelat sexuellt övergrepp eller fått sina personuppgifter stulna behöver t.ex. inte – i samma utsträckning som i dag – godta att materialet finns kvar digitalt och kan delas vidare även efter att gärningsmannen har lagförts. Brottsbekämpande myndigheter kommer i flera av dessa fall istället ha möjlighet att tillse att uppgifterna raderas eller i vart fall att fortsatt spridning av dessa begränsas eller förhindras. Den föreslagna lagen innehåller dessutom flera begränsningar och tillämpningen kommer att kräva noggranna överväganden och proportionalitetsbedömningar. Förslagen innebär samtidigt att myndighetens förutsättningar att fullgöra det brottsbekämpande uppdraget i hela det moderna samhället påtagligt förbättras – oavsett om brott begås i den fysiska eller den digitala miljön. För att lagstiftningen ska kunna användas i praktiken är det dock avgörande att dess tillämpningsområde inte begränsas ytterligare i det fortsatta lagstiftningsarbetet. I annat fall riskerar de förväntade positiva effekterna att helt eller delvis utebli.

Lagens tillämpningsområde bör begränsas (avsnitt 13.5)

Polismyndigheten delar utredningens bedömning att lagens tillämpningsområde i jurisdiktionshänseende bör begränsas genom de s.k. anknytningsfaktorerna. Som utredningen påpekar är den digitala miljön ett utmanande område för rättsordningen. Det moderna cybersamhället kännetecknas av att gärningsperson, brottsoffer, servrar och tekniska resurser ofta befinner sig i olika jurisdiktioner. Läget kan dessutom snabbt förändras med hjälp av molntjänster, proxyservrar och anonymiseringsnoder. Anonymiseringstjänster försvårar identifiering av misstänkta gärningsmän och möjligheten att förflytta data innebär att uppgifter snabbt kan skickas från ett land till ett annat. Om Polismyndigheten ska kunna utföra verkningsfulla ingripanden är det helt nödvändigt att åtgärder utan dröjsmål kan riktas även mot informationssystem utomlands, eller där dess hemvist är okänd, så länge det finns en tillräcklig anknytning till Sverige. Det är därför angeläget att anknytningsfaktorerna i 2 § inte ges en mer återhållsam utformning i det fortsatta lagstiftningsarbetet. Polismyndigheten kan annars vara förhindrad att genomföra ett ingripande även om det medges av en annan stat eller i fall där det inte gått att klarlägga inom vilken stats territorium ett informationssystem är beläget.

Beträffande det faktum att ett ingripande kan komma att riktas mot ett informationssystem utomlands vill Polismyndigheten understryka att

myndigheten har en väl utbyggd samverkan med utländska motsvarigheter inom EU, andra brottsbekämpande myndigheter och myndigheter på försvarsområdet. Det bör också framhållas att förslagen i betänkandet kan väntas inverka positivt på Sveriges internationella samarbete på det brottsbekämpande området. Brott i cybermiljö är komplexa samt gränsöverskridande och är därmed en angelägenhet för hela den internationella rättsordningen. Genom skyndsamma och effektiva ingripanden i cybermiljö kan Sverige bidra till minskad brottslighet och ökad trygghet i Sverige men också internationellt.

Ingripanden får endast avse brott eller brottslig verksamhet av viss svårhetsgrad (avsnitt 14.6)

Polismyndigheten instämmer i utredningens bedömning att ett ingripande endast ska kunna avse brott för vilket det är föreskrivet fängelse i ett år eller mer, eller brottslig verksamhet som innefattar sådant brott. För att myndigheten ska kunna möta brottsutvecklingen och fullgöra sitt brottsbekämpande uppdrag även i framtiden krävs ett flexibelt författningsstöd. Även brott som framstår som mindre allvarliga kan t.ex. utgöra led i en omfattande och systematisk organiserad brottslighet. Det är därför viktigt att ingripandemöjligheten inte begränsas till endast de allvarligaste brotten med de högre straffskalorna. Polismyndigheten vill särskilt betona vikten av att ingripandemöjligheten inte inskränks till endast en viss brottskatalog. Merparten av brotten har i dag en digital beståndsdel i många fall och en brottskatalog skulle göra det möjligt för den organiserade brottsligheten att anpassa sina tillvägagångssätt för att undgå eller minimera risken för ingripanden från brottsbekämpande myndigheter.

Metoder för genomförande (avsnitt 18.2)

Enligt 19 § i den föreslagna lagen om polisiära ingripanden i cybermiljö ska tekniska hjälpmedel som installerats vid ingripandet tas bort eller göras obrukbara så snart som möjligt efter att ingripandet genomförts eller beslutet om ingripande upphört att gälla.

Polismyndigheten bedömer att det kan uppstå situationer då det i samband med ett ingripande i cybermiljö uppkommer anledning att inleda förundersökning och vidta åtgärder enligt t.ex. lagen (2020:62) om hemlig dataavläsning. Om ett installerat tekniskt hjälpmedel i dessa fall tas bort innan dataavläsningen påbörjas kan det i vissa fall försvåra eller omöjliggöra att Polismyndigheten på nytt kan bereda sig tillgång till samma informationssystem.

Myndigheten föreslår därför ett tillägg i den aktuella bestämmelsen som gör det möjligt för den ingripande myndigheten att, om det kan antas att

informationssystemet kommer att omfattas av ett tillstånd till hemliga tvångsmedel, avvakta med avinstallation till dess tillståndet upphört eller hävts.

Skyldighet att medverka (avsnitt 18.4)

Som utredningen framhåller anser Polismyndigheten att skyldigheten att medverka vid ingripanden i cybermiljö inte bara bör omfatta de som enligt 2 kap. 1 § lagen (2022:482) om elektronisk kommunikation tillhandahåller vissa kommunikationsnät eller tjänster som inte är nummeroberoende interpersonella kommunikationstjänster. Skyldigheten bör även omfatta de som inom svensk jurisdiktion lagrar data, s.k. värdtjänstleverantörer. Det är dessa aktörer som i stor utsträckning har den tekniska rådigheten över den infrastruktur som ingripanden kommer att riktas mot. Utan en medverkans-skyldighet är Polismyndigheten beroende av frivillig medverkan från de aktörer där den behövs som mest. Vissa sådana bolag, s.k.”bulletproof hosts”, samverkar heller inte med brottsbekämpande myndigheter och är därför vanliga redskap för kriminella och statsaktörer med antagonistiska syften. Dessa bolag är centrala verktyg vid brott i cybermiljö.

Polismyndigheten ifrågasätter inte utredningens bedömning att en generell utvidgning av medverkansskyldigheten enligt lagen om elektronisk kommunikation är alltför komplex för att rymmas inom ramen för utredningen. I motsats till utredningen anser Polismyndigheten dock att en begränsad medverkansskyldighet – med innebörden att värdtjänstleverantörer inom svensk jurisdiktion ska lämna de upplysningar som behövs för att brottsbekämpande myndigheter ska kunna lokalisera och vidta åtgärder mot ett informationssystem – bör kunna omfattas av det fortsatta lagstiftningsarbetet. En sådan skyldighet skulle möjliggöra för Polismyndigheten att rikta åtgärder direkt mot den fysiska eller virtuella server som är föremål för ingripandet. Därmed skulle myndigheten heller inte behöva påverka annan verksamhet eller ta del av annan information än vad som är nödvändigt för ingripandet vilket minskar både kostnaderna och integritetsintrånget för enskilda.

För att bestämmelserna om medverkansskyldighet ska uppnå sitt syfte är det också avgörande att den som omfattas av skyldigheten skyndsamt tillmötesgår en sådan begäran. Operatörer respektive Polismyndigheten har i andra sammanhang haft skilda uppfattningar om tolkningen av begrepp så som ”utan dröjsmål”. Polismyndigheten efterfrågar därför ett tillägg i 7 § i den föreslagna förordningen om polisiära ingripanden i cybermiljö med innebörden att den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § lagen om elektronisk kommunikation *skyndsamt* ska bistå den ingripande myndigheten enligt myndighetens begäran. För att denna utformning inte ska

leda till utmaningar i rättstillämpningen är det angeläget att innebörden av skyndsamhetskravet också definieras i den fortsatta beredningen. Polismyndigheten bedömer att en operatör behöver efterfölja en begäran om medverkan inom några timmar om bestämmelsen ska vara ändamålsenlig.

En tidsbegränsad lag (avsnitt 19.4)

Polismyndigheten instämmer i utredningens bedömning att brott och brottslig verksamhet i cybermiljö ökat kraftigt under senare år och att det finns behov av verkningsfulla åtgärder för att motverka denna utveckling. Myndigheten ifrågasätter inte de skäl för en tidsbegränsad lag som utredningen för fram men delar inte bedömningen att dessa omständigheter överväger skälen för en permanent lag. De författningsändringar som utredningen föreslår bör därför inte tidsbegränsas. Lagstiftningen bör dock följas upp och utvärderas efter ikraftträdande för att eventuella nödvändiga författningsändringar ska kunna uppmärksammas och åtgärdas samt författningarnas effektivitet utvärderas.

Förhållandet till straffprocessuella tvångsmedel (avsnitt 20.1.3)

I likhet med utredningen anser Polismyndigheten att de ingripanden som föreslås i den nya lagen inte bör jämföras med de hemliga och preventiva tvångsmedlen. Även om åtgärder enligt dessa regelverk kan ha likheter i det tekniska tillvägagångssättet har de skilda syften. Ändamålet med den föreslagna lagen om polisiära ingripanden i cybermiljö är att under en begränsad tidsperiod ingripa för att avbryta, störa eller förhindra pågående brott och brottslig verksamhet – framför allt utan tydlig anknytning till enskilda personer. De hemliga och preventiva tvångsmedlen syftar istället till dold och systematisk övervakning av en viss person över tid för att möjliggöra utredning och lagföring av allvarliga brott. Det bör påpekas att polisiära ingripanden ofta kan uppvisa likheter i tillvägagångssätt men avse olika ändamål. Det gäller bl.a. husrannsakan och kroppsvisitation som kan genomföras för ett flertal ändamål enligt olika regelverk. Därmed skiljer sig också regelverken åt såvitt avser t.ex. behörig beslutsfattare och rättssäkerhetsfrågor så som dokumentationskrav. Ändamålsprincipen innebär att brottsbekämpande myndigheter inte får genomföra ingripanden i andra fall än lagstiftaren avsett. Att den nya lagen kan ha vissa metodmässiga likheter med de hemliga och preventiva tvångsmedlen är därmed varken problematiskt eller ett skäl att likställa dessa regelverk.

Yttrandet har beslutats av rikspolischefen Petra Lundh efter föredragning av juristen Gabriel Eriksson. Vid den slutliga handläggningen har tf. rättschefen Anders Ternström samt juristerna Ida Salomonsson och Matilda Svahn deltagit.

POLISMYNDIGHETEN

Petra Lundh

Gabriel Eriksson

Kopia till

Justitiedepartementet (INS)
Arbetstagarorganisationerna
Rikspolischefens kansli