Regeringskansliet
Justitiedepartementet

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

Mot bakgrund av de intressen som Åklagarmyndigheten har att bevaka lämnas följande yttrande.

Sammanfattning

Åklagarmyndigheten

- delar utredningens bedömning av det stora behovet av lagstiftning inom aktuellt område och välkomnar därför förslaget
- anser att det behövs fler överväganden och vägledning i frågan om jurisdiktion när uppgifter finns utomlands eller när lagringsplatsen är okänd
- anser att det behövs ytterligare vägledning om skillnaden mellan de olika ingripandena och gränsen mot andra straffprocessuella tvångsmedel.
- tillstyrker utredningens förslag om nivån på brottslighetens straffvärde som kan aktualisera ingripanden
- anser att det bör införas en möjlighet att underlåta underrättelse i vissa fall, att det införs tydligare reglering om hur länge underrättelseprövningen ska pågå och efterfrågar mer vägledning om under vilka förutsättningar underrättelse får uppskjutas.

Inledning och behov av lagstiftning

Den ökade digitaliseringen har medfört att kriminella i allt större utsträckning använder avancerad teknik för att begå brott och undanröja spår efter sin brottslighet. Tekniken kan användas både för angrepp mot samhällsviktig infrastruktur och som hjälpmedel vid grov brottslighet, samtidigt som lagstiftningen i huvudsak är utformad för att utreda brott i den fysiska miljön.

Den växande brottsligheten i cybermiljön utgör ett betydande samhällsproblem. För att de brottsbekämpande myndigheterna även fortsättningsvis ska kunna bedriva en effektiv brottsbekämpning krävs därför nya verktyg anpassade till den digitala utvecklingen. Utredningen har på ett tydligt sätt redogjort för brottsbekämpande myndigheters problembeskrivning

och för det sedan länge efterfrågade behovet av lagstiftning inom området. Åklagarmyndigheten instämmer fullt ut i utredningens problembeskrivning och dess slutsatser om behovet av en reglering på området. Mot denna bakgrund välkomnar Åklagarmyndigheten förslagen om ingripanden i cybermiljön.

Brott som begås i cybermiljö är ofta gränsöverskridande och tekniskt avancerade i syfte att försvåra brottsbekämpande myndigheters möjligheter att ingripa. Detta aktualiserar ett flertal frågor, såsom jurisdiktion, gränsdragningen mot befintliga tvångsmedel och avgränsningen mellan de olika ingripanden som föreslås i lagförslaget. Det finns därför ett betydande behov av tydlig vägledning och klargöranden i dessa frågor. I annat fall riskerar lagen att bli svår att tillämpa och därmed inte uppnå avsedd effekt. Detta gäller särskilt jurisdiktionsfrågan, där en felaktig tillämpning kan få oförutsedda konsekvenser för Sveriges internationella relationer. Mot denna bakgrund vill vi lämna följande synpunkter.

13.3 Frågor om jurisdiktion

Utredningen har utförligt redogjort för praxis och den internationella synen på jurisdiktion vid ingripanden i cybermiljö. I ett internationellt perspektiv framstår det aktuella lagförslaget som det mest långtgående regelverket, eftersom det inte uppställer krav på samtycke eller liknande från den stat där informationen finns tillgänglig.

När det gäller anknytningen till Sverige enligt 3 § för att lagen ska vara tillämplig anser vi att utredningens överväganden är väl avvägda. De angivna anknytningsfaktorerna bör täcka de flesta situationer där det finns behov av att bekämpa brott i cybermiljö. Om det i ett enskilt ärende kan konstateras att informationen finns inom svenskt territorium ser vi inga hinder mot att ingripanden enligt lagförslaget får genomföras. Situationen är emellertid en annan om det står klart att informationen är lagrad inom en annan stats territorium eller om lagringsplatsen är okänd.

Vi instämmer helt i utredningens slutsats att en stat enbart utövar territoriell verkställighetsjurisdiktion när den bereder sig tillgång till uppgifter som är allmänt tillgängliga inom den verkställande staten (se s. 218). Ingripanden enligt lagförslaget kommer emellertid i många fall att avse information som finns lagrad i slutna miljöer i andra länder, vilket innebär att Sverige i sådana fall skulle utöva extraterritoriell verkställighetsjurisdiktion. Därtill kommer att ingripanden enligt lagförslaget i många fall innebär att brottsbekämpande

myndigheter bereder sig tillgång till informationssystem genom att kringgå eller bryta systemskydd, vilket ytterligare komplicerar jurisdiktionsfrågan.

Utredningen har utförligt redovisat de mest relevanta avgörandena på området, nämligen NJA 2023 s. 231, ”Den okända lagringsplatsen”, och Norges Høyesteretts avgörande HR-2019-619-A. I båda fallen behandlades frågan om verkställande myndigheters jurisdiktion vid åtkomst till uppgifter som lagrats utomlands eller vars lagringsplats varit okänd.

I det norska avgörandet fann domstolen att verkställighetsjurisdiktion förelåg under förutsättning att inga ändringar gjordes i det lagrade materialet, exempelvis genom radering eller blockering, och att eventuella beslag tillgängliggjordes på egna lagringsenheter i Norge. I ”Den okända lagringsplatsen” uttalade Högsta domstolen att åtgärden får genomföras på ett sådant sätt att den eftersökta informationen inte raderas eller på annat sätt påverkas till sitt innehåll (p. 40). Dessa avgöranden ger enligt vår uppfattning stöd för slutsatsen att svenska brottsbekämpande myndigheters verkställighetsjurisdiktion när det gäller åtgärder som innebär att information raderas eller ändras är begränsad till det egna territoriet.

Därutöver måste även reglerna i Tallinnmanualen beaktas. Enligt regel 11 får en stat utöva extraterritoriell verkställighetsjurisdiktion i förhållande till personer, föremål eller cyberverksamhet endast med stöd av en särskild folkrättslig befogenhet eller med giltigt samtycke från den berörda staten. Mot bakgrund av suveränitetsprincipen enligt regel 1 är verkställighetsjurisdiktion avseende cyberinfrastruktur, cyberverksamhet och personer som bedriver sådan verksamhet i regel begränsad till den egna statens territorium samt till fartyg och luftfartyg registrerade i staten. Utövande av verkställighetsjurisdiktion utanför dessa ramar innebär enligt manualen ett intrång i den berörda statens suveränitet.

Eftersom det varken finns någon särskild folkrättslig befogenhet eller något generellt samtycke från andra stater som ger svenska myndigheter rätt att vidta sådana åtgärder som föreslås i betänkandet på andra staters territorium, föreligger en påtaglig risk att åtgärderna, som innebär att information påverkas till sitt innehåll, innebär en kränkning av andra staters suveränitet.

Som utredningen konstaterar finns det många situationer där det inte går att fastställa var informationen är lagrad. s.k. ”loss of location” är närmast en huvudregel för den information som finns på internet. Med utgångspunkt i vad

som uttalats i ”Den okända lagringsplatsen” kan verkställighetsjurisdiktion emellertid anses föreligga så länge åtgärden endast syftar till att bereda sig tillgång till uppgifterna utan att göra några ändringar i informationssystemet. Mot bakgrund av vad som framgår av avgörandet bör utrymmet för åtgärder såsom blockering eller radering enligt vår uppfattning vara mycket begränsat eller obefintligt. Lagringsplatsen kan dessutom i vissa fall bli känd genom att andra stater först i efterhand, med hjälp av tekniska metoder, upptäcker att en svensk myndighet har raderat information på deras territorium. Även detta talar för att gränserna för svenska myndigheters jurisdiktion måste vara klarlagda för att undvika risken för konflikter med andra länder.

Vi delar utredningens uppfattning att Sverige bör verka för att det egna territoriet inte används för kriminell verksamhet (s. 229). Detta utgör dock inte i sig tillräckligt stöd för svensk verkställighetsjurisdiktion. Utredningen hänvisar även till att det saknas folkrättsliga begränsningar mot att svenska brottsbekämpande myndigheter får tillgång till information som lagrats utomlands eller på okänd plats. Utifrån de avgöranden som behandlats ovan och de principer som kommer till uttryck i Tallinnmanualen finns det dock en tydlig skillnad mellan att ta del av information och att förändra den. Att bereda sig tillgång till uppgifter framstår i dag som relativt okontroversiellt under vissa förutsättningar. Avsaknaden av uttryckliga folkrättsliga begränsningar innebär däremot inte att svenska myndigheter därigenom ges rätt att vidta de mer ingripande åtgärder som föreslås i lagförslaget.

Sammanfattningsvis är vår bedömning att jurisdiktionsfrågan är olöst. Utan ett tydligt svar på denna fråga finns en betydande risk för att lagen tillämpas i strid med suveränitetsprincipen, vilket kan leda till oönskade konsekvenser. Det finns även en risk för att lagen inte kommer att användas i någon större omfattning på grund av osäkerhet kring jurisdiktionen. Mot denna bakgrund är det särskilt angeläget att den fortsatta beredningen innehåller fördjupade överväganden om grunden för svensk verkställighetsjurisdiktion samt att tydlig vägledning lämnas för hur dessa bedömningar ska göras.

14 Olika former av ingripanden

De föreslagna ingripandena svarar väl mot brottsbekämpande myndigheters behov av att förebygga och förhindra brott i cybermiljö. Vi har därför inga synpunkter på de föreslagna ingripandena som sådana. Ingripandenas karaktär kan emellertid ge upphov till olika överväganden avseende proportionalitet, jurisdiktion och frågan om vem som ska vara behörig beslutsfattare i det enskilda fallet. Det är därför viktigt att det inte råder några oklarheter kring

vilka åtgärder som omfattas av respektive ingripandeform eller hur dessa förhåller sig till övriga straffprocessuella tvångsmedel. Mot denna bakgrund lämnas följande synpunkter.

Skillnaden mellan blockering och liknande åtgärder som stör eller hindrar användningen av uppgifter i informationssystemet

Blockering och andra åtgärder som innebär att användningen av uppgifter i ett informationssystem hindras eller störs kommer ofta att leda till samma resultat, nämligen att informationssystemet inte kan användas på avsett sätt. Frågan är då vilken ingripandeform som bör väljas i det enskilda fallet.

Det framstår som självklart att blockering bör användas när det saknas tekniska förutsättningar att genomföra någon annan liknande åtgärd. Detsamma bör gälla när blockering som sådan inte är tekniskt möjlig men en annan åtgärd kan uppnå samma effekt. Eftersom det minst ingripande alternativet ska väljas får konsekvenserna för den enskilde stor betydelse vid valet av åtgärd (se s. 247). Om resultatet av olika åtgärder är detsamma kan det vara svårt att avgöra vilken av dem som är mest ingripande. I praktiken riskerar då de tekniska möjligheterna i det enskilda fallet att bli den avgörande faktorn.

Härvid bör även nämnas att en blockering som pågår längre än en månad föranleder en underrättelseskyldighet gentemot den enskilde. Sådan skyldighet föreligger däremot inte om en annan liknande åtgärd har vidtagits. Om det finns tekniska möjligheter att genomföra båda ingripandeformerna och dessa skulle leda till samma resultat för den enskilde, kan detta innebära att reglerna om underrättelse i praktiken sätts ur spel genom att blockering inte väljs som ingripandeform.

Utredningen lämnar sammanfattningsvis ingen närmare vägledning om hur valet mellan dessa åtgärder ska göras, utöver en hänvisning till proportionalitetsprincipen. Det bör därför övervägas att i den fortsatta beredningen lämna tydligare vägledning i denna fråga.

Skillnaden mellan blockering och radering

Som utredningen konstaterar kan det i vissa fall diskuteras om blockering i praktiken kan jämställas med radering (s. 245 f.). Det står klart att blockering ska vara en kortvarig åtgärd, medan radering är definitiv och oåterkallelig (s. 320). Frågan är emellertid hur länge en blockering kan bestå innan den i praktiken får samma effekt som en radering. Eftersom det ställs högre krav för

beslut om radering finns en risk att långvariga blockeringar i praktiken urholkar dessa bestämmelser. Detta får särskild betydelse eftersom olika beslutsfattare föreslås vara behöriga att besluta om blockering respektive radering. Betänkandet innehåller inte några vägledande uttalanden om hur denna bedömning ska göras, och frågan bör därför behandlas närmare i den fortsatta beredningen.

Särskilt om radering

Vi instämmer i utredningens slutsats att radering är en mer ingripande åtgärd än övriga föreslagna ingripanden. Kravet på att åtgärden ska vara av synnerlig vikt för att förhindra eller avbryta brott i cybermiljö framstår därför som väl avvägt. Vi har inte heller några invändningar mot utredningens uttalande att radering endast bör komma i fråga när det är mycket svårt, eller rent av omöjligt, att uppnå samma resultat genom andra ingripanden (s. 256). Det är också positivt att utredningen tydliggör att radering i vissa situationer, exempelvis av material som härrör från kränkande fotografering, kan vara den enda effektiva åtgärden för att förhindra fortsatt brottslighet.

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

Vi anser att utredningens överväganden är väl avvägda i denna del. Kravet på att det ska vara föreskrivet fängelse ett år eller mer för brottet utgör enligt vår uppfattning en rimlig avgränsning för att möjliggöra en effektiv bekämpning av brottslighet i cybermiljö.

16 Vem som bör besluta om ingripanden

Som vi tidigare har framfört instämmer vi i utredningens bedömning att radering utgör en mer ingripande åtgärd än övriga föreslagna ingripanden. Detta motiverar att högre krav ställs på rättssäkerhet och beslutsfattande. Med hänsyn till detta har vi inga invändningar mot förslaget att beslut om radering ska fattas av åklagare efter ansökan från den ingripande myndigheten.

Vi ansluter oss även till de överväganden som utredningen har gjort i frågan om en alternativ lösning för beslutsordningen vid radering som innebär att särskilt utpekade befattningshavare vid Polismyndigheten, Säkerhetspolisen eller Tullverket skulle kunna få besluta om radering av uppgifter i de fall där uppgifterna kan säkras genom en kopia (s. 285).

Interimistiska beslut

Vi anser att utredningens överväganden beträffande interimistiska beslut är väl avvägda och har inga invändningar mot att den ingripande myndigheten får fatta beslut om radering i brådskande fall. Vi har inte heller några invändningar mot att sådana beslut skyndsamt ska underställas åklagarens prövning.

Det kan emellertid ifrågasättas om det är nödvändigt att den ingripande myndigheten bifogar de raderade uppgifterna till sin anmälan på det sätt som föreskrivs i 13 §. I många fall kan informationen exempelvis bestå av skadlig kod eller annat tekniskt innehåll som inte tillför något av betydelse för åklagarens prövning. Det kan även uppstå situationer där den raderade informationen utgör exempelvis barnpornografiskt material. Sådant material bör som utgångspunkt inte behöva överföras eller ges in till åklagaren om det inte är nödvändigt för prövningen.

En anmälan i dessa fall kommer rimligen att innehålla de uppgifter som enligt 16 § ska framgå av beslutet. En tydlig och lättbegriplig redogörelse för de raderade uppgifterna bör därför normalt vara tillräcklig för att åklagaren ska kunna ta ställning till det interimistiska beslutet. Om det i det enskilda fallet finns behov av att ta del av de raderade uppgifterna innan prövningen genomförs bör det vara tillräckligt att åklagaren samråder med den ingripande myndigheten och tillsammans med denna bestämmer hur uppgifterna ska göras tillgängliga för granskning.

I 14 § regleras åklagarens prövning av interimistiska beslut och vilka skyldigheter som åvilar åklagaren om det saknats förutsättningar för radering. Vi instämmer i att det finns starka skäl att underrätta den som har berörts av beslutet. Mot detta måste emellertid i vissa fall vägas intresset av att inte skada en pågående utredning. Uppgifter som har raderats kan exempelvis ha betydelse i en förundersökning. En underrättelse till den enskilde kan då medföra att det avslöjas att det pågår en utredning om brott eller brottslig verksamhet. Detta riskerar att äventyra pågående utredningsåtgärder, såsom hemliga tvångsmedel, och i förlängningen försvåra eller omintetgöra utredningen. En underrättelse kan därför i vissa fall vara till betydande men för utredningen.

Detta kan jämföras med underrättelseskyldigheten enligt 21 §, där underrättelse får uppskjutas om den skulle skada utredningen (s. 421). Även om ingripandet i efterhand visar sig sakna rättslig grund kan det finnas starka utrednings-intressen som bör ges företräde. Mot denna bakgrund bör en underrättelse

enligt 14 § andra stycket endast lämnas om det kan ske utan men för utredningen. Om underrättelse inte kan lämnas omedelbart bör en kopia av beslutet bevaras till dess att underrättelse kan ske.

19 Rättssäkerhetsgarantier

Vi instämmer helt i utredningens bedömningar om rättssäkerhetsgarantier och har inga invändningar mot att underrättelse ska ske på så sätt som det har föreslagits. Vi anser även att det är en lämplig ordning att underrättelser ska lämnas av den ingripande myndigheten, även i de fall åklagaren har fattat beslut om radering.

Utredningen lämnar emellertid inga förslag till författningsändringar som reglerar hur länge en underrättelseprövning får pågå eller under vilka förutsättningar en underrättelse får skjutas upp. De uttalanden som görs, nämligen att en underrättelse får skjutas upp om den skulle vara till men för utredningen och att underrättelse ska lämnas så snart syftet med raderingen eller blockeringen inte längre äventyras och det inte heller i övrigt finns hinder mot det, är alltför allmänt hållna för att ge tillräcklig vägledning i praktiken (s. 421–422).

Som utredningen framhåller kommer det i många fall att vara känt för den vars uppgifter berörs att en blockering eller radering har genomförts. Det kan dock uppkomma situationer där sådana åtgärder vidtas utan att lämna spår, exempelvis för att inte äventyra en omfattande spaningsinsats mot organiserad brottslighet som kan pågå under lång tid. Att det inte i övrigt ska finnas hinder mot underrättelse ger emellertid ingen närmare vägledning om under vilka förutsättningar en underrättelse får skjutas upp. Inte heller föreslås någon yttersta tidsgräns för hur länge frågan om underrättelse ska prövas. Enligt vår uppfattning innebär detta att regleringen inte innehåller tillräckliga garantier för en rättssäker hantering av underrättelsefrågan. I den fortsatta beredningen bör det därför övervägas om förutsättningarna för att skjuta upp underrättelse och den tid under vilken underrättelsefrågan får hållas under prövning bör regleras närmare, antingen genom ändringar i författningsförslaget eller genom tydligare uttalanden i dessa frågor.

Utredningen behandlar inte heller frågan om det bör finnas en möjlighet att helt underlåta underrättelse. Enligt vår uppfattning finns det ett påtagligt behov av en sådan reglering. Kriminella aktörer anpassar fortlöpande sina verktyg och de informationssystem de använder utifrån de brottsbekämpande myndigheternas förmåga att vidta åtgärder mot dessa system. En underrättelse kan därför i vissa

fall innebära att den ingripande myndighetens förmågor eller metoder röjs trots att det är tekniskt möjligt att vidta åtgärderna utan att lämna spår. I likhet med vad som gäller för hemliga tvångsmedel bör det därför under vissa förutsättningar finnas en möjlighet att underlåta underrättelse, om en sådan skulle vara till men för utredningen eller riskera att röja myndighetens arbetsmetoder.

Som framgått ovan kommer den vars uppgifter berörs i de flesta fall ändå att förstå att en brottsbekämpande myndighet har ingripit. Möjligheten att underlåta underrättelse skulle därför endast aktualiseras i ett begränsat antal ärenden. En sådan ordning bedöms inte påverka den enskildes rättssäkerhetsgarantier i någon nämnvärd omfattning, samtidigt som den bättre tillgodoser brottsbekämpningens behov.

20.1.3 Förhållande till straffprocessuella tvångsmedel

Utredningen har bedömt att det inte finns något behov av författningsändringar för att avgränsa tillämpningsområdet i förhållande till hemliga och preventiva tvångsmedel eller andra tvångsmedel. Eftersom metoderna för att bereda sig tillgång till informationssystem enligt den nya lagen i många avseenden liknar dem som används vid hemlig dataavläsning finns det dock ett visst behov av ytterligare gränsdragningar.

Vi instämmer i att det finns ett behov av att kunna vidta åtgärder för att kartlägga om ett informationssystem används för brott eller brottslig verksamhet. Det är dock inte helt tydligt hur detta ingripande förhåller sig till hemlig dataavläsning och, i viss mån, till hemlig avlyssning av elektronisk kommunikation. Utredningen betonar att ingripanden enligt den nya lagen ska vara kortvariga, medan hemliga tvångsmedel typiskt sett används för att samla in bevisning under längre tid (s. 346). Utredningen bedömer därför att det inte finns någon risk för att den nya lagen används som ett substitut för hemliga tvångsmedel.

Hemlig dataavläsning kan emellertid användas även vid kortvariga åtgärder, exempelvis genom så kallad historisk hemlig dataavläsning, där syftet är att få en bild av vad som tidigare förekommit i ett informationssystem samt av trafiken till och från systemet. Därtill används hemlig avlyssning av elektronisk kommunikation redan i dag för att kartlägga vilka informationssystem som används vid brott, exempelvis genom en mobiltelefon, för att därefter rikta hemlig dataavläsning mot dessa system. Dessa förfaranden uppvisar betydande likheter med det nu aktuella ingripandet. Även om syftet med den nya lagen är att förhindra, störa eller avbryta brottsliga aktiviteter kan den information som

framkommer genom ingripandet samtidigt få betydelse som bevisning i en brottsutredning (jfr s. 346).

Det är självklart att hemliga tvångsmedel ska användas när syftet är att systematiskt och under längre tid samla in information. I de situationer som beskrivits ovan uppkommer dock frågan om vilken åtgärd som bör väljas vid kortvariga ingripanden. Ofta kommer det att finnas ett parallellt intresse av både bevisinhämtning och att förhindra eller avbryta brottslig verksamhet. Syftet med åtgärden kan då inte ensamt vara avgörande för valet av rättsligt verktyg, särskilt eftersom kraven för ingripanden enligt den nya lagen är lägre än de som gäller för hemliga tvångsmedel. Vi ser därför ett behov av att det i den fortsatta beredningen lämnas tydligare vägledning om avgränsningen mellan den föreslagna lagen och de hemliga tvångsmedlen.

23.3.5 Ekonomiska konsekvenser för myndigheterna

Vi instämmer i utredningens bedömning att lagförslaget kommer att medföra ökade kostnader för myndigheten och att det därför krävs ökade anslag under de kommande åren för att myndigheten ska kunna hantera de nya arbetsuppgifter som förslagen medför.

Detta yttrande har beslutats av riksåklagaren Katarina Johansson Welin efter föredragning av kammaråklagaren Kevin Öksuz. I den slutliga handläggningen av ärendet har också tf. rättschefen Marie Skåninger och vice överåklagaren Magnus Johansson deltagit. Byråcheferna Per Hedvall och Eva Bloch har medverkat i beredningen.

Katarina Johansson Welin

Kevin Öksuz

Kopia till
Kommunikationsavdelningen
Rättschefen
Biblioteket