REMISSYTTRANDE

2026-11-09

FRA beteckning
Dnr 2026FRA1585-2

Justitiedepartementet
Enheten för domstols- och åklagarfrågor

Er handläggare	Ert datum	Er beteckning
	2026-07-09	Ju2026/01670

FRA handläggare	FRA föreg. datum	FRA föreg. beteckning
Kári Ólafsson		

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

Försvarets radioanstalt (FRA) har, från de utgångspunkter myndigheten har att beakta, följande synpunkter på förslagen i betänkandet Effektiva ingripanden i mot brott i cybermiljö (SOU 2026:45). Remissvaret följer kapitelindelningen i betänkandet.

13.5.2 Anknytning till svenska förhållanden (s. 227 ff.)
Förslaget om anknytning till svenska förhållanden som en förutsättning för polisära ingripanden i cybermiljö innebär att lagen ger utrymme för att rikta ingripanden mot informationssystem som finns utanför Sveriges territorium. De som drabbas av ingripandena ska, så länge de kan identifieras och om inte sekretess enligt hindrar, underrättas om dessa. Det finns alltså en viss presumtion för att ingripanden ska vara kända.

Enligt FRA:s mening kan det inte uteslutas att ingripanden som myndigheterna föreslås få utföra utomlands skulle kunna få utrikespolitiska konsekvenser. Det kan därför ifrågasättas om den föreslagna beslutsordningen bör gälla vid ingripanden utomlands. Utformningen av bestämmelsen behöver behandlas i det fortsatta lagstiftningsärendet.

FRA
Box 301
161 26 BROMMA

Telefon
08 - 471 46 00

Telefax

Org.nr
20 21 00 - 0365

Oavsett hur regleringen slutligen utformas behöver myndigheterna vid eventuella ingripanden utomlands beakta kravet i 10 kap. 13 § regeringsformen.

16.1 Polismyndigheten, Säkerhetspolisen och Tullverket bör besluta om flertalet åtgärder (s. 281)

Enligt 6 § förslag till förordning om polisiära ingripanden i cybermiljö ska samråd ske med åklagare innan beslut om ingripande fattas om polisiära ingripanden riskerar att beröra en pågående undersökning.

Ingripanden enligt utredningens förslag kan rikta sig mot all form av brottslig verksamhet som förekommer på internet. Vissa aktörer skulle kunna vara föremål för kartläggning enligt den reglering som gäller för FRA:s signalspaning inom försvarsunderrättelseverksamheten.[1] Enligt FRA:s mening vore det därför lämpligt att föra in en motsvarande samrådsbestämmelse för det fall polisiära ingripanden kan beröra pågående försvarsunderrättelseverksamhet. Det bör överlåtas till berörda myndigheter att hitta samverkansformer för sådant samråd.

19.1.2 Underrättelse i vissa fall (s. 321 f.)
Enligt förslaget ska en enskild, vars uppgifter genom ett ingripande enligt lagen har raderats eller blockerats under längre tid än en månad, underrättas om ingripandet så snart det lämpligen kan göras, om inte han eller hon har fått kännedom om ingripandet på annat sätt. Underrättelseskyldigheten ska dock inte gälla om sekretess gäller enligt 18 kap. 9 § offentlighets- och sekretesslagen (2009:400) (OSL). Sekretessen gäller om det kan antas att syftet med metoden motverkas om uppgiften röjs.

Bestämmelsen är för snävt utformad enligt FRA:s mening. Om myndigheterna exempelvis använder sig av FRA:s underrättelserapporter för att identifiera informationssystem för att genomföra ingripanden skulle utlämnande av information om ingripandet kunna ge invisning till den aktör som ingripandet riktar sig mot om FRA:s metoder och förmågor. I sådana fall är inte 18 kap. 9 OSL tillämplig utan 15 kap. 2 § OSL.

[1] Enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (LSF) får FRA inhämta signaler i elektronisk form oavsett om de är under förmedling eller lagrade för att bl.a. kartlägga internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen.

Vidare behövs en ventil för att underlåta underrättelse vid ingripanden om informationen som lämnas kan riskera att underlätta för fortsatt brottslighet. Uppgifter om vilket informationssystem eller användarkonto eller annan avgränsad del av informationssystemen som åtgärden vidtagits mot kan ge aktörerna, särskilt kvalificerade aktörer, tillräcklig information för att anpassa sig och fortsätta sin verksamhet.

Sammanfattningsvis är det viktigt att skyddsvärd information rörande nationell säkerhet inte röjs vid ingripanden. Därför bör bestämmelsen om underlåtelse av underrättelseskyldigheten inte vara begränsad till en viss sekretessbestämmelse i OSL. I vart fall bör underrättelseskyldigheten kunna underlåtas om den skulle röja uppgifter som omfattas av 15 kap. 1-2 §§ samt 18 kap. 8 § OSL.

20.2.2 Likartat stöd kan komma att behövas i cybermiljö (s. 349)
FRA bedriver signalspaning i enlighet med lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (LSF). FRA lämnar underrättelser till berörda myndigheter. FRA:s underrättelser får inte användas för att utreda brott enligt lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott.

Enligt betänkandet är syftet med den föreslagna lagen inte att utreda brott utan att förhindra och stoppa brottslig verksamhet (se avsnitt 14.3, s. 250 f.). För FRA är det dock oklart hur bestämmelserna faktiskt kommer tillämpas i detta hänseende. Överskottsinformation från ingripanden får nämligen användas i förundersökning och för att berika myndigheternas underrättelseverksamhet (se avsnitt 20.1.2, s. 342 ff.).

Dessutom innehåller lagförslaget en bestämmelse som är av brottsutredande karaktär. Enligt 5 § har myndigheterna möjlighet att kartlägga trafik till och från ett informationssystem för att hitta ytterligare informationssystem som används för brottslig verksamhet. Bestämmelsens utformning gör att gränserna mellan brottsutredande åtgärder och verksamhet som syftar till att förhindra brott blir än mer oklar vilket kan påverka FRA:s möjligheter att lämna underrättelser i enlighet med gällande regelverk.

Dessa oklarheter behöver behandlas i det fortsatta lagstiftningsärendet.

FRA

23 Konsekvenser

Förslagen i betänkandet innebär att de brottsbekämpande myndigheterna kan komma att verkställa ingripanden enligt förslaget i informationssystem som finns på it-infrastruktur i andra länder. FRA kan inte se att utredningen behandlar frågan hur andra stater kan komma att agera för det fall förslaget blir verklighet.

En rimlig utgångspunkt är dock att andra länder kommer att förbehålla sig rätten att agera på motsvarande sätt i förhållande till Sverige. Det finns med andra ord en risk att stater kommer börja agera i den svenska cybermiljön för att förhindra och stoppa brottslig verksamhet som har anknytning till det egna landet. Det saknas även resonemang hur Sverige i så fall bör se på utländska ingripanden som t.ex. innebär blockering eller radering av svenska webbplatser. Rimligen utgör utländska polisiära ingripanden i svenska informationssystem dataintrång enligt svensk lagstiftning. På samma sätt behandlas inte risken att utländsk polis ingriper mot aktörer i svensk cybermiljö för att hindra eller stoppa åtgärder som inte är kriminaliserade enligt svensk rätt.

Dessa frågor behöver behandlas i det fortsatta lagstiftningsärendet.

I detta ärende har generaldirektören Björn Lyrvall beslutat. I den slutliga handläggningen har också överdirektören Maria Diamant, chefsjuristen Michaela Dráb, C GD:s stab Marika Dagenbrink, avdelningscheferna Iréne Ahlström Lundin (Cyber), Gunnar Hellenius (avd T) och Rickard Källstrand (avd V), stabshandläggaren Sarah Lindhoff (Cyber) samt juristen, tillika föredragande, Kári Ólafsson (Rätts 1) deltagit.

Försvarets radioanstalt

Björn Lyrvall

Kári Ólafsson

FRA

Sändlista

För kännedom
Försvarsdepartementet/EFU

Internt FRA
GD
ÖD
C JUR
Bitr. C JUR
C GD Stab
C PS
C KOM
AC