MYNDIGHETEN FÖR
SÄKERHET OCH
INTEGRITETSSKYDD

YTTRANDE

2026-11-11

Dnr
199-2026

Justitiedepartementet
ju.L4@regeringskansliet.se

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

Ju2026/01670

Myndigheten för säkerhet och integritetsskydd har ombetts att yttra sig över innehållet i rubricerat betänkande. Myndigheten har granskat förslagen främst med utgångspunkt från sin uppgift att värna rättssäkerheten och skyddet för den personliga integriteten och att – inom ramen för Säkerhets- och integritetsskyddsnämndens (nämndens) verksamhet – utöva tillsyn över viss brottsbekämpande verksamhet.

Sammanfattning

Myndigheten delar utredningens bedömning att de brottsbekämpande myndigheterna har ett angeläget behov av nya verktyg för att ingripa mot viss brottslighet i cybermiljö. Den föreslagna lagen har dock ett otydligt och alltför brett tillämpningsområde och saknar flera viktiga rättssäkerhetsgarantier. Myndigheten avstyrker därför lagförslaget i den nuvarande utformningen och anser att ingripandena, så långt det är möjligt, bör regleras på samma sätt och omgärdas av samma rättssäkerhetsgarantier som hemliga och preventiva tvångsmedel. Det innebär bl.a. att ingripandena bör beslutas av domstol.

Övergripande synpunkter

Myndigheten ställer sig bakom de synpunkter som framförs i det särskilda yttrandet av experterna Ida Olsson och Andreas Persson och delar således bedömningen att den föreslagna lagen inte är tillräckligt avgränsad och att den inte omgärdas av tillräckliga rättssäkerhetsgarantier.

Det är en grundläggande brist att utredningen inte i tillräcklig utsträckning beaktar det betydande integritetsintrång som beredandet av tillgång till ett informationssystem kan innebära. Åtgärden får verkställas dolt och, på samma sätt som vid hemlig dataavläsning, genom att bryta systemskydd eller utnyttja tekniska sårbarheter. När en brottsbekämpande myndighet har berett sig tillgång till ett informationssystem – t.ex. en mobiltelefon som kan innehålla stora mängder uppgifter av helt legitim, och privat, karaktär – kan det integritetsintrång som tillgängliggörandet av uppgifter innebär inte heller göras ogjort. I den meningen är redan beredandet av tillgång till ett informationssystem, i likhet med radering, en oåterkallelig åtgärd. Detta återspeglas inte i utredningens överväganden.

Förslaget innebär att ingripanden i cybermiljö ska beslutas av särskilt utsedda polisiära befattningshavare eller, i fråga om av radering, av åklagare. Dessutom ska sådana polisiära befattningshavare få besluta att den ingripande myndigheten i hemlighet får bereda sig tillträde till en intrångsskyddad plats, t.ex. en bostad, för att installera tekniska hjälpmedel. Enligt myndigheten är det inte en godtagbar beslutsordning när det handlar om så integritetskänsliga åtgärder.

Utredningen menar att ingripanden i cybermiljö inte syftar till att systematiskt och under längre tid samla in information för att utreda brott eller berika underrättelseverksamhet och att det därmed inte finns någon risk för att den nya lagen ska användas som en ersättning för hemliga och preventiva tvångsmedel. Myndigheten delar inte den uppfattningen. Även om utredningens avsikt är att ingripanden i cybermiljö ska vara tillfälliga medger regleringen, som den får förstås, att ett beslut om ingripande får verkställas under en tid upp till en månad. Lagen innehåller dessutom inte något förbud mot inhämtning av uppgifter och, som utredningen framhåller, kan ett ingripande resultera i att information tillförs en förundersökning eller underrättelseverksamheten. Det anförda innebär att endast avsikten bakom lagen utgör hinder för den ingripande myndigheten att inhämta uppgifter från ett informationssystem på samma sätt som vid hemlig dataavläsning. Myndigheten anser, i ljuset av det

tillämpningsområde och den beslutsordning som utredningen föreslår, att frånvaron av tydligare begränsningar i detta avseende är oacceptabel.

Myndigheten håller inte heller med utredningen om att ingripandena normalt kan förväntas göras helt öppet. Det kan nämligen inte förutsättas att en ändring, blockering eller radering alltid medför att den enskilde uppmärksammar att en åtgärd vidtagits i hans eller hennes informationssystem. Vidare står det inte nödvändigtvis klart för en enskild, som uppmärksammar att ett ingripande har gjorts, att det är en brottsbekämpande myndighet som ligger bakom åtgärden. Ett beredande av tillgång till ett informationssystem kommer inte heller alltid leda till att uppgifter ändras, blockeras eller raderas. Myndigheten anser därmed att ingripandenas förmenta öppenhet inte har någon avgörande betydelse för gränsdragningen mot hemliga och preventiva tvångsmedel.

Sammantaget anser myndigheten att de föreslagna ingripandena har sådana likheter med hemliga och preventiva tvångsmedel att åtgärderna, i den utsträckning det är möjligt utan att syftet med lagstiftningen går förlorat, bör omgärdas av samma begränsningar och rättssäkerhetsgarantier som sådana tvångsmedel. Detta innebär att utredningens förslag måste omarbetas i stora delar för att kunna ligga till grund för lagstiftning.

Nedan lämnas mer detaljerade synpunkter på förslagen i den ordning som följer av betänkandets kapitelindelning. Vissa av synpunkterna gäller för det fall lagstiftaren går vidare med lagen i huvudsakligen nuvarande utformning, dvs. utan flera sådana begränsningar och rättssäkerhetsgarantier som finns i regelverken om hemliga och preventiva tvångsmedel.

Begreppet cybermiljö (avsnitt 13.1)

Myndigheten anser att innebörden av att ett brott begås i cybermiljö inte är tillräckligt preciserad. I författningskommentaren anges t.ex. att det är tillräckligt att något rekvisit i en straffbestämmelse har koppling till cybermiljö för att brottet ska uppfylla kravet att det begås eller kommer att begås i cybermiljö. Samtidigt framhåller utredningen att exempelvis telefonsamtal som förs i syfte att förbereda brott i den fysiska miljön faller utanför tillämpningsområdet eftersom informationssystemet i ett sådant fall inte används som ett medel för att begå brottet utan enbart som ett sätt att kommunicera mellan två eller flera personer. Enligt myndigheten är det föreslagna tillämpningsområdet otydligt, för brett och svårt att överblicka. Det är t.ex. oklart hur förslagen förhåller sig till förberedelse, och även stämpling och anstiftan, till brott.

Ett otydligt tillämpningsområde är inte godtagbart när det är fråga om integritetskänsliga åtgärder av detta slag. I det fortsatta lagstiftningsarbetet bör det därför övervägas om begreppet cybermiljö verkligen innebär en lämplig avgränsning av lagens tillämpningsområde. Om begreppet ska användas anser myndigheten att innebörden av det måste förtydligas.

Begreppet informationssystem (avsnitt 13.2)

Den innebörd som utredningen ger begreppet informationssystem är mycket bred och innebär inte någon egentlig avgränsning av den föreslagna lagens tillämpningsområde. Utredningens avsikt är att begreppet ska kunna ta sikte på t.ex. en fullständig webbplats som används av ett stort antal enskilda. Samtidigt ska det kunna avse en mobiltelefon som används av en enskild men som i jämförelse med webbplatsen kan innehålla långt mer integritetskänsliga uppgifter. Myndigheten anser att arten och omfattningen av det rättighetsintrång som ett ingripande ger upphov till därmed kan skilja sig betydligt mellan olika fall. Det återspeglas inte i tillräcklig utsträckning i utredningens överväganden.

Vidare noterar myndigheten att begreppet informationssystem, trots att någon definition enligt utredningen inte är nödvändig, definieras i författningskommentaren. Definitionen är emellertid hämtad från förarbetena till lagen om hemlig dataavläsning och avser det snävare begrepp – avläsningsbart informationssystem – som avgränsar tillämpningsområdet för bl.a. den lagen. I det fortsatta lagstiftningsarbetet bör det övervägas om begreppet avläsningsbart informationssystem, som redan är etablerat och har en tydlig innebörd, ska användas i den föreslagna regleringen. Om regleringen ska vara tillämplig på informationssystem måste den närmare avgränsningen av begreppet övervägas vidare och förtydligas.

Slutsatser om lagens tillämpningsområde (avsnitt 13.6)

Utredningens bedömning grundar sig bl.a. på rättsfallet NJA 2023 s. 231 ”Den okända lagringsplatsen” där Högsta domstolen slog fast att genomsökning på distans kan beslutas även om den eftersökta informationen kan vara lagrad utomlands. Utredningen väger emellertid inte in den omständigheten att en förutsättning för domstolens bedömning var att åtgärden utförs på ett sådant sätt att den eftersökta informationen inte raderas eller på annat sätt påverkas till sitt innehåll (p. 40). Av utredningens slutsatser framgår inte heller hur möjligheten att ändra, blockera eller radera uppgifter i ett informationssystem som kan finnas i utlandet förhåller sig till Tallinnmanualen eller Norges

Høyesteretts avgörande HR-2019-619-A. Myndigheten konstaterar därmed att betänkandet saknar avgörande resonemang i frågan om jurisdiktion och att det krävs fortsatta överväganden innan förslagen kan ligga till grund för lagstiftning.

Ingripanden för att hindra, störa eller avbryta (avsnitt 14.2)

Ändring och annan liknande åtgärd bör regleras på samma sätt som blockering

Enligt myndigheten är det svårt att i förhållande till den enskilde se någon avgörande skillnad mellan att uppgifter krypteras – vilket enligt utredningen innebär en ändring – och att de blockeras. Även en annan liknande åtgärd för att störa eller hindra användningen av uppgifter kan leda till att den enskilde förlorar tillgång till information i samma utsträckning som blockering. Myndigheten anser därför att ändring och annan liknande åtgärd bör regleras på samma sätt som blockering. Det innebär bl.a. att ett beslut om ändring precis som blockering måste förlängas för att åtgärden ska kunna användas under mer än en månad.

Det bör i lag anges hur och när rådighet över uppgifter ska återgå

I författningskommentaren anges att den ingripande myndigheten ska möjliggöra att den, vars uppgifter är föremål för ändring eller blockering, kan återfå rådigheten över dem. Enligt myndigheten är det viktigt att det ställs krav på hur och när den enskilde ska återfå rådighet över uppgifterna. Eftersom återgåendet av rådighet är avgörande för att dessa ingripanden ska skilja sig mot den permanenta åtgärden radering – i fråga om vilken det bl.a. föreslås en annan beslutsordning – anser myndigheten att kraven bör framgå av lag.

Ingripande för att kartlägga brottslig verksamhet (avsnitt 14.3)

Enligt myndigheten skiljer sig ingripande för att kartlägga brottslig verksamhet väsentligt från övriga åtgärder enligt den föreslagna lagen. Kartläggningen utgör inte ett ingripande i ett informationssystem utan syftar till att undersöka vissa förhållanden kring systemet. Dessutom är det enligt utredningen en förutsättning att åtgärden verkställs dolt. I det avseendet är åtgärden ännu mer jämförbar med hemliga och preventiva tvångsmedel än övriga ingripanden. Det innebär att risken för att reglerna om sådana tvångsmedel ska kringgås, som myndigheten återkommer till nedan, är särskilt påtaglig när det gäller ingripande för att kartlägga brottslig verksamhet.

Samtidigt omfattar ingripandet endast trafikuppgifter under befordran och inte innehållet i meddelanden eller uppgifter som lagras i informationssystemet. Därmed framstår det som att integritetsintrånget typiskt sett skulle kunna bli mindre än vid användning av de ingripanden som ger de brottsbekämpande myndigheterna rätt att bereda sig tillgång till ett informationssystem. Enligt myndighetens mening saknar betänkandet dock tillräckliga analyser om vad ett ingripande för att kartlägga brottslig verksamhet skulle kunna innebära för enskilda i fall när riskerna för integritetsintrång är som störst.

Vid en avvägning mellan de brottsbekämpande myndigheternas behov av åtgärden och det integritetsintrång som den skulle kunna medföra anser myndigheten att det inte är proportionerligt att möjliggöra användning av åtgärden utanför Säkerhetspolisens verksamhetsområde. Det gäller särskilt om tillstånd till åtgärden i enlighet med utredningens förslag inte ska prövas av domstol. Tillämpningsområdet bör således avgränsas genom en begränsad katalog över brott som handläggs av Säkerhetspolisen. Först efter en utvärdering av Säkerhetspolisens tillämpning av regleringen bör det kunna bli aktuellt att ge ytterligare myndigheter samma möjlighet.

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

Regleringen bör innehålla krav på viss misstanke respektive viss risk

Myndighetens utgångspunkt är, som anförts ovan, att ingripandena bör regleras på samma sätt som hemliga och preventiva tvångsmedel. Det innebär att ett beslut om ingripande bör knytas till en utpekad person. En viktig del av utredningens förslag är emellertid att ingripanden ska kunna användas även när det är okänt vem som ligger bakom ett brott eller brottslig verksamhet i cybermiljö och myndigheten inser att syftet med regleringen riskerar att gå förlorat om det t.ex. ställs krav på att informationssystemet i fråga används av en skäligen misstänkt. Med hänsyn till det betydande integritetsintrång som åtgärderna kan ge upphov till anser myndigheten dock att det inte är godtagbart att införa en möjlighet att använda ingripanden i cybermiljö när omständigheterna är sådana att det varken finns någon brottsmisstanke eller viss kvalificerad risk för att brottslig verksamhet kommer att utövas.

Utredningen föreslår att det, i fråga om ingripande för att kartlägga brottslig verksamhet, ska krävas viss misstanke om att informationssystemet utnyttjas i brott eller brottslig verksamhet. När det gäller övriga ingripanden föreslås däremot inte något misstankekrav.

Myndigheten anser att det, när det pågår eller finns förutsättningar att inleda en förundersökning, bör krävas viss misstanke även om ingripandet innefattar ändring, blockering, annan liknande åtgärd eller radering. Det skulle kunna handla om att det ska krävas särskild anledning att anta att ett brott begås med hjälp av ett informationssystem. Utanför förundersökning, dvs. på underrättelsestadiet, anser myndigheten att ett krav bör utformas med lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen) som förebild. Det skulle kunna handla om att det måste finnas en påtaglig risk för att brottslig verksamhet kommer att utövas med hjälp av ett informationssystem.

Svårhetsgraden är för låg

Myndigheten anser att det föreslagna kravet att ett ingripande endast får avse brott, eller brottslig verksamhet som innefattar sådant brott, för vilket det är föreskrivet fängelse i ett år eller mer är alldeles för lågt ställt. Eftersom beredandet av tillgång till ett informationssystem är jämförbart med hemlig dataavläsning anser myndigheten att minst samma krav som gäller för det tvångsmedlet bör gälla i den föreslagna regleringen. Utgångspunkten bör således vara brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år. I sammanhanget kan nämnas att det, för att lagen (2026:1235) om avlägsnande av rekryteringsinnehåll online ska vara tillämplig, krävs att det är fråga innehåll som skäligen kan antas utgöra ett led i straffbar förberedelse eller stämpling till ett brott för vilket det är föreskrivet fängelse i två år eller mer eller involverande av en underårig i brottslighet enligt 16 kap. 5 a § brottsbalken.

Som anförs i det särskilda yttrandet saknar avgränsningen till brott för vilket det är föreskrivet fängelse i ett år eller mer motsvarighet i den internationella utblick som utredningen gjort. Myndigheten konstaterar t.ex. att det i Australien, där den enligt utredningen mest långtgående lagstiftningen inom cyberområdet finns, ställs betydligt högre krav på de brott som kan ligga till grund för ett tillstånd till dataavbrott eller övertagande av onlinekonto.

Myndigheten anser att en tvåårsregel vid behov kan kompletteras med en katalog av brott där straffskalan är lägre men behovet av att kunna använda ingripandena framstår som särskilt angeläget. Det kan, vid sidan av Säkerhetspolisens verksamhetsområde, handla om t.ex. olaga integritetsintrång, vissa sexualbrott mot barn, bedrägeri, utpressning och barnpornografibrott.

Vem som bör besluta om ingripanden (kapitel 16)

Myndigheten anser att ingripanden i cybermiljö bör beslutas av domstol.

Utredningen framhåller att husrannsakan i enskilda fall kan innebära ett lika stort intrång i den enskildes privatliv som ett hemligt tvångsmedel. Myndigheten konstaterar emellertid att den som drabbas av husrannsakan enligt rättegångsbalken som utgångspunkt har rätt att närvara vid verkställigheten och i annat fall ska underrättas om åtgärden så snart det kan ske utan men för utredningen. När det gäller husrannsakan enligt preventivlagen, där åtgärden får äga rum i hemlighet, krävs domstolsbeslut. Sammantaget anser myndigheten att utredningens jämförelse med husrannsakan inte är ett bärande argument i sammanhanget.

Som myndigheten anfört ovan innebär det förhållandet att ett ingripande enligt den nya lagen är avsett att vara kortvarigt och göras öppet inte någon avgörande skillnad i förhållande till sådana tvångsmedel som kräver domstolsprövning. I sammanhanget kan det framhållas att även hemliga och preventiva tvångsmedel kan användas för att kortvarigt, vid ett enskilt tillfälle, inhämta t.ex. historiska uppgifter om elektronisk kommunikation.

Därtill noterar myndigheten att åklagare visserligen beslutar om inhämtning enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen). Eftersom beredandet av tillgång till ett informationssystem får verkställas på samma sätt som hemlig dataavläsning måste jämförelsen emellertid göras med möjligheten att använda det tvångsmedlet i de s.k. inhämtningslagsfallen (10 § och 10 a § lagen om hemlig dataavläsning). För en sådan åtgärd krävs domstolsbeslut.

Som framförs i det särskilda yttrandet framstår den föreslagna beslutsordningen som avvikande i utredningens internationella utblick. Exempelvis kräver den enligt utredningen långtgående regleringen i Australien att tillstånd till dataavbrott, nätverksaktivitet och övertagande av kontroll över ett onlinekonto beslutas av domstol.

Slutligen anser myndigheten att en ordning där domstol beslutar om ingripanden kan kompletteras med en möjlighet för åklagare att fatta interimistiska beslut. Under förutsättning att Åklagarmyndigheten vidtar lämpliga anpassningar av sin organisation kan ett sådant beslutsfattande förväntas ta endast något mer tid i anspråk än om en särskilt utsedd befattningshavare vid den verkställande myndigheten beslutar.

Om regeringen väljer att gå vidare med ett förslag utan krav på domstolsprövning anser myndigheten att det under alla förhållanden, i mer kvalificerade

fall, bör vara upp till rätten att ta ställning till ett ingripande. Det skulle kunna handla om att det krävs domstolsbeslut när ett ingripande avser ett informationssystem som kan antas innehålla omfattande uppgifter eller när ett ingripande skulle medföra synnerlig olägenhet eller en liknande ordning (jfr 28 kap. 4 § rättegångsbalken).

Intermistiska beslut om radering (avsnitt 16.2.2)

För att markera att interimistiska beslut om radering bör användas restriktivt föreslår utredningen bl.a. att det i fråga om ändamålet att avbryta brott krävs att det handlar om pågående brott. Myndigheten, som ifrågasätter om det är möjligt att avbryta ett brott om det inte pågår, anser att det i det fortsatta lagstiftningsarbetet bör övervägas om rekvisitet pågående verkligen innebär att det gäller ett högre krav.

Förstöring av kopior (avsnitt 16.2.3)

Utredningen menar att förstöring av kopior av raderade uppgifter inte har någon betydelse för den enskildes rätt till en rättvis rättegång eftersom ingripande i cybermiljö inte syftar till att utreda brott. Myndigheten konstaterar dock att ingripanden enligt den föreslagna lagen kan ligga till grund för att förundersökning inleds. Lagen är även tillämplig när det pågår en förundersökning om det brott som ingripandet tar sikte på. Mot den bakgrunden anser myndigheten att frågan om hur förstöring av kopior av raderade uppgifter förhåller sig till den enskildes rätt till en rättvis rättegång måste övervägas vidare i det fortsatta lagstiftningsarbetet.

Tiden för ingripandet (avsnitt 17.1.2)

Utredningen föreslår att det i beslut om ingripande ska anges bl.a. när ingripandet senast ska genomföras och att tiden inte får överstiga en månad från dagen för beslutet. I den föreslagna författningskommentaren anförs att tidsgränsen avser den tid som får utnyttjas för genomförandet och inte den tid som själva ingripandet får ta. Myndigheten ställer sig frågande till vad det egentligen innebär och hur resonemanget förhåller sig till att beslut om blockering enligt utredningen behöver förlängas för att ingripandet ska få pågå i mer än en månad. Detta behöver förtydligas i det fortsatta lagstiftningsarbetet.

Aktsamhetskrav (avsnitt 18.3)

Även om den nya lagen möjliggör ändring, blockering och radering, och därmed syftar till att i fråga om tillgänglighet och riktighet påverka uppgifter i ett

informationssystem, anser myndigheteten att det bör ställas krav på att den generella informationssäkerheten i informationssystemet återställs när verkställigheten avslutas. Ett tänkbart alternativ är att införa ett aktsamhetskrav likt det som finns i lagen om hemlig dataavläsning. Det kan t.ex. handla om att den verkställande myndigheten, när verkställigheten avslutas, i den mån det är möjligt ska vidta åtgärder för att informationssäkerheten i informationssystemet ska hålla minst samma nivå som vid verkställighetens början.

Allmänt om behovet av underrättelse till enskilda (avsnitt 19.1.1)

En skyldighet att underrätta den enskilde bör gälla för alla ingripanden

Som framförts ovan måste beredandet av tillgång till ett informationssystem jämställas med hemlig dataavläsning i fråga om det integritetsintrång som åtgärden innebär för den enskilde. Av det skälet anser myndigheten att den enskilde, om det inte gäller sekretess för uppgifterna i underrättelsen, bör underrättas om alla former av ingripanden som innefattar beredande av tillgång till informationssystem. Myndigheten anser alltså att det inte är tillräckligt att den enskilde underrättas om blockering som pågår i mer än en månad och om radering.

En skyldighet att lämna en upplysning i informationssystemet bör införas

Det framgår inte av betänkandet om utredningen har övervägt att införa en skyldighet för den ingripande myndigheten att, i fall där det har beretts tillgång till ett informationssystem, lämna information i systemet eller på motsvarande sätt upplysa om att uppgifter ändrats, blockerats eller raderats. Myndigheten anser att en sådan upplysningsskyldighet bör införas. Det skulle bidra till att ingripandena får en mer öppen karaktär, vilket är i linje med utredningens avsikt. En upplysningsskyldighet skulle också bidra till att uppväga det rättighetsintrång som åtgärderna kan innebära, inte minst i förhållande till enskilda som berörs av ett ingripande men som inte skulle få en underrättelse enligt den föreslagna ordningen.

Eftersom det inte alltid kan förutsättas att den enskilde, vars uppgifter t.ex. har raderats, tar del av upplysningen anser myndigheten att skyldigheten endast bör vara ett komplement till det ovan berörda kravet på underrättelse till enskild. En upplysning bör alltså som utgångspunkt inte kunna ersätta en underrättelse.

Underrättelse i vissa fall (avsnitt 19.1.2)

Ändring och annan liknande åtgärd

Av de skäl som anförts ovan anser myndigheten att ändring och annan liknande åtgärd bör regleras på samma sätt som blockering. Det betyder att om lagstiftaren trots myndighetens invändning går vidare med förslaget att underrättelseskyldigheten ska omfatta blockering om den pågår längre än en månad, bör detsamma gälla även ändring och annan liknande åtgärd.

Så snart det lämpligen kan göras

Enligt den föreslagna författningskommentaren innebär kravet att en underrättelse ska lämnas så snart det lämpligen kan göras, att den ingripande myndigheten får dröja med underrättelsen om sekretess till skydd för den brottsutredande verksamheten gäller gentemot den enskilde och det skulle skada utredningen att underrätta om ingripandet. Enligt myndigheten bör en möjlighet att skjuta upp frågan om underrättelse på grund av sekretess tydligt regleras i lag, med angivande av de sekretessbestämmelser som kan tillämpas. Att göra frågan beroende av vad som anses lämpligt, utan närmare kriterier för bedömningen eller någon bortre tidsgräns för när underrättelse ska lämnas, är inte godtagbart.

Underlåtelse av underrättelse

Myndigheten anser att sekretess bör kunna föranleda underlåtelse av en underrättelse endast om det råder sekretess för uppgifterna i underrättelsen. Att i enlighet med utredningens förslag möjliggöra underlåtelse på den grunden att det föreligger sekretess enligt en viss bestämmelse, utan att uppgifterna i underrättelsen nödvändigtvis omfattas av sekretess, framstår inte som rimligt.

Vidare anser myndigheten att det kan ifrågasättas om 18 kap. 9 § offentlighets- och sekretesslagen (2009:400) skulle kunna utgöra skäl att underlåta underrättelse om ett ingripande. Det framgår nämligen inte av betänkandet hur uppgifter i en underrättelse skulle kunna motverka användningen av ett chiffer, en kod eller en liknande metod. Enligt myndigheten är det inte uppenbart hur sådana uppgifter som utredningen föreslår att en underrättelse ska innehålla skulle kunna röja vilka metoder som den verkställande myndigheten har använt.

Underrättelse om ett felaktigt beslut om radering (avsnitt 19.1.4)

Förslaget innebär att när en underrättelse av detta slag aktualiseras har åklagaren redan bedömt att ingripandet saknar grund. Det framstår därmed som överflödigt att även nämnden ska ta ställning i frågan. Av förslaget följer vidare att den enskilde underrättas om åklagarens ställningstagande, varför han eller hon själv, utan nämndens inblandning, har möjlighet att vända sig till t.ex. Justitiekanslern och framställa ett skadeståndsanspråk. Mot den bakgrunden anser myndigheten att det saknas skäl att införa en skyldighet att underrätta nämnden i denna situation.

Dokumentation (avsnitt 19.2)

För att det ska vara möjligt att utöva en effektiv tillsyn över tillämpningen av den nya lagen är det avgörande att de omständigheter som ligger till grund för ett beslut om ingripande dokumenteras. När det gäller hemliga och preventiva tvångsmedel framgår de omständigheter som en ansökan grundar sig på normalt i ett underlag som bifogas ansökan. Eftersom den föreslagna ordningen inte alltid kräver ett ansökningsförfarande bör det i det fortsatta lagstiftningsarbetet tydliggöras att dokumentationsskyldigheten normalt innefattar ett krav på att de omständigheter som ett beslut vilar på ska dokumenteras. Utan sådan dokumentation riskerar nämndens efterhandskontroll att bli helt beroende av befattningshavares minnesbilder, vilket inte är godtagbart.

Tillsyn (avsnitt 19.3)

Myndigheten delar utredningens bedömning att det behövs särskild tillsyn över ingripanden enligt den föreslagna lagen. Myndigheten tillstyrker vidare förslaget att tillsynen ska utövas av nämnden. För att tillsynen ska bli ändamålsenlig är det emellertid en förutsättning att lagens tillämpningsområde förtydligas i enlighet med det som myndigheten anfört ovan.

Förhållandet till andra brottsbekämpande åtgärder (avsnitt 20.1)

Myndigheten motsätter sig utredningens bedömning att det inte behövs någon reglering som begränsar användning av s.k. överskottsinformation. Som berörts ovan håller myndigheten inte med om att ingripanden enligt utredningens förslag normalt äger rum öppet. Vidare spelar det mindre roll i sammanhanget att åtgärderna inte syftar till att systematiskt och under längre tid inhämta information, eftersom regleringen inte innehåller något förbud mot inhämtning av uppgifter och ingripanden i princip kan verkställas under

lika lång tid som hemliga och preventiva tvångsmedel. Som utredningen framför kan resultatet av ett ingripande bli att det berikar inte bara en förundersökning utan också underrättelseverksamheten. Myndigheten ställer sig därför frågande till utredningens resonemang om att det, utom i de fall förundersökning inleds, inte kommer att bevaras något material som härrör från de sökningar som görs när tillgång bereds till ett informationssystem.

Myndigheten anser att det bör krävas åklagarbeslut för att uppgifter som inhämtas eller på annat sätt tillgängliggörs för de brottsbekämpande myndigheterna genom ett ingripande ska få användas för ett annat ändamål än det som legat till grund för ingripandet. Eftersom de föreslagna åtgärderna har ett helt annat syfte, och enligt förslaget är tillämpliga vid väsentligt mindre allvarlig brottslighet än preventiva och hemliga tvångsmedel, anser myndigheten att det därutöver bör föreskrivas att uppgifter endast får överlämnas till en förundersökning eller till underrättelseverksamhet om uppgifterna avser brott eller brottslig verksamhet som hade kunnat ligga till grund för tillstånd till hemliga respektive preventiva tvångsmedel. Utan en sådan ordning finns det risk för att ingripandena kan användas för att kringgå regelverket om hemliga och preventiva tvångsmedel.

Förhållandet till grundläggande fri- och rättigheter (avsnitt 21.3)

Utredningen berör endast i förbigående hur förslagen förhåller sig till yttrande- och informationsfriheten. Det anförs att det inte finns någon reell risk för att förslagen ska utgöra ett hot mot den fria åsiktsbildningen, bl.a. eftersom det i lagen införs både ett förbud mot att rikta ingripanden mot journalistisk verksamhet och en uttrycklig proportionalitetsregel. Enligt myndigheten är det emellertid uppenbart att det även vid ingripanden som görs utanför journalistisk verksamhet kan uppkomma konflikter med yttrande- och informationsfriheten. Frågan ställs på sin spets t.ex. vid publicering på en webbplats av uppgifter som skulle kunna aktualisera ansvar för olaga hot eller hets mot folkgrupp. Vad som i sådana fall är brottsligt eller endast ett uttryck inom ramen för den grundlagsskyddade yttrandefriheten är inte alltid en enkel bedömning. Att det då är upp till en särskilt utsedd befattningshavare vid Polismyndigheten, Säkerhetspolisen eller Tullverket – och inte en oberoende beslutsfattare – att bedöma om det är proportionerligt och även i övrigt finns förutsättningar att ändra eller blockera uppgifter, väcker frågan om den föreslagna ordningen verkligen är förenlig med regeringsformen.

Mot den anförda bakgrunden anser myndigheten att förslagens förhållande till grundläggande fri- och rättigheter bör analyseras vidare i det fortsatta lagstiftningsarbetet.

Ikraftträdande (avsnitt 22.1)

Den föreslagna regleringen kräver betydande förberedelser både för nämnden i egenskap av tillsynsorgan och för de brottsbekämpande myndigheterna som måste hinna säkerställa en rättssäker användning av de nya verktygen. Myndigheten, som konstaterar att det är fråga om helt ny och integritetskänslig reglering, betonar vikten av en ikraftträdandetidpunkt som tar hänsyn till behovet av dessa nödvändiga förberedelser.

Ekonomiska konsekvenser för Myndigheten för säkerhet och integritetsskydd (avsnitt 23.3.6)

Den föreslagna regleringen innebär att nämndens tillsynsområde utökas. Tillsynsuppgiften kommer dessutom att skilja sig från nämndens befintliga uppgifter. Myndigheten vidhåller det behov av resursförstärkningar som anges i betänkandet och anser att den föreslagna anslagshöjningen utgör en nödvändig miniminivå för att säkerställa en ändamålsenlig tillsyn.

Detta yttrande har beslutats av direktören Catharina Espmark efter samråd med Säkerhets- och integritetsskyddsnämnden. Föredragande har varit Viktor Wallén.

Catharina Espmark