UTSYN – FORUM FOR UTENRIKS OG SIKKERHET

# Høringssvar: PSTs etterretningsoppdrag og behandling av åpent tilgjengelig informasjon

## Innledning

Vil vil i dette høringssvaret belyse noen praktiske implikasjoner av forslaget til ny bestemmelse i politiregisterloven § 65 a om PSTs adgang til *behandling av åpent tilgjengelig informasjon til etterretningsformål*. Departementets høringsnotat redegjør for rettslige betraktninger knyttet til masseinnhenting og lagring av informasjon fra åpne kilder. I liten grad, foruten noen overordnede betraktninger, berøres bakgrunnen for lovforslaget og hvilke praktiske implikasjoner den foreslåtte ordlyden i lovbestemmelsen, vil medføre.

Slik ordlyden i forslaget til ny bestemmelse i politiregisterloven § 65 a er utformet i høringsnotatet, medfører dette lite forutberegnelighet for *hvem*, altså hvilke norske borgere, som vil bli rammet av informasjonsinnhentingen. Det er også uklart i hvilken *utstrekning* innhentingen av informasjon fra åpne kilder, vil forekomme. I tillegg er det i svært liten grad beskrevet hva som vil være *utløsende årsaker* for at PST vil innhente og lagre åpent tilgjengelig informasjon i inntil 15 år. Slik det fremgår av høringsnotatet, vil det i stor grad være opp til PST selv å vurdere hva som skal innhentes og når, basert på tjenestens egne vurderinger. Dette reiser flere praktiske og prinsipielle problemstillinger som burde vært berørt i departementets høringsnotat. Vi vil belyse noen slike problemstillinger i dette høringssvaret, med bruk av konkrete eksempler som knytter seg opp mot ulike former for trusler og kriminalitetsfenomener som faller inn under PSTs ansvarsområder.

## En endring av stor prinsipiell betydning

Innhenting av store mengder informasjon i bulk fra åpne kilder skal kunne utføres med hensikt å sette PST i stand til å utføre de oppgaver som tjenesten er pålagt etter politiloven § 17, og eventuelt med de foreslåtte endringene i bokstav a) og b). Det er nødvendig at PST som etterretningstjeneste settes i stand til å utføre sitt lovpålagte samfunnsoppdrag på en adekvat måte. Likevel reiser ordlyden i lovforslaget til politiregisterloven § 65 a, slik den står utformet i høringsnotatet, problemstillinger som berører kjerneverdier i vårt demokratiske samfunn. I særdeleshet forholdet mellom stat og borger, og forholdet til ytringsfriheten.

Fra at informasjon innhentet etter dagens politiregisterlov må være *formålstjenlig*, *nødvendig* og *relevant*, til at PST kan innhente og lagre åpent tilgjengelig informasjon i inntil 15 år uten en konkret vurdering av informasjonen som lagres, er i seg selv en endring av stor prinsipiell betydning. Dette åpner, slik departementet også påpeker, for potensielt svært omfattende lagring av norske borgeres opplysninger og ytringer på internett. I liten grad behandler det foreliggende høringsnotatet prinsipielle betraktninger knyttet opp imot en slik endring. I den grad det er behandlet, knyttes dette opp til forventningen om at PST må være i

stand til å utføre sitt etterretningsoppdrag. Det er imidlertid grunn til å anta at oppdraget kan la seg løse på en måte som lar PST innhente informasjon fra åpne kilder i bulk, samtidig som innsamlingen *begrenses* til det som vil være relevant for formålet med innhentingen. Dette vil utdypes nærmere i høringssvaret.

Skal man fravike prinsippet om at den konkrete informasjonen som innhentes skal vurderes opp imot formålet med innhentingen, så må det i det minste føres dokumentasjon om at nytteverdien, eller i det minste den antatte nytteverdien av en slik innretning, vil overstige de ulemper som inngrepet medfører. Slik dokumentasjon er fraværende i høringsnotatet, og det føres påstander som ikke noe sted nærmere blir dokumentert, slik som i kapittel 5.2.2, hvor departementet skriver: «*Etter departementets skjønn vil imidlertid dette tiltaket være en grunnleggende forutsetning for at PST skal kunne ivareta oppgaven med å kartlegge trender og utviklingstrekk og utarbeide analyser og etterretningsvurderinger av betydning for bekjempelsen av den alvorlige kriminaliteten som tjenesten har et særskilt ansvar for, herunder for å kunne utarbeide trusselvurderinger innenfor PSTs ansvarsområde.*»

I samme delkapittel (5.2.2) vurderer departementet det dit hen at risikoen for nedkjølende effekt på ytringsfriheten ikke tillegges avgjørende vekt, og at det vil etableres et sikkerhetsregime for tilgang til opplysningene. Dette er en vurdering som kan problematiseres. Ettersom store deler av den legitime norske samfunnsdebatten i dag foregår på internett og i sosiale medier, også om temaer som kan være kontroversielle og utenfor det "normale", burde det vært grundigere vurdert hvordan lovforslaget kan virke nedkjølende på samfunnsdebatten og deltakernes vilje til å ytre seg. Spesielt vil dette være tilfellet ettersom opplysningene *kan* lagres i opptil 15 år, noe som er svært lang lagringstid.

Ett av de få eksemplene som fremkommer i høringsnotatet gjelder journalister som kartlegger russiske GRU-offiserer i Norge, basert på et nedlastet russisk adresseregister. Dette er opplysninger av en helt annen karakter enn eksemplene som vi vil problematisere i dette høringssvaret, og departementets eksempel berører ikke problemstillinger knyttet til innhenting av informasjon om norske borgere. Det bør være mulig å utforme en lovbestemmelse som gir PST anledning til å innhente åpent tilgjengelig informasjon om både fremmede staters påvirknings-, etterretnings- og spionasjevirksomhet samt terror, ekstremisme og radikalisering, men som likevel gir mer forutberegnelighet for norske borgere som får data samlet inn, til tross for at de faller utenfor formålet med innhentingen.

Begrensninger knyttet til innhentingen vil uansett måtte utføres av praktiske årsaker og konkrete vurderinger – slik som *hvor*, altså hvilke nettsteder og plattformer som det vil være formålstjenlig å innhente informasjon fra, og av praktiske hensyn, som datalagringskapasitet. Ettersom den foreslåtte politiregisterloven § 65 a åpner opp for bulkinnhenting uten særlig begrensninger, bør departementet vurdere en innretning på ordlyden som legger opp til at det må foretas *konkrete vurderinger* av *eksplisitte vilkår*, før innhentingen finner sted.

Det bør i den forbindelse gjøres et grundigere arbeid for å identifisere hva som kan være relevante vilkår uten at PSTs forutsetninger til å utføre arbeidet, reduseres. *Nøkkelbegreper* og *identifikatorer* som er relatert til de trussel og kriminalitetsfenomen som man har behov for å innhente informasjon om, kan være sentralt i dette arbeidet.

## Ulik innhentingspraksis ved ulike trusler

Slik vi ser det, er det forskjell på hvordan de ulike truslene og kriminalitetsfenomenene som ligger innenfor PSTs ansvarsområde, kan utarte seg. Innhenting av informasjon i bulk fra åpne kilder, vil derfor måtte innrettes på ulike måter mot ulike trusselaktører og fenomener. Innhenting fra åpne kilder vil uansett måtte utføres i *tillegg til* ordinær etterretningsaktivitet.

Digitale påvirkningsoperasjoner utført av fremmede aktører mot norske borgere på sosiale medier, vil trolig måtte ha et annet omfang av innhenting enn dersom det er materiale tilknyttet ekstremisme, radikalisering og terror som skal avdekkes. Tilsvarende vil andre former for trusler som PST har ansvar for å motvirke kunne ha mindre nytteverdi av data fra åpne kilder dersom trusselaktørene utelukkende opererer skjult og fordekt. Departementet argumenterer med at lovforslaget vil gjøre PST bedre i stand til å avdekke "ukjente trusler". Dette reiser flere dilemmaer all den tid det ukjente ikke har materialisert seg i noe konkret. Implisitt ligger det da en forventning om at PST må være stand til å avdekke "det ukjente" noe som samtidig vil forutsette at mest mulig må gjøres kjent. Vi anbefaler at innhentingen primært retter seg mot *konkrete størrelser*, dersom lovgiver innfører slik bulkinnhenting.

## Påvirkningsoperasjoner utført på sosiale medier

Digitale påvirkningsoperasjoner utført på sosiale medier retter seg ofte mot temaer som representerer konfliktlinjer i samfunnet. Dette kan være politiske saker som engasjerer enhver borger. Dersom PST skal settes i stand til å identifisere slike påvirkningsoperasjoner, vil innhentingen potensielt måtte berøre svært mange norske borgere som deltar i den digitale samfunnsdebatten. Budskap som fremmes som del av en påvirkningsoperasjon kan målrettes mot enkeltindivider og grupper av mennesker. De kan også skreddersys både med tanke på budskap og målgruppe, for å spille på eksisterende konfliktlinjer. På den måten kan budskap som er del av en påvirkningsoperasjon virke splittende ved at de forsøker å utnytte allerede eksisterende uenigheter, eller de kan skape usikkerhet rundt hva som er sant.[1] Dersom man ikke kan enes om faktagrunnlaget blir politikkutvikling svært utfordrende. Det er derfor i det norske demokratiets interesse at våre etterretningstjenester settes i stand til å identifisere påvirkningsoperasjoner som utføres av fremmede aktører.

[1] Bergh, A. (2020). *Påvirkningsoperasjoner i sosiale medier – oversikt og utfordringer*. FFI-rapport. https://publications.ffi.no/nb/item/asset/dspace:6867/20-01694.pdf

Påvirkning ved bruk av mis- eller desinformasjon kan også utøves av aktører innenfor statens grenser. Dette er i dag ikke straffbar aktivitet. Slik påvirkning *kan* også ha store negative effekter på konfliktnivået, i likhet med illegitim påvirkning utført av fremmede stater. I en studie av russisk påvirkning under den amerikanske valgkampen i 2016, fant forskere ved Harvard University ut at bevisene på russisk påvirkning var sterk. Bevisene rundt *effektene* av påvirkningen var derimot mangelfull. Studien konkluderer med at desinformasjonen som ble spredt av aktører internt i USA, var et like stort problem. De russiske aktørene spredte i hovedsak innhold som allerede ble delt i alternative og tradisjonelle medier.[2] Hvorvidt PST skal ha mulighet til å avdekke denne formen for *innenlands* påvirkning er ikke diskutert i høringsnotatet, men er likevel en svært aktuell problemstilling.

Påvirkningsoperasjoner foregår ikke kun i forbindelse med demokratiske valgprosesser. De kan også foregå over lengre tid og kan dermed gradvis påvirke holdninger og oppfatninger om bestemte temaer i samfunnet, uten at den som utsettes for mis- og desinformasjon er bevisst påvirkningen.[3] Operasjonene kan være rettet mot konflikt- og skillelinjer som er vedvarende i samfunnet, og som derfor er enklere å identifisere for en fremmed trusselaktør som befinner seg utenfor statens grenser. I Norge vil saker som klima, innvandring, forholdet mellom nord og sør, by og land, forholdet til EU/EØS og NATO/USA være potensielle stridstemaer. Når samfunnet står overfor større endringer og omstillinger, som i dag, vil det kunne være enklere å utnytte eksisterende konfliktlinjer. I tillegg kan de utnytte konkrete og dagsaktuelle saker, som kan bidra til å undergrave troverdighet. Dette indikerer at det vil være mulig å identifisere en rekke *nøkkelbegreper* som kan utnyttes i forbindelse med illegitim påvirkningsvirksomhet. Samtidig kan det være slik at mange av begrepene vil være nært knyttet opp mot temaer som ellers blir benyttet i den legitime samfunnsdebatten.

For å illustrere noen sentrale dilemmaer knyttet til temaet: Vil kommentarfeltet til VG.no under noen omstendigheter kunne være av interesse for innhentingen? Hva med en Facebook-gruppe med svært mange medlemmer som har et tema av politisk aktualitet, som kan utnyttes av en trusselaktør? For eksempel Facebook-gruppen "Vi som krever billigere strøm" med 524 000 medlemmer? Hva med Twitter-meldinger fra brukere i Norge med det som i enkelte miljøer kan oppleves som kontroversielle budskap, og som deles i stor utstrekning, oppnår mange visninger, "retweets" og "likes"? Fremmede aktører *kan* benytte slike nettsteder og plattformer for å spre fordreid eller ukorrekt informasjon, med hensikt å påvirke en legitim samfunnsdebatt. Vil det være akseptabelt at PST innhenter informasjon som nevnt ovenfor, for å kunne avdekke forsøk på illegitim påvirkning fra fremmede aktører?

[2] Benkler, Y., Faris, R. & Roberts, H. (2018). *Are the Russians Coming?*. https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190923624.001.0001/oso-9780190923624-chapter-8

[3] Sivertsen, E., Hellum, N., Bergh, A. & Bjørnstad, A. (2020). *Hvordan gjøre samfunnet mer robust mot uønsket påvirkning i sosiale medier.* FFI-rapport. https://publications.ffi.no/nb/item/asset/dspace:7086/21-01237.pdf

Departementet kunne med fordel diskutert noen slike praktiske eksempler og avveininger i høringsnotatet. Dette for å gi en bedre og grundigere begrunnelse *dersom* departementet likevel mener at innhentingen ikke skal begrenses i lovens ordlyd. Alternativt kan et bedre faktagrunnlag føre til at departementet kommer frem til en annen konklusjon. Dette er til syvende og sist politiske avveininger mellom ulike samfunnshensyn og -verdier.

## Ekstremisme, radikalisering og terror

Når det gjelder spredning av materiale knyttet til ekstremisme, radikalisering og terror, vil meldingene og budskapene ofte kunne være knyttet til noe mer begrensede nettsteder og plattformer sammenliknet med påvirkningsoperasjoner. Departementet nevner selv "chan-foraer" i sitt høringsnotat. Det er derfor grunn til å anta at færre norske borgere som deltar i den ordinære samfunnsdebatten vil få sine ytringer og sin kommunikasjon samlet inn når innhentingen fra åpne kilder retter seg mot ekstremisme, radikalisering og terror.

I en amerikansk studie fra *National Consortium for the Study of Terrorism And Responses to Terrorism* vises det til at mye innsats gjøres fra plattformaktørenes side, slik som Facebook, Twitter og YouTube, for å fjerne ekstremistisk og radikaliserende materiale. Dette kan ifølge studien på sikt bidra til at miljøene flytter over til mindre og/eller mer lukkede plattformer.[4] I så tilfelle vil det på sikt bli et tydeligere skille mellom hvilke aktører som befinner seg på, og (mis)bruker de ulike plattformene. Dette *kan* på den ene siden bidra til at det blir enklere å rette innhentingen fra åpne kilder mot de bestemte miljøene man ønsker informasjon om, og at færre tredjepersoner blir eksponert for det radikaliserende materialet på mer allment tilgjengelige plattformer. *Dersom* utviklingen inntreffer, vil innsamlingen fra de relevante åpne kildene i større grad kunne målrettes, uten å ramme legitim samfunnsdebatt.

Et kjent eksempel på forflytningen fra plattformer som Facebook og Twitter over til alternative plattformer, finner vi i forbindelse med Trump og hans tilhengeres overgang til den mindre kjente plattformen *Parler*. I en artikkel i *The New York Times* fremkommer det at utestengningen av Trump fra Twitter og fjerningen av meldinger som inneholdt misinformasjon, var sentrale årsaker til forflytningen. Etter at dette ble kjent, fjernet Apple og Google applikasjonen *Parler* fra sine app-butikker. Deretter ble *Parler* tvunget bort fra *Amazon Web Service's* skytjenester, hvor selskapet leide infrastruktur.[5] Dette er bare ett eksempel som viser hvordan de globale aktørene responderer på (mis)bruk av egne plattformer, noe som igjen presser enkelte miljøer over på alternative plattformer.

[4] Jensen, M., James, P., LaFree, G., Safer-Lichtenstein, A. & Yates, E. (2018). *The Use of Social Media by United States Extremists*. START. www.start.umd.edu/pubs/START_PIRUS_UseOfSocialMediaByUSExtremists_ResearchBrief_July2018.pdf

[5] Nickas, J. & Alba, D. (9, januar 2021). *Amazon, Apple and Google Cut Off Parler, an App That Drew Trump Supporters*. The New York Times. https://www.nytimes.com/2021/01/09/technology/apple-google-parler.html

Dersom innhentingen fra åpne kilder skal begrenses, vil det være avgjørende *hvordan* innhentingen begrenses. Enten at den f.eks. retter seg mot spesifikke nettsteder/plattformer eller at det defineres *terskelverdier* for hva som er å anse som en *identifikator* på budskap som kan knyttes opp mot for eksempel ekstremisme. Slike vurderinger vil uansett måtte gjøres av PST selv i forbindelse med innhenting og/eller analyse av dataene, uavhengig av type trussel- og kriminalitetsfenomen. Derfor er det grunn til å stille spørsmål ved om det også ikke burde være noe mer direkte demokratisk kontroll over innhentingspraksisen, ved å utforme en ordlyd i lovforslaget som bidrar til større klarhet. Ettersom det ikke vil gis innsyn i opplysningene som innhentes fra åpne kilder, vil det være et større behov for offentligheten å vite hva som er utgangspunktet for innhentingen. Dette betyr ikke at offentligheten trenger å få innsikt i konkrete indikatorer og nøkkelord som danner utgangspunkt for innhentingen, men at det i lovens ordlyd gis mer forutsigbarhet for hvordan innhentingen begrenses. Dette kan igjen ha positive virkninger for legitimiteten til virkemiddelbruken.

## Om målrettet innhenting basert på indikatorer

I en studie fra 2017 skrevet av ansatte ved *Totalförsvarets forskningsinstitut (FOI)* i Sverige om innhenting og analyse av ekstremistisk innhold fra åpne kilder, tar de i bruk "web crawlers" for å laste ned *relevante data*. Dataene blir analysert ved hjelp av såkalt "natural language processing" for å identifisere tegn på voldelig ekstremisme. Ved identifisering av nøkkelord i sammenheng med hverandre, bidrar algoritmene til å identifisere tegn på radikalisering. Teknikken gjør det mulig for en analytiker å behandle relevante data i de enorme mengdene informasjon som tilgjengeliggjøres på internett. En slik tilnærming må ta utgangspunkt i *forhåndsdefinerte begreper* som ekstremister benytter seg av. Studien påpeker at innhenting av store datamengder vil kunne føre til at det forekommer mange falske positiver, men dersom fokuset blir begrenset til nettsteder og fora som er kjent for å inneholde ekstremistisk materiale, reduseres omfanget av falske positiver. Dette kan ha flere positive effekter ettersom større deler av samfunnet blir skånet fra urettmessig innhenting samtidig som at analytikerne får tilgang på flere relevante, og mindre irrelevante data.[6]

En annen studie fra 2013, skrevet av ansatte ved det samme forskningsinstituttet, beskriver hvordan solo-terrorister kan identifiseres ved bruk av teknikker som beskrevet ovenfor. På grunn av de enorme mengdene informasjon som finnes på internett, må man begrense søkene og fokusere på mindre deler av internett. Siden mange ekstremistiske sider allerede er godt kjente, og de ulike sidene ofte lenker mellom hverandre, kan disse gjennomsøkes med bruk av "web crawlers". På denne måten kan man lage et stort nettverk av nettsteder som bør analyseres nærmere. Studien anbefaler å ha en forhåndsdefinert liste av begreper som den søker etter på de ulike nettstedene. Hvis tilstrekkelig mange nøkkelbegreper

[6] Johansson, F., Kaati, L, & Sahlgren, M. (2017). *Detecting Linguistic Markers of Violent Extremism in Online Environments*. https://www.foi.se/download/18.7fd35d7f166c56ebe0b1000a/1542623725601/Detecting-linguistic-markers_FOI-S--5452--SE.pdf

identifiseres, blir nettstedet markert som interessant og dataene innhentens. Dersom nettstedet blir markert som ikke-relevant, blir lenker og innhold forkastet.[7]

På samme måte kan man se for seg at PST tar utgangspunkt i en liste av nøkkelbegreper som identifiserer relevante nettsteder, og at hele eller deler av innholdet på de relevante nettstedene lagres. En slik liste kan revideres av interne og eksterne kontrollmekanismer, slik at det etableres en form for demokratisk kontroll over innhentingen samtidig som at PST gis forutsetninger til å løse sine lovpålagte oppgaver. En innretning som dette må imidlertid understøttes av teknologiske løsninger som *muliggjør* innhentingen som er beskrevet her.

Hvilken teknologi som velges vil derfor også påvirke hva som er praktisk gjennomførbart. Derfor må lovteksten utformes på en måte som muliggjør operasjonalisering, altså å utvikle og/eller anskaffe informasjonssystemer og applikasjoner som understøtter behandlingen.

## Forholdet mellom innenlands- og utenlandsetterretning

I høringsnotatet kapittel 2.1 står det følgende: «*PST har i dag ikke tilsvarende muligheter som E-tjenesten til å bidra med rettidig og relevant innenlandsetterretning.*» Departementet skriver videre at: «*tjenestens mulighet til å behandle informasjon for å bidra med generelle etterretningsvurderinger og analyser knyttet til trender og utvikling i trusselbildet, er begrenset.*»

Det vil være naturlig at PST ikke uten videre kan benytte tilsvarende kapabiliteter mot egne borgere som det Etterretningstjenesten kan benytte mot trusselaktører utenfor egen stat. Etter Etterretningstjenesteloven § 4-1 har Etterretningstjenesten et forbud mot bruk av innhentingsmetoder mot personer i Norge. Dette gjelder for alle innhentingsmetoder beskrevet i Etterretningstjenesteloven kapittel 6, herunder også fra åpne kilder etter § 6-2.

En følge av at norske borgere i utgangspunktet må kunne forvente et sterkere vern mot innhenting av informasjon fra egen stat sammenliknet med hva utenlandske borgere kan forvente fra en fremmed etterretningstjeneste, tilsier at PSTs og Etterretningstjenestens kapabiliteter ikke uten videre kan sidestilles. PST kan allerede i dag behandle opplysninger om egne borgere ved målrettet innhenting av informasjon fra åpne kilder. Spørsmålet her er i hvilken *utstrekning* den aktuelle kapabiliteten som diskuteres også skal kunne benyttes mot nettsteder der det foregår helt legitim aktivitet og samfunnsdebatt.

Når det gjelder fenomenet påvirkningsvirksomhet, som dette lovforslaget har til hensikt å gi PST bedre forutsetninger for å identifisere, er denne aktiviteten i utgangspunktet illegitim

[7] Brynielsson, J., Horndahl, A., Johansson, F., Kaati, L., Mårtenson, K. & Svenson, P. (2013). *Harvesting and analysis of weak signals for detecting lone wolf terrorists*. Security Informatics 2013, 2:1. https://www.foi.se/download/18.7fd35d7f166c56ebe0b1002d/1542623788802/Harvesting-and-analysis_FOI-S-4594-SE.pdf

når den utføres av aktører som befinner seg utenfor Norges grenser. Påvirkning som utføres av og på vegne av borgere, organisasjoner og interessegrupper som befinner seg innenfor statens grenser, er i utgangspunktet å anse som legitim. Det er i den forbindelse grunn til å stille spørsmål om påvirkningsvirksomhet, utført av fremmede stater mot norske borgere, primært bør være et ansvar som faller inn under Etterretningstjenestens ansvarsområde.

Et unntak vil være påvirkning som utføres *av norske borgere på vegne av en fremmed etterretningstjeneste*, slik de nylig foreslåtte straffebudene i Straffelovens § 130 og § 130 a har til hensikt å forby. Dersom Etterretningstjenesten skal være den aktøren som primært innhenter informasjon relatert til påvirkningsoperasjoner utført av fremmede stater mot Norge, taler dette for at PSTs innhenting fra åpne kilder relatert til påvirkningsoperasjoner, kan avgrenses. Dette er imidlertid ikke uproblematisk, da Etterretningstjenesten har et forbud mot innhenting av opplysninger tilhørende norske borgere etter § 4-1.

For å være i stand til å identifisere digitale påvirkningsoperasjoner rettet mot den norske samfunnsdebatten, må minst én av etterretningstjenestene kunne behandle informasjon om både fremmede trusselaktører, óg norske borgere. Hvordan denne problemstillingen skal løses på en adekvat måte, slik at det er samsvar mellom lov, organisering og praksis, bør være tydelig. Disse forholdene er ikke nærmere berørt i departementets høringsnotat. Det er ikke en ønskelig situasjon dersom det eksisterer juridiske og organisatoriske “hull” mellom sikkerhets- og etterretningstjenestene som kan utnyttes av fremmede trusselaktører.

## Avsluttende bemerkninger

Vi ser positivt på at det foreslås lovhjemler som setter sikkerhets- og etterretningstjenestene våre bedre i stand til å utføre sine lovpålagte oppgaver. Det er sentralt at innretningen på lovforslagene som fremlegges er av en slik karakter at de faktisk bidrar til å løse den samfunnsutfordringen som lovforslaget har til hensikt å løse. Samtidig må de være utformet og begrunnet på en måte som gjør det mulig for offentligheten å gjøre seg opp en reell formening om forholdet mellom nytteverdi og ulemper av inngrepet. Dette er viktig for å sikre at virkemiddelbruken har nødvendig legitimitet.

Et lovforslag som griper direkte inn i forholdet mellom stat og borger og som sterkt berører ytringsfriheten, må være grundig utredet. Vi håper dette høringssvaret bidrar med innspill som gjør det mulig å utforme et bedre begrunnet lovforslag, med en klarere ordlyd.

Hedda Langemyr, daglig leder i UTSYN - Forum for utenriks og sikkerhet

Simen Bakke, fagprofil i UTSYN - Forum for utenriks og sikkerhet