Norges nasjonale institusjon
for menneskerettigheter

Høringsuttalelse om forslag til ny lov om Etterretningstjenesten

Deres ref.: 2016/2773-5/FD II 4/SIH

Postadresse: Postboks 299 Sentrum, 0103 Oslo – **Tlf:** (+47) 23 31 69 70 – **Webside:** www.nhri.no

Innhold

1. Innledning

Vi viser til høringsbrev fra Forsvarsdepartementet med høringsfrist 12. februar 2019.

Norges institusjon for menneskerettigheter («NIM») har som hovedoppgave å fremme og beskytte menneskerettighetene i tråd med Grunnloven, menneskerettsloven og den øvrige lovgivning, internasjonale traktater og folkeretten for øvrig. NIM skal blant annet gi råd til Stortinget, regjeringen og andre offentlige organer om gjennomføringen av menneskerettighetene. Innspill i relevante høringsprosesser er en sentral del av vårt mandat. I utgangspunktet er det ikke nødvendigvis NIMs oppgave å uttale seg om hensiktsmessigheten eller prioriteringen av virkemidler for å oppfylle menneskerettslige forpliktelser.

1.1. Høringsnotatet og forslaget

Forslaget til ny lov om Etterretningstjenesten (E-tjenesten) er omfattende. Det gjelder E-tjenestens virksomhet og metoder generelt. Det foreslås blant annet innført et system for såkalt «tilrettelagt innhenting», som innebærer bulkinnsamling av data fra kabler som krysser landegrensene.

Som et utgangspunkt er NIM positive til at det fremmes en ny lov om E-tjenesten som med større grad av åpenhet beskriver E-tjenestens kapasiteter, etterretningsbehov og arbeidsmåte. Dette er viktig for å sikre den nødvendige tillit til norsk etterretning. Dette åpner også opp for større grad av offentlig debatt rundt E-tjenestens metodebruk, en debatt som har demokratisk verdi.

Forslaget reiser mange teknisk og juridisk kompliserte spørsmål. Bildet kompliseres av at både relevant teknologi og jus er i fortløpende endring. Blant annet er relevante dommer fra Den europeiske menneskerettsdomstol (EMD), som gir grunnleggende premisser til drøftelsen av de menneskerettslige rammene, påanket og fremmet til behandling for storkammeret i EMD, jf. Big Brother Watch v. Storbritannia og Centrum for Rättvisa v. Sverige. Dette gjør de rettslige premissene for diskusjonen av forslaget mer uklare.

På grunn av omfanget av forslaget og høringsfristen, har NIM i herværende høringssvar måttet prioritere enkelte temaer. At andre temaer ikke er kommentert, kan ikke tas til inntekt for at forslaget støttes eller at det anses uproblematisk i lys av menneskerettslige krav. NIM vil i sin høringsuttalelse fokusere på sentrale menneskerettslige aspekter ved lovforslaget, særlig vedrørende tilrettelagt innhenting. Vi tar imidlertid forbehold om å komme tilbake med ytterligere kommentarer knyttet til de øvrige deler av forslaget.

At NIMs kommentarer ikke kan forstås uttømmende, henger også sammen med at NIM synes det er vanskelig å overskue hva forslaget innebærer – både rettslig og faktisk – og slik overskue hvor stort inngrep forslaget reelt kan innebære i relevante menneskerettigheter som retten til privatliv, personvernet og ytringsfriheten, herunder kildevernet.

Oversiktsvansker er et signal NIM har mottatt fra flere høringsinstanser. Dette er et signal departementet bør ta på alvor. Mangel på transparens og oversikt vil kunne ha menneskerettslige implikasjoner i seg selv.

1.2. Overordnede premisser for interesseavveiningen

Forslaget om tilrettelagt innhenting balanserer som et utgangspunkt to viktige interesser, som begge er vanskelige å måle. På den ene siden har staten ved E-tjenesten et behov for virkemidler for å kunne forsvare norske interesser mot blant annet cybertrusler og hybride trusler. Det vises i denne forbindelse til E-tjenestens nylige vurdering av aktuelle sikkerhetsutfordringer, offentliggjort 11. februar 2019. Norge er et av verdens mest digitaliserte samfunn, og hendelser i den senere tid, herunder Helse Sør-Øst-saken, har avdekket sårbarhet for angrep på vesentlig digital infrastruktur. Helse Sør-Øst-saken er et godt eksempel, fordi det viser at også privatlivsvernet vil være under trussel dersom sensitiv helseinformasjon ikke tilstrekkelig beskyttes mot målrettede dataangrep. Gitt at store deler av E-tjenestens virksomhet er hemmelig, er det også vanskelig for utenforstående å overprøve tjenestens behovsvurderinger og effekten av de tiltak som foreslås for å oppnå målet om å bedre beskytte norske interesser, særlig i den digitale sfære. Derfor er det så viktig at E-tjenesten er så åpne som de kan, både om sårbarheter, kapasiteter og udekkede etterretningsbehov, slik at dette så langt det er mulig kan underlegges reell demokratisk kontroll. Samtidig har NIM forståelse for at det er sider ved E-tjenestens virksomhet som ikke kan belyses. Departementet skal berømmes for å gå lenger enn tidligere i å belyse ulike forhold i denne sammenheng i høringsnotatet. NIM viser blant annet her til drøftelsen av alternativer til tilrettelagt innhenting i forslaget under punkt 11.7, som gir en systematisk fremstilling av etterretningsverdien av mindre inngripende alternativer. Dette er i utgangspunktet tillitsvekkende.

På bakgrunn av blant annet disse beskrivelsene, legger NIM som et utgangspunkt til grunn at E-tjenesten har et reelt behov for å innføre et system med tilrettelagt innhenting, primært for å beskytte Norge mot hybride trusler og cyberangrep. NIM har heller ingen forutsetning for å overprøve høringsnotatets premiss om at dette ikke generelt kan gjøres på noen mindre inngripende måte som gir tilsvarende etterretningsverdi. Når det er sagt, er det neppe noen menneskerettslig plikt å innføre et slikt system.[1]

På den andre siden medfører lovforslaget et stort inngrep i nordmenns privatliv og personvern. I denne vektskålen ligger også vernet av ytringsfriheten, herunder pressefriheten og kildevernet, et menneskerettsområde som er avgjørende for et fungerende demokrati, og som forslaget har flere klare sider til.

Forslaget om tilrettelagt innhenting innebærer et grunnleggende skifte fra et utgangspunkt om at E-tjenesten kun i unntakstilfeller befatter seg med nordmenns

[1] Høringsnotatet side 221.

kommunikasjon, til at dette vil bli en tilnærmet hovedregel, fordi praktisk talt all norsk kommunikasjon flyter over landegrenser. Det innebærer også en grunnleggende endring fra et normativt utgangspunkt om at staten ikke skal benytte den type inngripende virkemidler annet enn i tilfeller hvor en bestemt person er under konkret mistanke for å ha utført noe straffbart, og etter en individuell vurdering av en dommer. At det er teknisk umulig å innrette systemet basert mer målrettede kriterier fordi man må ha høystakken for å finne nålen, endrer ikke på dette.

Konsekvensen for personvernet og privatlivsbeskyttelsen er vanskelig å forutse. I hvilken grad dette vil få såkalt nedkjølende effekt på både den enkeltes ytringer og andre handlinger, og ikke minst på kommunikasjon som er gitt særlig menneskerettslig beskyttelse, som for eksempel knyttet til kildevernet og forholdet mellom advokat og klient, lar seg heller ikke kvantifisere. Den nedkjølende effekten vil i stor grad avhenge av hvor informerte nordmenn faktisk er om E-tjenestens kapasiteter og gjeldende rettsikkerhetsgarantier, og ikke minst om den iboende faren for misbruk som ethvert slikt system innebærer, manifesterer seg. Som et generelt utgangspunkt, mener NIM at det er en svakhet ved høringsnotatet at de negative konsekvensene ved innføring av tilrettelagt innhenting, underspilles. NIM er her enig med Datatilsynets høringsuttalelse i at man i vurderingen av den potensielt nedkjølende effekten ikke bare kan ta utgangspunkt i «et informert kunnskapsgrunnlag knyttet til hva Etterretningstjenesten lovlig kan og ikke kan gjøre.» Slik forslaget er lagt opp, er det illusorisk å tro at nordmenn flest vil ha et slikt kunnskapsgrunnlag. Slik loven er utformet er dette heller ikke mulig, fordi det er en rekke detaljer knyttet til den konkrete innretningen og tjenestens tekniske kapasiteter som ikke er allment tilgjengelig. Den nedkjølende effekten av innføringen av tilrettelagt innhenting vil med andre ord potensielt virke videre enn en rent kjølig analyse av tiltaket basert på et informert kunnskapsgrunnlag skulle tilsi, fordi det fort vil etterlate et inntrykk av at E-tjenesten driver med vid masseovervåkning. På samfunnsnivå må dette likevel adresseres som en effekt av innføringen, hvis ikke blir dette en effekt som ingen gis eierskap til eller ansvar for.

Det er imidlertid en kjensgjerning at den nedkjølende effekten vanskelig lar seg måle og vekte i en avveining mot det mer håndfaste hensynet til å beskytte borgerne mot hybride trusler og cyberangrep. Det er derfor presist formulert når EMD operasjonaliserer dette som et dilemma hvor «a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it.» Dette er et reelt dilemma som må tas på alvor.

NIM mener det er et helt sentralt utgangspunkt for diskusjoner om forslaget at staten viser en reell forståelse for de sterke implikasjonene dette kan ha for personvern og privatliv, på samme måte som at staten har fremhevet viktigheten av at motstandere av forslaget må anerkjenne E-tjenestens behov og begrunnelser for å innføre tiltaket.

Uavhengig av hvilken side man ser dette fra, er utgangspunktet her at det er tale om krevende avveininger hvor vekten av argumentene i begge vektskåler er vanskelig å operasjonalisere og måle. Fordi disse materielle avveiningene er så krevende, har EMD i sin tilnærming til problematikken lagt vesentlig vekt på hvorvidt slike systemer og kapasiteter innføres med strenge, operative og effektive rettsikkerhetsmekanismer. EMD har altså i vesentlig grad vektlagt de prosessuelle og regulatoriske sidene ved slike tiltak.

I skrivende stund er det rettslig uavklart om og under hvilke betingelser EMD vil akseptere bulkinnsaming. I ikke-rettskraftige dommer har domstolen lagt til grunn at det ikke finnes noen absolutte skranker mot innføringen av et system, men at det krever at sterke og effektive kontrollmekanismer er på plass. Det er i så fall grunn til å tro at EMD vil tilkjenne staten en ganske vid skjønnsmargin med hensyn til valg av system. Testen vil trolig bestå i om det er oppstilt mekanismer som i tilstrekkelig grad motvirker misbruksrisikoen. Hvilke mekanismer som er tilstrekkelige kommer an på misbruksrisikoen ved det aktuelle systemet. Hensett til omfanget av overvåkingskapasiteten må den iboende misbruksrisikoen i bulkinnsamlingssystemer anses svært høy. Det vil kunne stille svært strenge krav til sikkerhetsmekanismer, muligens også strengere krav enn EMD har lagt til grunn i tidligere saker.

Som også påpekt av Lysne II-utvalget, er det hårfine avveininger det er snakk om, og selv små justeringer i de aktuelle rettsikkerhetsmekanismene vil kunne få som konsekvens at et slikt system anses menneskerettstridig. Det er derfor grunnleggende i den videre prosessen at alle steiner snus for å sørge for at reelle og operative garantier mot misbruk og at det etableres effektive rettsmidler ved rettsbrudd.

Dette har også vært premissgivende for utformingen av NIMs høringsuttalelse. Vi har tatt utgangspunkt i forslaget slik det foreligger, og bestrebet oss på å komme med konkrete innspill til hvordan forslaget bedre kan ivareta menneskerettslige krav. Vi har lagt stor vekt på den grunnleggende betydningen av å sikre tilstrekkelig kapasitet og kompetanse hos kontrollmekanismene.

Vi har vanskelig for å se at det i denne kompliserte konteksten med raskt endrede rettslige og tekniske premisser er mulig å fremme noen absolutte synspunkter på hvorvidt forslaget (kun basert på hvordan det ser ut på papiret) vil stå seg i en menneskerettslig prøving, men vi mener at forslaget må endres på en rekke punkter for å bedre ivareta menneskerettslige krav.[2]

[2] Til det er vurderingen for kompleks. Den vil bero på en konkret helhetsvurdering av hvordan dette vil fungere i praksis, herunder omfanget av bruken, avgrensninger av søkekriterier, hvor operative rettsikkerhetsmekanismene faktisk vil være, herunder hvor effektive kontrollmekanismer EOS-utvalget klarer å bygge inn i sine systemer, i tillegg til hvordan praksis i EMD utvikler seg.

1.3. Hovedpunkter i høringsuttalelsen og videre fremstilling

Under punkt 2 og 3 behandler vi lovutkastets omtale av Norges menneskerettighetsforpliktelser anvendt på E-tjenestens virksomhet. NIM mener det kan være grunn til å vurdere om lovteksten burde være basert på Norges menneskerettighetsforpliktelser, både materielt og jurisdiksjonsmessig.

I punkt 4 vurderer vi forholdet mellom forslaget om tilrettelagt innhenting og retten til privatliv. Vi mener det er rettslig uavklart om og eventuelt under hvilke betingelser det kan innføres et system for bulkinnsamling av elektronisk kommunikasjon. I den grad et slikt system kan innføres, mener vi det er alvorlige svakheter ved lovutformingen og kontrollmekanismene som må utbedres.

Punkt 5 omhandler ytringsfriheten og kildevernet. Her påpeker vi at det er vanskelig å overskue hvor stort inngrep forslaget kan innebære i kildevernet og dermed også ytringsfriheten. Vi påpeker også her på svakheter ved lovutformingen og kontrollmekanismene.

2. Omtale og anvendelse av menneskerettigheter

2.1. Folkerettslige rammer

På side 26 i høringsnotatet sies det: «I væpnet konflikt vil bestemmelsene i krigens folkerett gjelde som ytre ramme for hvordan etterretningsvirksomhet kan gjennomføres.» Dette er upresist. I mange situasjoner med væpnet konflikt[3] kan de militære styrkene likevel være involvert i politi-operasjoner, og E-tjenesten kan bidra til slike. Er formålet med en konkret operasjon rettshåndhevelse (for eksempel pågripelse av en kriminell) i motsetning til utøvelse av fiendtligheter, er det menneskerettighetene som gjelder som ytre rammer for virksomheten.

2.2. Formålsbestemmelsen i § 1-1

Forslagets § 1-1 bokstav c sier at e-tjenestens virksomhet «skal utøves i samsvar med menneskerettighetene og øvrige grunnleggende rettsprinsipper og verdier i et demokratisk samfunn». Det følger av menneskerettsloven og Grunnloven at E-tjenesteloven må anvendes innenfor de rammene menneskerettighetene setter.[4] NIM mener likevel at en egen bestemmelse som henviser eksplisitt til at E-tjenestens virksomhet skal utøves i samsvar med menneskerettighetene har en pedagogisk funksjon, og at det er ryddig å understreke dette på en tydelig måte i lovteksten, slik det er gjort her.

[3] Som omfattes av loven, jf § 1-2, 3. ledd.

[4] menneskerettsloven § 2 og 3, Grunnloven § 92.

2.3. Forholdet til folkeretten i §1-3 (og § 10-6)

Lovforslaget §1-3 første ledd sier at loven skal gjelde med de «begrensninger som er anerkjent i folkeretten eller som følger av overenskomst med fremmed stat».

Av forslagets § 1-3 annet ledd fremgår at E-tjenesten ikke skal gjennomføre eller medvirke til virksomhet som «innebærer en reell risiko for at ufravikelige og andre grunnleggende menneskerettigheter krenkes».

Det er uklart hvordan disse bestemmelsene henger sammen og hvordan de skal forstås. Bestemmelsen i 1-3 første ledd konsumerer i stor grad de forpliktelsene som fremgår av § 1-3 annet ledd. Menneskerettighetene fremgår jo nettopp av folkeretten (og Norges traktatforpliktelser).

Høringsnotatet forklarer ikke hva som er ment med begrepet «ufravikelige og andre grunnleggende menneskerettigheter» i § 1-3 annet ledd, og det drøfter ikke implikasjonene av denne spesifiseringen.[5] I en menneskerettskontekst forstås gjerne begrepet «ufravikelige» som synonymt med «ikke-derogable» rettigheter. Slike menneskerettigheter er listet opp i EMK og SP som rettigheter som aldri kan fravikes, selv i nød-situasjoner som krig eller andre krisesituasjoner. [6] Listen omfatter retten til liv, forbudet mot tortur eller annen grusom, umenneskelig eller nedverdigende behandling eller straff, forbudet mot slaveri, forbud mot manglende eller tilbakevirkende lovhjemmel for straff.

I høringsnotatets eneste (og indirekte) omtale av begrepet «ufravikelige og andre grunnleggende menneskerettigheter» (om § 10-6, som igjen viser til § 1-3 annet ledd), vises det imidlertid ikke til reglene om derogasjon, men til det departementet omtaler som «*jus cogens*-regler, det vil si menneskerettslige regler som aldri kan fravikes ved nasjonal lov».[7] I høringsnotatet vises det i denne forbindelse kun til torturforbudet, og ikke til de andre ikke-derogable rettighetene.

Listen over ikke-derogable menneskerettigheter er ikke sammenfallende med listen over de såkalte *jus cogens* bestemmelsene, som ifølge Wien-konvensjonen om traktatrett er regler som «the international community of states as a whole» er enige om at det aldri kan gjøres unntak fra.[8] Det finnes ingen endelig liste over hvilke rettigheter dette omfatter, men det er antatt at forbudet mot apartheid, forbudet mot rasediskriminering,

[5] Begrepet nevnes 3 ganger i høringsnotatet men uten å forklare hva som er ment.

[6] Listen over ufravikelige menneskerettigheter er noe lengre i SP enn i EMK, og det er følgelig sistnevnte Norge er bundet av ettersom vi er part til begge konvensjoner, og begge konvensjoner er gitt forrang i menneskerettsloven.

[7] Høringsnotatet side 340.

[8] Wien-konvensjonen om traktatrett (1969) artikkel 53.

forbudet mot slaveri, forbudet mot piratvirksomhet, forbudet mot tortur og forbudet mot folkemord, er regler som faller innenfor kategorien *jus cogens*.[9]

Hvis departementet her har ment å henvise til de ikke-derogable rettighetene, burde det ha vært vist til noe mer enn torturforbudet.

Uansett må det stilles spørsmål ved sammenhengen mellom og § 1-3 første ledd på den ene siden og § 1-3 annet ledd på den andre siden. Etter §1-3 første ledd (og Grunnloven og menneskerettsloven) skal e-tjenestens virksomhet utøves i samsvar med menneskerettighetene i sin alminnelighet. Det vil si at det som høringsnotatet kaller «brudd på *jus cogens*-regler» åpenbart er forbudt. Implikasjonen av spesifiseringen i § 1-3 annet ledd er at menneskerettsansvaret kan oppfattes som begrenset til et lite antall menneskerettigheter (enten det er *jus cogens* eller ikke-derogable rettigheter det siktes til). Retten til privatliv, som er en viktig del av drøftelsene i tilknytning til denne loven, faller for eksempel åpenbart utenfor det som beskyttes etter 1-3 annet ledd.

Lovforslaget § 1-3 annet ledd viser for øvrig også til begrepet «andre grunnleggende menneskerettigheter». Dette er ikke et begrep som gir mening rettslig. Ingen menneskerettskonvensjoner sondrer mellom grunnleggende og ikke-grunnleggende menneskerettigheter, de utgjør et universelt hele. Begrepet brukes likevel flere steder i høringsnotatet.

Lovforslagets § 10-6, som handler om utlevering av etterretningsinformasjon som et ledd i internasjonalt samarbeid, krever at utlevering skal skje i overensstemmelse med særskilte bestemmelser som skal sikre «overholdelse av forbudet i § 1-3 annet ledd». Med andre ord skal slik utlevering ikke skje hvis dette kan medføre en reell risiko for krenking av «ufravikelige og andre grunnleggende menneskerettigheter». I høringsnotatet forklares dette dels ved henvisning til *jus cogens* og torturforbudet, og dels ved henvisning til «andre former for folkerettsbrudd, herunder brudd på krigens folkerett.»[10] Mens det første alternativet er svært snevert, er det andre vagt. Rekkevidden av disse reglene er usikker.

Det er etter NIMs oppfatning uklart hva departementet har ment å gjøre gjennom § 1-3 annet ledd. Man har trolig ment å avgrense e-tjenestens virksomhet mot operasjoner som innebærer en reell risiko for at noen utsettes for tortur eller krigsforbrytelser, men dette kan altså motsetningsvis forstås dit at krenkelser av andre menneskerettigheter som en følge av E-tjenestens virksomhet ikke omfattes. Uansett burde det være unødvendig med en slik presisering, særlig i lys av formålsbestemmelsen.[11]

---

[9] Norge anerkjente for øvrig ikke kategorien *jus cogens* under forhandlingene av Wien-konvensjonen, og har ikke ratifisert konvensjonen.

[10] Høringsnotatet side 340.

[11] Se forslag til mulig lovtekst under.

3. Jurisdiksjon og differensiert rettighetsbeskyttelse

I høringsnotatet på side 30 – 34 diskuterer departementet den territorielle og personelle rekkevidden av rettighetsbeskyttelsen etter EMK artikkel 1. NIM er enig med departementet i at det vil kunne være vanskelig å fastslå i hvilke tilfeller EMK eventuelt får ekstraterritoriell anvendelse der utlendinger eller norske borgere overvåkes i utlandet fra Norge, og der E-tjenesten opererer i utlandet uten tilknytning til norsk territorium. Departementet søker på grunnlag av praktiske og politiske vurderinger å løse dette ved å utforme loven uavhengig av jurisdiksjonsspørsmålet, slik at loven helt generelt pålegger E-tjenesten å operere innenfor de materielle og prosessuelle rammene i EMK, uavhengig av hvor virksomheten utøves og hvem som berøres. Det heter bl.a.:

> «Dette lovforslaget er utformet for å tilfredsstille menneskerettighetene uavhengig av utfallet av hver enkelt konkrete jurisdiksjonsvurdering (….) Lovforslaget er generisk og legger ikke opp til å differensiere normeringen ut i fra hvor eller overfor hvem en gitt aktivitet finner sted. I så måte kan man si at regelverket er utformet nasjonalitets- og geografinøytralt, og at prinsipper og krav som utledes av våre menneskerettslige forpliktelser således i praksis blir anvendt overfor alle individer Etterretningstjenesten får befatning med.»[12]

Det understrekes i høringsnotatet at denne tilnærmingen ikke er et utslag av en rettslig forpliktelse, «men gjøres av policy- og praktiske hensyn.»[13] Det er imidlertid uklart hva høringsnotatet viser til når det sies at regelverket er utformet «nasjonalitets- og geografinøytralt». Denne forståelsen fremkommer ikke av selve lovteksten, som henviser til «menneskerettighetene», med andre ord slik de er bindende for Norge, også jurisdiksjonsmessig.

NIM mener det er et uheldig grep å si i forarbeidene at menneskerettighetene skal gjelde uten de begrensninger som følger av menneskerettighetskonvensjonenes jurisdiksjonsregler. Selv om anvendelsen av reglene kan være utfordrende å fastslå i enkelte tilfeller, er det likevel en risiko for utvanning av menneskerettsvernet når man hevder å skulle sikre universell anvendelse av alle menneskerettigheter over alt. Norge har ikke praktisk mulighet og heller ikke plikt, (jf. EMK artikkel 1 og SP artikkel 2) til å sikre alle rettigheter i EMK eller SP overfor for eksempel potensielle opprørere i Afghanistan eller andre personer i E-tjenestens søkelys. At reglene i EMK og SP skal gjelde for E-tjenestens virksomhet er ikke til hinder for at rettighetsbeskyttelsen differensieres avhengig av hvor virksomheten utøves og hvem som berøres. En universell tilnærming kan i verste fall føre til en relativt sett svakere rettighetsbeskyttelse for personer som befinner seg på norsk territorium og norske borgere, enn det som hadde vært tilfelle hvis rettighetsbeskyttelsen var territorielt og personelt differensiert. Det er gode grunner til

[12] Høringsnotatet side 33-34.

[13] Høringsnotatet side 34.

at personer på norsk territorium og norske borgere kan ha behov for sterkere rettighetsvern enn utlendinger i utlandet, uten at det med det fremholdes at den sistnevnte gruppen ikke skal ha et vern som oppfyller de (til enhver tid) gjeldende reglene i EMK eller SP. Personer som oppholder seg i Norge og norske borgere er underlagt norsk jurisdiksjon og er dermed for eksempel eksponert for mulige statlige inngrep eller sanksjoner på grunnlag av opplysninger som fremkommer gjennom hemmelig overvåking. Utlendinger i utlandet er i utgangspunktet ikke eksponert for denne typen følgevirkninger. Av samme grunn må det videre antas at de potensielle skadevirkningene for samfunnet er større i Norge enn i utlandet. Risikoen for at et overvåkingssystem har negativ effekt, f.eks. i form av at folk modererer sin kommunikasjon med hverandre eller avstår fra å ytre seg eller snakke med journalister, kan reduseres gjennom effektive rettssikkerhetsmekanismer.

Selv om forslaget om tilrettelagt innhenting bulkovervåkingssystemet er innrettet mot utenlandske forhold, berører det også i stor grad nasjonal kommunikasjon, i hovedsak som utilsiktet konsekvens. Videre kan det ikke utelukkes at overvåkingsinfrastrukturen som foreslås etablert ved lovforslaget på sikt vil kunne få et utvidet virkeområde som i større grad retter seg mot nasjonale forhold.

NIM mener på denne bakgrunn at det kan være grunn til å vurdere en lovtekst som er basert på Norges menneskerettsforpliktelser, både materielt og jurisdiksjonsmessig. Dette innebærer sterkere rettssikkerhetsmekanismer for overvåking som direkte berører personer på norsk territorium og norske borgere. Det gjelder blant annet spørsmål om krav til notifikasjon, tilgang på effektive rettsmidler, krav til spesifikasjon i kjennelser som tillater søk mot personer i Norge, domstolkontroll ved søk i kommunikasjon som er underlagt særlig rettsbeskyttelse, mv. Dette kommer vi tilbake til under de tematiske delene i det følgende. Dette innebærer imidlertid også at Norge må sikre menneskerettigheter i situasjoner og overfor personer, i utlandet, hvor Norge har jurisdiksjon i menneskerettskonvensjonenes forstand.

En måte å løse spørsmålet om lovens henvisning til menneskerettigheter, både materielt og jurisdiksjonsmessig, kunne være en alternativ tekst til § 1-3. Dette forslaget innebærer at det er Norges menneskerettsforpliktelser, slik de til enhver tid gjelder, som skal sikres:

Loven gjelder med de begrensinger som er anerkjent i folkeretten eller følger av overenskomst med fremmed stat.

Etterretningstjenesten skal ikke gjennomføre eller medvirke til virksomhet som gjør det sannsynlig at Norges menneskerettsforpliktelser brytes.

4. Tilrettelagt innhenting og retten til privatliv

4.1. Generelt

Tilrettelagt innhenting kan, som departementet påpeker, støte an mot flere menneskerettigheter, inklusive retten til privatliv. Det er særlig kapittel 7 og 8 i lovforslaget, samt § 5-4 om forholdsmessighet, som er de mest relevante bestemmelsene i så måte. Som det understrekes i høringsnotatet,[14] er retten til privatliv beskyttet i Grunnloven § 102, EMK artikkel 8 og SP artikkel 17.

Artikkel 8 sier at enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse. Videre at offentlige myndigheters eventuelle inngripen i denne retten må ha hjemmel i lov og være nødvendig i et demokratisk samfunn av hensyn til bl.a. den nasjonale sikkerhet. Det er ingen tvil om at retten til privatliv i utgangspunktet beskytter mot den typen overvåkning som det her er snakk om. Spørsmålet er hvordan denne rettigheten balanseres opp mot nødvendigheten av inngripen. Lovforslagets § 5-4 inneholder derfor en forholdsmessighetsvurdering som må anvendes ved inngripen i retten til privatliv. I det følgende vil vi vurdere forslaget om tilrettelagt innhenting med utgangspunkt i EMK artikkel 8 og relevant praksis fra EMD.

NIM kommenterer først EMDs avgjørelser i *Centrum for Rättvisa v. Sverige (no. 35252/08)* («*Rättvisa*»), og *Big Brother Watch m.fl*. v. *Storbritannia (no. 58170/13, 62322/14 og 24960/15)*, («*Big Brother*»), som ble avgjort av EMD henholdsvis 18. juni 2018 og 13. september 2018. Etter at høringsnotatet ble skrevet, er det imidlertid besluttet at disse skal behandles av EMD i storkammer.

NIM vil vurdere sentrale sider av forslaget med utgangspunkt i enkelte momenter EMD særlig vektlegger i helhetsvurderingen av om overvåkingssystemer er kompatible med konvensjonen: (1) typen overvåking, (2) virkeområde, (3) varighet, (4) autorisasjon og gjennomføring, (5) kontroll og (6) tilgang på effektivt rettsmiddel.[15]

Vi har særlig valgt å kommentere nærmere på virkeområdet for forslaget om tilrettelagt innhenting, kontrollmekanismene, samt notifikasjon og rettsmidler.

4.2. Centrum for Rättvisa mot Sverige og Big Brother Watch mot Storbritannia

I disse sakene tok EMD stilling til forholdet mellom bulkinnsamling av elektronisk kommunikasjon og retten til privatliv i EMK artikkel 8. *Big Brother*-saken gjaldt også forholdet til EMK artikkel 10. I begge sakene la EMD generelt til grunn at det ligger

[14] Høringsnotatet side 210 ff.

15 Se bl.a. *Szabó og Vissy v. Ungarn* (no. 37138/14) avsnitt 57.

innenfor statens skjønnsmargin å innføre et bulkeroverv̊akingssystem for å ivareta nasjonal sikkerhet.[16]

Avgjørelsen i *Rättvisa* gjaldt spørsmål om det svenske FRA-systemet for bulkinnsamling var forenelig med retten til privatliv. EMD tok utgangspunkt i de generelle vurderingsmomentene nevnt over. På tross av at det ble påpekt enkelte svakheter ved ordningen, blant annet tilgangen på effektivt rettsmiddel fordi det i praksis ikke ble gitt notifikasjon om overvåkingen, kom EMD til at det samlet sett forelå tilstrekkelige rettssikkerhetsmekanismer og at det dermed ikke forelå krenkelse av EMK artikkel 8.

I *Big Brother* tok EMD stilling til om det britiske systemet for bulkinnsamling var forenelig med EMK artikkel 8 og 10. Med utgangspunkt i den samme generelle tilnærmingen som i saken mot Sverige, kom EMD til at det britiske systemet ikke var i samsvar med minimumsstandardene i EMK artikkel 8 og 10. Det ble særlig vist til at seleksjonsprosessen for innhenting av datatrafikk ikke var underlagt tilstrekkelig kontroll og at det ikke var reelle sikkerhetsmekanismer for utvelgelse og analyse av metadata.[17]

Departementet legger i høringsnotatet disse avgjørelsene til grunn for sine vurderinger av nødvendighetskriteriet. Begge saker er nå imidlertid besluttet fremmet for EMD i storkammer. Sett i lys av normal saksbehandlingstid for storkammersaker i EMD er det mye som tyder på at det vil ta nokså lang tid det foreligger endelig avgjørelse i de to sakene, og det er neppe realistisk at sakene vil bli avgjort tidsnok til at de kan iakttas i den videre lovgivningsprosessen. Rettstilstanden er med det ganske uklar, noe som skaper visse utfordringer.

At *Rättvisa* og Big *Brother* skal behandles av storkammeret medfører likevel ikke at avgjørelsene er helt uten betydning i den videre lovgivningsprosessen.

På bakgrunn av tidligere praksis fra EMD er det grunn til å anta at EMD i storkammer vil bygge på de samme vurderingstemaene ved den foregående behandlingen. Forutsatt at også EMD i storkammer vil legge til grunn at det ligger innenfor statens skjønnsmargin å innføre de aktuelle bulkinnsamlingssystemene som virkemiddel for å ivareta nasjonal sikkerhet, er det nærliggende at EMDs prøving *in abstracto* vil skje med utgangspunkt i de samme seks minstekravene («minimum safeguards»), som skal ivareta forutberegnelighet, forholdsmessighet og minimere risikoen for myndighetsmisbruk. Disse er også lagt til grunn i en rekke tidligere avgjørelser knyttet til annen type overvåkning.[18] Det som fremstår mer usikkert er hvordan disse vil bli anvendt i kontekst av bulkovervåking.

---

[16] *Centrum for Rättvisa v. Sverige (no. 35252/08)* avsnitt 112, *Big Brother Watch m.fl.* v. *Storbritannia (no. 58170/13, 62322/14 og 24960/15)* avsnitt 314.

[17] *Big Brother Watch m.fl.* v. *Storbritannia (no. 58170/13, 62322/14 og 24960/15)*, avsnitt 387-388.

[18] Se f.eks. *Roman Zakharov v. Russland* (no. 47143/06), avsnitt 231, med videre henvisninger.

Praksis fra EMD om hemmelig overvåking viser at det foretas en helhetlig vurdering og at momentene som inngår i vurderingen er generelt formulerte. Det har naturlig nok sammenheng med at de anvendes på en rekke ganske ulike overvåkingssystemer, hvorav det i tillegg er ganske store nasjonale variasjoner. Selv om avgjørelsene i *Rättvisa* og *Big Brother* ikke nødvendigvis blir stående, vil de kunne tjene som eksempler på hvordan de relevante momentene *kan* anvendes i kontekst av et bulkovervåkingssystem. Premissene kan også ha egenverdi som realargumenter. I enkelte sammenhenger vil det derfor også bli vist til avgjørelsene i herværende høringsuttalelse.

En observasjon fra de to avgjørelsene er at i alt fjorten EMD-dommere enstemmig har lagt til grunn at det ligger innenfor statens skjønnsmargin å innføre et bulkovervåkingssystem for å ivareta nasjonal sikkerhet. Man skal imidlertid være forsiktig med å trekke slutninger fra dette all den tid sakene skal behandles i storkammer.

4.3. Bulkovervåking og rettslige utgangspunkter fra EMDs praksis

(i) Inngrepet

Eksistensen av et bulkovervåkingssystem kan i seg selv anses som et inngrep i retten til privatliv etter EMK artikkel 8. Inngrepet konstitueres av den latente overvåkingstrusselen som ligger i at ordningen i det hele tatt eksisterer.[19] I alle tilfeller er det klart at hemmelig innhenting av elektronisk kommunikasjon er et inngrep i retten til privatliv.

(ii) Forholdsmessighetskravet og lovskravet

I saker om hemmelig overvåking er det gjennomgående at EMD vurderer forholdsmessighetskravet og lovskravet under ett:[20]

> «In cases where the legislation permitting secret surveillance is contested before the Court, the lawfulness of the interference is closely related to the question whether the "necessity" test has been complied with and it is therefore appropriate for the Court to address jointly the "in accordance with the law" and "necessity" requirements (…). The "quality of law" in this sense implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when "necessary in a democratic society", in particular by providing for adequate and effective safeguards and guarantees against abuse."

Ettersom hemmelig overvåking kun kan skje i den utstrekning det er nødvendig i et demokratisk samfunn og lovskravet innebærer at det må foreligge regelverk og rettssikkerhetsmekanismer som ivaretar at overvåkingskapasiteten kun brukes dersom det er nødvendig, blir vurderingen i praksis overlappende.

[19] Se bl.a. *Szabó og Vissy v. Ungarn* (no. 37138/14), avsnitt 53 og *Klass m.fl. v Tyskland* (5029/71), avsnitt 41.

[20] Se f.eks. *Roman Zakharov v. Russland* (no. 47143/06) avsnitt 232.

(iii) Statens skjønnsmargin og EMDs prøving

Tilsynelatende er ikke EMDs praksis helt entydig når det gjelder statenes skjønnsmargin for innføring av hemmelige overvåkingssystemer. I høringsnotatet på side 49-50 vises det til EMDs avvisningsavgjørelse i *Weber og Saravia* v.*Tyskland* (no. 54934/00) fra 2006, der EMD legger til grunn at statene «(…) enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security (…)». Denne konstateringen av at statene har en vid skjønnsmargin er ikke helt forenelig med EMDs senere storkammeravgjørelse i *Roman Zakharov v. Russland (no. 47143/06)* fra 2015 («Roman Zakharov»), der EMD i avsnitt 232 legger til grunn at statene «(…) enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security (…).» Her fremgår det at statene har en viss («certain») skjønnsmargin i avveiningen mellom borgernes rett til privatliv og valg av virkemidler for å ivareta nasjonal sikkerhet. I *Rättvisa* og *Big Brother Watch* la EMD til grunn at statene har en «wide» skjønnsmargin i valget av overvåkingssystem for å ivareta nasjonal sikkerhet. Hvorvidt EMD i storkammer vil vurdere det på samme måte er usikkert. Sammenligner man premissene i tidligere saker om overvåking hvor EMD har lagt til grunn at staten har en «certain» eller «fairly wide» skjønnsmargin er det imidlertid vanskelig å identifisere substansielle forskjeller i rettens nærmere vurderinger og om valget av formulering innebærer en reell forskjell. Det er flere grunner til at retten til privatliv setter grenser for statens overvåking. En gjennomgående begrunnelse for grensene EMD har satt er at overvåking kan «undermine or even destroy democracy under the cloak of defending it».[21] Denne risikoen må ikke nødvendigvis imøtekommes gjennom å sette grenser for hvilke overvåkingssystemer staten kan innføre. For å begrense den iboende faren med statlig overvåking har EMD i hovedsak oppstilt krav til rettssikkerhetsgarantier som ivaretar at systemene ikke misbrukes:

> "(…) the Court must be satisfied that there are adequate and effective guarantees against abuse."[22]

Det er gjennomgående at EMD foretar en inngående prøving av om overvåkingssystemer er innrettet med rettssikkerhetsmekanismer som hindrer misbruk, og på dette punktet har statene en vesentlig smalere skjønnsmargin enn i valg av system.

Utgangspunktet for prøvingen av dette spørsmålet er formulert slik i Szabó og Vissy v. Ungarn fra 2016 (no. 37138/14), avsnitt 57:

> "The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. The Court has to determine

[21] *Roman Zakharov v. Russland* (no. 47143/06) avsnitt 232.

[22] *Roman Zakharov v. Russland* (no. 47143/06) avsnitt 232.

> whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society."

Vurderingen av om overvåkingen er underlagt sikkerhetsmekanismer som i tilstrekkelig grad begrenser misbruksrisikoen beror på en helhetlig vurdering. Her presiserer også retten at vurderingen knytter an mot at sikkerhetsmekanismene må være tilstrekkelige for at inngrepet begrenses til det som nødvendig i et demokratisk samfunn. Det er en selvstendig rettslig norm, og det er følgelig ikke tilstrekkelig at systemet er innrettet på en måte som kun ivaretar at det praktiseres i henhold til det nasjonale lovgrunnlaget. Ved utarbeidelse av en ny lov som har store menneskerettslige implikasjoner, er det derfor en fordel om de menneskerettslige normene i stor grad gjenspeiles i det nasjonalrettslige rammeverket for å sikre best mulig menneskerettslig etterlevelse i praksis. Ettersom det legges opp til en helhetsvurdering, hvor det er et nært samspill mellom de enkelte momentene, og hvor svakheter i ett ledd kan kompenseres i et annet, gir i og for seg også denne tilnærmingen et visst handlingsrom for hvordan rettssikkerhetsmekanismene skal legges opp. Utover at de skal hindre misbruk er det imidlertid til dels uklart hva rettssikkerhetsmekanismene må være innrettet mot å ivareta. Mens EMD i Roman Zakharov la til grunn at overvåking må avgrenses til hva som er «necessary in a democratic society», har EMD i enkelte saker stilt strengere krav til avgrensningen av overvåkingen. I *Szabó og Vissy v. Ungarn* (no. 37138/14) avsnitt 73, la EMD til grunn at overvåkingen ikke bare må være «necessary», men at den må oppfylle et krav om «strict necessity».[23] Det legges til grunn at dette skjerpede nødvendighetskravet innbefatter at overvåkingen må være innrettet mot å beskytte demokratiske institusjoner, og at det kun kan brukes for å fremskaffe vitale opplysninger i individuelle operasjoner. At dette er ment som en generell norm kommer særlig til uttrykk ved at EMD sier at ethvert system for hemmelig overvåking som ikke korresponderer med denne normen, vil kunne misbrukes.[24] Kravet om «strict necessity» korresponderer også med linjen i EU-domstolens avgjørelse i sak C-203/15 og C-698/15 av 21. desember 2015, («Tele2»).

Samlet sett legger EMD til grunn en vid skjønnsmargin i valget av overvåkingssystem for å ivareta nasjonal sikkerhet. EMDs prøving av om systemet er innrettet med rettssikkerhetsmekanismer som ivaretar at det ikke misbrukes er derimot ganske intensiv.

---

[23] "However, given the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy, the Court considers that the requirement "necessary in a democratic society" must be interpreted in this context as requiring "strict necessity" in two aspects. A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal."

[24] En tilsvarende norm er lagt til grunn i en del andre avgjørelser og går tilbake til *Klass m.fl. v. Tyskland* (no. 5029/71) fra 1978 avsnitt 42. Se også *Mustafa Sezgin Tanrikulu v Tyrkia* (no. 27473/06) avsnitt 49 og *Rotaru v. Romania* (no. 28341/95) avsnitt 47.

På dette punkt fremstår det også uklart om det er tilstrekkelig at rettssikkerhetsmekanismene ivaretar at overvåkingen begrenses til det som er «necessary» eller om de må ivareta at overvåkingen ytterligere innskrenkes til hva som er «strictly necessary». Hvis det sistnevnte legges til grunn oppstår en motsetning mellom utgangspunktet om at statene har vid skjønnsmargin til å velge overvåkingssystem og krav til rettssikkerhetsmekanismer, ettersom et bulkovervåkingssystem kan være vanskelig å forene med målrettingskravet som ligger i «strict necessity».

Det skjerpede nødvendighets- og målrettingskravet lagt til grunn i saker om omfattende overvåkingssystemer rettet mot «citizens».[25] EMDs overordnede begrunnelse for å oppstille strenge krav til rettssikkerhetsgarantier er også at overvåking kan ha en skadelig effekt på demokratiet. På bakgrunn av dette, og at EMK generelt gjelder forholdet mellom borgerne og den enkelte stat, kan det tilsi at det ikke vil bli lagt til grunn et krav om «strict necessity» for overvåking som er rettet mot utenlandske forhold og som i utgangspunktet er avgrenset mot interne forhold i staten og personer som oppholder seg der. Det på tross av at egne borgeres kommunikasjon vil bli lagret som konsekvens av hvordan systemet virker, noe som for så vidt skaper den type misbrukspotensial som begrunner kravene EMD oppstiller. Uten at det skal tillegges rettslig betydning, er det også grunn til å nevne at verken Rättvisa eller Big Brother etablerer noe krav om «strict necessity».

Som det fremgår av gjennomgangen er det ikke avklart om det ligger innenfor statens skjønnsmargin å innføre et bulkinnsamlingssystem som er innrettet mot utenlandske forhold, men som i betydelig grad også rammer statens egne borgere. I den grad det tillates er det ikke sikkert hvilke krav til rettssikkerhetsmekanismer som vil bli oppstilt, ei heller hvor strengt EMD vil vurdere allerede etablerte krav til rettssikkerhetsmekanismer, gitt misbrukspotensialet i slike systemer, som trolig også vil øke i takt med teknologiutviklingen. NIM mener at departementet i den videre vurderingen i større grad må ta inn over seg denne usikkerheten. Det kan særlig reflekteres i ytterligere styrking av rettssikkerhetsmekanismene.

(iv) Dynamisk tolkning

Som nevnt er det en del iboende egenskaper ved bulkinnsamlingssystemer som kan være vanskelig å forene med eksisterende krav om rettssikkerhetsmekanismer og som følgelig kan indusere en del normative tilpasninger fra EMDs side. Retten har blant annet uttalt følgende:[26]

> "In the face of this progress the Court must scrutinize the question as to whether the development of surveillance methods resulting in masses of data collected has

[25] *Klass m.fl. v. Tyskland* (no. 5029/71) og *Szabó og Vissy v. Ungarn* (no. 37138/14),

[26] Szabó og Vissy v. Ungarn (no. 37138/14) avsnitt 68.

been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights."

I dette ligger det et ganske klart signal om at retten vil kunne komme til å videreutvikle gjeldende krav til rettssikkerhetsmekanismer for å imøtekomme det ekspanderende overvåkingspotensialet i ny teknologi. For bulkinnsamling kan det f.eks. medføre at retten oppstiller ytterligere eller skjerpede krav til rettssikkerhetsmekanismer. Dette bør departementet være oppmerksomme på i utformingen av loven.

(v) Oppsummering

Generelt sett avtegner praksis et bilde hvor staten har stort handlingsrom i valg av type overvåkingssystem for å ivareta nasjonal sikkerhet, mer begrenset handlingsrom i implementeringen og bruken av overvåkingssystemet. Hvis og i den grad overvåkingssystemet ikke bare rettes mot utenlandske forhold, men også brukes overfor egne borgere, begrenses handlingsrommet ytterligere og krav til sikkerhetsmekanismer skjerpes.

Egenarten ved bulkinnsamling innebærer at det har et betydelig misbrukspotensial overfor egne borgere, selv om det i utgangspunktet er rettet mot utenlandske forhold. NIM mener det er nærliggende at dette vil medføre at EMD vil vurdere kravet til sikkerhetsmekanismer strengt. Det er også en mulighet for at domstolen vil kunne oppstille særegne krav til sikkerhetsmekanismer som adresserer særegenhetene ved bulkinnsamlingssystemer. Dette bør departementet være særlig oppmerksom på i sin videre behandling av saken.

I det følgende vil vi vurdere enkelte sider av forslaget nærmere opp mot sentrale momenter som EMD ser hen til, særlig anvendelsesområdet for overvåkingen, autorisasjon og domstolkontroll, gjennomføringskontroll og etterkontroll, samt notifikasjon og rettsmidler.

4.4. Anvendelsesområdet for tilrettelagt innhenting

(vi) Rettslige utgangspunkter

For å motvirke den iboende misbruksrisikoen i hemmelige overvåkingssystemer og ivareta forutberegnelighet, er det et sentralt aspekt at virkeområdet for overvåkingssystemet er noenlunde klart angitt og avgrenset. Hensynet til forutberegnelighet står likevel i et visst motsetningsforhold til erkjennelsen av at det ikke er mulig å overskue alle situasjoner der bruk av hemmelig overvåking er nødvendig. Effekten av slike systemer svekkes dessuten dersom muligheten for innrettelse blir for stor.[27] Med dette som bakteppe har EMD lagt til grunn følgende utgangspunkt, blant annet i *Roman Zakharov*, avsnitt 243:

[27] *Roman Zakharov v. Russland* (no. 47143/06) avsnitt 247.

> "The Court reiterates that national law must define the scope of application of secret surveillance measures by giving citizens an adequate indication as to the circumstances in which public authorities are empowered to resort to such measures (…)"

At virkeområdet skal være angitt tjener flere formål. Det første er å gi borgerne en viss forutberegnelighet og innsyn i hvilke overvåkingskapasiteter staten har. I og med egenarten av hemmelig overvåking og formålene det skal ivareta, medfører imidlertid ikke dette hensynet at det stilles spesielt strenge krav til klarhet og detaljnivå. EMD har i flere saker vist til at dette kravet ikke innebærer at statene i detalj må angi i hvilke tilfeller hemmelig overvåkning kan iverksettes, da dette fort vil lede til at borgerne tilpasser sin adferd for å omgå slik overvåkning.[28]

Hvor langt hensynet til forutberegnelighet rekker illustreres blant annet av at EMD har lagt til grunn at "The reference to terrorist threats or rescue operations can be seen in principle as giving citizens the requisite indication.»[29] Forutberegnelighet er imidlertid bare ett hensyn og er ikke alene avgjørende for hvilke krav som skal stilles til angivelsen av virkeområdet for et overvåkingssystem.

Viktigere er det at angivelsen av virkeområdet skal bidra til å begrense misbruksrisikoen som oppstår dersom den diskresjonære kompetansen til å bruke overvåkingskapasiteten blir for omfattende:[30]

> "in matters affecting fundamental rights it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a discretion granted to the executive in the sphere of national security to be expressed in terms of unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference

Bruken av overvåkingssystemer må nødvendigvis bero på en grad av etterretningsfaglig skjønn, men lovgivningen må sette rammer for skjønnsutøvelsen og med en viss presisjon fastsette hvordan skjønnet skal utøves for å sikre at overvåkingen er forholdsmessig i lys av det legitime formålet den skal ivareta. Hva som ligger nærmere i dette er blant annet illustrert i *Roman Zakharov* avsnitt 248:

> "It is significant that the OSAA does not give any indication of the circumstances under which an individual's communications may be intercepted on account of

[28] *Szabó og Vissy v. Ungarn* (no. 37138/14) avsnitt 62.

[29] *Szabó og Vissy v. Ungarn* (no. 37138/14), avsnitt 64.

[30] *Szabó og Vissy v. Ungarn* (no. 37138/14) avsnitt 65.

> events or activities endangering Russia's national, military, economic or ecological security. It leaves the authorities an almost unlimited degree of discretion in determining which events or acts constitute such a threat and whether that threat is serious enough to justify secret surveillance, thereby creating possibilities for abuse"

Misbruksfaren som ligger i at staten har diskresjonær kompetanse til å iverksette og bruke overvåkingskapasiteter stiller etter omstendighetene ganske strenge krav til angivelsen av virkeområde, herunder særlig terskelangivelser for i hvilke tilfeller og hvordan overvåkingssystemer kan brukes samt hva overvåkingen kan gå ut på.

Et spørsmål som ikke er avklart i EMDs praksis er hvordan disse kravene skal anvendes ved bedømmelsen av bulkinnsamlingssystemer. At det her er ulike innfallsvinkler illustreres av de ganske forskjellige tilnærmingene i *Big Brother Watch* og *Rättvisa*. I Big Brother Watch adresserer EMD at egenarten ved bulkovervåkingssystemer kan fordre en viss tilpasning av hvordan virkeområdet for systemet vurderes. I avgjørelsen avsnitt 329 fremgår følgende:

> "In a targeted interception regime, the nature of the communications to be intercepted should be tightly defined, but once interception takes place it is likely that all – or nearly all – of the intercepted communications are analysed. The opposite will normally be true of a bulk interception regime, where the discretion to intercept is broader, but stricter controls will be applied at the selection for examination stage."

I *Big Brother Watch* viser EMD videre til at overvåkingssystemet opererer i fire stadier: (1) Tilkobling på en liten andel internettbærere som antas å ha ekstern kommunikasjon med etterretningsverdi, (2) filtrering og automatisert sletting av en stor del av dataene som minst sannsynlig vil ha etterretningsverdi, i nær samtid, (3) bruk av enkle og komplekse søkekriterier for å ytterligere filtrere hvilke data som lagres og hvilke data som slettes, og til slutt (4) analyse av lagrede data.

Med dette som utgangspunkt, ser EMD først på grunnlaget for å gi tillatelse til bulkinnsamling i utgangspunktet, og deretter på om reguleringen gir adekvat forutberegnelighet om i hvilke tilfeller kommunikasjon kan innhentes og eventuelt utvelges for analyse.[31] I det følgende foretar EMD den nærmere vurderingen med utgangspunkt i de fire stadiene for bulkovervåkingsprosessen. Ettersom denne tilnærmingen og EMDs nærmere vurderinger er nytt med avgjørelsen i *Big Brother*-saken, er det ikke gitt at vurderingen vil bli den samme ved en eventuell storkammerbehandling. Tilnærmingen her skiller seg også en del fra tilnærmingen *Rättvisa*, der EMDs analyse fremstår noe mer overordnet og i mindre grad knyttet til de enkelte ledd i

[31] *Big Brother Watch m.fl.* v. *Storbritannia (no. 58170/13, 62322/14 og 24960/15)* avsnitt 330.

overvåkingsprosessen. På den andre siden kan det ses som en ren operasjonalisering av de allerede etablerte kravene for angivelsen av virkeområdet for overvåkingssystemer, som er spesielt tilpasset særegenhetene ved bulkovervåking. Etter vårt syn må vurderingen uansett legges opp slik at den iakttar de særlige egenskapene ved overvåkingssystemet som er reelt avgjørende for virkeområdet. Dette vil vi også være utgangspunktet for den videre vurderingen.

Et åpent spørsmål ved bulkinnsamlingssystemer er i hvilken grad det kan bli oppstilt nærmere målrettingskrav i ulike deler av overvåkingsprosessen, jf. diskusjonen over om «strict necessity» i romertall iii.

I det videre vil vi se nærmere på konkrete sider av lovforslaget som gjelder virkeområdet for tilrettelagt innhenting.

(i) Formålet

I høringsnotatet er det lagt opp til at bulkinnsamling og søk i rådata i bulk kun kan skje dersom det er nødvendig og forholdsmessig for å frembringe informasjon som er relevant for «etterretningsformål». Innhentingen har etterretningsformål dersom den tar sikte på å ivareta en eller flere av E-tjenestens oppgaver etter forslaget kapittel 3.[32] Etterretningstjenestens oppgaver etter kapittel 3 er primært rettet mot «utenlandske militære og sivile forhold», jf. forslaget §§ 3-1 og 3-2.

At bulkinnsamling skal brukes for å innhente utenlandsetterretning er i utgangspunktet en sentral avgrensning av virkeområdet, som bidrar til å overholde EMDs krav som er redegjort for over.

Innenfor rammen av hva som kan karakteriseres som «utenlandske militære og sivile forhold» synes det å være få klare avgrensninger. Blant annet fremgår det i forslaget § 3-2, første ledd, bokstav a, at E-tjenesten skal innhente og analysere informasjon for «ivaretakelse av prioriterte utenriks-, forsvars- eller sikkerhetspolitiske interesser knyttet til forhold og utviklingstrekk i andre stater og regioner,». Umiddelbart fremstår det som at dette går videre enn å kun dreie seg om nasjonal sikkerhet.

Ettersom oppgavebeskrivelsen i kapittel 3 danner yttergrensen for adgangen til bulkinnsamling er det også helt sentralt at disse oppgavene fastsettes på en måte som ikke i altfor stor grad overlater til E-tjenesten å definere innholdet.

NIM mener derfor at det innenfor rammen av oppgavebeskrivelsene i kapittel 3, bør fastsettes ytterligere innskrenkninger eller presiseringer av hvilke formål som kan berettige tilrettelagt innhenting. Det på ingen måte gitt at det er nødvendig at virkeområdet korresponderer med E-tjenestens generelle oppgavebeskrivelse.

(ii) Territorialbegrensningen

[32] Høringsnotatet side 68.

I forslaget § 4-1 er det forbudt å «rette» informasjonsinnhenting mot «en fysisk person som oppholder seg i Norge.» Tilsvarende gjelder virksomhet i Norge som utøves av en juridisk person. Videre fremgår det av forslaget § 4-2, sjette ledd, at innhenting av rådata i bulk, som nødvendigvis vil omfatte mye data om personer og virksomheter i Norge, ikke omfattes av forbudet i § 4-1. Det er en naturlig konsekvens av hvordan bulkinnsamlingen fungerer. I samme bestemmelse syvende ledd, fremgår det at det kan foretas søk i rådata med utgangpunkt i en personselektor som kan knyttes til en person som er omfattet av forbudet i § 4-1 dersom søket ikke er «rettet» mot denne personen og det kan få «vesentlig betydning» for ivaretakelsen av E-tjenestens oppgaver etter kapittel 3. På bakgrunn av EMDs praksis som er redegjort for ovenfor, er det nærliggende at dette vil bli ansett som overvåking av egne borgere og følgelig underlagt et krav om «strict necessity». NIM mener derfor at dette bør reflekteres i lovteksten slik at det fremgår at dette kun er tillatt når det er «strengt nødvendig». Antageligvis kan dette kravet også medføre en begrensning i hvilke av E-tjenestens oppgaver som kan berettige søket, og det bør derfor vurderes om den generelle henvisningen til oppgavene i forslaget kapittel 3 reflekterer dette.

En uklarhet i den foreslåtte reguleringen om territorialbegrensning er forholdet mellom rekkevidden av forbudet i § 4-1 og unntakene i § 4-2. Ettersom forbudet er begrenset til å «rette» innhentingen oppstår spørsmålet om det kan tenkes tilfeller hvor det kan innhentes informasjon om personer i Norge, uten at det er «rettet» mot vedkommende, som likevel ikke er dekket av unntakene i § 4-2. I den grad slike tilfeller er tiltenkt bør det presiseres som unntak fra hovedregelen. Hvis det ikke er meningen at det skal være en slik «mellomkategori», bør det klargjøres at unntakene i § 4-2 er uttømmende.

(iii) Politiformål

I forslaget § 4-4 er det et generelt forbud mot at E-tjenestens virksomhet skal ha politi- og rettshåndhevelsesformål. I bestemmelsens andre ledd, første punktum, heter det det:

> «At informasjon innhentet for etterretningsformål også kan være relevant for politiet eller andre norske rettshåndhevende myndigheter, er ikke i strid med forbudet etter første ledd.»

Det er helt uklart hva som menes med denne bestemmelsen isolert sett. Hvis meningen er å klargjøre at forbudet ikke er til hinder for at E-tjenesten i medhold av bestemmelsene i forslaget kapittel 10 deler informasjon som opprinnelig ble innhentet for etterretningsformål, bør det fremkomme klarere.

For så vidt gjelder virkeområde vil det trolig være et viktig moment i vurderingen etter EMK artikkel 8 at bulkovervåkingssystemet i utgangspunktet er avgrenset til utenlandsetterretningsformål, og at regelverket er innrettet for å hindre formålsutglidning i praksis, f.eks. i form av at systemet helt eller delvis også brukes for å innhente informasjon til politiformål. Slik sett er NIM positive til forbudene i §§ 4-4 og 10-

3. Denne avgrensningen kan ivaretas selv om det i en viss utstrekning kan deles informasjon fra E-tjenesten til politiet, jf. forslaget kapittel 10. Det er sentralt at delingsadgangen ikke skaper uklarhet rundt det reelle virkeområdet for ordningen. I dette perspektivet mener NIM at adgangen til å dele overskuddsinformasjon etter forslaget § 7-3 bør ytterligere presiseres. Herunder bør det særlig klargjøres hva som menes med «avverges», og det bør også stilles kvalifikasjonskrav til hvilken betydning overskuddsinformasjonen kan ha. Videre er det ikke gitt at alle overtredelser av bestemmelser i straffeloven kapittel 17 og 18 kan begrunne slik informasjonsdeling.

(iv) Tilretteleggingsplikten og valg av kommunikasjonsbærere

Etter forslaget § 7-2 har tilbydere som er omfattet av ekomloven § 1-5 nr. 16 og «tilbydere av internettbaserte kommunikasjons- og meldingstjenester som er tilgjengelig for allmennheten» plikt til å tilrettelegge for at E-tjenesten kan iverksette tilrettelagt innhenting. Det fremstår uklart hvem som vil bli ansett som «tilbydere av internettbaserte kommunikasjons- og meldingstjenester som er tilgjengelig for allmennheten». I utgangspunktet vil det også være opp til E-tjenesten selv å avgjøre hvem som omfattes. Dette tillegget synes også å medføre at forslaget går betydelig lenger enn Lysne II-utvalgets forslag, hvor det kun var tilbydere av kabel som skulle være omfattet.

Hvilke tilbydere som har tilretteleggingsplikt er avgjørende for det potensielle omfanget av overvåkingen.

I forslaget § 7-5 fremgår det videre at E-tjenesten ved valg av kommunikasjonsnett og kommunikasjonstjenester skal «prioritere» tilgang til nett, tjenester og linker som «antas å frembringe mest mulig etterretningsmessig relevant informasjon i lys av oppgavene som er fastsatt i forslaget kapittel 3.

Med dette fremstår det som at E-tjenesten har et svært omfattende skjønn og at det i praksis er få begrensinger på hvilke kommunikasjonsbærere E-tjenesten kan lagre kommunikasjon fra. I utgangspunktet er det heller ikke tidsbegrensninger eller krav om at behovet vurderes fortløpende eller med gitte intervaller.

Det er på det rene at innhentingen i seg selv innebærer et inngrep i retten til privatliv. Utvalget av kommunikasjonsbærere og den initielle lagringen av kommunikasjon må derfor også være forholdsmessig. Selv om det gjelder et helt generelt forholdsmessighetskrav i forslaget § 5-4, mener NIM at reglene om tilretteleggingsplikt og utvalg av kommunikasjonsbærere må gjenspeile at E-tjenesten kun har tilgang til kommunikasjonsbærere og kan kreve tilrettelegging i den grad det er nødvendig ut fra formålet. Videre bør det også fastsettes momenter som skal inngå i vurderingen og som reflekterer nødvendighetskravet.

Et tilgrensende spørsmål, som vi vil komme tilbake til nedenfor under punkt 4.5 er om det også bør legges inn en domstolkontroll på dette stadiet, hvoretter tilretteleggingsplikten og omfanget av den fastsettes i tidsbegrensede kjennelser overfor den enkelte tilbyder.

(v) «Grunn til å undersøke»

Det følger av § 5-1 at etterretningstjenesten kan iverksette målsøk når det er «grunn til å undersøke» om innhenting kan bidra til å frembringe informasjon som er relevant for etteretningsformål. Etter § 5-2 kan Etterretningstjenesten iverksette målrettet innhenting når *konkrete holdepunkter* tilsier at det foreligger *grunn til å undersøke* om etterretningsmålet besitter, kommuniserer eller vil motta, eller om innhenting på annen måte kan frembringe, informasjon som er relevant for etterretningsformål. Dette kriteriet synes å gi E-tjenesten et utstrakt skjønn som det er vanskelig å overprøve.

Ordlyden høringsbrevet gir ikke mange holdepunkter for å forstå hva som gjør at det er en «grunn til å undersøke». NIM mener at vilkårene «grunn til å undersøke» i §§ 5-1 og 5-2, bør operasjonaliseres nærmere slik at det blir tydeligere hvor terskelen ligger. Dette vil også bidra til at saken opplyses bedre ved domstolprøvingen. NIM har vanskelig for å se hvordan domstolen ellers på en hensiktsmessig måte ellers skal kunne vurdere forbudet mot diskriminering i § 9-1 og for øvrig ellers vurdere det generelle spørsmålet om forholdsmessighet, som er helt sentralt menneskerettslig.

4.5. Autorisasjon og domstolkontroll

(vi) Rettslige utgangspunkter

For å ivareta at hemmelige overvåkingskapasiteter kun brukes i henhold til lov og innenfor rammen av hva som er forholdsmessig for å ivareta legitime hensyn, har EMD lagt stor vekt på om og hvordan bruken av overvåkingssystemet er underlagt uavhengig kontroll.[33]

Uavhengig kontroll kan komme inn på ulike stadier i overvåkingsprosessen: ved at det gis tillatelse til å overvåke, ved gjennomføringen av overvåkingen og etter at overvåkingen er avsluttet. Avhengig av hvilket stadium kontrollen skjer på, ligger det i sakens natur at saksbehandlingen må være hemmelig. At det i disse tilfellene ikke er mulighet for kontradiksjon stiller særlige krav til saksbehandlingen, som må kompensere for at den eller de det gjelder ikke har anledning til å ta til motmæle og at saken fremlegges av en part som allerede mener det er nødvendig å iverksette de aktuelle virkemidlene. EMD har i flere saker lagt til grunn at det er «desirable» at kompetansen til å autorisere hemmelig overvåking legges til domstolene, som regelmessig har sterk institusjonell uavhengighet og forsvarlig saksbehandling.[34] Det er imidlertid hverken nødvendig eller i seg selv tilstrekkelig at autorisasjonskompetansen legges til domstolene. Som EMD videre la til grunn i Roman Zakharov mot Russland avsnitt 257 beror det i alle tilfeller på en nærmere vurdering:

[33] *Roman Zakharov v. Russland* (no. 47143/06) avsnitt 233.

[34] *Roman Zakharov v. Russland* (no. 47143/06) avsnitt 233.

> "The Court will take into account a number of factors in assessing whether the authorisation procedures are capable of ensuring that secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration. These factors include, in particular, the authority competent to authorise the surveillance, its scope of review and the content of the interception authorisation."

At kompetansen til å autorisere overvåking legges til domstolene, tillegges generelt vekt i positiv retning, forutsatt at domstolen er uavhengig og saksbehandlingen er forsvarlig. I lys av det overordnede målet om å sikre at overvåkingen er i henhold til lov og forholdsmessig, ses det det imidlertid også hen til rekkevidden og innholdet av domstolens prøving, samt innholdet i rettens avgjørelser.

I spørsmålet om rekkevidden og innholdet av prøvingen, er det sentralt at domstolen har tilgang på alle relevante opplysninger og reelt sett kan prøve om overvåkingen er i henhold til lov og forholdsmessig.[35] I forlengelsen av dette har EMD også lagt til grunn at kontrollen normalt bør forestås av en «judge with special expertise».[36] Vekten av dette momentet vil nok i praksis avspeile hvor teknisk komplisert det er å reelt vurdere saken, herunder implikasjonene av å iverksette de aktuelle overvåkingstiltakene. For så vidt gjelder innholdet i avgjørelsen som autoriserer overvåkingen har EMD lagt til grunn følgende:[37]

> "Lastly, as regards the content of the interception authorisation, it must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such identification may be made by names, addresses, telephone numbers or other relevant information (…)"

Denne rettssetningen er neppe direkte anvendelig i den grad EMD aksepterer bulkovervåking. Den bærer likevel klart bud om at tillatelsen må være relativt spesifikk. For bulkovervåking vil muligheten for spesifisering i stor grad bero på hvilket stadium i overvåkingsprosessen domstolkontrollen skjer, men det er klart at styrket kontroll også i relasjon til autoriseringen vil være av betydning i den menneskerettslige vurderingen.

Et videre aspekt ved innretningen av autorisasjonssystemet er hvilken funksjon autorisasjonen har. I Roman Zakharov avsnitt 269 viste EMD til følgende:

> "The Court considers that the requirement to show an interception authorisation to the communications service provider before obtaining access to a person's communications is one of the important safeguards against abuse by the law-

[35] *Roman Zakharov v. Russland* (no. 47143/06) avsnitt 261.

[36] *Szabó og Vissy v. Ungarn* (no. 37138/14) avsnitt 77.

[37] *Roman Zakharov v. Russland* (no. 47143/06) avsnitt 264.

> enforcement authorities, ensuring that proper authorisation is obtained in all cases of interception."

Selv om det neppe er nødvendig, ser EMD på dette som et viktig virkemiddel for å motvirke misbruk. I kontekst av bulkovervåking vil det innebære at private tilbydere må forelegges avgjørelse fra retten før de kan gi tilgang til bulkinnsamling. Hvilken betydning det vil ha om det integreres en slik mekanisme kommer nok særlig an på hvilke stadier i overvåkingsprosessen det ellers er integrert kontrollmekanismer og hva den øvrige kontrollen går ut på.

EMD ser helhetlig på kontrollsystemet. Svakheter ved autorisasjonskontrollen kan som utgangspunkt oppveies ved mekanismer som ivaretar gjennomførings- og etterhåndskontroll, men ikke i alle tilfeller, f.eks. hvor overvåkingen er rettet mot pressen:[38]

> "In that connection the Court held that a post factum review cannot restore the confidentiality of journalistic sources once it is destroyed (…). For the Court, supervision by a politically responsible member of the executive, such as the Minister of Justice, does not provide the necessary guarantees."

Gjennomførings- og etterhåndskontrollen kommer vi tilbake til nedenfor under punkt 4.6.

På bakgrunn av redegjørelsen over vil vi i det følgende gå nærmere inn på konkrete deler av forslaget som gjelder autorisasjon av overvåkingen og domstolkontroll.

(vii) Domstolkontrollen og stadiene i innsamlingen

I forslaget kommer domstolkontrollen inn på det som kan karakteriseres som det tredje stadiet i bulkinnsamlingsprosessen, hvor det allerede er valgt en kommunikasjonsbærer og samlet inn store mengder data, hvorav noe allerede er filtrert ut. Rettens oppgave er å ta stilling til E-tjenesten begjæringer om å foreta søk etter forslagets § 7-8 og innhenting og lagring etter § 7-9.

På bakgrunn av EMDs praksis og det omfattende inngrepet i retten til privatliv som skjer på de foregående stadiene i innsamlingsprosessen, mener NIM det er grunn til å vurdere om det også bør legges inn domstolkontroll på et tidligere stadium.

Slik forslaget er utformet er det gode grunner som tilsier at tilretteleggingsplikten og omfanget av den bør være gjenstand for domstolkontroll. Forslaget inneholder ikke mekanismer som ivaretar at E-tjenesten begrenser innsamlingen til kommunikasjonsbærere som er nødvendige ut fra formålet. Dertil kommer at det heller ikke er klart hvem som vil omfattes av tilretteleggingsplikten. Riktignok er det lagt opp til at EOS-utvalget skal føre kontroll med gjennomføringen, men utvalget har ikke kompetanse til å treffe bindende avgjørelser. NIM mener det er grunn til å vurdere om

[38] *Szabó og Vissy v. Ungarn* (no. 37138/14) avsnitt 77.

tilretteleggingsplikten skal forutsette rettslig kjennelse. I denne sammenhengen kan man også se for seg mulighetene for å differensiere mellom tilbydere som er omfattet av ekomloven og andre, slik at domstolkontroll kun er påkrevet for den sistnevnte gruppen hvorav aktørene ikke allerede er definert. NIM mener at kjennelsene også bør kunne være tidsbegrensede for å sikre kontinuitet i vurderingen av om det er nødvendig å innhente fra den enkelte tilbyder. Domstolkontroll på dette stadiet vil også kunne bidra til å praktisk klargjøre hva tilretteleggingsplikten innebærer for den enkelte tilbyder, herunder særlig hvilken kryptering tilbyderne skal legge til rette for at E-tjenesten kan forbigå.

(viii) Teknisk og etterretningsfaglig kompetanse

Det må sikres at domstolkontrollen er reell og holder høy kvalitet. Avgjørelser etter forslaget § 8-1 synes å forutsette betydelig grad av etterretningsfaglig og teknisk kompetanse. Det er f.eks. svært vanskelig å vurdere om et søk på grunnlag av en modusselektor er forholdsmessig eller ikke, uten å vite noe mer om omfanget av søkeresultater, mv. Likeledes vil det være vanskelig å vurdere i hvilken utstrekning det f.eks. kan medføre at søk frembringer opplysninger om personer i Norge eller kommunikasjon med særlig vern.

Behovet for særskilt kompetanse er fremhevet av EMD. Ettersom det er lagt opp til at avgjørelsene skal treffes av ordinære dommere, er det nærliggende at retten gis fagkyndig bistand. Av hensyn til domstolens uavhengighet er NIM i utgangspunktet lite positive til forslaget om at dette alene ivaretas ved E-tjenesten selv medbringer fagkyndig. Etter NIMs oppfatning bør det legges opp til et spor hvor domstolen kan innhente uavhengig faglig bistand, og på den måten også sikre at domstolens kontroll oppleves som reell, effektiv og uavhengig.

(ix) Rettens tilgang på ytterligere opplysninger

I forslaget er det ikke sagt noe nærmere om hvilke konkrete opplysninger retten skal ha tilgang på, utover det som skal fremgå av begjæringen etter § 8-2.

For at retten skal anses å ha mulighet til å foreta en fullstendig prøving av saken, bør det fremgå eksplisitt at retten skal ha tilgang på alle relevante opplysninger i saken og at retten helt generelt kan kreve fremlagt ytterligere opplysninger. At retten skal ha slik tilgang synes forutsatt i høringsnotatet på side 238.

(x) Særskilt advokat

I forslaget § 8-5 første ledd fremgår det at retten «kan» beslutte at det skal oppnevnes en særskilt advokat for å ivareta rettighetene til dem innhentingen retter seg mot. For å kompensere for fraværet av ordinær kontradiksjon, mener NIM at det alltid bør oppnevnes særskilt advokat.

(xi) E-tjenestens begjæringer og rettens kjennelser

I høringsnotatet på side 238 fremgår det at det er tilstrekkelig at E-tjenestens begjæringer «består av et sakskompleks». Det fremstår uklart hvilken grad av spesifisering det her er snakk om. Videre på samme sted i høringsnotatet fremgår det at det ikke er lagt opp til et krav om at begjæringene må «individualiseres». Her må det klargjøres nærmere hvor omfattende eller avgrensede E-tjenestens begjæringer må være, noe som igjen spiller inn på omfanget av rettens kjennelser. Som det fremgår over, har EMD lagt vekt på i hvilken grad kjennelser som autoriserer overvåking er spesifiserte. For å sikre en kvalitativt forsvarlig domstolkontroll, mener NIM det er viktig at det fastsettes kriterier som avgrenser omfanget av begjæringene på en måte gjør at rettens vurdering ikke bare knytter an til generelle behov i et overordnet sakskompleks, men heller de konkrete stadiene i saken som gjør søk og innhenting nødvendig. Det fremgår for eksempel av lovforslaget § 8-6 at rettens tillatelse ikke skal gis lenger enn nødvendig. For at domstolene skal kunne vurdere dette på en forsvarlig måte, er det nødvendig at begjæringen inneholder informasjon om begrunnelse for foreslått tidsramme slik at domstolen også har mulighet til å begrense denne etter en selvstendig vurdering. Retten skal dessuten kontrollere at E-tjenesten ikke behandler personopplysninger utelukkende på bakgrunn av hva som er kjent om en persons «etnisitet eller nasjonale bakgrunn, politiske, religiøse eller filosofiske overbevisning, språk, politiske virksomhet, fagforeningstilhørighet eller helsemessige eller seksuelle forhold.» For å kunne foreta en meningsfull kontroll av dette, kreves også mer konkretisert innsikt i hvilke vurderinger som ligger bak E-tjenestens begjæring.

I høringsnotatet på side 238 fremgår det at E-tjenesten i sin begjæring skal angi hva eller hvem søkene rettes mot, men at den ikke må angi hvilke søkebegreper som skal benyttes.

Søkebegrepene vil være direkte avgjørende for hva E-tjenesten får tilgang på og omfanget av tilgangen. Følgelig er det vanskelig å se annet enn at søkebegrepene nødvendigvis utgjør den direkte og avgjørende faktoren for om søk og innhenting er forholdsmessig i konkrete saker. En ordning der retten kun tar stilling til abstraherte person- og moduselektorer og E-tjenesten utarbeider konkrete søkekriterier på grunnlag av disse, vil potensielt gi E-tjenesten et betydelig skjønn ved påfølgende innhenting og søk, noe som skaper en ganske klar risiko for misbruk. Videre kommer det at EOS-utvalget ikke er bemyndiget til å stanse søk eller slette informasjon fra søk som ikke omfattes av kjennelsen eller som er uforholdsmessige.

For at rettens prøving skal anses fullstendig, mener NIM at E-tjenestens begjæring bør inneholde søkebegreper og at E-tjenesten med rettens kjennelse ikke kan gå ut over disse. Dette medfører også at retten kan ekskludere enkelte søkekriterier, f.eks. hvis det er stor risiko for at disse vil frembringe særlig beskyttet kommunikasjon eller i for stor grad ramme personer i Norge. Hvis det viser seg at de aktuelle søkebegrepene ikke er tilstrekkelige og at andre søkebegreper kan frembringe relevante resultater, kan E-tjenesten fremme en ny begjæring for retten. Dette kan medføre at E-tjenesten i en

operasjon må begjære flere tillatelser, noe som igjen bidrar til minimalisering og ivaretakelse av at søk og innhenting begrenses til hva som er nødvendig og forholdsmessig.

(xii) Tilgang på rettspraksis

I Høringsnotatet på side 153 står det:

> «I forholdsmessighetsregelen ligger det implisitt et krav om objektivitet, likebehandling av like tilfeller, saklighet og plikt til ikke å legge vekt på utenforliggende hensyn.»

Den enkelte dommer som skal avgjøre saken alene, må ha tilgang til tidligere rettspraksis, slik at det blir en enhetlig tolkning av loven. Tilgangen bør være elektronisk og søkbar.

NIM mener også at avgjørelsene bør offentliggjøres i anonym form i den grad hensynet til hemmelighold ikke gjør seg gjeldende.

4.6. Gjennomføringskontroll og etterkontroll

(xiii) Rettslige utgangspunkter

For å etterse at overvåkingen skjer innenfor rammen av en forutgående autorisasjon og for øvrig er i samsvar med loven og er forholdsmessig, kan gjennomførings- og etterkontroll etter omstendighetene ha stor betydning i vurderingen av forholdet til EMK artikkel 8.[39]

Kontrollmyndigheten må være uavhengig fra myndigheten som forestår overvåkingen og må være tillagt kompetanse som muliggjør effektiv og kontinuerlig kontroll. Et sentralt moment i vurderingen av gjennomførings- og etterkontrollsystemer er hvilken myndighet kontrollorganet har[40]

Det tillegges vekt i positiv retning at kontrollorganet har myndighet til å fastsette at overvåkingen avsluttes eller at det innhentede materialet slettes. At kontrollorganet ikke har slik myndighet er ikke avgjørende, men vil være et moment i helhetsvurderingen av hvorvidt nødvendige rettsikkerhetsmekanismer er på plass.

Videre er det av sentral betydning at kontrollorganet ikke bare har nødvendige formelle rammebetingelser, herunder tilgang og innsyn mv., men også om kontrollorganet har tilstrekkelig kompetanse og ressurser.

(xiv) EOS-utvalgets særlige kontrollfunksjon

[39] *Kennedy v. Storbritannia* (26839/05) avsnitt 166.

[40] *Roman Zakharov v. Russland* (no. 47143/06) avsnitt 275 og 282.

I forslaget § 2-8, jf. § 7-11 er EOS-utvalget tillagt en særlig oppgave ved å føre «styrket kontroll» med E-tjenestens bruk av tilrettelagt innhenting. I den forbindelse skal EOS-utvalget ha tilgang på all informasjon som er av betydning for tilrettelagt innhenting.

Det legges altså opp til at EOS-utvalget skal føre både løpende kontroll og etterkontroll.

Slik NIM ser det, skaper særlig den løpende kontrollen noen utfordringer i lys av EOS-utvalgets arbeidsform. Som konsekvens av en intensivert løpende kontroll er det f.eks. nærliggende at det kan oppstå saker eller problemstillinger som er tidssensitive. Det kan være vanskelig å forene med at utvalget ikke er permanent samlet og at utvalget bare er beslutningsdyktig med fem medlemmer til stede. Dette skaper en treghet i arbeidsformen som klart innvirker på effektiviteten av den løpende kontrollen. NIM mener derfor at det bør vurderes om sekretariatet, eventuelt ved sekretariatsleder bør ha hastekompetanse til å treffe beslutninger, som senere behandles av utvalget. Mer generelt kan man tenke seg at de funksjonene som knytter seg til den styrkede kontrollen operasjonaliseres på en mer selvstendig måte, uavhengig av den mer tradisjonelle kontrollen som EOS-utvalget forøvrig foretar, og som er tilpasset at dette er en kontroll som skal utføres i sanntid og som ikke nødvendigvis så lett lar seg forene med en utvalgsmodell.

(xv) Avgjørelsesmyndighet

I den helhetlige vurderingen av forholdet til EMK artikkel 8 vil det slå positivt ut dersom EOS-utvalget gis kompetanse til å treffe bindende avgjørelser. I så fall er det nærliggende at EOS-utvalget bør ha myndighet til å avgjøre opphør av iverksatte overvåkingstiltak, sletting av innhentede opplysninger, samt fastsette erstatning for rettskrenkelser. Hvis denne kompetansen kan utøves av eget tiltak i forbindelse med kontrollvirksomheten og på grunnlag av enkeltsaker, vil det også sikre ivaretakelse av kravet til effektivt rettsmiddel, som er omtalt nedenfor.

NIM tviler ikke på at EOS-utvalgets arbeidsform under nåværende omstendigheter fungerer godt, men utvalget er selv tydelige på at de utfører stikkprøvekontroller og ikke har kapasitet utover dette. Innføring av et bulkinnsamlingssystem, som potensielt er omfattende, og som vil stille strenge krav til effektiv kontroll, innebærer en ganske betydelig endring i forutsetningene for EOS-utvalgets nåværende kompetanse og arbeidsform.

Som en innvending mot at EOS-utvalget skal ha formell beslutningsmyndighet er det fremholdt at det vil «rokke ved grunnleggende prinsipper i vårt statsrettslige system» dersom et organ underlagt Stortinget treffer avgjørelser med bindende virkning for et organ underlagt den utøvende makt. Riktignok kan en slik kompetanse fremstå utradisjonell, men det er vanskelig å se at det skulle foreligge noen absolutte konstitusjonelle hinder for en slik ordning. NIM mener det er grunn til at denne problemstillingen vurderes nærmere. Hvis konklusjonen skulle være at en slik ordning ikke er konstitusjonelt mulig, mener vi at kontrollsystemet for tilrettelagt innhenting bør

revurderes mer helhetlig, eventuelt slik at departementet følger opp noe i retning av Lysne II-utvalgets forslag om et «DGF-tilsyn», som EOS-utvalget igjen vil føre kontroll med.

(xvi) Ressurser og kapasitet

For at kontrollen skal være effektiv er det helt sentralt at EOS-utvalget tildeles tilstrekkelige ressurser og kapasitet. NIM har ikke forutsetninger for å vurdere hvilken tilførsel av personell og teknologiske ressurser som er nødvendig. Sett i lys av at EOS-utvalget er et uavhengig kontrollorgan, mener NIM det er naturlig at EOS-utvalgets egen behovsvurdering må veie tungt. Det bemerkes imidlertid at for EOS-utvalget vil funksjonen knyttet til styrket kontroll innebære en betydelig endring i omfanget av oppgaver. Fra en situasjon hvor involvering av norske borgere i E-tjenestens portefølje var en unntaksregel, vil innføring av tilrettelagt innhenting innebære at norske borgeres kommunikasjon regulært blir samlet inn av E-tjenesten. I forslaget er det lagt opp til at E-tjenesten skal få tilført 4 ekstra stillinger i sekretariatet for å ivareta disse nye funksjonene. Med dette utgangspunktet for øye, stiller NIM spørsmål ved hvorvidt dette gjenspeiler de omfattende oppgavene som E-tjenesten er ment å ivareta gjennom forslaget, og da særlig med tanke på den nye funksjonen som den styrkede, løpende kontrollen er ment å ivareta.

(xvii) Merking av data

Tilrettelagt innhenting vil medføre behandling av store datamengder. En viktig del av EOS-utvalgets kontroll vil være å etterse at dataene behandles i henhold til loven, f.eks. at det ikke deles overskuddsinformasjon med PST, som EOS-utvalget også kontrollerer. Denne kontrollen forutsetter at det er mulig å identifisere hvor dataene kommer fra. En form for merking av dataene vil bedre forutsetningene for EOS-utvalgets mulighet for å kontrollere at dataene behandles på riktig måte og f.eks. ikke deles ut over det loven tillater. Tilsvarende vil en form for merking også effektivisere kontrollen med behandlingen av testdata.

4.7. Notifikasjon og rettsmidler

(xviii) Rettslige utgangspunkter

Et sentralt moment i vurderingen om overvåkingssystemer er kompatible med EMK artikkel 8 er om den som overvåkes gis etterfølgende notifikasjon og tilgangen på effektive rettsmidler. Det er nær sammenheng mellom disse to komponentene. Sammenhengen er at reell tilgang på effektive rettsmidler normalt forutsetter informasjon om at man har blitt overvåket. Følgende uttalelse fra EMD er illustrerende:[41]

[41] *Szabó og Vissy v. Ungarn* (no. 37138/14) avsnitt 86. Se tilsvarende *Roman Zakharov v. Russland* (no. 47143/06) avsnitt 287.

> "Moreover, the Court has held that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for any recourse by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their justification retrospectively. As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should be provided to the persons concerned (…)"

Fravær av notifikasjon er imidlertid ikke problematisk hvis et uavhengig organ kan ta stilling til saken med endelig virkning uten at det er nødvendig å påvise at man har blitt overvåket. *I Kennedy v. Storbritannia* (no. 26839/05) avsnitt 167 la EMD blant annet til grunn følgende:

> "The jurisdiction of the IPT does not, therefore, depend on notification to the interception subject that there has been an interception of his communications. (…) In the event that the IPT finds in the applicant's favour, it can, inter alia, quash any interception order, require destruction of intercept material and order compensation to be paid (…)."

Det sentrale her var at det aktuelle organet var institusjonelt uavhengig og upartisk, hadde en omfattende prøvingsadgang, herunder tilgang på alle nødvendige opplysninger, og videre hadde kompetanse til å tilsidesette overvåkingstillatelser, beslutte sletting av innhentede opplysninger og fastsette erstatning

(xix) Notifikasjon

På bakgrunn av utgangspunktene over mener NIM at det prinsipielt sett blir feil å oppstille en kategorisk regel om at den som har blitt overvåket ikke skal notifiseres, jf. forslaget § 11-8. Hovedregelen er at den som har vært gjenstand for informasjonsinnhenting har krav på notifikasjon. Fra denne hovedregelen er det adgang til å fastsette til dels omfattende unntak som ivaretar behovet for hemmelighold.

Forutsetningen for at det ikke under noen omstendighet skal gis notifikasjon må i så fall være at det er tilgang på effektivt rettsmiddel uten at det er nødvendig å påvise at man har blitt utsatt for overvåking.

(xx) Rettsmidler

NIM er ikke overbevist om at forslaget i tilstrekkelig grad ivaretar kravet om effektivt rettsmiddel, slik det er innfortolket som et element i EMK artikkel 8 og selvstendig følger av EMK artikkel 13.

Selv om det nok i praksis kan ha betydning at EOS-utvalget anbefaler at det utbetales erstatning for rettskrenkelse, kan det forekomme at staten ikke tar anbefalingen til følge,

hvoretter staten i et påfølgende sivilt søksmål ikke opphever bevisforbudet etter tvisteloven § 22-1, som etter omstendighetene kan være nødvendig for en fullstendig prøving av saken. Under slike omstendigheter vil klager i realiteten være avskåret fra et effektivt rettsmiddel.

Avhengig av hvordan de konstitusjonelle forholdene rundt EOS-utvalget bedømmes, er den mest åpenbare løsningen på dette problemet å gi EOS-utvalget kompetanse til å vedta erstatning i enkeltklagesaker.

NIM antar at en alternativ løsning kan være å legge opp til et behandlingsspor i domstolen som muliggjør at retten kan prøve saken fullt ut, samtidig som nødvendig hemmelighold ivaretas.

4.8. Kort om bulkinnsamling av kommunikasjon via satellitt

Bulkinnsamling som forutsetter tilrettelegging etter forslaget § 7-2 er underlagt særlige rettssikkerhetsmekanismer i forslaget kapittel 7 og 8. I medhold av forslaget § 6-7 kan E-tjenesten også foreta bulkinnsamling av kommunikasjon via satellitt. Slik innsamling er ikke underlagt bestemmelsene i forslaget kapittel 7 og 8.

På bakgrunn av de rettslige utgangspunktene og nærmere vurderingene som er gjort i over om tilrettelagt innhenting, mener NIM det er grunn til å vurdere om tilsvarende rettssikkerhetsmekanismer bør gis anvendelse for bulkinnsamling av kommunikasjon via satellitt. NIM mener at dette kan være nødvendig, særlig i tilfeller der slik overvåking berører personer i Norge, jf. forslaget § 4-2 syvende ledd.

5. Ytringsfrihet og kildevern

5.1. Innledning

Flere deler av lovforslaget berører ytringsfriheten. NIM vil konsentrere sine kommentarer om kildevernet og pressefriheten, som sentrale deler av ytringsfrihetens vern.

Som nevnt innledningsvis, er oversiktsvansker er et signal NIM har mottatt fra flere høringsinstanser. Dette er et signal departementet bør ta på alvor, blant annet siden det kan ha noe å si for det foreslåtte systemets tillit hos pressen, deres kilder og allmennheten – og slik kan ha noe å si for hvilken *nedkjølende effekt* forslaget kan ha for kildevernet og ytringsfriheten, dersom det skulle bli innført. Mangel på transparens og oversikt vil kunne ha (negative) menneskerettslige implikasjoner i seg selv.[42]

5.2. Kildevernet generelt og vernets begrunnelse

[42] Til illustrasjon, se nylige, ikke-rettskraftige *Big Brother Watch v. Storbritannia* (58170/13, 62322/14 og 24960/15) avs. 492.

Ytringsfriheten er beskyttet av Grunnloven § 100, EMK artikkel 10 og FNs konvensjon om sivile og politiske rettigheter artikkel 19. Ethvert inngrep i ytringsfriheten må oppfylle de tre vilkårene for inngrep: Inngrepet må ha lovhjemmel, ivareta et legitimt formål og inngrepet må være nødvendig (herunder forholdsmessig).[43]

Pressefriheten, herunder kildevernet, er en sentral del av ytringsfriheten, og nyter et særlig sterkt vern.[44] EMDs praksis viser at nødvendighetsvurderingen i kildevernsaker er svært streng. Det er et område hvor EMD foretar en relativ intens prøving av nødvendigheten – og statens såkalte skjønnsmargin er tilsvarende begrenset. Terskelen for å gripe inn i kildevernet er at inngrepet må være «justified by an overriding requirement in the public interest».[45]

Den høye terskelen for inngrep og den intense prøvingen, må forstås i lys av kildevernets begrunnelse. Kildevernet (mis)forstås tidvis som et privilegium for journalister. Men som både EMD og Høyesterett har understreket, er begrunnelsen for vernet hensynet til samfunnet som helhet: Uten et solid kildevern kan ikke pressen ivareta sine viktige samfunnsroller som offentlig vaktbikkje, informasjonskanal og tilrettelegger for den offentlige samtale – som alle er av vesentlig betydning for å realisere og sikre sentrale hensyn bak ytringsfriheten.[46]

Et inngrep i kildevernet kan derfor ikke kun vurderes på bakgrunn av de negative virkninger det vil ha i den konkrete sak. Det må vurderes helhetlig ut fra den negative virkning et slikt inngrep vil ha i en bredere samfunnsmessig kontekst. Dersom potensielle kilder ikke har tilstrekkelig tillit til at deres anonymitet vil bli ivaretatt, vil det kunne svekke pressens kildetilfang generelt (gi en «nedkjølende effekt») – med de negative konsekvenser det vil ha for pressens mulighet til å utøve sine nevnte oppgaver på vegne av samfunnet.[47] Det er den nedkjølende effekten som «any perceived interference» med pressens fortrolige kommunikasjon og kildenes anonymitet kan gi, som følgelig kan bli sentralt i vurderingen, og som typisk vil kunne være relevant i tiknytning til etterretningsområdet.[48]

I tillegg til å være beskyttet av ytringsfriheten mot statlige inngrep (statens *negative* plikt), har kildevernet også en klar side til statens *positive* plikt til å sikre ytringsfriheten, jf. blant

[43] Noe ulikt regulert i hhv. EMK artikkel 10 (2), SP artikkel 19 (3) og Grunnloven § 100 (2) og (3), men vurderingen vil i det vesentlige være lik. Det er imidlertid ingen automatikk i at terskelen for inngrep vil være lik i et konkret tilfelle. NIM vil i det videre konsentrere seg om EMK artikkel 10. Årsaken til dette er primært (praktisk) grunnet tilfanget av praksis om denne type saker som knytter seg til EMK artikkel 10 – fra både EMD og Høyesterett.

[44] Bl.a. understreket i EMDs praksis, jf. f.eks. *Goodwin v. Storbritannia* (17488/90) avs. 39–40, som er referert til en rekke ganger senere av EMD og Høyesterett.

[45] Jf. bl.a. *Goodwin v. Storbritannia* avs. 39–40, *Sanoma Uitgevers B.V. v. Nederland* (38224/03) avs. 51 og *Financial Times og andre v. Storbritannia* (821/03) avs. 59–63.

[46] Ibid.

[47] Se f.eks. Rt. 2013 side 1210 avs. 34, med henvisning til Rt. 2010 side 1381 (avs. 62), hvor Høyesterett fastslår at det må ses hen til «den mer langsiktige effekten av å skulle gjøre unntak – den såkalte 'chilling effect'», og at det i «det lange løp er [...] en risiko for at en mer utstrakt bruk av vitneplikt vil kunne medføre at viktige kilder blir borte».

[48] Som illustrert av nylige, ikke-rettskraftige *Big Brother Watch v. Storbritannia* (58170/13, 62322/14 og 24960/15) avs. 495.

annet Grunnloven § 100 sjette ledd.[49] NIM går ikke her nærmere inn på den positive plikten, herunder ikke nærmere inn på sondringen mellom statens positive og negative menneskerettslige forpliktelser (som her kan være glidende og overlappende), men understreker at et velfungerende kildevern vil være av sentral betydning for å oppfylle Grunnloven § 100 sjette ledd.

I vurderingen av om et inngrep i kildevernet oppfyller den strenge nødvendighetsvurderingen som EMD har oppstilt, er det sentralt for vurderingen hvilke kontrollmekanismer og rettssikkerhetsgarantier som foreligger, for å sikre at kildevernet (og den høye inngrepsterskelen) blir ivaretatt og for å forhindre misbruk.[50]

5.3. Kildevernets virkeområde (særlig § 9-6)

Lovforslagets § 9-6 har, i det minste intuitivt, den mest åpenbare siden til kildevernet. Dette er en sekkebestemmelse for E-tjenestens behandling av fortrolig kommunikasjon med særlige yrkesutøvere, deriblant kommunikasjon mellom journalist og kilde. NIM vil her konsentrere seg om kildeverndelen.[51]

Det er positivt at departementet gjennom lovteksten søker å sette opp særskilte skranker for behandlingen av denne typen opplysninger.

Hvorvidt en slik sekkeregulering generelt er hensiktsmessig er ikke nødvendigvis NIMs oppgave å mene noe om. NIM ønsker likevel å understreke at slike sekkereguleringer kan ha sine utfordrende sider fra et menneskerettslig ståsted: For eksempel ved at vilkår og reguleringer blir romslige. Betydningen av tydelige vilkår når det kommer til kildevernet, kommer NIM tilbake til under punkt 5.4. Et alternativ til sekketilnærmingen vil være å dele opp bestemmelsen og innta mer differensierte og konkrete terskler. For eksempel ved at kildevern skilles ut til en egen bestemmelse, slik dette er gjort i straffeprosessloven og tvisteloven. En annen lignende innsigelse kan til en viss grad gjøres gjeldende for kildevernreguleringens nære kobling til personopplysningsbehandling i lovforslaget. Også denne koblingen kan potensielt medføre at reguleringen eller praktiseringen fører noe galt av sted (sammenlignet med de hensyn kildevernet er ment å ivareta).

Kildeopplysningene som etter § 9-6 gis et særskilt vern, er knyttet til om opplysningene er å anse som «fortrolig kommunikasjon» mellom (i denne sammenheng) journalist og kilde. Dette er, så vidt NIM forstår forslaget, ikke i samsvar med hvilken informasjon som omfattes av kildevernet i henhold til EMDs praksis.

---

[49] Grl. § 100 (6): «Det påligger statens myndigheter å legge forholdene til rette for en åpen og opplyst offentlig samtale.» Den positive plikten følger også som en del av EMK og SP (dog ikke like eksplisitt av ordlyden), se f.eks. EMDs dom i *Appleby og andre v. Storbritannia* (44306/98).

[50] Se f.eks. *Sanoma Uitgevers B.V. v. Nederland* (38224/03) avs. 88 flg.

[51] NIM har i denne høringsuttalelsen ikke prioritert å kommentere nærmere på andre typer «fortrolig kommunikasjon» med et særlig menneskerettslig vern. NIM understreker, slik departementet også anerkjenner i høringsnotatet, at blant annet kommunikasjon mellom advokat og klient vil nyte et slikt vern og at man må sørge for at dette vernet ivaretas på en tilfredsstillende måte. Flere av NIMs kommentarer knyttet til hvordan kildevernet best kan ivaretas, vil kunne ha generell verdi i denne sammenheng.

Etter EMDs praksis er det ikke avgjørende for vurderingen av om opplysningene omfattes av kildevernet, hvor de stammer fra eller mellom hvem de utveksles (for eksempel mellom journalist og kilde, selv om det naturligvis ofte kan være tilfellet). Det avgjørende kan heller sammenfattes som hvorvidt opplysningene er *egnet til å avsløre* en kildes identitet.[52] Justis- og beredskapsdepartementet har nylig sendt forslag til endringer i kildevernreglene i straffeprosessloven og tvisteloven på høring, med mål om å endre kildevernreglenes ordlyd til bedre å reflektere den høye inngrepsterskelen som følger av praksis fra EMD og Høyesterett.[53] Et av forslagene til Justis- og beredskapsdepartementet er nettopp å kodifisere at kildevernet omfatter alle opplysninger som er egnet til å avsløre kilder.[54]

Det er uklart for NIM om forslaget i § 9-6 er ment å innebære noen begrensning med hensyn til hvilket format opplysningene kan stamme fra – om det må være fra selve «kommunikasjonen» (eposter etc.) mellom journalist og kilde. Dette vil i tilfellet være en avsporing sammenlignet med hva som er relevant å vurdere i henhold til EMDs praksis. Kildevernet har ikke nødvendigvis for øye å verne kommunikasjonen som sådan, men å verne den generelle tilliten til at kilders identitet forblir anonym (uavhengig av hvordan identiteten eventuelt kan avsløres). Det vil også være en avsporing om det her legges opp til en eventuell vurdering av hvorvidt vedkommende er «journalist» i tradisjonell forstand eller lignende. [55] Når lovforslaget viser til «tilsvarende fortrolig kommunikasjon» er det uklart om dette sikter på andre kategorier av personer enn de som er listet opp i § 9-6 første ledd, eller om det siktes til kommunikasjon som sådan.

NIM anbefaler at vilkåret for hvilken informasjon som gis et særlig vern gjøres mer fleksibel og i større grad knyttes opp mot hvorvidt opplysninger (uansett format, mellom hvem etc.) er egnet til å avsløre kilder. NIM forstår at dette i praksis kan være mer krevende å regulere, men NIM savner en vurdering av dette og eventuelle alternative reguleringer. Dette er noe som bør foretas i det videre lovarbeidet. En alternativ regulering kan være at vilkåret i tillegg knytter seg mer til hvorvidt opplysningene stammer fra journalistisk materiale eller lignende (se også punkt 5.9 nedenfor).

Videre er det uklart for NIM fra hvilket tidspunkt, og i hvilke tilfeller i E-tjenestens virksomhet at skranken i § 9-6 kommer til anvendelse. Og viktigere, i hvilke eventuelle tilfeller skranken ikke kommer til anvendelse. NIM mener det bør presiseres i ordlyd eller forarbeider om hvilke tilfeller eller fra hvilke tidspunkt i innsamling/søk/lagring/behandlingsprosessen (om noe tidspunkt) som «kildevernet» i §

[52] Se bl.a. *Nagla v. Latvia* (73469/10) avs. 81, *Financial Times og andre v. Storbritannia* (821/03) og Rt. 2015 side 1286 avs. 54.
[53] Høringsbrev og høringsnotat av 24. september 2018 fra Justis- og beredskapsdepartementet. NIMs høringsuttalelse til dette forslaget av 1. februar 2019 er tilgjengelig på www.nhri.no.
[54] Ibid. bl.a. side 4, 65 og 71.
[55] F.eks. Rt. 2015 side 2308 gjaldt en dokumentarfilmskaper, hvor Høyesterett kom til at det foreslå et ulovlig inngrep i kildevernet. Også på dette punkt kan det være nyttig å se hen til Justis- og beredskapsdepartementets nylige forslag og vurderinger, se høringsnotatet (ibid.) pkt. 5.

9-6 ikke vil gjelde. Man bør i forarbeidene kommentere og trekke opp grensene mellom ulike tilfeller/tidspunkt hvor bestemmelsen i praksis vil komme til anvendelse eller ikke komme til anvendelse, herunder tydeliggjøre hva som ligger i ordlyden «behandle opplysninger» i denne sammenheng. Dette gjelder for eksempel opp mot metadatalageret, kortidsdatalageret, tilbydere, åpne kilder etc.

I den grad man gjennom ordlyden har ment å begrense anvendelsesområdet til skranken, mener NIM at nødvendigheten av dette må begrunnes nærmere opp mot kildevernet (inkludert nevnte EMD-vurdering av hvorvidt opplysninger er egnet til å avsløre kilder). Med forbehold om at NIM kan ha misforstått noe, er NIM generelt usikker på hvordan kildevernet sikres ivaretatt på de ulike stadiene i innsamling/søk/lagring/behandlingsprosessen, herunder er NIM usikker på om og hvordan kildevernet vil ivaretas i forbindelse med den nåværende generelle domstolkontrollen etter § 8-1. Sammenhengen og grenseoppgangen mellom den generelle kontrollen i § 8-1 og den særskilte kontrollen i § 9-6 er også uklar for NIM (se punkt 5.5 nedenfor).

NIM er også forbeholden til forslaget til det *eksplisitte* unntaket fra § 9-6. Dette foreslåtte unntaket (i § 9-7) fremstår som (for) vidt og uklart i NIMs øyne (se punkt 5.7 nedenfor).

5.4. Terskel/vilkår for å fravike kildevernet (etter § 9-6)

Det er positivt at departementet har sett hen til den menneskerettslige terskelen i tilknytning til når skranken i § 9-6 skal komme til anvendelse, og at departementet slår fast at skranken må tolkes og anvendes i lys av menneskerettslige forpliktelser (noe som naturligvis vil gjelde uavhengig av utformingen i nasjonalt lovverk).

EMD-terskelen for inngrep i kildevernet, «justified by an overriding requirement in the public interest», er søkt oversatt til norsk på ulike måter i ulike sammenhenger. Det er ikke nødvendigvis mulig eller avgjørende å gi noen fullgod oversettelse i en norsk lovtekst. Men av hensyn til dem som skal anvende disse reguleringene i praksis, både kontrollere i forkant og i etterkant, mener NIM det vil være en fordel om ordlyden i så stor grad som mulig reflekterer nevnte terskel og er så klar som mulig.[56]

Departementets forslag til inngrepsterskel lyder: «[...] med mindre vektige samfunnshensyn gjør behandlingen strengt nødvendig». NIM stiller spørsmål ved om dette er den ordlyden som best gjenspeiler hvor høy terskelen faktisk er. Spørsmålet må forstås i lys av klargjøringer av terskelen i praksis fra EMD og Høyesterett, hvor terskelens høyde ytterligere understrekes. Et eksempel er Rt. 2004 side 1400, hvor Høyesterett på bakgrunn av EMDs praksis, legger til grunn «at kildevernet *langt på vei er absolutt* så lenge de opplysninger kilden har gitt er av samfunnsmessig betydning. Men Goodwin-saken

[56] Se f.eks. også *Sanoma Uitgevers B.V. v. Nederland* (38224/03) avs. 92.

viser også at det må foreligge *meget tungtveiende hensyn* for å pålegge vitneplikt selv om opplysningene er uten slik betydning».[57]

Justis- og beredskapsdepartementet sendte nylig på høring forslag til endringer i kildevernreglene i straffeprosessloven og tvisteloven, fra nettopp dagens ordlyd «vektige samfunnsinteresser», med mål om bedre å reflektere den høye terskelen i praksis fra EMD og Høyesterett. NIM har i den forbindelse gitt mer utfyllende kommentarer og forslag til hvordan forsøke å ivareta EMD-terskelen så godt som mulig i en norsk lovtekst.[58]

NIM tror det kan ha flere fordeler om man ser hen til disse eventuelle endringene på straffeprosessområdet, og at man i stor grad forsøker å samstemme ulike kildevernreguleringer i nasjonalt lovverket hva gjelder ordlyd og vilkår. Samtidig tror NIM at pedagogiske hensyn vil være av større betydning i ordlyden i etterretningstjenesteloven enn det formodentlig vil være i straffeprosessloven, hvor kildevernproblematikken i det minste må antas å være mer kjent for relevante aktører.

NIM tror for det første at det vil være en fordel å sette punktum i bestemmelsen (nåværende forslag § 9-6), slik at hovedregelen (skranken) kommer klart frem innledningsvis, mens unntaket (det som står etter siste komma i første ledd) står som en egen setning eller et eget ledd. I tillegg stiller NIM altså spørsmål om kildevernet endog bør skilles ut til en egen bestemmelse (se punkt 5.3 ovenfor).

Videre mener NIM at ordlyden «vektige samfunnshensyn» etter en naturlig språklig forståelse ikke leder tanken hen til en så høy terskel som EMDs og Høyesteretts praksis tilsier. Det kan være betegnende at Justis- og beredskapsdepartementet nå foreslår å gå bort fra denne ordlyden i straffeprosessloven/tvisteloven. NIM vil i hvert fall foreslå at «vektige samfunnshensyn» kvalifiseres til «*meget* vektige» eller lignende. Et mulig alternativ kan være tilsvarende det NIM skisserte til Justis- og beredskapsdepartementet: «Kun i ekstraordinære tilfeller og dersom det er strengt nødvendig ...».[59]

Videre mener NIM at det vil kunne gi en pedagogisk fordel for rettsanvenderen (kontrollen i forkant og etterkant) å få frem i ordlyden at det alltid må foretas en helhetlig vurdering av om det foreligger tungtveiende nok grunner til å fravike kildevernet i den enkelte sak. I denne helhetsvurderingen må man legge vekt på de langsiktige negative virkningene et kildeverninngrep vil ha for ytringsfriheten utover den aktuelle sak (se nærmere under punkt 5.2 ovenfor).[60]

Til sist stiller NIM spørsmål ved om det kan være en fordel å konkretisere, enten i lovens ordlyd eller i forarbeider, hvilke formål som potensielt kan ende opp som tungtveiende nok til å fravike kildevernet. Ordlyden «vektige samfunnshensyn» eller lignende

[57] Rt. 2004 side 1400 avs. 46 (våre uthevninger).
[58] NIMs høringsuttalelse til Justis- og beredskapsdepartementet av 1. februar 2019 punkt 4.

[59] Ibid.

[60] Se også NIMs forslag til Justis- og beredskapsdepartementet (ibid.).

(uavhengig av eventuell kvalifikasjon), er i så måte diffus, og potensiell vid, sammenlignet med for eksempel straffeprosessområdet. For sistnevnte har man i det minste en mer klar knagg i at inngrep kun *kan* bli aktuelt i tilfeller hvor det er avgjørende for å oppklare (alvorlig) kriminalitet. Når det gjelder E-tjenestens virksomhet er slike knagger ikke like tydelige for NIM. Det er heller ikke like tydelig som på straffeprosessområdet hvilke samfunnsmessige gevinster som man kan/vil oppnå med inngrepet, og når og hvorfor disse gevinstene vil kunne veie tyngre enn de samfunnsgevinstene som ligger til grunn for kildevernet og følgelig kunne oppfylle den strenge nødvendighetsvurderingen.

NIM har forståelse for at en konkretisering kan være mer krevende i denne sammenheng enn på straffeprosessområdet. Men NIM tror likevel at konkretisering av formål og en tydeligere begrunnelse, vil være en fordel av hensyn til både rettsanvenderen og en fordel av hensyn til den generelle tilliten til systemet utad om at det ikke misbrukes (formålsutglidning etc.), for slik å avdempe en nedkjølende effekt.

5.5. Kildevernets forutgående kontroll – domstolskontroll?

Det er positivt at departementet anerkjenner behovet for særskilte kontrollmekanismer for kildesensitiv informasjon. NIM stiller imidlertid spørsmål ved om de foreslåtte kontrollmekanismene er tilstrekkelige.

NIM mener det er en svakhet ved høringsnotatet at det ikke foretas en vurdering av på hvilket nivå beslutningen om å ta stilling til kildeopplysninger bør ligge – også da i lys av de skranker og føringer som følger av EMDs praksis. Praksis fra EMD viser at hvilke kontrollmekanismer som foreligger er av stor betydning for vurderingen av om EMK artikkel 10 er ivaretatt når det kommer til kildesensitiv informasjon.[61]

Forslaget, slik NIM forstår det, innebærer at den *uavhengige* kontrollen vil være etterfølgende (av EOS-utvalget). Kontrollen i forkant vil være intern, av sjefen for E-tjenesten (eventuelt departementet), jf. § 9-6 andre ledd.

EMDs praksis viser imidlertid at det er den forutgående uavhengige kontrollen som er viktigst for å sikre ivaretakelse av kildevernet. Dersom eventuelle ulovlige inngrep eller feil først blir avdekket i ettertid, er de langsiktige skadene på kildevernet langt på vei allerede inntruffet, slik EMD understreker i *Sanoma Uitgevers B.V. v. Nederland*.[62] Nederland ble da dømt for krenkelse av EMK artikkel 10 siden kildeverninngrep ble foretatt uten en forutgående kontroll og avgjørelse fra en domstol eller et annet uavhengig organ. Selv om denne dommen gjaldt straffeprosessuelle inngrep, vil begrunnelsen og de bakenforliggende hensynene som kildevernet hviler på (om blant annet å sikre tilliten til at kilders konfidensialitet generelt blir ivaretatt) gjøre seg gjeldende også på etterretningsområdet. Nylige *Big Brother Watch v. Storbritannia*, som

[61] F.eks. *Sanoma Uitgevers B.V. v. Nederland* (38224/03) avs. 88 flg.
[62] Ibid. avs. 91.

skal behandles i EMDs storkammer og følgelig ikke har rettslig relevans som sådan, bidrar til å illustrere at kontrollmekanismer vil kunne ha betydning på etterretningsområdet.[63] Følgelig er ikke EMDs vurderinger i Sanoma-saken enkle å forene med lovforslaget i sin nåværende form (da også i lys av mangelen på nærmere begrunnelser i høringsnotatet).

NIM anbefaler at den forutgående kontrollen for kildevernet vurderes og begrunnes nærmere. I lys av føringer fra EMD og manglende begrunnelser i høringsnotatet (samt hvordan kildevernet reguleres i eksempelvis straffeprosessloven), mener NIM at vurderingen av behandlingen av kildeopplysninger som et klart utgangspunkt bør legges til en domstol (eller et annet uavhengig organ), for å sikre at kildevernet ivaretas i henhold til de krav som EMK artikkel 10 oppstiller.

Dersom nåværende sekkeregulering eller jurisdiksjonsproblematikk spiller inn i departementets vurdering i denne sammenheng, mener NIM at man bør se på tilnærmingen mer overordnet, og i hvert fall se på alternativer til differensierte løsninger knyttet til eksempelvis territoriell eller personell avgrensning.[64] Av hensyn til helhet i kontrollmekanismene kan det da være relevant å se hen til virkeområdet for EOS-utvalgets kontroll.

NIM legger til grunn til at det er riktig forstått at den foreslåtte generelle domstolskontrollen etter § 8-1, jf. bl.a. § 8-4, ikke innebærer at retten vil foreta den strengere nødvendighetsvurderingen som § 9-6 oppstiller. Se også punkt 5.3 ovenfor om fra hvilket tidspunkt (i innsamling/søk/lagring/behandlingsprosessen) skranken i § 9-6, og følgelig den særskilte kontrollen, bør gjelde.

NIM mener at den generelle domstolskontrollen også må ha kildevernet for øye (i så stor grad som det er mulig på det tidspunkt). Og at retten i forbindelse med denne generelle kontrollen foretar den vurdering og kontroll som er nødvendig (så langt som da mulig) for å sikre at kildevernet ivaretas i forbindelse med innhenting, søk og lagring. NIM anbefaler at dette inkluderes/presiseres i domstolsprøvingens «mandat» (§ 8-4), for eksempel ved en henvisning til kildevernet eller § 9-6. I tillegg vil det være en fordel å klargjøre sammenhengen og grenseoppgangen mellom den generelle domstolskontrollen i § 8-1 og den særskilte kontrollen som følger av § 9-6, og hvordan kildevernet ivaretas i disse ulike tilfellene (og hvordan man unngår at noe «faller mellom to stoler» uten kontroll), se også punkt 5.3 ovenfor.

Det er også noe uklart for NIM hva «hastekompetansen» i lovforslagets § 8-10 innebærer, og hvilke eventuelle konsekvenser dette vil kunne ha for ivaretakelsen av ytringsfriheten og kildevernet. NIM vil ikke kommentere dette nærmere her, men legger til grunn at

[63] *Big Brother Watch v. Storbritannia* (58170/13, 62322/14 og 24960/15) avs. 492. Ikke rettskraftig.
[64] For jurisdiksjonsspørsmål mer generelt, se høringsuttalelsens punkt 2.

bruken av en slik hastekompetanse og utsettelse av domstolsbehandling, vil måtte foretas i samsvar med menneskerettslige krav.[65]

5.6. Etterfølgende kontrollmekanismer

Det er positivt at man ønsker å legge til rette for EOS-utvalgets (etterfølgende) kontroll, jf. forslaget om merking i § 9-6 tredje ledd. NIM vil likevel understeke at man i denne sammenheng må være bevisst på dilemmaet om at slik merking ikke må få den konsekvens at kildevernet blir skadelidende, og at slike opplysninger følgelig oppbevares så forsvarlig og fortrolig som forholdene og menneskerettslige krav tilsier.

Videre er det viktig at EOS-utvalget gjøres kapabelt, i form av tilstrekkelige ressurser, personell og kompetanse, til å foreta kontrollen – herunder de viktige vurderingene av hvordan E-tjenesten praktiserer nødvendighetskravet for å gripe inn i kildevernet – på en forsvarlig og god måte. Uten tilstrekkelige ressurser til EOS-utvalget og dets sekretariat kan kontrollen komme til å fremstå som lite overbevisende.

I tillegg til den foreslåtte kontrollen gjennom EOS-utvalget, mener NIM det vil være en fordel å opprette en eller flere ytterligere former for (uavhengige) kontrollmekanismer.[66] Et alternativ kan være en variant av et «DGF-tilsyn», slik som Lysne II-utvalget foreslo. Et annet alternativ kan være å se nærmere på mulighetene for klage- og innsynsmuligheter, for eksempel for enkelte bestemte aktører, slik som innenfor pressen. NIM mener at det nåværende lovforslagets begrensede innsynsmuligheter fremstår som lite tillitsvekkende generelt.

Et poeng i seg selv er at kontrollen bør ligge til flere uavhengige steder. På den måten kan man bidra til å sikre at kontrollen, og de skranker og rettssikkerhetsgarantier kontrollen er ment å innebære, blir reell ved blant annet å minske risikoen for systemiske svikt. Når systemet fremstår som såpass lite transparent, med få muligheter til innsyn i praktiseringen, er det desto viktigere med gode kontrollmekanismer – for slik også å kunne korrigere eventuell svikt i praksis både hos både E-tjenesten og hos dem som kontrollerer.

I forlengelsen understreker NIM betydningen av evalueringer av loven og praktiseringen, og at det legges til rette for at fremtidige evalueringer kan gjennomføres på en god og grundig måte – ved at man sikrer notoritet, sporbarhet og skriftlighet underveis i lovens praktisering (samtidig som at denne informasjonen oppbevares så forsvarlig og fortrolig som blant annet hensynet til kildevernet tilsier).

5.7. Unntaket fra kildevernet (§ 9-7)

[65] For kildevernets del, se f.eks. *Sanoma Uitgevers B.V. v. Nederland* (38224/03) avs. 99.
[66] For mer generelle kommentarer om kontrollmekanismer, se høringsuttalelsens punkt 4.5 og 4.6.

NIM er også forbeholden til forslaget til det eksplisitte unntaket i § 9-7 om at opplysninger kan behandles dersom det er nødvendig for å avklare om kravene i for eksempel § 9-6 er oppfylt. NIM overskuer ikke den praktiske rekkevidden av denne bestemmelsen – og følgelig ikke omfanget av det inngrep bestemmelsen potensielt kan innebære i for eksempel kildevernet. I sin nåværende form, fremstår dette som et svært vidt unntak, og et unntak som endog kan ende opp med å gjøre kildevernreguleringen i § 9-6 nærmest illusorisk.

NIM savner en begrunnelse for hvorfor en så vid unntaksregulering er nødvendig sett opp mot de krav kildevernet stiller. NIM mener at det også her bør gis en nærmere vurdering av alternativer, både når det gjelder ordlyd og til hvem en slik vurdering kan og bør ligge. For eksempel hvorvidt dette også kan legges til en domstol eller et uavhengig organ, og på hvilken måte man gjennom praktiseringen av unntaket vil sikre at eventuelle inngrep i kildevernet blir så få og så minimale som mulig. NIM viser her til kommentarene under punkt 5.2 og 5.3 ovenfor om fra hvilket tidspunkt kildevernet kan bli skadelidende.

5.8. Delingsadgang

Det er positivt at departementet foreslår å avgrense delingsadgangen for kildesensitiv informasjon, herunder at overskuddsinformasjon av denne typen ikke kan deles (§ 10-8 tredje ledd). NIM er enig i at dette er et tiltak for å forebygge en nedkjølende effekt.

Det er likevel vanskelig å overskue hvilken *de facto* mulighet som nå eksisterer for deling av (annen) kildeinformasjon, for eksempel hva første vilkår for informasjonsdeling (§ 10-5 a) reelt innebærer, og hvilke skranker loven her oppstiller. For eksempel lyder nevnte vilkår: «Utleveringen skjer for etterretningsformål eller er nødvendig for å *fremme mottakerens oppgaver* eller for å *hindre at virksomhet blir utøvd på en uforsvarlig måte»* (våre uthevninger).

Såpass uklare og vide vilkårsstillinger er etter NIMs mening ikke et godt bidrag til å motvirke en nedkjølende effekt. NIM viser til kommentarene ovenfor om betydningen av å konkretisere formål: Dette både for å forenkle og bedre den forutgående og etterfølgende kontrollen, men også for å bedre tilliten utad til at systemet ikke misbrukes og for hindre formålsutglidninger. NIM anbefaler at man vurderer og begrunner dette nærmere i det videre lovarbeidet, og at man oppstiller så tydelige, og snevre, vilkår som mulig for en eventuell delingsadgang av kildeinformasjon. NIM stiller også spørsmål ved til hvem beslutningen om deling av slik informasjon bør ligge, herunder om også den kan, og bør, ligge til et uavhengig organ (slik som en domstol). Se også kommentarene under punkt 5.5 ovenfor, som til dels vil ha generell overføringsverdi.

5.9. Vern av journalistisk materiale generelt

Dersom tilliten svekkes til at journalistisk materiale generelt ikke får være i fred fra statlig innblanding (også der materialet ikke er kildeavslørende som sådan), vil også det kunne

ha en nedkjølende effekt på bakgrunn av flere av de samme hensyn som er redegjort for ovenfor.[67]

Vern av slikt journalistisk materiale generelt nyter også et visst vern etter EMK artikkel 10.[68] Og også her vil et inngrep måtte oppfylle vilkårene etter EMK artikkel 10 andre ledd, selv om det vil ha betydning for nødvendighetsvurderingen hvorvidt informasjonen vil være kildeavslørende eller ikke.

NIM savner en nærmere vurdering av hvordan man vil sikre at dette vernet ivaretas opp mot ulike forslag i loven. Dette er ikke nødvendigvis kun en utfordring som knytter seg til metadatalageret, men også når det kommer til kortidsdatalageret, informasjon fra såkalte åpne kilder og tilbydere og andre metoder.

Selv om denne vurderingen av nødvendighet (forholdsmessighet) i det vesentlige vil være lik som i tilknytning til inngrepsvurderingen etter EMK artikkel 8, er det ingen automatikk i at terskelen vil være lik i konkrete tilfeller.[69]

NIM anbefaler at man i det videre lovarbeidet vurderer dette nærmere, og hvordan det best kan sikres at dette vernet blir ivaretatt. For eksempel kan dette tydeliggjøres i forarbeidene knyttet til forslagets § 5-4 eller at det oppstilles kontrollmekanismer med dette for øye. Et alternativ kan være, som kommentert under punkt 5.3 ovenfor, å knytte den særskilte skranken i § 9-6 i større grad opp mot journalistisk materiale.

Merk at ovennevnte til en viss grad vil kunne ha overføringsverdi til lovforslagets betydning for ytringsfriheten generelt – og forslagets potensielle negative konsekvenser (nedkjølende effekt) for om den enkelte borger generelt vegrer seg for å ytre seg.

Til sist, uavhengig av endelig utforming i nasjonalt lovverk, forventer NIM at de menneskerettslige kravene som følger av ytringsfriheten og kildevernet overholdes ved praktiseringen av loven. Det er særlig viktig at kravet til konkrete vurderinger av nødvendighet ivaretas. Det er også viktig at regjeringen og departementet sikrer at man på alle relevante myndighetsnivåer (E-tjenesten, EOS-utvalget etc.) er seg bevisst (herunder har tilstrekkelig kapasitet og kompetanse) om hvor inngripende tvangsmidler som rammer journalistisk virke og kildesensitiv informasjon potensielt kan være, ikke bare i den konkrete sak, men særlig i den større kontekst.

---

[67] Se også NIMs høringsuttalelse til Justis- og beredskapsdepartementet av 1. februar 2019 punkt 5.

[68] *Nordisk Film & TV A/S v. Danmark* (40485/02), senere vist til av EMD i *Sanoma Uitgevers B.V. v. Nederland* (38224/03) avs. 65 og *Nagla v. Latvia* (73469/10) avs. 80. Se også Rt. 2015 side 1286 avs. 57 hvor Høyesterett viser til førstnevnte: «Etter EMDs praksis kan i spesielle tilfelle også upublisert materiale som ikke inneholder informasjon som kan føre til avsløring av en kildes identitet, nyte et visst vern. […] Vernet i en situasjon som dette er imidlertid svakere enn det tradisjonelle kildevernet».

[69] Se Nagla v. Latvia (73469/10) avs. 103–104; Tillack v. Belgia (20477/05), der artikkel 8 ikke blir drøftet selv om det gjaldt ransakelse i journalistens hjem; Saint-Paul Luxembourg S.A. v. Luxembourg (26419/10), der EMD i det konkrete tilfellet kom til et brudd på begge artikler, men hvor forskjellen eksspliseres av dissenterende dommers votum; ikke rettskraftige Big Brother Watch v. Storbritannia (58170/13, 62322/14 og 24960/15) er til en viss grad også illustrerende for betydningen av artikkel 10 som referansepunkt i tilfeller hvor begge bestemmelser gripes inn i.

6. Avslutning

NIM stiller seg til disposisjon for å gi råd og ha dialog med departementet i den videre behandlingen av saken.

Vennlig hilsen
for Norges nasjonale institusjon for menneskerettigheter

Adele Matheson Mestad

konstituert direktør

Kristian Reinert Haugland Nilsen

seniorrådgiver

Dette dokumentet er elektronisk godkjent og har dermed ingen signatur.