

FD

FORSVARSDPARTEMENTET

Høringsnotat

Forslag til lov om endringer i etterretningstjenesteloven

27. juni 2022

Innhold

1. HOVEDINNHALDET I HØRINGSNOTATET	4
2. BAKGRUNN	4
3. KILDEVERNET	6
3.1. Gjeldende rett	6
3.2. Grunnloven og internasjonale forpliktelser	7
3.3. Vurdering	8
3.4. Utforming av høringsforslag	10
4. BESLUTNING OM TILRETTELEGGING	10
4.1. Gjeldende rett	10
4.2. Uavhengig autorisasjon	11
4.2.1. Grunnloven og internasjonale forpliktelser	11
4.2.1.1. Grunnloven § 102	11
4.2.1.2. Den europeiske menneskerettskonvensjon – nyere rettspraksis	11
4.2.2. Hva omfattes av autorisasjonen? Nærmere om ulikhetene i de nasjonale systemene	13
4.2.3. Etterretningstjenestens oppgaver og teknologiske forutsetninger	14
4.3. Autorisasjon på ulike stadier	16
4.3.1. Nærmere om testinnhenting og testanalyse	16
4.3.2. Beslutning om speiling for testinnhenting og testanalyse	17
4.3.3. Speiling av kommunikasjonsstrømmer som grunnlag for søk	17
4.3.4. Nærmere om «Over the top- tjenester» («OTT-tjenester»)	18
4.4. Ytterligere vurderingskriterium om det generelle trusselbildet?	18
4.4.1. EØS-rettslige rammer – særlig om <i>La Quadrature du Net</i> -kriteriene	18
4.4.2. Vurdering	23
4.5. Utforming av høringsforslag	24
5. LOVTEKNISKE RETTELSER	25
6. ØKONOMISKE OG ADMINISTRATIVE KONSEKVENSER	25
7. MERKNADER TIL DE ENKELTE BESTEMMELSER	25
Til § 4-2	25
Til § 5-2	26
Til § 7-2	26
Til § 7-3	27

Til kapittel 8.....	28
Til § 9-6	28
Til § 9-8	29
8. LOVFORSLAG	30

1. HOVEDINNHOLDET I HØRINGSNOTATET

Formålet med høringsnotatet her er å sikre at lov 19. juni 2020 nr. 77 om Etterretningstjenesten (etterretningstjenesteloven) er i samsvar med Norges menneskerettslige og øvrige internasjonale forpliktelser. Det gjelder både etterretningstjenesteloven § 7-3, som ennå ikke er satt i kraft, og lovens øvrige bestemmelser. Vurderingen gjøres på bakgrunn av avgjørelser fra overnasjonale domstoler som ble avsagt høsten 2020 og våren 2021. Det vises i denne forbindelse til Prop 80 L (2019-2020) punkt 11.5.3.5 og punkt 11.6 der departementet gjorde oppmerksom på at man ventet på forestående avgjørelser fra Den europeiske menneskerettsdomstolen (EMD) og EU-domstolen. Det ble gjort klart at man ville komme tilbake til Stortinget dersom avgjørelsene tilsa at det var nødvendig.

Høringsnotatet foreslår lovendringer som skal sikre at loven er i samsvar med rettsikkerhetsgarantier for ivaretagelse av kildevernet. Mens gjeldende rett legger beslutningsmyndighet til Forsvarsdepartementet om eventuell bruk av kildeidentifiserende materiale for etterretningsformål, foreslås det en lovendring som i stedet legger beslutningsmyndigheten til Oslo tingrett. Videre foreslås en lovendring om at målrettet innhenting som med stor sannsynlighet vil frembringe kildeidentifiserende materiale etter § 9-6 første ledd skal besluttes av Oslo tingrett og bare kan iverksettes dersom det er strengt nødvendig at de hensyn som begrunner kildevernet, viker for nasjonale sikkerhetsinteresser.

For det andre foreslås endringer i bestemmelsen om hvem som beslutter tilrettelegging om tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon i etterretningstjenesteloven kapittel 7. Den vedtatte, men ikke ikraftsatte, § 7-3 legger beslutningsmyndigheten til sjefen for Etterretningstjenesten. Det foreslås at beslutningsmyndigheten i stedet legges til Oslo tingrett. For beslutning om å speile kommunikasjonsstrømmer etter § 7-2 som utelukkende skal benyttes for testing og analyse etter § 7-5 og § 7-7 fjerde ledd med sikte på å avklare om det foreligger grunnlag for å fremme begjæring om rettens beslutning etter annet ledd, foreslås at beslutningsmyndigheten fortsatt bør ligge til sjefen for Etterretningstjenesten. For de avgjørelser som retten skal treffe, foreslås lovfestet i § 7-3 hvilke forhold som skal prøves av domstolen. Dette inkluderer en prøving av om speiling av grensekryssende kommunikasjonsstrømmer er forholdsmessig sett i lys av hvorvidt det kan antas at det foreligger en alvorlig trussel mot nasjonal sikkerhet som er reell og aktuell eller forutsebar og som ikke kan avdekkes i tilstrekkelig grad ved mindre inngripende tiltak.

For øvrig foreslås lovtekniske rettelser i etterretningstjenesteloven §§ 4-2, 7-2 og 9-6.

2. BAKGRUNN

I kongelig resolusjon 19. juni 2020 ble Stortingets vedtak til lov om Etterretningstjenesten (etterretningstjenesteloven) av 15. juni 2020 sanksjonert. Det ble samtidig fastsatt at loven skulle tre i kraft i sin helhet 1. januar 2021.

EU-domstolen avsa den 6. oktober 2020 dom i forente saker C-511/18, C-512/18 og C-520 (La Quadrature du Net), og sak C-623/17 (Privacy International), om tolkning av direktiv 2002/58 EF (kommunikasjonsvernndirektivet). EU-domstolens avgjørelser er ikke direkte bindende for Norge, men tillegges vekt som tolkningsfaktor innenfor de områder som er omfattet av EØS-avtalen – noe som ikke er åpenbart hva gjelder regulering av nasjonal sikkerhet. Dette fordi EØS-avtalen ikke omfatter samarbeid og bestemmelser om nasjonal sikkerhet, og heller ikke EUs felles utenriks- og sikkerhetspolitikk (FUSP). Dette gjelder selv om Norge har valgt å samarbeide med EU om sikkerhetspolitiske temaer på områder som ligger utenfor EØS-avtalen, som eksempelvis European Defence Agency (EDA). Kommunikasjonsvernndirektivet er innlemmet i EØS-avtalen og dermed bindende for Norge, men må likevel tolkes i lys av EØS-rettens materielle begrensninger. EUs Charter om grunnleggende rettigheter («Charteret») er ikke en del av EØS-avtalen.

EU-domstolen slo i overnevnte tolkingsavgjørelser fast at kommunikasjonsvernndirektivet etter omstendighetene får anvendelse også når formålet med innsamlingen av data er ivaretagelsen av nasjonal sikkerhet, selv om det følger av EU-traktaten artikkel 4(2) at nasjonal sikkerhet er statenes eneansvar.

I lys av at avgjørelsene måtte analyseres grundig for å vurdere i hvilken utstrekning de har betydning for den norske lovgivningen, og i lys av at en på dette tidspunktet også avventet to storkammeravgjørelser fra Den europeiske menneskerettsdomstol (EMD), samt under hensyntagen til at etterretningstjenesteloven § 12-1 åpner for at de ulike bestemmelsene kan tre i kraft til ulik tid, ble det ved kongelig resolusjon 10. november 2020 vedtatt delt ikrafttredelse av etterretningstjenesteloven. Loven trådte etter dette i kraft 1. januar 2021 med unntak av kapittel 7 og 8. Disse kapitlene omhandler tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon (forkortet «tilrettelagt innhenting»).

Den 25. mai 2021 avsa EMD to storkammerdommer om bulkinnhentingsregimer i *Case of Centrum för Rättvisa v. Sweden* (application no. 35252/08), og i *Case of Big Brother Watch and Others v. the United Kingdom* (application no. 58170/13, 62322/14 og 24690/15).

Berørte departementer utarbeidet en felles juridisk analyse som vurderte hvorvidt de internasjonale rettsavgjørelsene fordret endringer i etterretningstjenesteloven. Analysen, som ble offentliggjort 26. august 2021 og som er tilgjengelig på regjeringens hjemmesider, har hatt et primærfokus på mulige behov for endringer i kapittel 7-9 i loven, men har også sett på om andre deler av loven må endres. Den juridiske analysen konkluderte slik:

«Tilrettelagt innhenting vurderes å være i overensstemmelse med de menneskerettslige kravene som følger av EMDs storkammeravgjørelser 25. mai 2021, med de presiseringer om ytterligere utredninger som er omtalt i denne analysen. Behovet for utredning knytter seg i hovedsak til spørsmålet om forhåndsautorisasjon og dermed beslutningsprosedyren i § 7-3.

Loven anses også forenlig med avgjørelsene fra EU-domstolen, med forbehold for at LQN-kriteriene trolig bør komme klarere til uttrykk i § 7-3.

Etter en samlet vurdering legges det til grunn at det er rettslig forsvarlig å treffe en beslutning om å sette i kraft kapittel 7 og 8 i etterretningstjenesteloven nå, med følgende presiseringer:

- Ettersom E-tjenesten ikke har tilgang til de innhentede data før domstolen har tatt stilling til om vilkårene er oppfylt, herunder om tilgangen er nødvendig og forholdsmessig, kan det anføres at beslutningsprosedyren i § 7-3 sett i lys av EOS-utvalgets løpende kontroll og anledning til å fremme begjæring om stans til Oslo tingrett, er forholdsmessig og tilfredsstillende både EMKs og EØS-rettens krav. Det er imidlertid knyttet rettslig usikkerhet til et slikt standpunkt og spørsmålet bør utredes nærmere. Ikrafttredelse av § 7-3 bør avvente en slik ytterligere utredning, som kan resultere i forslag om lovendringer. Utredningen bør sendes på offentlig høring. Det følger av lovens § 12-1 at bestemmelsene kan settes i kraft til ulik tid.
- Det bør utredes om uavhengig forhåndsautorisasjon av målrettet innhenting overfor journalister eller målrettet innhenting som vil medføre tilgang til kildeidentifiserende materiale i etterretningstjenesteloven kapittel 5 er i overensstemmelse med EMK. Det bør også utredes om bestemmelsen i kapittel 9 om beslutningsmyndigheten for unntaksvis bruk av kildeidentifiserende materiale er i overensstemmelse med EMK. Utredningen bør sendes på offentlig høring. Begrunnelsen for eventuelle lovendringsforslag er ikke primært av hensyn til tilrettelagt innhenting, men av hensyn til at de deler av etterretningstjenesteloven som allerede er ikraftsatt, skal være fullt ut i samsvar med Norges menneskerettslige forpliktelser. Eventuelle lovendringer bør likevel tre i kraft før tilrettelagt innhenting settes i operativ drift.»

Ved kgl. res. 26. august 2021 nr. 2581 fastsatte Kongen i statsråd, med hjemmel i etterretningstjenesteloven § 12-1, delt ikrafttredelse om at loven kapittel 7 og 8 trer i kraft 1. januar 2022, med unntak av § 7-3.

Etter ikrafttredelsesvedtaket har departementet arbeidet videre med de problemstillinger som den juridiske analysen mente burde utredes nærmere. Departementet har kommet til at det bør gjøres endringer som foreslått i høringsnotatet her.

3. KILDEVERNET

3.1. Gjeldende rett

Etterretningstjenesteloven § 9-6 første ledd fastsetter et generelt forbud mot å behandle kildeidentifiserende opplysninger. Forbudet innebærer at Etterretningstjenesten som hovedregel ikke skal behandle informasjon som er egnet til å avsløre identiteten til en journalistisk kilde. Etter bestemmelsens annet ledd kan informasjonen likevel behandles dersom det er strengt nødvendig at de hensyn som begrunner kildevernet viker for nasjonale sikkerhetsinteresser, som etter forarbeidene, se Prop. 80 L (2019-2020) punkt 12.8.6, er formulert for å gjenspeile den høye terskelen som følger av de menneskerettslige forpliktelser (EMDs forståelse av «*justified by an overriding requirement in the public interest*»).

Beslutningen om å fravike hovedregelen er etter tredje ledd lagt til Forsvarsdepartementet.

Beslutningen skal være skriftlig, redegjøre for det faktiske og rettslige grunnlaget og meddeles EOS-utvalget.

Etterretningstjenesteloven § 9-6 gjelder kun behandling etter innhenting, jf. § 9-3. Selv om bestemmelsen ikke får direkte anvendelse på innhentingsstadiet, er den ikke uten betydning i denne sammenheng. Det fremgår av lovens forarbeider, se Prop. 80 L (2019-2020) pkt. 11.9.3.3, at for tilrettelagt innhenting skal domstolen prøve saker som innebærer innhenting overfor journalister eller som av andre grunner med sannsynlighet vil frembringe konfidensielt journalistisk materiale, som ledd i hva retten skal prøve etter § 8-4:

«Den høye terskelen for inngrep i kildevernet vil likevel være gjenstand for prøving av domstolen som et ledd i forholdsmessighetsvurderingen etter § 5-4. Dette innebærer for eksempel et tilnærmet absolutt forbud mot målrettet innhenting etter lovforslaget § 7-9 av kommunikasjon mellom en journalist mv. som er vernet av lovforslaget § 9-6 og en kilde, og dette vil prøves av retten.»

Etter gjeldende rett er det ikke domstolskontroll av kildevernsaker som ikke er knyttet til søk og innhenting i forbindelse med tilrettelagt innhenting, verken før eller etter innhenting av informasjon. Etter gjeldende rett er imidlertid behandlingen av kildeidentifiserende opplysninger gjenstand for uavhengig etterhåndskontroll av det stortingsoppnevnte EOS-utvalget, da dette vil falle innenfor kontrollområdet etter EOS-kontrollloven.

3.2. Grunnloven og internasjonale forpliktelser

Utgangspunktet for vurderingen er Grunnloven § 100 og EMK artikkel 10 om ytringsfrihet. De konstitusjonelle og menneskerettslige rammer for Etterretningstjenestens virksomhet er generelt redegjort for i Prop. 80 L (2019-2020) pkt. 4. Behandling av kildeidentifiserende opplysninger er nærmere redegjort for i proposisjonen pkt. 12.8. Det fremgår her at kildevernet omfattes av EMKs ytringsfrihetsbegrep.

I lys av kildevernets betydning for et velfungerende og informert demokrati, har EMD lagt til grunn en høy terskel for når myndighetsutøvelse som griper inn i kildevernet kan aksepteres. Det er av stor betydning å hindre en nedkjølende effekt på pressens kildetilfang, da en slik effekt kan ha sterke skadevirkninger på demokratiet. På den annen side er det klart at det ikke kan oppstilles et absolutt forbud.

EMDs avgjørelse i *Big Brother Watch vs. UK* har tydeliggjort det menneskerettslige vernet som kildeidentifiserende materiale nyter i relasjon til det å operere et strategisk bulkinnhentingsregime slik som tilrettelagt innhenting. Avgjørelsen tydeliggjør også de menneskerettslige prinsippene som gjelder generelt for etterretningstjenesters innhenting og bruk av kildeidentifiserende materiale.

I *Big Brother Watch vs. UK* vurderer EMD at det i relasjon til den britiske lovgivningen som ble prøvd, ble gjort et ulovlig inngrep i kildevernet etter EMK artikkel 10, se avsnitt 448 flg. Målrettet innhenting mot journalister vurderes som mer inngripende enn tilfeller av

innhenting hvor det er mer eller mindre tilfeldig at en etterretningstjeneste får tilgang til kildeidentifiserende materiale. Domstolen uttaler at bruk av selektorer eller søkebegreper tilknyttet en journalist med stor sannsynlighet vil resultere i besittelse av betydelige mengder konfidensielt journalistisk materiale som kan undergrave kildevernet i større grad enn et pålegg om å avsløre en kilde. Følgelig vurderer EMD at en domstol eller en annen uavhengig og upartisk instans med beslutningsmyndighet må godkjenne etterretningstjenestenes bruk av selektorer eller søkebegreper som man vet er tilknyttet en journalist eller som svært sannsynlig vil medføre tilgang til konfidensielt journalistisk materiale. Denne instansen må ha kompetanse til å avgjøre om bruk av selektorene/søkebegrepene er rettferdiggjort av hensyn til et overordnet krav i allmennhetens interesse («*justified by an overriding requirement in the public interest*»), og om mindre inngripende tiltak ville vært tilstrekkelig for å ivareta dette formålet.

EMD uttaler videre at når det gjelder kildeidentifiserende materiale som mer tilfeldig kommer i etterretningstjenesters besittelse som et biprodukt av annen innhenting, vil det ikke være mulig å gjennomføre en forhåndsautorisasjon av slik innhenting. Derimot må en uavhengig instans ta stilling til videre behandling i de tilfeller det fremstår som klart («*if and when it becomes apparent*») at det dreier om kildeidentifiserende materiale. Den uavhengige instansen må ha kompetanse til å avgjøre om videre behandling er rettferdiggjort av hensynet til et overordnet krav i allmennhetens interesse.

3.3. Vurdering

Departementet har kommet til at kildevernet bør styrkes i etterretningstjenesteloven, og foreslår at de prinsipper som EMD har lagt til grunn bør gjøres gjeldende for all innhenting som Etterretningstjenesten gjennomfører – ikke bare som ledd i tilrettelagt innhenting.

For målrettet innhenting ved bruk av selektorer som tilhører personer som er omfattet av etterretningstjenesteloven § 9-6, vurderes at dagens ordning om forhåndsprøving av domstolen – for så vidt gjelder tilrettelagt innhenting – er tilstrekkelig for å oppfylle kravene som EMD oppstiller. Departementet mener likevel at det i selve lovteksten, i grunnvilkåret for målrettet innhenting i § 5-2, kan være grunn til å tydeliggjøre domstolens rolle i disse tilfellene. Gjennom å klargjøre grunnvilkårene for slik målrettet innhenting, vil dette tydeliggjøre domstolens generelle rolle i slike saker, og gjøre det klart at domstolsbehandling er påkrevet for all innhenting, ikke bare som ledd i tilrettelagt innhenting.

Departementet foreslår derfor en tilføyelse i etterretningstjenesteloven § 5-2 om at all målrettet innhenting, uansett hvilken innhentingsmetode som benyttes, som med stor sannsynlighet vil frembringe kildeidentifiserende materiale etter § 9-6 første ledd, bare kan iverksettes dersom det er strengt nødvendig at de hensyn som begrunner kildevernet, viker for nasjonale sikkerhetsinteresser. Det foreslås at beslutning om innhenting skal treffes av domstolen etter begjæring av sjefen for Etterretningstjenesten, og at reglene i kapittel 8 får tilsvarende anvendelse så langt de passer.

Det foreslås at regelen kommer til anvendelse når det foreligger «stor sannsynlighet» for at innhenting vil frembringe kildeidentifiserende materiale. Dette er i samsvar med den terskelen som er lagt til grunn av EMD i *Big Brother Watch mot UK* («*high probability*»/«*highly probable*»). Det bør foreligge særskilte holdepunkter og en slik kvalifisert sannsynlighetsterskel før plikten til å innhente rettens avgjørelse inntreffer. Dersom målrettet innhenting skjer overfor personer som tilsynelatende er omfattet av § 9-6 første ledd, legger departementet til grunn at det – med unntak for åpenbare omgåelsestilfeller hvor for eksempel en fremmed etterretningsoffiser fingerer å være journalist for å unngå at etterretningsevne skal bli oppdaget – alltid vil være stor sannsynlighet for at innhenting vil frembringe kildeidentifiserende materiale.

Et annet spørsmål er om etterretningstjenesteloven er tilfredsstillende når det gjelder beslutningsinstans for unntaksvis bruk av kildeidentifiserende materiale som Etterretningstjenesten har kommet i besittelse av som et biprodukt av annen innhenting, ettersom det er departementet – ikke domstolen eller et annet uavhengig organ – som etter § 9-6 tredje ledd bestemmer om informasjonen kan behandles i et slikt tilfelle. EMD uttaler at det er imperativt at den nasjonale lovgivningen inneholder robuste rettssikkerhetsmekanismer knyttet til lagring, bruk, videreformidling og sletting av kildeidentifiserende materiale. Dersom Etterretningstjenesten på et senere tidspunkt får kunnskap om at dataene inneholder kildeidentifiserende opplysninger, forutsetter fortsatt lagring og bruk av opplysningene at vurderingen av om vilkårene for dette er oppfylt foretas av en domstol eller et annet uavhengig og upartisk organ med beslutningsmyndighet.

Departementets beslutning om videre bruk etter § 9-6 tredje ledd skal meddeles EOS-utvalget. Beslutningen skal være utformet på en måte som er egnet for overprøving, og EOS-utvalget vil derfor være i stand til å gjennomføre uavhengig legalitetskontroll av om terskelen er nådd i hvert enkelt tilfelle. Denne ordningen vil formodentlig ha en betydelig disiplinerende effekt, og det vil derfor kunne argumenteres for at EOS-utvalget vil fungere som en *de facto* uavhengig prøvingsmyndighet i disse sakene. EOS-utvalget vil i saker om tilrettelagt innhenting også kunne benytte seg av myndigheten i etterretningstjenesteloven § 7-12 til å fremme begjæring overfor domstolen om stans i pågående innhenting og sletting av innhentede data.

Det er likevel usikkert om denne reguleringen tilfredsstiller EMDs krav til *hvem* som skal treffe beslutningen. Det tilføyes at det i forbindelse med komitebehandlingen av lovforslaget våren 2020 ble vurdert, etter innspill fra pressens organer, å justere lovteksten slik at beslutningsmyndigheten ble tillagt domstolen og ikke departementet, men endringsforslaget ble ikke vedtatt av Stortinget.

I saker om unntaksvis bruk av kildeidentifiserende materiale som Etterretningstjenesten har kommet i besittelse av som et biprodukt av annen innhenting, enten gjennom tilrettelagt innhenting eller på annen måte, foreslås på denne bakgrunn en endring i § 9-6 om at det er domstolen (Oslo tingrett) og ikke departementet som skal bestemme om informasjonen kan behandles i et slikt tilfelle.

Dette innebærer at dersom det fremstår som klart at informasjon som Etterretningstjenesten behandler inneholder kildeidentifiserende opplysninger etter § 9-6, skal disse opplysningene enten slettes eller – dersom man vil søke å bruke opplysningene til etterretningsformål etter den snevre unntaksregelen i annet ledd – holde opplysningene adskilt og sikre at disse ikke er tilgjengelige for bruk til etterretningsformål inntil retten har truffet sin beslutning.

Etterretningstjenesteloven § 9-8 omhandler sletting av personopplysninger. Kildeidentifiserende opplysninger vil som regel være personopplysninger. I den utstrekning opplysningene ikke er personopplysninger, f. eks. dersom opplysningene avslører en organisasjon som kilde, bør det gjelde en tilsvarende regel. Det foreslås derfor en særskilt bestemmelse om dette i § 9-8 første ledd nytt annet punktum.

Departementet har vurdert om hensynet til kildevern tilsier at det bør gjøres unntak fra hastekompetansen til sjefen for Etterretningstjenesten i § 8-10, men anbefaler ikke dette. Hastekompetansen er en meget snever unntaksregel, og bruken av den vil kontrolleres både av domstolen og EOS-utvalget. Det er et reelt behov for en slik bestemmelse og det må vektlegges at det kan dreie seg om svært alvorlige saker hvor rikets sikkerhet kan stå i fare.

3.4. Utforming av høringsforslag

Det foreslås at § 5-2 nytt annet ledd skal lyde:

Målrettet innhenting som med stor sannsynlighet vil frembringe kildeidentifiserende opplysninger etter § 9-6 første ledd, kan bare iverksettes dersom det er strengt nødvendig at de hensyn som begrunner kildevernet, viker for nasjonale sikkerhetsinteresser. Beslutning om innhenting skal treffes av retten etter begjæring av sjefen for Etterretningstjenesten. Reglene i kapittel 8 får tilsvarende anvendelse så langt de passer.

Videre foreslås at § 9-6 tredje ledd endres slik:

Beslutning om å behandle opplysninger etter andre ledd skal treffes av retten. Reglene i kapittel 8 får tilsvarende anvendelse så langt de passer.

Det foreslås også følgende nytt annet punktum i § 9-8 første ledd:

Kildeidentifiserende opplysninger som det er gitt tillatelse til å behandle etter § 9-6 tredje ledd og som ikke er personopplysninger, skal slettes når opplysningene ikke lenger er nødvendige for formålet med behandlingen.

4. BESLUTNING OM TILRETTELEGGING

4.1. Gjeldende rett

For tilrettelagt innhenting kreves det forhåndsautorisasjoner fra de ordinære domstoler (Oslo tingrett) dersom Etterretningstjenesten ønsker å gjennomføre søk i lagrede metadata eller innhente og lagre innholdsdata, jf. etterretningstjenesteloven §§ 7-8 og 7-9, jf. § 8-1. Loven etablerer en ordning med særskilt advokat som skal ivareta rettssikkerheten til enkeltindivider og samfunnets interesser (§ 8-5).

Domstolen og den særskilte advokaten vil få seg forelagt både formålet med søket eller innhenting og det faktiske og rettslige grunnlaget for dette. Som ledd i angivelsen av det faktiske grunnlaget, vil domstolen få opplysninger om hvilke kommunikasjonsstrømmer som søkene vil bli gjort i. Oslo tingrett vil videre få seg forelagt hvilke søkebegreper eller kategorier av søkebegreper som skal benyttes.

Den vedtatte, men ikke ikraftsatte bestemmelsen i etterretningstjenesteloven § 7-3 første ledd første punktum legger beslutningsmyndigheten om tilretteleggingsplikt overfor ekomtilbydere i det enkelte tilfellet – som inkluderer speiling av datastrømmer – til sjefen for Etterretningstjenesten. Beslutningen kan fattes når grunnvilkårene er oppfylt. Det følger av § 5-3 at rådata kan innhentes i bulk når dette er nødvendig for å få tilgang til et relevant og tilstrekkelig informasjonsgrunnlag. Det innebærer at rådata i bulk ikke kan hentes inn dersom mindre inngripende alternativer vil gi tilgang til et adekvat informasjonsgrunnlag. I tillegg må det foretas en forholdsmessighetsvurdering etter § 5-4. Ekomtilbydere som pålegges å tilrettelegge for speiling av kommunikasjonsstrømmene skal så langt mulig gis anledning til å uttale seg, jf. § 7-3 første ledd annet punktum.

Beslutningen kan etter § 7-3 annet ledd påklages til departementet (Forsvarsdepartementet), som kan gi klagen oppsettende virkning. Departementets beslutning kan angripes for de ordinære domstoler. Videre skal beslutning om tilrettelegging, herunder pålegg om å speile kommunikasjonsstrømmer, meddeles EOS-utvalget og Nasjonal kommunikasjonsmyndighet, jf. § 7-3 tredje ledd første punktum. Hvis EOS-utvalget mener at pålegget om speiling er i strid med loven, kan utvalget fremme begjæring for Oslo tingrett med krav om at ulovlig virksomhet opphører og at ulovlig innhentet informasjon slettes, jf. § 7-12.

4.2. Uavhengig autorisasjon

4.2.1. Grunnloven og internasjonale forpliktelser

4.2.1.1. Grunnloven § 102

Retten til respekt for privatliv og kommunikasjon er nedfelt i Grunnloven § 102 første ledd første punktum. Rettigheten er ikke absolutt. Inngrep kan tillates dersom det har hjemmel i lov, forfølger et legitimt formål og er forholdsmessig. Det vises til fremstillingen i Prop. 80 L (2019-2020) pkt. 4 og 11.5 som redegjør for og drøfter de krav som Grunnloven oppstiller, med relevant rettspraksis. Det foreligger ikke ny rettspraksis knyttet til Grl. § 102 av betydning for § 7-3, og bestemmelsen drøftes derfor ikke videre her.

4.2.1.2. Den europeiske menneskerettskonvensjon – nyere rettspraksis

Den europeiske menneskerettskonvensjon (EMK) artikkel 8 oppstiller en rett til respekt for privatliv, familieliv, hjem og kommunikasjon. Artikkel 8 skal i henhold til menneskerettsloven gjelde som norsk lov og ved motstrid gå foran bestemmelser i annen lovgivning. Adgangen til å gjøre inngrep i rettigheten følger av artikkel 8 nr. 2. Det vises til fremstillingen i Prop. 80 L (2019-2020) punkt 4 og 11.5 som redegjør for og drøfter de krav EMK oppstiller, med relevant rettspraksis.

I lys av EMDs avgjørelser i *Big Brother Watch mot UK* og *Centrum för Rättvisa mot Sverige* fra 2021 er det grunn til å vurdere nærmere om den norske ordningen tilfredsstillende kriteriet om uavhengig forhåndsautorisasjon, gitt at beslutningsmyndigheten knyttet til speilingen av kommunikasjonsstrømmene i § 7-3 er lagt til sjefen for Etterretningstjenesten.

EMD uttaler i *Centrum för Rättvisa mot Sverige* at bulkinnhenting må være gjenstand for uavhengig autorisasjon fra starten av, når formålet og rekkevidden av operasjonen defineres. Fra avgjørelsens avsnitt 264 hitsettes:

«[...] in order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to “end-to-end safeguards”, meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined [...].»

Dette beskrives, sammen med kravene til løpende og etterfølgende kontroll, som et sentralt krav (*Centrum för Rättvisa mot Sverige* avsnitt 264):

«In the Court’s view, these are fundamental safeguards which will be the cornerstone of any Article 8 compliant bulk interception regime.»

Domstolen presiserer at innhenting må autoriseres av en instans som er uavhengig fra den utøvende (*Centrum för Rättvisa mot Sverige* avsnitt 265):

«[...] bulk interception should be authorised by an independent body; that is, a body which is independent of the executive.»

At det er tale om en uavhengig instans som skal autorisere på tidspunktet for innhenting av kommunikasjonsstrømmer i bulk, fremkommer også gjennom domstolens uttalelse om hva denne instansen skal informeres om for å kunne foreta nødvendighets- og forholdsmessighetsvurderingen (*Centrum för Rättvisa mot Sverige* avsnitt 266):

«Furthermore, in order to provide an effective safeguard against abuse, the independent authorising body should be informed of both the purpose of the interception and the bearers or communication routes likely to be intercepted. This would enable the independent authorising body to assess the necessity and proportionality of the bulk interception operation and also to assess whether the selection of bearers is necessary and proportionate to the purposes for which the interception is being conducted.»

EMD forklarer ikke nærmere hva som ligger i kravet om at instansen skal være «*independent of the executive*». Det er imidlertid klart at det ikke er ensbetydende med en domstol. Det fremgår av første setning i *Centrum för Rättvisa mot Sverige* avsnitt 265 («*judicial authorisation [...] is not a «necessary requirement»*).

EMD beskriver kravet om uavhengig autorisasjon som et sentralt krav. Det er dermed noe uklart hvorvidt mindre strenge løsninger i denne delen av bulkinnhentingssystemet i en helhetsvurdering vil kunne veies opp av styrker i kontrollmekanismene i andre deler av systemet. Det må like fullt legges til grunn at innholdet i kravet om uavhengig instans må

forstås på bakgrunn av domstolens uttalelser om at lovligheten og forholdsmessigheten i bulkinnhentingsregimer undergis en helhetlig vurdering («*global assessment*»), se *Centrum för Rättvisa mot Sverige* avsnitt 366.

Det må også tas høyde for de nasjonale særegenheter i det svenske og britiske system og lovgivning som ble prøvd av EMD i *Centrum för Rättvisa mot Sverige* og *Big Brother Watch mot UK*. Det må dessuten tas i betraktning at EMD understreker at den initielle innhenting av kommunikasjonsstrømmer, som blir umiddelbart etterfulgt av bortfiltrering av deler av kommunikasjonen, ikke utgjør et betydelig inngrep etter EMK artikkel 8 («*does not constitute a particular significant interference*»), se *Big Brother Watch mot UK* avsnitt 330).

Ettersom Etterretningstjenesten etter gjeldende rett ikke vil ha tilgang til de speilede dataene før domstolen har tatt stilling til om lovens vilkår er oppfylt, herunder om tilgangen er nødvendig og forholdsmessig, kan det argumenteres for at gjeldende beslutningsprosedyre i § 7-3, sett i lys av EOS-utvalgets løpende kontroll etter § 7-11 og anledning til å fremme begjæring om stans til Oslo tingrett etter § 7-12, er forholdsmessig og tilfredsstillende EMDS krav. Det fremstår dessuten som noe uklart hvorvidt EMD mener at den autoriserende instansen i alle tilfeller skal treffe selve beslutningen om hvilke kommunikasjonsstrømmer som skal være tilgjengelige for søk, eller hvorvidt instansen kun skal være informert («*should be informed*»), se *Big Brother Watch mot UK* avsnitt 352) om dette, slik at den er i stand til å vurdere proporsjonalitet og nødvendighet opp mot hvilke kommunikasjonsstrømmer det er tale om.

Departementet mener likevel det er knyttet en viss rettslig usikkerhet til om tilrettelagt innhenting oppfyller EMDS krav, og har derfor vurdert om det er mulig å styrke rettssikkerheten ved å innføre uavhengig autorisasjon i form av domstolskontroll også på speilingstidspunktet. En slik domstolsbehandling må tilpasses det norske bulkinnstillingsystemet, og for øvrig de tekniske og faktiske realiteter, for å gi en reell merverdi som rettssikkerhetsmekanisme.

4.2.2. Hva omfattes av autorisasjonen? Nærmere om ulikhetene i de nasjonale systemene

I fortolkningen av dommene fra EMD, og i forståelsen av hvordan kriteriene skal kunne gjennomføres i norsk rett, må det tas hensyn til de nasjonale forskjellene som er mellom de ulike landenes rettssystemer, i dette tilfellet britisk, svensk og norsk rett. Det norske og svenske systemet har flest likhetspunkter, og avgjørelsen i *Centrum för Rättvisa mot Sverige* legges derfor til grunn i den videre drøftelsen. Det må likevel understrekes at det er flere grunnleggende forskjeller mellom det norske og svenske systemet, som må tillegges vekt.

Etter svensk lovgivning er det krav om at hver enkelt «*signals intelligence mission*» må autoriseres av domstolen. Dette er et relativt vidt begrep som dekker omfattende innhentingsvirksomhet. Den anmodende tjenesten behøver ikke gå tilbake til domstolen for å få tillatelse til å gjennomføre søk basert på mer konkrete søkekriterier. Det følger av den svenske signalspaningslagen § 4 a at den svenske Försvarsunderrättelsesdomstolen skal behandle søknader om «*vilken eller vilka signalbärare avseende signaler i tråd som*

signalspaningsmyndigheten behöver ha tillgång till för att fullgöra uppdraget» samtidig som det søkes rettens godkjenning av «de sökbegrepp eller kategorier avsökbegrepp som är avsedda att användes vid inhämtningen».

Den norske etterretningstjenesteloven følger en annen fremgangsmåte. Beslutning om tilrettelegging fra ekomtilbydere, jf. § 7-2, som omfatter speiling av kommunikasjonsstrømmer, kan fattes av sjefen for Etterretningstjenesten, jf. § 7-3. Informasjonen blir deretter filtrert og lagret. Etterretningstjenesten kan ikke gjennomføre søk i de lagrede dataene før dette er godkjent av Oslo tingrett. For å kunne gjøre søk må tjenesten utforme en begrunnet begjæring etter § 8-2. Retten bestemmer om det skal holdes muntlige forhandlinger, jf. § 8-3, og det skal oppnevnes en særskilt advokat, jf. § 8-5. Retten skal prøve om lovens vilkår er oppfylt jf. § 8-4, derunder skal det gjøres en vurdering av nødvendighet og proporsjonalitet etter § 5-4. Dette inkluderer en vurdering av om mindre inngripende tiltak i tilstrekkelig grad kan ivareta formålet, inngrepets virkning for den som rammes, sakens betydning og forholdene ellers.

Når Etterretningstjenesten går til domstolen og ber om tillatelse til å foreta søk, er det etter det norske systemet, og til forskjell fra det svenske, en forutsetning at man allerede har et søkegrunnlag å gjennomføre søkene i.

4.2.3. Etterretningstjenestens oppgaver og teknologiske forutsetninger

En hensiktsmessig regulering må forholde seg til de oppgavene Etterretningstjenesten er pålagt å løse og de premissene som de teknologiske realitetene setter. Tre forhold er særlig relevante her. For det første skal ikke Etterretningstjenesten bare følge kjente trusler. Tjenesten har som sentral oppgave å søke å avdekke ikke kjente trusler og andre forhold av betydning for norsk sikkerhet. Dette kalles målsøking og reguleres i § 5-1. For det andre er det internasjonale ekomnett bygget på en slik måte at man på forhånd ikke kan forutse hvilken rute en kommunikasjon tar. For det tredje er det behov for å gjøre retrospektive søk tilbake i tid, hvilket forutsetter at beslutning om speiling av kommunikasjonsstrømmer for lagring av metadata i tid kommer forut for rettens tillatelse til å gjøre søk i lagrede data.

Det vises i denne forbindelse til at EMD i *Big Brother Watch mot UK* avsnitt 322 uttaler at bulkinnhentingens formål blant annet er å identifisere nye trusler fra både kjente og ukjente trusselaktører. Videre at disse i dagens digitaliserte samfunn kommuniserer ved bruk av de globale kommunikasjonsnettverkene som benytter raskeste og billigste vei uten noen meningsfull referanse til nasjonale grenser. EMD påpeker i denne forbindelse i avsnitt 424 at *«the nature of the global Internet means that the route a particular communication would travel had become hugely unpredictable».*

Dersom Etterretningstjenesten skal ha en mulighet til å finne de etterretningsrelevante truslene og aktørene, må i prinsippet all kommunikasjon som krysser landegrensen inngå i søkegrunnlaget – fordi man på forhånd ikke kan vite hvilke kommunikasjonsveier inn i landet trusselaktørenes kommunikasjon vil ta. I utgangspunktet vurderer derfor departementet at et krav om at all kommunikasjon som krysser grensen skal kunne speiles som grunnlag for å kunne gjøre domstolautoriserte søk, er nødvendig og forholdsmessig. Det gir begrenset

mening å forsøke å oppstille kriterier som tar sikte på å redusere søkegrunnlaget ved å kreve at det på forhånd og på kvalifisert grunnlag skal velges ut enkelte av de kommunikasjonsstrømmene som krysser grensen. Dette har sammenheng med at man ikke med sikkerhet kan vite hvilken kommunikasjon som går hvor. Som EMD påpeker i *Big Brother Watch mot UK* avsnitt 376:

«In any event, as neither the sender nor the recipient of an electronic communication could control the route it took to its destination, in practice any further restrictions on the choice of bearers would not have made domestic law any more foreseeable as to its effects.»

At Etterretningstjenesten ikke har kapasitet til enhver tid til å håndtere all utenlandskommunikasjon, og dermed må gjøre utvalg basert på de kommunikasjonsstrømmene som antas å transportere mest mulig etterretningsrelevant informasjon, jf. Prop. 80 L (2019-2020) s. 215, endrer ikke på det prinsipielle utgangspunktet. Før metadata lagres, skal Etterretningstjenesten så langt mulig gjøre ytterligere utvalg og filtrering etter § 7-6. I dette ligger å velge ut de mest relevante kommunikasjonsstrømmene. Dette er imidlertid et utvalg som Etterretningstjenesten gjør i kommunikasjonsstrømmer som allerede er speilet. På tilretteleggingsstadiet er utvalget nødvendigvis bredere, ut fra de hensyn som sitatet fra EMD ovenfor viser til.

For at en uavhengig forhåndskontroll knyttet til speiling av kommunikasjonsstrømmer skal gi mening, må den autoriserende instans kunne avsi beslutninger som baserer seg på et faktisk grunnlag og reelle vurderinger. For særskilte kommunikasjons- og meldingstjenester, såkalte OTT-tjenester (se nærmere om disse under pkt. 4.3.4 nedenfor), vil en uavhengig instans kunne vurdere om kommunikasjonen kan antas å inneholde etterretningsrelevant informasjon eller ikke. For de store kommunikasjonsstrømmene som transporterer kommunikasjon over landegrensene stiller dette seg annerledes. Forutsetningen for å kunne si noe kvalifisert om hvilke av disse som kan være bærere av utenlandsetterretningsrelevant informasjon, er at det først gjøres maskinell test og analyse av kommunikasjonsstrømmene. Uten slik forutgående test og analyse vil utvalget av bærere basere seg på ren gjetning, fordi Etterretningstjenesten i et slikt tilfelle ikke vil ha noe faktisk grunnlag å basere sine vurderinger på. Den autoriserende instansen vil dermed heller ikke kunne få seg forelagt noe reelt beslutningsgrunnlag knyttet til hvilken verdi kommunikasjonsstrømmene vil kunne ha som søkegrunnlag.

Etterretningsvirksomhet innebærer å sette sammen informasjonsbiter over tid. Trusselaktører er sikkerhetsbevisste, men små informasjonsbiter satt sammen over tid kan likevel avsløre en aktivitet. Når Etterretningstjenesten får rettens tillatelse til å gjøre søk, er det derfor av stor betydning at det finnes et historisk søkegrunnlag. Behovet for å gjøre retrospektive søk tilbake i tid underbygger således ytterligere at det ikke er mulig å foreta en samlet vurdering av hvilke kommunikasjonsstrømmer som bør speiles sett opp mot de søkene som man begjærer om rettens samtykke til å gjennomføre.

Tilretteleggingsplikt i form av speiling av kommunikasjonsstrømmer må også reflektere realiteten i hvor dette kommer til å finne sted. Som anført i Prop. 80 L (2019-2020) s. 213, vil speilingspunktet avhenge av tekniske og praktiske forhold. Det kan f. eks. være aktuelt å

speile på tjenere tilknyttet 5G (IMS-tjenere m.m.) eller Internett (DNS-tjenere m.m.). Et eksempel er at speiling kan måtte finne sted der hvor krypterte tunneler ender opp i eksempelvis 5G-sammenkoplingsutstyr. Punktene må velges ut fra hensynet til å få best mulig dekning. Trafikk som kommer inn i flere kabler tilhørende flere tilbydere vil noen ganger samles i knutepunkter for utenlandskommunikasjon. Å speile disse knutepunktene kan være nødvendig. Økt kryptering og den teknologiske utviklingen for øvrig kan medføre at selve speilingen også vil kunne omfatte norsk innenlandsk kommunikasjon som ikke krysser grensen. Dette skyldes behovet for å speile noe kommunikasjon rett før eller inne i datamaskinene som bl.a. fasiliterer elektroniske meldingstjenester eller 5G-talekommunikasjon som tjeneste, for å unngå kryptering som tjenesteleverandøren selv har lagt på. Kommunikasjonen til tjenesten vil kunne ta mange veier inn i Norge, og vil kunne være blandet med innenlandskommunikasjon som ikke lar seg filtrere bort før speilingspunktet. Innenlandskommunikasjon skal så langt mulig filtreres bort tidligst mulig i prosessen. Alle begjæringer om søk etter §§ 7-8 og 7-9 skal knyttes til grensekryssende kommunikasjon. Dersom det mot formodning skulle bli gjennomført søk som medfører treff i ikke-grensekryssende kommunikasjon skal slike opplysninger slettes i henhold til etterretningstjenesteloven § 9-8 første ledd, og kan ikke utleveres, jf. § 7-13 første ledd.

4.3. Autorisasjon på ulike stadier

Basert på drøftelsen over mener departementet det er grunn til å skille mellom speiling som skal muliggjøre testinnhenting og testanalyse i etterretningstjenesteloven §§ 7-5 og 7-7 fjerde ledd på den ene siden, og speiling for å etablere et søkegrunnlag etter §§ 7-1 og § 5-3 som grunnlag for etterretningsbaserte søk og innhenting, jf. §§ 7-8 og 7-9, på den andre siden.

4.3.1. Nærmere om testinnhenting og testanalyse

Testinnhenting og testanalyser reguleres i etterretningstjenesteloven §§ 7-5 og 7-7 fjerde ledd. Dette er nødvendig aktivitet for å kunne besvare spørsmålene om hva slags trafikk som går i ulike kommunikasjonsstrømmer, hvor speiling og tilgjengeliggjøring bør gjøres (som igjen er avgjørende for hvem som bør pålegges en tilretteleggingsplikt), hvilken kommunikasjon som skal prioriteres når det ikke er datakraft og overføringskapasitet til å behandle alt, og for å muliggjøre utvalg og filtrering etter § 7-6. For å kunne besvare disse spørsmålene må det gjøres teknisk analyse av metadata i kommunikasjonsstrømmene samt gjennomføres ufiltrerte uttrekk fra én eller flere kommunikasjonsstrømmer. Det er oppstilt svært strenge vilkår i § 7-5, både når det gjelder antall og tidsbegrensning for uttrekk (maksimalt 30 sekunder én gang i timen), lagringstid (ikke lenger enn nødvendig og maksimalt 14 dager) og behandlingsformål (ikke etterretningsformål). Testinnhenting, testanalyser og annen teknisk understøttelse skal bare utføres av tekniske spesialister med særskilt opplæring og som ikke har etterretningsanalyse som oppgave. Det skal alltid være to spesialister til stede ved oppsett og analyse av uttrekk. Informasjon som er innhentet for testinnhenting og -analyse kan ikke benyttes for etterretningsformål. Informasjonen kan heller ikke deles med andre. Det er strenge krav til internkontroll og aktivitetslogger jf. § 7-10, og EOS-utvalget skal føre løpende kontroll, jf. § 7-11.

Forut for å gjøre testing og analyse med sikte på å besvare spørsmålene som listes opp over, må speiling allerede ha funnet sted i en viss utstrekning.

4.3.2. Beslutning om speiling for testinnhenting og testanalyse

Departementet har vurdert i hvilken grad det er hensiktsmessig å legge beslutning om speiling av kommunikasjonsstrømmer for testinnhenting og testanalyse til domstolen, men har kommet til at dette ikke vil gi noen merverdi som rettssikkerhetsgaranti, og foreslår derfor ikke dette.

Som det fremgår av redegjørelsen over er testinnhenting og testanalyse forberedende handlinger som blant annet skal sørge for at det ikke hentes inn mer informasjon enn nødvendig. I praksis må det antas at for å kunne foreta en selvstendig vurdering av om speiling skal kunne skje etter kapittel 7, må domstolen i realiteten bygge opp en egen dublerende teknologisk og etterretningsfaglig kompetanse. I tillegg må Etterretningstjenesten, for å kunne gjøre seg opp en mening om hvilke kommunikasjonsstrømmer som den vil begjære speilet for dette formålet, nettopp måtte ha et datagrunnlag å ta utgangspunkt i som grunnlag for å kunne begrunne sin begjæring til domstolen.

Departementet foreslår på denne bakgrunn at sjefen for Etterretningstjenesten skal kunne fatte beslutning om speiling av kommunikasjonsstrømmer for test og analyse etter §§ 7-5 og 7-7 fjerde ledd. Formålet med speilingen er å kunne avklare om det foreligger grunnlag for å fremme begjæring til retten om å tillate speiling som grunnlag for søk og innhenting etter §§ 7-8 og 7-9. Informasjonen som speiles kan ikke benyttes for etterretningsformål etter loven § 1-3 første ledd bokstav c, dvs. for å løse en av Etterretningstjenestens oppgaver etter kapittel 3.

4.3.3. Speiling av kommunikasjonsstrømmer som grunnlag for søk

Med utgangspunkt i EMDs uttalelser om at bulkinnsamling skal være gjenstand for uavhengig autorisasjon fra starten av («*independent authorisation from the outset*») foreslår departementet at det bør gjelde krav om at pålegg om speiling av kommunikasjonsstrømmer, når disse skal inngå som grunnlag for søk og innhenting etter § 7-8 og 7-9, skal forhåndsautoriseres av en uavhengig instans. Som påpekt tidligere (pkt. 4.2.1.2), utelukkes det ikke at gjeldende rett etter en nærmere prøving vil oppfylle EMDs krav, men det er knyttet rettslig usikkerhet til dette.

Uavhengig forhåndsautorisasjon vil kreve mer saksbehandling, både hos Etterretningstjenesten og hos den autoriserende instansen, og således være fordyrende. Gitt de teknologiske forutsetninger om at trusselkommunikasjon blander seg med all annen kommunikasjon, og at man ikke på forhånd kan vite hvilken rute en enkelt kommunikasjon vil ta, bør det heller ikke oppstilles for store forventninger knyttet til hvilken rettssikkerhetsgaranti forhåndsautorisasjonen vil utgjøre i praksis.

Det må også tas i betraktning at det i mange tilfeller ikke vil være mulig å sondre mellom kommunikasjonsstrømmer av større eller mindre verdi, og at det derfor vil være vanskelig å foreta reelle nødvendighets- og forholdsmessighetsvurderinger i disse tilfellene.

Departementet har likevel etter en nærmere vurdering, der det særlig er lagt vekt på at uavhengig forhåndsautorisasjon kan øke tilliten til ordningen med tilretteleggingsplikt, både generelt og hos tilbyderne, kommet til at man vil foreslå dette.

Av hensyn til sammenhengen med Oslo tingretts rolle som avgjørelsesmyndighet for søk og innhenting, mener departementet at avgjørelsesmyndigheten bør legges til Oslo tingrett og ikke til en ny særskilt instans som opprettes utelukkende for det formål å ta stilling til speiling. Også kompetansemessige, samfunnsøkonomiske, administrative og tungtveiende sikkerhetsmessige hensyn taler for å legge avgjørelsene til domstolen.

4.3.4. Nærmere om «Over the top- tjenester» («OTT-tjenester»)

For særskilte tilbydere av internettbaserte kommunikasjons- og meldingstjenester, såkalte OTT-tjenester, gjelder det andre forutsetninger enn ved speiling av de store kommunikasjonsstrømmene som passerer over landegrensen. Dette vil være leverandører av særskilte innholdstjenester som leveres over det åpne internettet slik som f.eks. Telegram, Whatsapp, Messenger mv. Her vil det i utgangspunktet bare være behov for å speile trafikken dersom man på forhånd har ledetråder eller holdepunkter for at relevante etterretningsmål bruker akkurat denne tjenesten som kommunikasjonskanal. I slike tilfeller vil det være grunnlag for en mer substansiell prøving av hvilke ledetråder dette gjelder, hvilke etterretningsmål som muligens benytter kommunikasjons-tjenesten, viktigheten av å avdekke mulige aktørers kommunikasjon sett opp mot andre hensyn (herunder omfanget av norske brukere av tjenesten) og andre relevante forhold. Disse forholdene vil kunne inngå i en prøving av om speilingen av kommunikasjon over den konkrete tjenesten er nødvendig og forholdsmessig etter grunnvilkårene i etterretningstjenesteloven §§ 5-3 første ledd og 5-4. I vurderingene som nevnt vil Etterretningstjenesten kunne ta utgangspunkt i andre kilder enn teknisk analyse av kommunikasjonen, og det er derfor mindre behov for å dele opp autorisasjonsprosessen i ulike stadier for OTT. Departementet foreslår derfor at Etterretningstjenesten må fremme en begjæring for domstolen for å kunne speile kommunikasjon i OTT-tjenester og at vilkår for dette fastsettes i § 7-3.

4.4. Ytterligere vurderingskriterium om det generelle trusselbildet?

4.4.1. EØS-rettslige rammer – særlig om *La Quadrature du Net*-kriteriene

Det er knyttet rettslig usikkerhet til hvilken betydning EU-domstolens avgjørelser fra oktober 2020 – i sakene *Privacy International* og *La Quadrature du Net* – har for utformingen av etterretningstjenesteloven. Det skyldes summen av en rekke forhold, herunder vesentlige forskjeller mellom etterretningstjenesteloven og de lover som ble prøvd i EU-domstolen, usikkerhet om betydningen av tilpasningsteksten i kommunikasjonsverndirektivets artikkel 15 («de allmenne prinsippene i EØS-retten») og det forhold at Norge ikke er bundet av EUs Charter om grunnleggende rettigheter («Charteret»). EU-domstolens drøftelser gir videre ikke noe klart svar på hvilke kriterier som skal gjelde og hvorledes disse skal forstås i en norsk sammenheng. Avgjørelsene omtaler i liten grad hvilke trussel- og teknologiforutsetninger domstolen har lagt til grunn. Samlet sett gjør dette det vanskelig å operasjonalisere avgjørelsene i en norsk kontekst.

I den juridiske analysen som det vises til i pkt. 2 i høringsnotatet pekes det på at, uavhengig av den nevnte rettslige usikkerheten, har EU-domstolen i *La Quadrature du Net* åpnet for at tilbydere kan pålegges en plikt til å lagre metadata av hensyn til nasjonal sikkerhet i situasjoner hvor det foreligger en alvorlig trussel mot nasjonal sikkerhet som er reell og aktuell eller forutsebar. I analysen heter det videre i punkt 3.3.4:

«Tilsvarende må legges til grunn for overføring av de samme data for nasjonale sikkerhetsformål, uten at tilbyderne pålegges å lagre dataene selv. Ved tilrettelagt innhenting vil det være en statlig aktør som står for overføringen av data etter at speilingen har funnet sted, samt for lagringen av dataene. Siden E-tjenesten ikke får aksess/tilgang til dataene før det foreligger tillatelse fra domstolen, jf. etterretningstjenesteloven kapittel 8, kan det anføres at systemene i praksis vil være nokså sammenlignbare og at det ikke har betydning *hvem* som står for lagringen, så lenge lagringssystemene hindrer at uvedkommende får tilgang.»

Den juridiske analysen går i punkt 3.4.1 nærmere inn på hvordan domstolens vilkår om alvorlig trussel mot nasjonal sikkerhet skal forstås:

«For det første presiserer domstolen at den ikke tidligere har tolket kommunikasjonsverndirektivet i saker som angår tiltak for å beskytte nasjonal sikkerhet. I denne sammenheng viser domstolen til EU-traktaten artikkel 4(2), og slår fast at statenes eneansvar for nasjonal sikkerhet etter denne bestemmelsen korresponderer med de primære interessene statene har i å verne essensielle statlige funksjoner, herunder å avverge og straffe aktivitet som er egnet til å destabilisere fundamentale konstitusjonelle, politiske, økonomiske eller sosiale statlige strukturer eller som er egnet til å direkte true samfunnet, befolkningen eller staten selv, slik som terrorisme.

Videre presiserer domstolen at tiltak med formål å beskytte nasjonal sikkerhet er viktigere enn de øvrige formålene som kan begrunne unntak etter artikkel 15(1), herunder kriminalitetsbekjempelse og beskyttelse av offentlig sikkerhet. På grunn av deres natur og høye alvorlighetsgrad kan truslene som omfattes av nasjonal sikkerhet distingveres fra den generelle risikoen som intern spenning og uro – også der denne er av en alvorlig karakter – kan forårsake. Tiltak for å beskytte nasjonal sikkerhet kan dermed rettferdiggjøre mer alvorlige inngrep i grunnleggende rettigheter enn de øvrige formålene i artikkel 15(1).

På denne bakgrunn konkluderer domstolen med at artikkel 15(1), lest i lys av Charteret artikkel 7, 8, 11 og 52(1) ikke forbyr lovgivning som åpner for at kompetente myndigheter kan pålegge tjenestetilbydere å lagre metadata fra alle brukerne av elektroniske kommunikasjonssystemer for en begrenset periode, forutsatt at det foreligger

«[...] *sufficiently solid grounds for considering that the Member State concerned is confronted with a serious threat, [...], to national security which is shown to be genuine and present or foreseeable.*»

Domstolen oppstiller her grunnvilkårene som må være oppfylt for at tjenestetilbydere skal kunne pålegges en plikt til å lagre data av hensyn til nasjonal sikkerhet. For det første kreves at det er *tilstrekkelig konkrete omstendigheter* som gjør det mulig å anta at det er en *alvorlig trussel mot den nasjonale sikkerhet*. For det andre må trusselen anses *reell og aktuell eller*

mulig å forutse. Ordlyden «reell og aktuell» henspeiler på at trusselen må være genuin, mens alternativet om forutsebarhet henspeiler på at trusselen i det minste må være påregnelig med en viss grad av sannsynlighet. Kravene til bevis framstår som vage og ikke spesielt strenge («*sufficiently solid grounds for considering*»/«*circonstances suffisamment concrètes permettant de considérer*»), og truslene som kan gi grunnlag for lagring av metadata er også formulert nokså bredt («*activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country*»). Uttalelsen viser videre at det trolig er tilstrekkelig at trusselen er av generell art, også fordi fremtidige trusler er omfattet dersom de kan forutses/er påregnelige («*which is shown to be genuine and present or foreseeable*»/«*qui s'avère réelle et actuelle ou prévisible*»).

Domstolen uttaler videre:

«Even if such a measure is applied indiscriminately to all users of electronic communications systems, without there being at first sight any connection, within the meaning of the case-law cited in paragraph 133 of the present judgment, with a threat to the national security of that Member State, it must nevertheless be considered that the existence of that threat is, in itself, capable of establishing that connection.»

Dette må forstås slik at selv om et tiltak gjelder for alle brukere av elektroniske kommunikasjonstjenester, uten at det i utgangspunktet synes å være noen sammenheng med en trussel mot nasjonal sikkerhet, må eksistensen av en slik trussel i seg selv anses egnet til å etablere en slik forbindelse. Videre kan det ikke være nødvendig at trusselen har konkretisert seg, i den forstand at man må kjenne navnet på personer eller grupper som antas å være involvert i trusselaktivitet. EU-domstolens bemerkning om at det ikke kreves noen forbindelse mellom de dataene det er snakk om å lagre, og trusselen mot nasjonal sikkerhet, ville ellers ikke gi noen mening.

En slik plikt til preventiv lagring av alle brukeres opplysninger må begrenses i tid til det strengt nødvendige. Tiltaket kan forlenges hvis trusselen fortsatt er til stede («*owing to the ongoing nature of such a threat*»/«*en raison de la persistance d'une telle menace*»), men bare innenfor en tidshorison som kan forutses. Lagringen må være gjenstand for begrensninger, og være rammet inn av strenge minstekrav som gjør det mulig å effektivt beskytte opplysningene mot misbruk, se nærmere nedenfor. Lagringen kan derfor ikke være av systematisk karakter. Det ligger i dette at det ikke vil være adgang til å ha et permanent system for generell og uddifferensiert lagring av metadata, som ikke er direkte knyttet til potensielt alvorlige trusler mot nasjonal sikkerhet.

EU-domstolen understreker også at det må sikres at bruk av slike tiltak faktisk begrenses til der hvor det er en slik trussel mot den nasjonale sikkerhet. Det er derfor avgjørende at beslutninger om slike tiltak undergis effektiv kontroll, enten av domstolene eller tilsvarende uavhengig organ.

Trusselen må være genuin og påregnelig. Domstolen går ikke nærmere inn på hva som ligger i disse begrepene. Det er nærliggende å tolke domstolens uttalelse om at det ikke kreves noen forbindelse mellom dataene det er tale om å lagre (altså for alle brukere) og trusselen, dithen at trusselen kan være av generell art. I lys av at et av formålene med etterretningsvirksomhet er å avdekke hittil ukjente trusler, er det vanskelig å forstå kravene som noe annet enn at E-

tjenesten må besitte informasjon som etter en nærmere etterretningsfaglig analyse tilsier at et gitt forhold innebærer et trusselpotensial for den nasjonale sikkerheten. En praktisk tilnærming til kriteriet vil være å innfortolke et krav om at det må være mulig å saklig begrunne at trusselpotensialet vil eller kan realiseres dersom ulike forutsetninger er til stede. Videre tilsier nødvendighets- og effektivitetshensyn at man må følge personer, grupper og fenomener over tid for å kunne avdekke og motvirke truslene i tide.

Grunnvilkåret i etterretningstjenesteloven for innhenting av rådata i bulk i § 5-3 første ledd må være oppfylt for at tilrettelagt innhenting skal kunne benyttes. Det oppstilles her et krav om at innhenting må være «nødvendig for å få tilgang til et relevant og tilstrekkelig informasjonsgrunnlag.» Hva som vil være nødvendig i det enkelte tilfellet må vurderes konkret. Der Norges internasjonale forpliktelser stiller særlige krav til innhenting, må dette tas høyde for i lovtolkingen.

E-tjenesten må fremme begjæring for Oslo tingrett om tillatelse til å gjennomføre søk i metadata som lagres gjennom tilrettelagt innhenting. Etterretningstjenesteloven § 8-2 oppstiller krav til begjæringen, herunder at tjenesten må angi oppdraget som søket knytter seg til og det faktiske og rettslige grunnlaget for søket, jf. bokstav a og b. Begjæringen skal gjøres kjent for EOS-utvalget, jf. § 8-1 siste ledd andre punktum. Både domstolen og utvalget vil dermed kunne vurdere E-tjenestens tilnærming til kravene over, og ettergå disse i henhold til egen kompetanse, dersom det oppfattes at tjenesten legger en uriktig tolkning til grunn.

I tillegg til den løpende overprøvingen fra domstolen i forbindelse med begjæringer om søk i lagrede metadata, og den løpende kontrollen fra EOS-utvalget, vil også regjeringen regelmessig revurdere om potensielle trusler mot rikets sikkerhet tilsier bruk av tilrettelagt innhenting. Dette gjøres minimum årlig gjennom behandling av E-tjenestens og PSTs graderte trusselvurderinger. Trusselvurderingene forelegges også for offentligheten i ugraderte versjoner. Lovens ordlyd gjengir imidlertid ikke LQN-kriteriene direkte, og arbeidsgruppen mener det kan være grunn til å vurdere dette nærmere i forbindelse med en videre utredning av beslutningsprosedyren i § 7-3. I denne forbindelse bør det etter arbeidsgruppens syn vurderes om det er behov for å knytte beslutningen om tilrettelegging opp mot en vurdering av trusselsituasjonen og dermed behovet for tilrettelegging.»

I den juridiske analysen går det i punkt 3.4.3 ytterligere inn på hva som menes med nasjonal sikkerhet i *La Quadrature du Net*:

«I LQN åpnes det bare for tiltak knyttet til trusler mot den nasjonale sikkerheten. Hva som menes med nasjonal sikkerhet er bredt formulert:

«the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities.»

Beskrivelsen overlapper i stor utstrekning med formålsbestemmelsen i etterretningstjenesteloven § 1-1 bokstav a. Også opplistingen av etterretningsformål i § 3-1

synes å være innenfor denne rammen. I tillegg angir EU-domstolen at straff («punishment») for aktiviteter som nevnt er en del av statens eneansvar for den nasjonale sikkerheten. På dette punktet er formålet med etterretningstjenesteloven mer avgrenset enn det EU-retten tillater, ettersom loven er avgrenset til innhenting og analyse for å avdekke og motvirke at utenlandske trusler mot Norge og norske interesser aktualiseres.

Tilrettelagt innhenting kan bare brukes for etterretningsformål etter lovens kapittel 3. Dette kapitlet omfatter utenlandske trusler (§ 3-1) og forhold (§ 3-2), okkupasjonsberedskap (§ 3-3), internasjonalt etterretningssamarbeid (§ 3-4) og evneinformasjon (§ 3-5). Adgangen til å innhente informasjon med hjemmel i en av bestemmelsene i kapittel 3 beror ikke på en tolkning av bestemmelsen alene, men må leses i sammenheng med vilkår i loven for øvrig, herunder kravet til forholdsmessighet etter § 5-4. Formålet med innhenting er et sentralt moment i denne vurderingen. Dette har igjen betydning for hvilke metoder som E-tjenesten kan benytte seg av, herunder om søk i metadata fra tilrettelagt innhenting er forholdsmessig. Jo viktigere formålet er, jo mer inngripende metodebruk kan aksepteres.

LQN åpner som nevnt kun for tiltak knyttet til trusler mot den nasjonale sikkerheten. Det kan dermed argumenteres for at bruk av tilrettelagt innhenting bør avgrenses mot §§ 3-2 til 3-5, som ikke direkte gjelder trusler mot Norge og norske interesser. På den andre siden er disse etterretningsformålene i praksis så nært knyttet til formålet om å avdekke og motvirke utenlandske trusler i § 3-1, at de i EØS-rettslig sammenheng må anses som en del av det overordnede formålet om å motvirke utenlandske trusler. I forarbeidene ble særlig forholdet mellom §§ 3-1 og 3-2 belyst, og således tatt stilling til ved stortingsbehandlingen:

«Paragraf 3-1 kommer først til anvendelse dersom man står overfor en *trussel*. Lovforslaget gir ingen nærmere beskrivelse av *når* noe regnes som en trussel. Det må avgjøres konkret i den enkelte situasjon. Likevel er det klart at forholdet må være av en viss alvorlighetsgrad for å kunne utgjøre en trussel. Dersom Etterretningstjenesten utelukkende skal innhente informasjon om etablerte trusler og kjent truende aktivitet, vil den ikke evne å avdekke fremtidens trusselbilde. Etterretningsvirksomhet er predikativ i sin natur, og det å detektere avvik fra normalen er en viktig oppgave. For å kunne varsle om avvik fra det normale, må normaltilstanden være kjent. Forholdet mellom §§ 3-1 og 3-2 kan illustreres med et eksempel fra våre nærområder. Norges forhold til Russland er i stor grad preget av forutsigbarhet. Russland utgjør ingen militær trussel mot Norge i dag. Vår geografiske plassering i forhold til russiske strategiske kapasiteter betyr likevel at utviklingen i Russland og nordområdene har vedvarende stor betydning for norsk og alliert sikkerhet. God og tidsriktig situasjonsforståelse, herunder inngående kunnskap om utviklingen i russisk utenriks- og sikkerhetspolitikk og om moderniseringen av den russiske militærmakten i våre nærområder, er dermed avgjørende forutsetninger for å kunne utforme norsk utenriks-, forsvars- og sikkerhetspolitikk. Uten hjemmel til å innhente informasjon om disse forholdene, som ikke kan karakteriseres som en trussel, men som et prioritert område, vil man ikke besitte den dybdekunnskapen som kreves for å evne å varsle om endringer av betydning. Litt forenklet sagt vil derfor informasjonsinnhenting etter § 3-2 ofte være en avgjørende forutsetning for å kunne innhente informasjon om trusler etter § 3-1.»

Tilsvarende argumentasjon er relevant i forholdet mellom § 3-1 og E-tjenestens øvrige oppgaver (§§ 3-3 til 3-5).

Tilrettelagt innhenting vil inkludere en evne til å gjøre retrospektive søk i datagrunnlaget der Oslo tingrett har tillatt dette. Tatt i betraktning mengden informasjon som går via tjenestetilbyderne, vil tilrettelagt innhenting først og fremst utgjøre en viktig kapasitet for å avdekke trusler etter § 3-1. Det kan samtidig tenkes tilfeller hvor sentral informasjon om forhold som ikke enda utgjør en trussel, men hvor en slik utvikling er påregnelig, også vil kunne detekteres gjennom søk i data fra tilrettelagt innhenting. I alle tilfeller vil det være opp til Oslo tingrett å avgjøre om den faktiske og rettslige begrunnelsen, herunder E-tjenestens forholdsmessighetsvurdering, er tilstrekkelig konkret til at søk kan tillates. Domstolskontrollen vil dermed ytterligere sikre at tilrettelagt innhenting ikke benyttes for formål som ikke møter terskelen.

På denne bakgrunn anføres at tilrettelagt innhenting oppfyller kravet om å være avgrenset til trusler mot nasjonal sikkerhet.»

4.4.2. Vurdering

I lys av den juridiske analysen har departementet vurdert om en uavhengig instans bør prøve om *La Quadrature du Net*-kriteriene er oppfylt på overordnet nivå, som grunnlag for å vurdere om speiling av kommunikasjonsstrømmer fra tjenestetilbyderne bør gjennomføres. Det vises til domstolene som den generelt foretrukne uavhengige instans, selv om den refererte rettspraksis ikke utelukker andre uavhengige instanser.

Dersom en slik vurdering skal gjøres, reises spørsmålet om hvilken reell overprøving domstolen i praksis kan gjøre, dersom EOS-tjenestene vurderer at det foreligger alvorlige trusler mot nasjonale sikkerhetsinteresser. En slik ordning reiser også et prinsipielt spørsmål om domstolene bør ha prøvingsrett og siste ord på et område som tradisjonelt har vært et prerogativ for den utøvende makt. Det er den utøvende makt som har ansvaret for å ivareta norsk suverenitet og beskytte norsk statsikkerhet og samfunnssikkerhet.

På den annen side vil krav om uavhengig prøving av disse kriteriene fjerne eventuell tvil om hvorvidt etterretningstjenesteloven er i samsvar med Norges internasjonale forpliktelser. Det kan også anføres at uavhengig autorisasjon kan øke tilliten til ordningen med tilretteleggingsplikt, både generelt og hos tilbyderne.

Av hensyn til sammenhengen med Oslo tingretts rolle som avgjørelsesmyndighet for søk og innhenting, bør myndigheten etter departementet syn legges til Oslo tingrett og ikke til en ny uavhengig særskilt instans som opprettes utelukkende for det formål. Også kompetansmessige hensyn, samfunnsøkonomiske hensyn, administrative hensyn og tungtveiende sikkerhetsmessige hensyn taler for å legge avgjørelsene til domstolen.

Departementet har på denne bakgrunn etter en helhetlig vurdering utformet et forslag til justert lovtekst i § 7-3. Domstolen skal etter forslaget ta stilling til hvorvidt det foreligger en alvorlig trussel mot nasjonal sikkerhet som er reell og aktuell eller forutsebar og som ikke kan avdekkes i tilstrekkelig grad ved mindre inngripende tiltak.

Det er likevel grunn til å understreke at verdien av en slik overprøving ved retten ikke må overdrives. De forhold som tingretten skal prøve, faller utenfor hva en dommer normalt er forutsatt å vurdere og gjelder en vurdering som forutsetter omfattende innsikt i alle deler av trusselbildet mot Norge og norske interesser. Det vil derfor være naturlig å anta at domstolen vil se hen til de regelmessige vurderinger av trusselbildet som blant annet fremkommer av Etterretningstjenestens og PSTs graderte vurderinger. Disse fremlegges også for offentligheten i ugraderte versjoner.

Det bes særskilt om høringsinstansenes synspunkter om forslaget.

4.5. Utforming av høringsforslag

Forslag til ny § 7-3:

§ 7-3 Beslutninger om tilrettelegging

Sjefen for Etterretningstjenesten treffer beslutning om å speile kommunikasjonsstrømmer etter § 7-2 som utelukkende skal benyttes for testing og analyse etter §§ 7-5 og 7-7 fjerde ledd med sikte på å avklare om det foreligger grunnlag for å fremme begjæring om rettens beslutning etter annet ledd. Tilbyderne skal så langt som mulig gis anledning til å uttale seg før beslutningen fattes. Tilbyderne kan påklage beslutningen til departementet. Fristen for å klage er tre uker fra beslutningen ble meddelt tilbyderen. Departementet kan på anmodning fra tilbyderen bestemme at beslutningen ikke skal iverksettes før klagen er avgjort.

Beslutning om å tillate speiling av kommunikasjonsstrømmer etter § 7-2 som grunnlag for søk og innhenting etter § 7-8 og 7-9 treffes av retten. Reglene i kapittel 8 gjelder tilsvarende så langt de passer, med mindre annet følger av tredje og fjerde ledd.

Begjæring om kjennelse skal være skriftlig og angi forhold som gjør at retten kan prøve

- a) om kommunikasjonsstrømmene inneholder kommunikasjon som transporteres over den norske grensen*
- b) om speiling av kommunikasjonsstrømmer fra særskilt utvalgte internettbaserte kommunikasjons- og meldingstjenester er nødvendig etter § 5-3 første ledd og forholdsmessig etter § 5-4*
- c) om speiling er forholdsmessig sett i lys av hvorvidt det kan antas at det foreligger en alvorlig trussel mot nasjonal sikkerhet som er reell og aktuell eller forutsebar og som ikke kan avdekkes i tilstrekkelig grad ved mindre inngripende tiltak.*

Rettens kjennelse skal ikke gis for lengre tid enn nødvendig, og skal ikke overstige to år. Etterretningstjenesten skal av eget tiltak sørge for å avslutte speiling av kommunikasjonsstrømmer dersom det blir klart at forutsetningene for dette ikke lenger er tilstede.

Øvrige beslutninger om tilretteleggingsplikt etter § 7-2 treffes av sjefen for Etterretningstjenesten. Første ledd annet til femte punktum gjelder tilsvarende.

Beslutninger etter første og annet ledd skal meddeles EOS-utvalget og Nasjonal kommunikasjonsmyndighet. Nasjonal kommunikasjonsmyndighet har ved forespørsel rett til

informasjon fra Etterretningstjenesten om tekniske og operasjonelle løsninger som tjener til å oppfylle tilretteleggingsplikten.

Departementet kan gi forskrift om beslutning om tilrettelegging og om klagebehandling etter første ledd.

5. LOVTEKNISKE RETTELSER

Ved en inkurie gjentar § 4-2 annet ledd regelen i § 4-1 annet ledd. Det fremgår tydelig av merknadene til bestemmelsen, se Prop. 80 L (2019-2020) s. 202, at det var meningen at § 4-2 annet ledd skal regulere forholdet hvis det er tvil om en person opptrer på vegne av fremmed stat eller statslignende aktør, ikke hvorvidt det er tvil om personen befinner seg i Norge eller utlandet. Slik bestemmelsen lyder nå, gir den ingen mening eller tilleggsverdi. Forholdet foreslås rettet opp.

I § 7-2 første ledd bokstav b heter det at tilbydere skal tillate at Etterretningstjenesten midlertidig eller permanent etablerer tilstedeværelse hos tilbyder for å drifte utstyr på steder som kontrolleres av tilbyder. Ordene «midlertidig eller permanent» er overflødige og foreslås fjernet. Ordlyden kan i tillegg gi inntrykk av at Etterretningstjenesten nærmest evigvarende kan etablere tilstedeværelse hos tilbydere, uten at dette er nødvendig i forbindelse med et konkret behov knyttet til at vedkommende tilbyder faktisk er underlagt tilretteleggingsplikt.

Lov 29. mai 2020 nr. 59 om redaksjonell uavhengighet og ansvar i redaktørstyrte journalistiske medier (medieansvarsloven) trådte i kraft 1. juli 2020. Fra samme tidspunkt ble lov 13. juni 2008 nr. 41 om redaksjonell fridom i media (mediefridomslova) opphevet. Som en konsekvens må henvisningen til mediefridomslova § 2 i etterretningstjenesteloven § 9-6 første ledd erstattes med henvisning til medieansvarsloven § 2.

6. ØKONOMISKE OG ADMINISTRATIVE KONSEKVENSER

Forslagene vil i begrenset grad medføre økonomiske og administrative konsekvenser.

Antall kildevernsaker forventes å være meget få. Kostnadene ved å behandle disse for retten er derfor ikke vesentlige.

Det foreslås at Oslo tingrett skal forhåndsautorisere hvilke kommunikasjonsstrømmer som skal speiles i den hensikt å skape et søkegrunnlag for de senere beslutninger som domstolen skal treffe om søk i datastrømmene. Administrative kostnader forbundet med dette, både hos Etterretningstjenesten og Oslo tingrett, forventes å kunne dekkes innenfor gjeldende budsjetter.

7. MERKNADER TIL DE ENKELTE BESTEMMELSER

Til § 4-2

Det foreslås en rettelse i *annet ledd første punktum*, se pkt. 5 i høringsnotatet.

Til § 5-2

Det tilføyes et nytt *annet ledd* som skal sikre uavhengig autorisasjon forut for målrettet innhenting i saker hvor det er stor sannsynlighet for at innhenting vil frembringe kildeidentifiserende opplysninger som omfattes av lovens § 9-6 første ledd. Målrettet innhenting mot journalister og andre personer som tilsynelatende omfattes av § 9-6 første ledd vil, unntatt i åpenbare omgåelsestilfeller hvor for eksempel en fremmed etterretningsoffiser fingerer å være journalist for å unngå at etterretningsvirksomhet skal bli oppdaget, være saker hvor det er stor sannsynlighet for at innhenting vil frembringe slike kildeidentifiserende opplysninger. Den høye terskelen gjelder kun dersom det fremstår med høy grad av sannsynlighet at innhenting vil frembringe kildeidentifiserende opplysninger. I mange tilfeller vil det på innhentingsstadiet ikke være mulig å legge en slik høy sannsynlighetsovervekt til grunn, som krever særskilte holdepunkter. Det må tas i betraktning at det aldri er et formål med Etterretningstjenestens innhenting å avsløre medienes kilder, og at enhver person potensielt kan være en kilde. På innhentingstidspunktet er det derfor normalt umulig å sikre at innhenting ikke vil kunne frembringe slik informasjon utilsiktet.

Utgangspunktet er at dersom stor sannsynlighet konstateres, skal målrettet innhenting ikke finne sted. I tråd med menneskerettighetene og EMDs praksis, er kildevernet likevel ikke absolutt. Unntak fra kildevernet kan gjøres dersom det er strengt nødvendig av hensyn til nasjonale sikkerhetsinteresser. Terskelen er høy, og unntaksmuligheten skal forstås på samme måte som i etterretningstjenesteloven § 9-6 annet ledd. Det vises også til omtalen i Prop. 80 L (2019-2020) s. 154-160 og 226.

Beslutning om målrettet innhenting legges til Oslo tingrett etter de prosessregler som følger av etterretningstjenesteloven kapittel 8 med henvisninger. Kapittel 8 er utformet med sikte på domstolskontroll med tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon. Det er derfor nødvendig at reglene kommer til anvendelse «så langt de passer» i disse sakene. Det inkluderer reglene om oppnevning av særskilt advokat (§ 8-5). I vurderingen av hva retten skal prøve (§ 8-4) vises det bl.a. til om grunnvilkårene etter kapittel 5 er oppfylt. Det vil stå sentralt for retten å prøve om den høye terskelen for innhenting er nådd, jf. kildevernets rettslige beskyttelse etter Grunnloven § 100 og EMK artikkel 10. I denne vurderingen vil den nedkjølende effekten inngrepet vil kunne ha for medienes mulighet til å motta informasjon i fremtiden, bli særlig vektlagt. Det er således ikke tvilsomt at rettslig prøving av kildevernet er omfattet av § 8-4, se også Prop. 80 L (2019-2020) s. 120.

§ 8-1 gjelder kun kjennelse om tillatelse til tilrettelagt innhenting. Det legges til grunn at kjennelse også kan gis for beslutninger som nevnt i forslaget til § 5-2 og § 9-6 i saker om kildeidentifiserende opplysninger, og at de øvrige regler i § 8-1 kommer tilsvarende til anvendelse.

Til § 7-2

Det foreslås en rettelse i første ledd bokstav b, se pkt. 5 i høringsnotatet.

Til § 7-3

Etter *første ledd* kan sjefen for Etterretningstjenesten treffe beslutning om å speile kommunikasjonsstrømmer etter § 7-2 som utelukkende skal benyttes for testing og analyse etter §§ 7-5 og 7-7 fjerde ledd, med sikte på å avklare om det foreligger grunnlag for å fremme begjæring om rettens beslutning etter annet ledd. Dersom formålet er et annet, skal beslutningen treffes av retten etter annet ledd.

Reglene om at tilbyderne så langt som mulig skal gis anledning til å uttale seg før beslutningen fattes, og om klage til departementet, tilsvarer den vedtatte (men ikke ikraftsatte) § 7-3 annet ledd.

Etter *annet ledd* kan retten treffe beslutning om å tillate speiling av kommunikasjonsstrømmer etter § 7-2 som grunnlag for søk og innhenting etter § 7-8 og 7-9. Reglene i kapittel 8 gjelder tilsvarende så langt de passer. Kapittel 8 er utformet med tanke på beslutninger om søk og innhenting, ikke med tanke på å tillate tilrettelegging. Ordlyden «med mindre annet følger av tredje og fjerde ledd» tydeliggjør hvilke hovedtilpasninger som er nødvendig.

Tredje ledd omhandler hvilke forhold som skal angis i begjæringer til retten og hvilke forhold retten skal prøve. De kriterier som er angitt her, er ment å være uttømmende for hva retten skal prøve. Kriteriene må sammenholdes med det som er beskrevet i pkt. 4.2.3 i høringsnotatet. Det må i vurderingen av om kjennelsen skal innvilges tas hensyn til at det avgjørende med speilingen er å etablere et søkegrunnlag basert på utenlandskommunikasjon. Det vises til uttalelsene fra EMD i punkt 4.2.3 om at man ikke kan vite hvilken rute en kommunikasjon tar. Hensikten med en uavhengig prøving på speilingsstadiet er derfor å ta stilling til om det er sannsynlig at det går utenlandskommunikasjon i kommunikasjonsstrømmene som begjæres speilet. Etterretningstjenesten får ikke direkte tilgang til søkegrunnlaget, men må tilbake til domstolen med en begrunnet begjæring før det kan gjennomføres søk for etterretningsformål.

Bokstav b kommer bare til anvendelse dersom det fremmes begjæring om å speile kommunikasjonsstrømmer fra såkalte OTT-tjenester (internettbaserte kommunikasjons- og meldingstjenester), se nærmere om dette i pkt. 4.3.4

Når det gjelder vurderingskriteriet i *bokstav c* om at speiling skal være forholdsmessig sett i lys av hvorvidt det kan antas at det foreligger en alvorlig trussel mot nasjonal sikkerhet som er reell og aktuell eller forutsebar og som ikke kan avdekkes i tilstrekkelig grad ved mindre inngripende tiltak, er dette en henvisning til de såkalte *La Quadrature du Net*-kriteriene. Disse skal forstås på den måte som er angitt i den juridiske analysen som er sitert i pkt. 4.4.1 i høringsnotatet her. Vurderingskriteriet er en særlig forholdsmessighetsvurdering sett i forhold til den alminnelige forholdsmessighetsregelen i etterretningstjenesteloven § 5-4.

Etter *fjerde ledd* skal rettens kjennelse ikke gis for lengre tid enn nødvendig, og ikke overstige to år. Trusselbildet og behovet for tilrettelegging endres ikke over natten. Etterretningsfaglige og økonomiske hensyn tilsier at speiling og tilgjengeliggjøring av utenlandskommunikasjon ikke må revurderes for ofte. Det har også sammenheng med behovet for lagring av metadata for retrospektive søk. Erfaring fra blant annet avdekking av fremmede staters cyberoperasjoner er at dette krever lagring av historiske metadata i en lengre tidsperiode. For at speilingen av data skal kunne oppfylle sitt formål som relevant søkegrunnlag må det i vurderingen av tidsavgrensning tas hensyn til at utenlandsetterretning er et langsiktig arbeid og at trusselaktørene er meget sikkerhetsbevisste.

Etterretningstjenesten skal av eget tiltak sørge for å avslutte speiling av kommunikasjonsstrømmer dersom det blir klart at forutsetningene for dette ikke lenger er tilstede. Bestemmelsen er utformet etter mønster av tilsvarende bestemmelse i § 8-6 annet ledd.

Det er behov for å treffe beslutning om en rekke mindre inngripende og detaljerte plikter om tilrettelegging, f. eks. plikt til å dele kunnskap om tilbyderens systemer og om sikkerhetsmessige forhold. Slik øvrige beslutninger om tilretteleggingsplikt etter § 7-2 treffes av sjefen for Etterretningstjenesten jf. *femte ledd*.

Bestemmelsene i *sjette og syvende ledd* tilsvarer bestemmelsene i den vedtatte (men ikke ikraftsatte) § 7-3 tredje og fjerde ledd.

Til kapittel 8

Fordi kapittel 8 utvides til å gjelde et begrenset antall saker som ikke gjelder tilrettelagt innhenting, endres overskriften i kapittel 8 til å hete «Domstolskontroll».

Til § 9-6

Det gjøres en rettelse i *første ledd første punktum*, se pkt. 5 i høringsnotatet.

Beslutningsnivået for å tillate behandling av kildeidentifiserende opplysninger for etterretningsformål endres fra departementet til retten. Dette fremkommer av § 9-6 *tredje ledd*.

Beslutning om behandling av opplysninger etter § 9-6 annet ledd legges til Oslo tingrett etter de prosessregler som følger av etterretningstjenesteloven kapittel 8 med henvisninger. Kapittel 8 er utformet med sikte på domstolskontroll med tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon. Det er derfor nødvendig at reglene kommer til anvendelse «så langt de passer» i disse sakene. I all hovedsak vil de enkelte bestemmelsene i kapittel 8 være anvendelige. Det inkluderer reglene om oppnevning av særskilt advokat (§ 8-5).

I vurderingen av hva retten skal prøve (§ 8-4) vises det bl.a. til om grunnvilkårene etter kapittel 5 er oppfylt. Det vil stå sentralt for retten å prøve om den høye terskelen for

behandling er nådd, jf. kildevernets rettslige beskyttelse etter Grunnloven § 100 og EMK artikkel 10. I denne vurderingen vil den nedkjølende effekten inngrepet vil kunne ha for medienes mulighet til å motta informasjon i fremtiden, bli særlig vektlagt.

§ 8-1 gjelder kun kjennelse om tillatelse til tilrettelagt innhenting. Det legges til grunn, uten at det har vært nødvendig å justere ordlyden i § 8-1, at kjennelse også kan gis for beslutninger som nevnt i forslaget til § 9-6 i saker om kildeidentifiserende opplysninger, og at de øvrige regler i § 8-1 kommer tilsvarende til anvendelse.

Som følge av at retten skal treffe beslutningen, er det ikke behov for å ha en regel i § 9-6 tredje ledd om at beslutningen skal være skriftlig og redegjøre for det faktiske og rettslige grunnlaget for behandlingen. Det samme gjelder regelen om at beslutningen skal meddeles EOS-utvalget. Dette vil følge av § 8-1, sammenholdt med §§ 8-2 og 8-4.

Kapittel 8 gjelder gjennomgående begjæring og kjennelser om «søk» og «innhenting», mens § 9-6 gjelder «behandling» av opplysninger som allerede er fremkommet gjennom søk og innhenting. Ordlyden «så langt de passer» skal forstås dithen at ordlyden i kapittel 8 skal forstås å omfatte «behandling» etter § 9-6.

Til § 9-8

§ 8-6 omhandler varigheten av rettens kjennelser. Dersom retten gir tillatelse til behandling, vil det ligge i sakens natur at behandlingen skal skje så lenge behandlingen er nødvendig for etterretningsformål. Etterretningstjenesten skal slette opplysningene når de ikke lenger er nødvendige for formålet med behandlingen, jf. § 9-8 første ledd.

Kildeidentifiserende opplysninger vil som regel være personopplysninger. I den utstrekning opplysningene ikke er personopplysninger, f. eks. dersom opplysningene avslører en organisasjon som kilde, bør det gjelde en tilsvarende regel. Det innføres derfor en særskilt bestemmelse om dette i § 9-8 *første ledd nytt annet punktum*.

8. LOVFORSLAG

Forslag til lov om endringer i etterretningstjenesteloven

I

I lov 19. juni 2020 nr. 77 om Etterretningstjenesten (etterretningstjenesteloven) gjøres følgende endringer:

§ 4-2 annet ledd første punktum skal lyde:

Ved tvil om en person *opptrer på vegne av fremmed stat eller statslignende aktør*, skal Etterretningstjenesten søke å avklare forholdet.

§ 5-2 nytt annet ledd skal lyde:

Målrettet innhenting som med stor sannsynlighet vil frembringe kildeidentifiserende opplysninger etter § 9-6 første ledd, kan bare iverksettes dersom det er strengt nødvendig at de hensyn som begrunner kildevernet, viker for nasjonale sikkerhetsinteresser. Beslutning om innhenting skal treffes av retten etter begjæring av sjefen for Etterretningstjenesten. Reglene i kapittel 8 får tilsvarende anvendelse så langt de passer.

§ 7-2 første ledd bokstav b skal lyde:

b) tillate at tjenesten installerer utstyr og etablerer tilstedeværelse for å drifte utstyr på steder som kontrolleres av tilbyder

§ 7-3 skal lyde:

§ 7-3 *Beslutninger om tilrettelegging*

Sjefen for Etterretningstjenesten treffer beslutning om å speile kommunikasjonsstrømmer etter § 7-2 som utelukkende skal benyttes for testing og analyse etter §§ 7-5 og 7-7 fjerde ledd med sikte på å avklare om det foreligger grunnlag for å fremme begjæring om rettens beslutning etter annet ledd. Tilbyderen skal så langt som mulig gis anledning til å uttale seg før beslutningen fattes. Tilbyderen kan påklage beslutningen til departementet. Fristen for å klage er tre uker fra beslutningen ble meddelt tilbyderen. Departementet kan på anmodning fra tilbyderen bestemme at beslutningen ikke skal iverksettes før klagen er avgjort.

Beslutning om å tillate speiling av kommunikasjonsstrømmer etter § 7-2 som grunnlag for søk og innhenting etter § 7-8 og 7-9 treffes av retten. Reglene i kapittel 8 gjelder tilsvarende så langt de passer, med mindre annet følger av tredje og fjerde ledd.

Begjæring om kjennelse skal være skriftlig og angi forhold som gjør at retten kan prøve

a) *om kommunikasjonsstrømmene inneholder kommunikasjon som transporteres over den norske grensen*

- b) om speiling av kommunikasjonsstrømmer fra særskilt utvalgte internettbaserte kommunikasjons- og meldingstjenester er nødvendig etter § 5-3 første ledd og forholdsmessig etter § 5-4
- c) om speiling er forholdsmessig sett i lys av hvorvidt det kan antas at det foreligger en alvorlig trussel mot nasjonal sikkerhet som er reell og aktuell eller forutsebar og som ikke kan avdekkes i tilstrekkelig grad ved mindre inngripende tiltak.

Rettens kjennelse skal ikke gis for lengre tid enn nødvendig, og skal ikke overstige to år. Etterretningstjenesten skal av eget tiltak sørge for å avslutte speiling av kommunikasjonsstrømmer dersom det blir klart at forutsetningene for dette ikke lenger er tilstede.

Øvrige beslutninger om tilretteleggingsplikt etter § 7-2 treffes av sjefen for Etterretningstjenesten. Første ledd annet til femte punktum gjelder tilsvarende.

Beslutninger etter første og annet ledd skal meddeles EOS-utvalget og Nasjonal kommunikasjonsmyndighet. Nasjonal kommunikasjonsmyndighet har ved forespørsel rett til informasjon fra Etterretningstjenesten om tekniske og operasjonelle løsninger som tjener til å oppfylle tilretteleggingsplikten.

Departementet kan gi forskrift om beslutning om tilrettelegging og om klagebehandling etter første ledd.

Kapittel 8 overskriften skal lyde:

Kapittel 8. Domstolskontroll

§ 9-6 første ledd første punktum skal lyde:

Etterretningstjenesten skal ikke behandle opplysninger som er betrodd noen i deres journalistiske virke og som kan avsløre hvem som er kilde for opplysningen, dersom den som betror seg eller som er betrodd opplysningen, er bosatt i Norge, norsk statsborger eller arbeider på oppdrag for virksomhet i Norge som omfattes av medieansvarsloven § 2.

§ 9-6 tredje ledd skal lyde:

Beslutning om å behandle opplysninger etter andre ledd skal treffes av retten. Reglene i kapittel 8 får tilsvarende anvendelse så langt de passer.

§ 9-8 første ledd nytt annet punktum skal lyde:

Kildeidentifiserende opplysninger som det er gitt tillatelse til å behandle etter § 9-6 tredje ledd og som ikke er personopplysninger, skal slettes når opplysningene ikke lenger er nødvendige for formålet med behandlingen.

II

Loven trer i kraft fra den tiden Kongen bestemmer. De enkelte bestemmelsene i loven kan settes i kraft til ulik tid.