Digital innhenting;
En menneskerettslig krenkelse eller forpliktelse?

Vil tilrettelagt innhenting være forenelig med retten til privatliv i Grunnloven og EMK?

Kandidatnummer: 19

Antall ord: 14751

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

10. desember 2019

Innholdsfortegnelse

Kapittel 1: Innledning

1.1 Problemstilling og tema

Temaet for denne avhandlingen er hvorvidt et system for innhenting av grenseoverskridende elektronisk kommunikasjon vil være forenelig med Norges menneskerettighetsforpliktelser. Systemer for kommunikasjonsinnhenting blir stadig vanligere i demokratiske samfunn, noe som reiser nye problemstillinger for rettsstaten og ivaretakelsen av grunnleggende menneskerettigheter.[1] Betegnelsen grenseoverskridende elektronisk kommunikasjon benyttes i denne forbindelse om kommunikasjonsdata som krysser landegrensen i transportsystemer for datatrafikk.

Temaet har sin bakgrunn i Forsvarsdepartementets forslag til ny lov om Etterretningstjenesten, som ble sendt på høring til faginstanser den 12. november 2018.[2] I dette lovforslaget har departementet foreslått regulering av et innhentingssystem for grenseoverskridende elektronisk kommunikasjon, betegnet som tilrettelagt innhenting.[3] Forslaget bygger videre på utredningen av digitalt grenseforsvar foretatt av Lysne II-utvalget i 2016.[4] For tiden er lovforslaget under behandling av Forsvarsdepartementet, og er per dags dato ikke fremmet for Stortinget. Forslaget befinner seg dermed tidlig i lovgivningsprosessen, som har pågått helt siden Stortinget i 2017 anmodet regjeringen om en revisjon av gjeldende lov om Etterretningstjenesten.[5]

En innføring av system for innhenting av grenseoverskridende kommunikasjonsdata har vært på agendaen siden Lysne II-utvalgets utredning og anbefaling av en innføring.[6] Denne målsettingen kan nå sies å ha kommet ett steg lenger i prosessen, da et lovforslag er utarbeidet. Fremveksten av systemer for elektronisk- og telekommunikasjonsinnhenting har vært en trend i flere rettsstater de senere år, herunder Storbritannia, Sverige og Nederland.[7]

---

[1] Rubinstein, Nojeim, Lee (2017), *Systematic Government Access to Private-Sector Data,* s. 6.
[2] Forsvarsdepartementet, Høringsnotat – Forslag til ny lov om etterretningstjenesten (12.11.2018). https://www.regjeringen.no/contentassets/556459ec77bd448f828af034dd573e11/horingsnotat---forslag-til-ny-lov-om-etterretningstjenesten.pdf
[3] Høringsnotat – Forslag til ny lov om etterretningstjenesten, punkt. 11.14.
[4] Lysne II-utvalget, *Digitalt grenseforsvar (DGF).* (26.08.2016).
[5] Lov 20. mars 1998 nr. 11 om Etterretningstjenesten.
[6] Lysne II-utvalget, *Digitalt grenseforsvar (DGF).* (26.08.2016).
[7] Se om dette: [Høringsnotatet, punkt 11.4] og [Rubinstein, Nojeim, Lee (2017), *Systematic Government Access to Private-Sector Data,* s. 6]

Denne utviklingen av digitale innhentingssystemer i andre land, gjør det nærliggende å forvente at en form for innhentingssystem vil søkes gjennomført også i Norge. Hvorvidt dette blir et system etter modell av tilrettelagt innhenting, er mer uvisst. Utarbeidingen av et lovforslag har satt spørsmålet på dagsordenen i det norske samfunn, og muligheten for en innføring synes derav mer reell enn før.

Formålet med å innføre et system som tilrettelagt innhenting er å gi den norske utenlandsetterretningen en mulighet til å holde tritt med utviklingen av trusselbildet i det digitale samfunn.[8] Innhentingssystemet er tiltenkt benyttet av Etterretningstjenesten, med det formål å innhente kommunikasjonsdata som passerer den norske landegrensen. Det overordnede målet med innhentingen er å frembringe informasjon om utenlandske og grenseoverskridende trusler mot samfunnets og borgernes sikkerhet.[9] Tilgang til grenseoverskridende elektronisk kommunikasjon, reiser imidlertid spørsmål til myndighetenes forpliktelser til å respektere og ivareta enkeltindividets menneskerettigheter. Særlig aktuelt blir spørsmålet om et innhentingssystem vil være i overenstemmelse med individets rett til privatliv.

Hovedproblemstillingen for denne avhandlingen er hvorvidt tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon er forenelig med retten til privatliv i Grunnloven § 102 og EMK art. 8.[10] Et annet spørsmål som aktualiseres er hvordan et innhentingssystem stiller seg i relasjon til myndighetenes plikt til å sikre borgernes menneskerettigheter etter Grunnloven § 92 og EMK art. 1.[11] En underproblemstilling i denne avhandlingen er dermed om et innhentingssystem ala tilrettelagt innhenting kan havne innenfor myndighetenes plikt til å beskytte borgernes menneskerettigheter.

1.2 Rettskildebildet og metode

Ved behandling av hovedproblemstillingen vil det tas utgangspunkt i retten til privatliv, slik denne er nedfelt i Grunnloven § 102 og EMK art. 8. Med utgangspunkt i det dualistiske prinsipp er det praksis fra Høyesterett som har prejudikatsvirkning ved

[8] Høringsnotat – Forslag til ny lov om etterretningstjenesten, s. 15.
[9] Høringsnotat – Forslag til ny lov om etterretningstjenesten, punkt 11.6.
[10] Grunnloven § 102 og EMK art. 8 jf. menneskerettighetsloven § 2.
[11] Grunnloven § 92 og EMK art. 1 jf. menneskerettighetsloven § 2.

grunnlovsfortolkningen.[12] Det er imidlertid ingen norske rettsavgjørelser som behandler det spørsmål som reises i avhandlingens hovedproblemstilling. Dette kommer av at det ikke eksisterer et innhentingssystem av denne karakter i Norge per i dag. De norske rettsavgjørelser som behandles vil dermed først og fremst ha betydning for de generelle retningslinjer som kan utledes om myndighetenes inngrepsadgang. Den nærmere analysen av Grl. § 102 vil dermed måtte foretas i lys av de folkerettslige forbilder.[13]

Ved tolkningen av EMK art. 8 vil rettslig bindende praksis avsagt av Den Europeiske Menneskerettighetsdomstolen (heretter EMD), få sentral betydning. Det vil særlig tas utgangspunkt i de retningslinjer utpenslet av EMD i relasjon til overvåkningstiltak. Denne praksis kan også få betydning som tolkningsmomenter i relasjon til Grl. § 102. For underproblemstillingen vil tilsvarende rettslige utgangspunkter gjøre seg gjeldende.

Videre vil selve høringsnotatet som inneholder forlaget til ny lov om Etterretningstjenesten gi viktige anvisninger på innholdet og utformingen av innhentingssystemet. Uttalelser fra høringsinstansene kan være veiledende både for hvordan innhentingssystemet tilrettelagt innhenting må forstås, og for hvordan de menneskerettslige krav vil anvendes på innhentingssystemet. De vil derfor benyttes for å underbygge den rettslige argumentasjonen, der dette er relevant.

Et viktig metodisk utgangspunkt er at analysen av tilrettelagt innhenting er basert på et lovforslag. Den metodiske utfordringen ligger da i å ta høyde for at en senere lovregulering vil kunne komme til å fravike den foreslåtte reguleringen på flere sentrale punkter. I analysen vil det dermed søkes å ha et mer prinsipielt blikk på hvordan et innhentingssystem som tilrettelagt innhenting vil stille seg mot de menneskerettslige kravene. Selv om en lovregulering vil kunne utformes annerledes, er det nærliggende å anta at et innhentingssystem i en viss utstrekning vil bygge på en utforming à la tilrettelagt innhenting. I avhandlingen vurderes derfor tilrettelagt innhenting ut ifra et premiss om at et slikt innhentingssystem vil kunne bli innført i fremtiden.

1.3 Det digitale samfunn og grenseoverskridende terrorisme

[12] Rt. 2015 s. 93, avsnitt 57.
[13] Rt. 2015 s. 93, avsnitt 57.

1.3.1 Grenseoverskridende terrorisme i et digitalt samfunn

Dagens samfunn er preget av sterk digitalisering. Dette har også i mange år vært en ønsket samfunnsutvikling. Fremveksten av internett og digitaliseringen av samfunnet har imidlertid gitt terroraktører en mer grenseoverskridende rekkevidde enn før, der terrororganisasjoner kan operasjonaliseres på tvers av landegrenser.[14] Dette har gitt grenseoverskridende terrorisme muligheten til å danne virtuelle nettverk fremfor fysiske, samt benytte nettsider og meldingstjenester til propaganda, rekruttering og angrepsplanlegging.[15] I lys av denne utviklingen har fremveksten av digitale innhentingsverktøy de senere år vært betydelig, også i demokratiske stater. Implementeringen av innhentingssystemer kan anses som et forsøk på å holde tritt med utviklingen av trusselbildet på internett.

1.3.2 Etterretningstjenestens virksomhet

Forsvarsdepartementets lovforslag er ment å erstatte dagens Etterretningstjenestelov, og instruks 31. august 2001 nr. 1012 om Etterretningstjenesten (E-instruksen). Den fremtredende endringen i forslaget til ny lov, er innføringen av tilrettelagt innhenting. Etterretningstjenestens virksomhet består i dag av informasjonsinnhenting for å utføre sitt samfunnsoppdrag om strategisk varsling om ytre trusler, samt å gi etterretningsstøtte til forsvarets operasjoner og viktige politiske beslutningsprosesser.[16] Ved innføring av et digitalt innhentingssystem, vil E-tjenesten få et verktøy for innhenting av elektronisk kommunikasjon om grenseoverskridende forhold, som ikke foreligger i dag.

1.4 Avgrensning og fremstillingen videre

Avhandlingen tar ikke sikte på å foreta en uttømmende behandling av alle relevante spørsmål som reiser seg i relasjon til elektronisk kommunikasjonsinnhenting. Dette fordi det ville gå ut over grensene for hva som er mulig og hensiktsmessig i denne analysen, og fordi en senere lovregulering kan komme til å avvike fra lovforslaget på en del vesentlige punkter. Det vil følgelig foretas en prioritering av de tekniske og rettslige aspekter som antas å få størst betydning for gyldigheten av et system som tilrettelagt innhenting.

---

[14] Macdonald og Mair (2015), s. 28.
[15] Macdonald og Mair (2015), s. 28.
[16] Høringsnotat – Forslag til ny lov om etterretningstjenesten, s. 16-17.

Videre vil avhandlingen avgrenses fra å behandle tilgrensende spørsmål, som den ekstraterritorielle virkning av de menneskerettigheter som behandles.

I det følgende vil det først i kapittel 2 redegjøres for ordningen tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon, og hva dette systemet vil innebære. Dette danner grunnlaget for innhentingens omfang, som har betydning for den rettslige analysen. Deretter vil det i kapittel 3 gis en kort redegjørelse av retten til privatliv og adgangen til å gjøre inngrep i Grunnloven § 102 og EMK art. 8. Den nærmere analysen av de menneskerettslige krav som oppstilles til lovgivning som autoriserer digitale innhentingstiltak, vil foretas i avhandlingens kapittel 4. Analysen vil ta for seg de tre overordnede krav som må innfris for at inngrep skal være forenelig med retten til privatliv, som er henholdsvis lovkravet, formålskravet og forholdsmessighetskravet. I kapittel 5 vil det foretas en analyse av hvorvidt et innhentingssystem som tilrettelagt innhenting kan inngå som en del av statens preventive forpliktelser mot grenseoverskridende terrorisme. Denne analysen vil ta utgangspunkt i statens menneskerettslige forpliktelse til å sikre retten til liv etter Grunnloven § 93 og EMK art. 2. I kapittel 6 vil det avslutningsvis sammenfattes sentrale normative betraktninger om de komplekse juridiske og tekniske spørsmål som innhentingssystemet aktualiserer, og gis en konklusjon på problemstillingen om tilrettelagt innhenting være forenelig med retten til privatliv i Grunnloven og EMK.

Kapittel 2: Tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon

2.1 Innholdet i tilrettelagt innhenting

«Tilrettelagt innhenting» er betegnelsen på et etterretningsverktøy for innhenting og analyse av kommunikasjonsdata som transporteres over landegrensene i fiberoptiske kabler.[17] Denne innhentingsvirksomheten går i grove trekk ut på at etterretningstjenesten får tilgang til datastrømmer som transporteres i fiberoptiske kabler ut av landet. Tilgangen etableres ved at tjenesteleverandører i ekomindustrien tilrettelegger for installasjon og drift

[17] Høringsnotatet, s. 187.

av nødvendig overvåkningsutstyr på kablene.[18] Kommunikasjonsdata som innsamles ved dette virkemiddelet omfatter både gjensidig kommunikasjon mellom flere parter, og ensidig overføring av lyd, bilde, tekst og andre data.[19]

Mer presist knytter tilrettelagt innhenting seg til innsamling av to hovedkategorier av kommunikasjonsdata; lagring og søk i metadata, og innhenting og lagring av innholdsdata.[20] Etter lovforslagets definisjon er metadata «data som beskriver annen data», eller som «inneholder ekstra informasjon knyttet til data».[21] Dette omfatter data som beskriver elektronisk kommunikasjon, herunder informasjon som avsender og mottaker, formatet eller typen innhold, samt størrelse, tidspunkt og varighet for kommunikasjon.[22] Innholdsdata om elektronisk kommunikasjon skal etter lovforslaget forstås som «data som ikke er metadata», og omfatter selve innholdet i kommunikasjonen.[23] Et typisk eksempel på elektronisk kommunikasjon som kan illustrere forskjellen mellom meta- og innholdsdata, er data som stammer fra en melding på et sosialt medium. Informasjonen om avsender, mottaker, typen innhold og tidspunkt for en facebook-melding regnes som metadata, mens selve meldingen og dens innhold er innholdsdata.

I utformingen av tilrettelagt innhenting inndeles innhentingsaktiviteten i henholdsvis lagring av metadata, søk i lagrede metadata, samt innhenting og lagring av innholdsdata.[24] Lagring av metadata skjer ved bulkinnsamling, som innebærer en innsamling av store kvantum data fra fiberkablene, der også en vesentlig del av dataene ikke er relevante for etterretningsformål.[25] Etter metadataene er lagret hos E-tjenesten, kan det foretas søk i den lagrede datasamlingen basert på person- eller modusselektorer.[26] Den siste

---

[18] Høringsnotatet, s. 289. Begrepet «ekomindustrien» sikter til «*enhver fysisk eller juridisk person som tilbyr andre tilgang til elektronisk kommunikasjonsnett eller -tjeneste*» jf. ekomloven § 1-5 nr. 16. Tilretteleggingsplikten er også ment å omfatte «*tilbydere av internettbaserte kommunikasjons- eller meldingstjenester*» etter høringsnotatet punkt 18, *Forslag til lovtekst*, s. 385. Nærmere om dette under kapittel 2.3.

[19] Høringsnotatet, punkt 11.3, s. 187.

[20] Høringsnotatet, s. 283-287.

[21] Høringsnotatet, s. 284 og 386.

[22] Høringsnotatet, punkt 11.14.6, s. 284.

[23] Høringsnotatet, s. 286 og 386.

[24] Høringsnotatet, s. 283-287.

[25] Høringsnotatet, punkt 8.3.2, s. 118. Se også definisjonen fra U.S National Research Council (2015), Bulk Collection of Signals Intelligence: Technical Options, s. 33: "*Although the amount of information retained from bulk collection is often large, and often larger than the amount of information retained from targeted collection, it is not their size that makes them "bulk." Rather, it is the (larger) proportion of extra data beyond currently known targets that defines them."*

[26] Høringsnotatet, s. 284. Med «personselektor» siktes det til «*identifikator knyttet til en bestemt person eller virksomhet, for eksempel et telefonnummer, en epostadresse eller et brukernavn på en gitt tjeneste*», mens «modusselektor» sikter til

innhentingsmetoden innenfor «tilrettelagt innhenting» er innhenting og lagring av innholdsdata. Lagring av innholdsdata skiller seg fra bulkinnsamling, ved at innhentingen av data skjer målrettet mot aktører identifisert som etterretningsmål.[27]

Et særtrekk som skiller «tilrettelagt innhenting» fra andre former for bulkinnhenting og målrettet innhenting, er tilretteleggingsplikten som er foreslått ilagt kommersielle teletilbydere.[28] Kjernen i denne tilretteleggingsplikten er et pålegg om å tilgjengeliggjøre kommunikasjonsstrømmene for E-tjenesten, ved å tilrettelegge for installering og medvirke til drift av overvåkningsutstyr på fiberkabler i tilbyderens lokaler, samt levere datastrømmer uten linkkryptering eller lignende kryptering.[29]

2.2 Nærmere om målsøking og målrettet innhenting

Videre har Forsvarsdepartementet i sitt lovforslag kategorisert de nevnte innhentingsaktiviteter som henholdsvis målsøking og målrettet innhenting.[30] Målsøking er etter lovforslaget § 1-4 nr. 9 definert som «systematisk arbeid for å identifisere nye etterretningsmål», og går gjerne ut på å kartlegge nettverk og identifisere hittil ukjente og nye trusselaktører.[31] Dette gjennomføres ved søk i datagrunnlaget, basert på søkekriterier i form av modus- eller personselektorer.[32] For å iverksette målsøking må det etter lovforslaget foreligge «grunn til å undersøke» om det kan frembringes informasjon av relevans for etterretningsformål.[33]

Kategorien målrettet innhenting omfatter etter lovforslagets § 1-4 nr. 8 «systematisk arbeid for å finne informasjon knyttet til identifiserte etterretningsmål».[34] Formålet med målrettet innhenting er å finne mest mulig informasjon om indentifiserte etterretningsmål, herunder om intensjoner, aktiviteter og nettverk.[35] Dette utføres gjerne ved søk i

---

«*søkebegrep eller søkestreng som beskriver et bestemt mønster eller avgrensning, herunder handlingsmønster eller geografisk område*». Definisjon hentet fra høringsnotatet punkt 18, *Forslag til lovtekst,* s. 379.

[27] Høringsnotatet, punkt 11.14.7, s. 287

[28] Høringsnotatet, punkt 11.3, s. 187.

[29] Høringsnotatet, punkt 11.15.3, s. 289.

[30] Høringsnotatet, s. 379.

[31] Høringsnotatet, s. 149-150.

[32] Høringsnotatet, s. 149-150.

[33] Høringsnotatet, s. 382.

[34] Høringsnotatet, s. 379.

[35] Høringsnotatet, s. 149.

datagrunnlag eller innhenting basert særlig på personselektorer, men også tidvis modusselektorer.[36] Terskelen for å foreta målrettet innhenting er imidlertid høyere enn for målsøkingsaktivitet, da det må foreligge «konkrete holdepunkter for at det er grunn til å undersøke» jf. lovforslagets § 5-2.[37] Det må presiseres at termen målrettet innhenting i det følgende nyttes både om Forsvarsdepartementets innhentingskategori, og om det som av EMD er betegnet som «targeted interception», da det forutsettes et visst sammenfall mellom disse.

2.3 Nærmere om rekkevidden av tilrettelagt innhenting

Tilrettelagt innhenting omfatter utelukkende innhenting av grenseoverskridende kommunikasjon, og er følgelig begrenset til datastrømmer som passerer landegrensene i fiberoptiske kabler.[38] Denne territorielle begrensningen hindrer etterretningstjenesten å benytte tiltaket til innhenting av kommunikasjonsdata som overføres i signalsystemer internt i Norge.[39] Videre vil den foreslåtte utformingen av informasjonstilgangen avgrenses mot data lagret på nett, da dette er lagrede data som ikke er i transitt i et system for signaltransport.[40]

På den annen side er det en realitet at store mengder kommunikasjon mellom norske parter passerer landegrensen i fiberoptiske kabler, ettersom datatrafikken fra de fleste globale kommunikasjonstjenester på nett går via servere i utlandet.[41] Dette gjelder kommunikasjonstjenester som Facebook, Instagram, Whatsapp og Gmail. Dette vil medføre at vesentlige mengder ren norsk kommunikasjon "følger med på lasset" ved bulkinnsamling av metadata.

For å begrense mengden ren norsk kommunikasjon som innhentes, er det foreslått iverksatt filtreringsmekanismer før metadata kan lagres. Filtreringsmekanismene skal sortere bort det som er mulig basert på nasjons- eller geografibestemte identifikatorer, som telefonnummer

[36] Høringsnotatet, s. 149-150.
[37] Høringsnotat – Forslag til ny lov om etterretningstjenesten, s. 382.
[38] Høringsnotat – Forslag til ny lov om etterretningstjenesten, punkt 11.14.2, s. 277.
[39] Høringsnotat – Forslag til ny lov om etterretningstjenesten, punkt 11.14.2, s. 277.
[40] Høringsnotat – Forslag til ny lov om etterretningstjenesten, punkt 11.14.2, s. 277.
[41] Lysne II-utvalget (2016), *Digitalt grenseforsvar,* s. 48-49.

ol.[42] Det er imidlertid en rekke identifikatorer som ikke er nasjonsspesifikke, og filtreringsmekanismene vil dermed ikke kunne avgjøre kommunikasjonens opprinnelsessted.[43] Dette gjelder blant annet for IP-adresser. Ved bulkinnsamling av metadata vil det dermed følge med betydelige mengder kommunikasjon som foregår internt i Norge, selv etter filtrering. Mesteparten av denne kommunikasjonen er såkalt overskuddsinformasjon, som ikke har selvstendig relevans for etterretningsmål.

Bulkinnsamling innebærer følgelig at det vil lagres betydelige mengder metadata om norske personer. Etter Forsvarsdepartementets vurdering vil innhenting av innholdsdata være mer inngripende overfor enkeltindividet, da dette gir innsyn i hva vedkommende kommuniserer.[44] Også innhenting av metadata vil kunne gi et betydelig innsyn i privat kommunikasjon og opplysninger. Metadata kan avsløre hvem man kommuniserer med, tidspunkt og varighet av kommunikasjon med andre, internettsider man besøker, informasjon om meldinger og e-poster sendt via internett, herunder tidspunkt, adresse og vedlegg, og geografiske data som lokalisering og bevegelser (dette gjelder særlig i relasjon til telekommunikasjon, men også elektronisk kommunikasjon).[45] Det er med andre ord betydelige mengder personopplysninger som kan leses ut av metadata.

En sentral bemerkning i den forbindelse, er at Forsvarsdepartementet foreslår en adgang til å foreta innhenting av metadata to ledd ut i kommunikasjonskjeden ved søk basert på personselektorer.[46] Med andre ord vil E-tjenesten med utgangspunkt i søk på en identifisert aktør innhente metadata om dennes kontakters kommunikasjon og forbindelser, og deretter metadata om disse forbindelsers kommunikasjon. I en studie ført ved Stanford i 2016 ble det indikert at man ved søk basert på personselektor(telefonnummer) to ledd ut i kommunikasjonskjeden, kunne få tilgang til metadata om telefonkommunikasjon til nærmere 25 000 personer.[47] Selv om det ikke kan fastslås med sikkerhet hvilket omfang metadata som kan innhentes, illustrer det at tilrettelagt innhenting vil gi tilgang til metadata

[42] Høringsnotat – Forslag til ny lov om etterretningstjenesten, punkt 11.13.8 s. 274.
[43] Høringsnotat – Forslag til ny lov om etterretningstjenesten, punkt 11.13.8 s. 274.
[44] Høringsnotat – Forslag til ny lov om etterretningstjenesten, s. 199.
[45] Tzanou (2013), *Is Data Protection the same as Privacy? An Analysis of Telecommunications Metadata Retention Measures,* s. 28.
[46] Høringsnotat – Forslag til ny lov om etterretningstjenesten, s. 285.
[47] Mayer, Mutchler, Mitchell (2016), *Evaluating the privacy properties of telephone metadata*, s. 3.

om et stort antall mennesker. Dette befestes av at teletilbydere som leverer metadataene er foreslått ilagt en potensielt utstrakt plikt til dekryptering av dataene.

2.3.3 Innhentingsforbudet som begrensning av tilrettelagt innhenting

I lovforslagets § 4-1 første og andre ledd er det foreslått nedfelt et forbud mot å «rette innhenting» mot en person eller virksomhet som oppholder seg i Norge.[48] Etter Forsvarsdepartementets vurdering skal kriteriet «å rette innhenting» forstås som et forbud mot innhenting med overvåkningshensikt overfor norske fysiske og juridiske personer.[49] Dette innebærer i praksis at E-tjenesten ikke skal kunne utføre målrettet innhenting mot norske personer.

Unntak fra dette innhentingsforbudet er inntatt i lovforslagets § 4-2. Departementet foreslår her å gjøre unntak for søk i metadata basert på personselektor, dersom «søket ikke er rettet mot denne personen» og har eller kan få «vesentlig betydning» for etterretningsformål.[50] Også her skal vilkåret «rettet mot» forstås å måtte innebære en overvåkningshensikt overfor den innhentingen utføres mot.[51] Departementet legger videre til grunn at søk med utgangspunkt i personselektorer tilknyttet norske personer ikke vil anses å ha overvåkningshensikt, dersom det gjøres for å undersøke om vedkommende har kommunisert med utenlandske mål av interesse.[52] Etter departementet vurdering vil søkeaktivitet med denne hensikt kategoriseres som målsøking og ikke målrettet innhenting, selv om det benyttes personselektorer tilknyttet nordmenn. Ettersom lovforslaget opererer med lavere terskel for å iverksette målsøking enn målrettet innhenting, vil dette kunne medføre at det faktisk kan gjennomføres søk mot egne borgere med utgangspunkt i en videre hjemmel for innhenting.[53] Dette reiser en problemstilling tilknyttet rekkevidden av tilrettelagt innhenting, som vil behandles nærmere under kapittel 4.2 om lovkravet.

[48] Høringsnotat – Forslag til ny lov om etterretningstjenesten, s. 381.
[49] Høringsnotat – Forslag til ny lov om etterretningstjenesten, s. 125.
[50] Høringsnotat – Forslag til ny lov om etterretningstjenesten, s. 382.
[51] Høringsnotat – Forslag til ny lov om etterretningstjenesten, s. 139.
[52] Høringsnotat – Forslag til ny lov om etterretningstjenesten, s. 139.
[53] Lignende synspunkter er fremhevet av NIM (2019) i *Høringsuttalelse om forslag til ny lov om Etterretningstjenesten*, s. 22. Hvilke implikasjoner dette kan få, er gjenstand for nærmere vurdering under kapittel 4.

Kapittel 3: Retten til privatliv i Grunnloven og EMK

3.1 Retten til privatliv etter Grl. § 102

Retten til privatliv ble etter Grunnlovsrevisjonen i 2014 nedfelt i Grunnloven § 102, som slår fast at «enhver har rett til respekt for sitt privatliv».[54] Av forarbeidene til revisjonen fremgår det at bestemmelsen er ment å omfatte «privatlivets fred, personvern og personopplysningsvern».[55] Personopplysningsvern omhandler en persons rett til vern mot «bruk og spredning av informasjon om seg selv», som omfatter beskyttelse mot innsyn i sensitiv og privat informasjon.[56]

En særskilt inngrepsadgang fremkommer ikke uttrykkelig av ordlyden i Grl. § 102. Adgangen til å på nærmere bestemte vilkår foreta et inngrep i individets rett til privatliv, har imidlertid blitt innfortolket i Grl. § 102 av Høyesterett. I Rt. 2014 s. 1105 innfortolket Høyesterett en begrensningsadgang etter mønster fra EMK art. 8.[57] Høyesterett la til grunn at hvorvidt en lov som griper inn i privatlivet er forenelig med Grl. § 102, «beror på om loven ivaretar et legitimt formål og er forholdsmessig».[58] Blant de formål som er tiltenkt legitime etter § 102, nevnes «rikets sikkerhet» eksplisitt i forarbeidene til grunnlovsrevisjonen.[59] I HR-2018-104-A er det lagt til grunn at forholdsmessighetskravet etter Grl. § 102 innebærer at «tiltaket må i det konkrete tilfellet være egnet, nødvendig og forholdsmessig» i et demokratisk samfunn.[60]

I forarbeidene til Grl. § 102 er det understreket at den nærmere vurderingen av hvor langt grunnlovsvernet om privatliv strekker seg, «vil måtte forstås i lys av og suppleres med det internasjonale konvensjonsvernet».[61]

3.2 Retten til privatliv etter EMK art. 8

[54] Grunnloven § 102.
[55] Dok.nr.16 (2011–2012), s. 177.
[56] Dok.nr.16 (2011–2012), s. 172-173.
[57] Rt. 2014 s. 1105, avsnitt 28.
[58] Rt. 2014 s. 1105, avsnitt 28.
[59] Dok.nr.16 (2011–2012), s. 178.
[60] HR-2018-104-A, avsnitt 23.
[61] Dok.nr.16 (2011–2012), s. 175.

Den sentrale internasjonale bestemmelse om rett til privatliv i norsk rett, er EMK art. 8.[62] Bestemmelsen slår fast at «everyone has the right to respect for his private [...] life».[63] EMD har regelmessig lagt til grunn at bestemmelsen omfatter enkeltindividets rett til vern mot innhenting, bruk og oppbevaring av personopplysninger og kommunikasjon mot dennes vilje.[64] Etter bestemmelsens andre ledd er det adgang til å gjøre inngrep i retten til privatliv, såfremt det er «in accordance with the law» og er «necessary in a democratic society in the interests of national security[…]». [65]

Disse kravene er videre utpenslet i flere dommer fra EMD som omhandler overvåkningstiltak. Av betydning for adgangen til målrettet innhenting er særlig *Szabo og Vissy mot Ungarn.* Videre vil avgjørelsene i *Centrum för Rättvisa mot Sverige* og *Big Brother Watch mot Storbritannia* være av særlig betydning for kravene ved bulkinnsamling. De to sistnevnte dommene er imidlertid påanket til behandling i EMDs storkammer, og er følgelig ikke rettskraftige på dette tidspunkt. Det er derfor mulig at de rettslige utgangspunkt og retningslinjer utpenslet i den relevante praksis, vil danne et annet bilde i fremtiden. Med dette forbehold vil det likevel tas utgangspunkt i de retningslinjer og krav som foreligger etter EMDs praksis på dette tidspunkt.

3.3 Forholdet mellom Grunnloven § 102 og EMK art. 8

Til tross for at de to bestemmelsene har en noe forskjelligartet utforming og rang, har Grl. § 102 i betydelig grad blitt tolket i lys av den parallelle bestemmelsen i EMK art. 8. De sentrale eksempel på dette er nok Rt. 2014 s. 1105 og HR-2018-104-A, hvor Høyesterett innfortolket en inngrepsadgang i Grl. § 102 etter mønster av EMK art. 8.[66]

I den forbindelse er det et sentralt poeng at konvensjonsrettighetene er ansett å etablere et minimumsvern, og at de dermed ikke skal benyttes til å tolke nasjonale rettigheter snevrere.[67] Dette minimumsvernet bør følgelig ivaretas ved tolkningen av Grunnloven, noe

[62] Jamfør inkorporeringen etter menneskerettighetsloven §§ 2 og 3. Se også Strand og Larsen (2016), *Menneskerettigheter i et nøtteskall,* s. 89 og 96-96 om EMKs betydning og EMD-avgjørelsers rettslige bindende virkning.
[63] EMK artikkel 8 (1) jf. menneskerettighetsloven § 2.
[64] [*Leander v. Sweden*, avsnitt 48] og [*Klass and others vs. Germany*, avsnitt 41].
[65] EMK artikkel 8 (2) jf. menneskerettighetsloven § 2.
[66] [Rt. 2014 s. 1105, avsnitt 28-30] og [HR-2018-104-A, avsnitt 23].
[67] Dok.nr.16 (2011–2012), s. 87.

som også ble understreket Lønningsutvalget.[68] På denne bakgrunn ble det lagt til grunn at «Grunnlovens menneskerettighetsbestemmelser i fremtiden må tolkes i lys av de internasjonale menneskerettighetskonvensjonene og praksis knyttet til disse».[69] Ettersom Høyesterett enda har til gode å behandle saker om implementering av digitale innhentingstiltak, er det imidlertid naturlig å se hen til EMK art. 8 og EMDs praksis tilknyttet denne bestemmelse.

Kapittel 4: Tilrettelagt innhenting og retten til privatliv

4.1 Inngrep i retten til privatliv

EMD har gjennomgående lagt til grunn at «the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures» kan utgjøre et inngrep i retten til privatliv.[70] Dette er begrunnet i at lovgivning som tillater hemmelig overvåkning innebærer «a threat of surveillance for all those to whom the legislation may be applied».[71] Dette gjelder særlig bulkinnsamling, hvor enhver person potensielt kan få sin kommunikasjon innsamlet og lagret (om enn utilsiktet), uten å bli informert.[72] Det vil uansett utgjøre et inngrep i privatlivet for den som har fått sin kommunikasjon innhentet og lagret ved bulkinnsamling eller målrettet innhenting.[73]

4.2 Lovkravet

4.2.1 Lovkravets innhold

Det er fast forankret i EMDs praksis at ordlyden «in accordance with the law», innebærer at overvåkningstiltak må ha hjemmel «in domestic law», og være forenelig med «the rule of law».[74] I dette ligger det at det må foreligge lovgivning som er «accessible» og «forseeable» for de som kan bli berørt av overvåkningstiltak.[75] Det stilles således både et krav om

---

[68] Dok.nr.16 (2011–2012), s. 89.
[69] Dok.nr.16 (2011–2012), s. 89.
[70] [*Centrum för Rättvisa v. Sweden,* avsnitt 90] og [*Big Brother Watch and others vs. The United Kingdom*, avsnitt 392].
[71] *Weber and Saravia v. Germany,* avsnitt 78.
[72] Se kapittel 2.3.
[73] *Rotaru v. Romania,* avsnitt 46.
[74][*Weber and Saravia v. Germany,* avsnitt 84]; [*Roman Zakharov v. Russia*, avsnitt 228]; [*Centrum för Rättvisa v. Sweden,* avsnitt 100]; [*Big Brother Watch and others vs. The United Kingdom*, avsnitt 305].
[75] *Big Brother Watch and others vs. The United Kingdom,* avsnitt 305.

hjemmel i formell lov, og visse materielle innholdskrav til lovgivning som autoriserer innhenting av elektronisk kommunikasjonsdata.

I relasjon til kravet om tilstrekkelig forutsigbarhet i lovgivningen, understreket Domstolen i Big Brother Watch mot Storbritannia at kravet må sees i kontekst av at det er tale om skjulte overvåkningstiltak.[76] Dette medfører at forutsigbarhetskravet ikke kan innebære at "an individual should be able to foresee when the authorities are likely to resort to such measures **so that he can adapt his conduct accordingly**».[77] På den annen side er faren for vilkårlighet til stede ved bruk av skjulte tiltak, og EMD har følgelig understreket at lovgivningen likevel må være «sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures»[78]. I vurderingen må det følgelig tas høyde for at lovreguleringen må være tilstrekkelig klar til å minimere risikoen for maktmisbruk, uten å gå på bekostning av skjermingsbehovet for enkelte områder av utenlandsetterretningen.[79]

EMD har derav utviklet seks minimumskriterier som må være oppfylt for at lovgivningen kan anses tilstrekkelig forutsigbar.[80] Etter dette må lovgivningen klargjøre; karakteren av de forhold som kan føre til en beslutning om innhenting, hvilke kategorier mennesker som er ventet å bli rammet av innhenting, begrensninger på overvåkningens varighet, prosedyrene for analyse, bruk og lagring av tilegnede data, sikkerhetstiltak ved deling av informasjon med andre statsorganer, samt under hvilke omstendigheter innhentede data kan eller må slettes.[81] De nevnte kriteriene gjelder både for bulkinnhenting og målrettet innhenting av kommunikasjon.[82] Videre ble det i Roman Zakharov mot Russland lagt til grunn av Domstolen at minimumskriteriene også gjelder for innhenting begrunnet i nasjonal sikkerhet, noe som ble bekreftet i Big Brother Watch mot Storbritannia.[83]

---

[76] *Big Brother Watch and others vs. The United Kingdom,* avsnitt 306.
[77] *Big Brother Watch and others vs. The United Kingdom,* avsnitt 306. (Forfatters utheving).
[78] *Big Brother Watch and others vs. The United Kingdom,* avsnitt 306.
[79] *Big Brother Watch and others vs. The United Kingdom,* avsnitt 307 og 315.
[80] [*Centrum för Rättvisa v. Sweden,* avsnitt 103] og [*Big Brother Watch and others vs. The United Kingdom*, avsnitt 307].
[81] [*Roman Zakharov v. Russia*, avsnitt 238]; [*Centrum för Rättvisa v. Sweden,* avsnitt 103]; [*Big Brother Watch and others vs. The United Kingdom*, avsnitt 307].
[82] *Big Brother Watch and others vs. The United Kingdom*, avsnitt 315.
[83] [*Roman Zakharov v. Russia*, avsnitt 238] og [*Big Brother Watch and others vs. The United Kingdom*, avsnitt 307].

De seks kriteriene danner dermed utgangspunktet for vurderingen av hvorvidt lovreguleringen av tilrettelagt innhenting vil være tilstrekkelig tilgjengelig og forutsigbar til å oppfylle det materielle lovkravet. I Big Brother Watch slo domstolen imidlertid fast at den nasjonale lovgivningen i tillegg må sikre at overvåkningstiltak kun benyttes når dette er «necessary in a democratic society».[84] EMD har derav gitt uttrykk for at vurderingen av hvorvidt lovreguleringen oppfyller de materielle kravene om tilgjengelighet og forutsigbarhet i loven, er nært forbundet med nødvendighets-testen.[85] Essensen i kvalitetskravene er følgelig at lovgivningen må være tilstrekkelig forutsigbar, men også etablere effektive garantier mot vilkårlighet og misbruk som er egnet til å holde utøvelsen innenfor forholdsmessighetsgrensen.[86] På denne bakgrunn ble vurderingen av henholdsvis lovkravet og nødvendighetskravet sammenføyd av domstolen i Big Brother Watch mot Storbritannia. For å ivareta oversiktligheten vil disse kravene imidlertid behandles separat i det følgende. Nødvendighetsbegrensningen vil derimot utgjøre et relevant moment i vurderingen av lovkravet, og motsatt, og vil behandles deretter.[87]

4.2.2 Tilrettelagt innhenting og kvalitetskravene til lovregulering

4.2.2.1 Rekkevidden av innhentingstiltakene

Hva gjelder de to første minimumskravene, har domstolen gitt uttrykk for at de vil anses oppfylt dersom nasjonal lovgivning klargjør rekkevidden av de aktuelle innhentingstiltakenes anvendelse, på en måte som gir borgerne "an **adequate indication as to the cirumstances** in which public authorities are empowered to resort to such measures".[88] Lovgivningen må altså gi en tilstrekkelig indikasjon på hvilke omstendigheter som må foreligge for at innhentingsmetodene kan benyttes, og hvem som kan bli rammet av dem. Det er derfor sentralt at vilkårene for å iverksette et overvåkningstiltak fremgår av regelverket.

---

[84] *Big Brother Watch and others vs. The United Kingdom*, avsnitt 322.
[85] *Big Brother Watch and others vs. The United Kingdom*, avsnitt 322.
[86] *Centrum för Rättvisa v. Sweden,* avsnitt 107: "*The "quality of law" in this sense implies that the domestic law must not only be accessible and foreseeable in its application, but 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**".*
[87] *Big Brother Watch and others vs. The United Kingdom*, avsnitt 322.
[88] *Roman Zakharov v. Russia*, avsnitt 243] og [*Big Brother Watch and others vs. The United Kingdom*, avsnitt 328]. (Forfatters utheving).

I den sammenheng er det grunnleggende at regelverket angir hvilke formål en ordning som tilrettelagt innhenting kan benyttes til. I lovforslagets kapittel 3 er det angitt en rekke generelle etterretningsformål som innhenting kan iverksettes med bakgrunn i, herunder avdekking og motvirkning av; «trusler mot Norges sikkerhet» og «grenseoverskridende terrorisme».[89] At etterretningsformålene angis generelt, er ikke nødvendigvis uforenelig med kravet til forutsigbarhet. I Centrum för Rättvisa godtok EMD at formål angis generelt i regelverket, med det forbehold om at formålene likevel utdypes i eksempelvis lovforarbeider.[90] Dette ble godtatt fordi lovforarbeider er en sentral rettskilde i svensk rett.[91] Dette synspunkt er overførbart til norsk rett, hvor lovforarbeider også utgjør en sentral rettskilde.[92] Det vil dermed kunne være tilstrekkelig forutsigbart, dersom formålene for innhenting gis en nærmere utdyping i lovforarbeider som eventuelt utarbeides i en lovgivningsprosess.

Videre er det sentralt at grunnvilkårene for innhenting utformes med tilstrekkelig klarhet om når innhenting kan iverksettes. I lovforslaget er disse grunnvilkårene inntatt i kapittel 5. Etter den foreslåtte utforming kreves det «grunn til å undersøke» om det kan frembringes relevant informasjon, for å iverksette innhenting av data i form av målsøking.[93] Dertil kreves det «konkrete holdepunkter» som tilsier at det er «grunn til å undersøke», for å iverksette målrettet innhenting.[94] Med forbehold om at grunnvilkårenes endelige utforming vil kunne endres, er det likevel grunn til å bemerke vilkårenes vage og vidtrekkende formulering. Med utgangspunkt i forutberegnelighetskravet, må vilkårene være så presist angitt at det gir en «adequate indication» av innhentingsadgangen.[95] Klare legislative rammer for når innhenting kan iverksettes er sentralt for å hindre at adgangen kan anvendes uforholdsmessig eller vilkårlig, og er følgelig en betydningsfull rettssikkerhetsmekanisme.

Selv om det ikke er grunn til å anta at etterretningstjenestens innhenting faktisk vil anvendes vilkårlig, vil denne uklarheten rundt hvilken form for innhenting man kan bli rammet av, og under hvilke omstendigheter, være egnet til at innhentingsaktiviteten kan fremstå vilkårlig

[89] Høringsnotat – Forslag til ny lov om etterretningstjenesten, s. 380-381.
[90] *Centrum för Rättvisa v. Sweden,* avsnitt 120.
[91] *Centrum för Rättvisa v. Sweden,* avsnitt 120.
[92] Blandhol, Tøssebro og Skotheim (2015), s. 323.
[93] Høringsnotat – Forslag til ny lov om etterretningstjenesten, s. 382.
[94] Høringsnotat – Forslag til ny lov om etterretningstjenesten, s. 382.
[95] *Big Brother Watch and others vs. The United Kingdom*, avsnitt 328.

for den gjense borger. Misbrukspotensialet er iboende innhentingsadgangen, og det vil da være særlig viktig med både forutberegnelighet for borgerne, og effektive garantier i form av kontroll med e-tjenestens beslutninger.[96] Uklarheten vil imidlertid også kunne påvirke domstolenes prøving av hvorvidt vilkår for innhenting er oppfylt, all den tid det kan spørres om domstolen vil inneha den tekniske og etterretningsfaglige innsikt som er nødvendig for å vurdere når de ulike innhentingshjemler vil være oppfylt. Dette poeng vil behandles nærmere under kapittel 4.4 om forholdsmessighetskravet.

Av innhentingsforbudet i § 4-1, fremgår det at målrettet innhenting ikke skal foretas mot norske personer. I kapittel 2.3 ble det likevel belyst at store mengder rene norske kommunikasjonsdata vil innhentes ved bulkinnsamling. Dette fremgår imidlertid ikke tydelig av den foreslåtte lovregulering, noe som gjør det vanskelig å forutberegne det reelle omfanget av mulig berørte personer. Videre er det foreslått adgang til å foreta søk mot norske personer, såfremt søket ikke har overvåkningshensikt. Dette kan vanskelig leses ut av formuleringen «rettet mot» norske personer.[97] Den innhentingsbegrensning Forsvarsdepartementet legger opp til, fremgår således ikke tydelig av den foreslåtte regulering. Dette er betenkelig i relasjon til borgernes tillit til myndighetsutøvelsen.

4.2.2.2 Varigheten av innhentingstiltakene

Videre er det et minimumskriterium at lovgivningen angir begrensninger på innhentingens varighet. En tidsbegrensning er sentralt for at oppbevaringen og bruken av personopplysninger ikke strekkes ut i tid. Dette minimumskriteriet henger sammen med at regelverket må sikre at innhentingsvirksomheten ikke skal gå lenger enn det som er nødvendig for å ivareta etterretningsformålet.[98] Det er følgelig sentralt at det fastsettes begrensninger for varighet av innhenting, lagring og bruk av kommunikasjonsdata. Etter forsvarsdepartementets foreslåtte regulering av metadatalagring i § 7-7, er den øvre grensen for lagring av metadata satt til 18 måneder.[99] I og med at metadatalageret vil inneholde mye irrelevante data om norsk kommunikasjon, vil

---

[96] Det ble fremhevet av EMD i *Big Brother Watch and others vs. The United Kingdom* at; "*regard must be had to the actual operation of the system of interception,* ***including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse***", avsnitt 320. (Forfatters utheving).

[97] Høringsnotat – Forslag til ny lov om etterretningstjenesten, s. 139.

[98] Se kapittel 4.2.1 om lovkravets innhold.

[99] Høringsnotat – Forslag til ny lov om etterretningstjenesten, s. 283-284.

forholdsmessighetsbegrensningen nødvendiggjøre at lagrede metada slettes så snart det blir klart at det er tale om irrelevante data, eller dersom formålet for innhentingen ikke lenger er til stede. Dette punkt vil behandles nærmere nedenfor.

4.2.2.3 Gjennomføringen av innhentingstiltakene

Det stilles videre visse krav til å regulere gjennomføringen av lagring, bruk, deling og sletting av innhentede eller tilgjengelige data.[100] At regelverket legger opp til klare og etterprøvbare prosedyrer for bl.a. innhenting, deling og sletting, er sentralt for å sikre en forutsigbar og legitim etterlevelse av innhentingsregimet, som er i tråd med konstitusjons- og konvensjonsforpliktelser.

For det første er det nødvendig å klargjøre i hvilken utstrekning det kan innhentes data i medhold av en tilretteleggingsplikt. Et sentralt poeng er at selve innhentingen fra kommunikasjonslinker og den etterfølgende lagringen i seg selv utgjør et inngrep overfor den som har fått sine data innhentet.[101] Det er derfor viktig at omfanget av data som innhentes begrenses til det som er nødvendig for å ivareta nasjonal sikkerhet. Det har også betydning for hvilke kommunikasjonsbærere og -tjenester som skulle være omfattet av en plikt til dekryptering. Dette er viktig både for borgernes anledning til å overskue hvilket omfang av data som er foreslått adgang til å innhente, samt for kontrollmulighetene med den innhenting som foretas. Samtidig er det vesentlig at regelverket ikke er forutsigbart i den utstrekning at potensielle etterretningsmål kan innrette seg deretter. Det må følgelig aksepteres et visst hemmelighold av hvilke kommunikasjonsbærere og tjenester det innhentes fra. Det sentrale blir dermed at det oppstilles tydelige formåls- og forholdsmessighetsbegrensninger for selve innhentingen, og tilstrekkelige mekanismer til å etterleve disse begrensninger.

I forlengelsen av dette er det viktig at det inntas reguleringer egnet til å begrense lagringen av data som er irrelevante for etterretningsformål. Det foreslåtte regelverket legger opp til en automatisert filtrering av innhentede metadata, før de kan lagres og oppbevares i E-

[100] Se punkt 4.2.1 om lovkravets innhold.
[101] *Rotaru v. Romania,* avsnitt 45-46. Dette poeng er også understreket av: NIM (2019), *Høringsuttalelse om forslag til ny lov om Etterretningstjenesten*, s. 14 og 23.

tjenestens dataservere.[102] Denne filtreringen er essensiell for å begrense omfanget av ren norsk kommunikasjon som "følger med på lasset" ved innsamlingen, og således ivareta innhentingsbegrensningen og forholdsmessighetskravet så langt som praktisk mulig. Filtreringsmekanismene vil likevel ha sine begrensninger, da de vanskelig kan sortere ut data hvor opprinnelsessted ikke er identifiserbart.[103] For å motvirke at lagrede data kan misbrukes eller benyttes ut over det som er nødvendig, blir det dermed sentralt å fastsette tydelige rammer for søk, deling og sletting av data.

Etterretningstjenestens oppgave er å utarbeide etterretningsanalyser, og kommunikasjonsdata vil dermed brukes til å finne relevant informasjon og sammenstille disse analysene. Etter lovforslaget fremgår det at tilgangen til metadatalageret for å foreta søk, skal legges til opplært personell «i henhold til søkeprivilegier som er tilpasset dennes oppdragsportefølje».[104] En slik begrensning i tilgangen til datalageret og søkeaktivitet er sentralt for å hindre at datagrunnlaget kan misbrukes. Videre skal søkene som utføres «baseres på personselektorer eller modusselektorer».[105] Det fremgår likevel ikke hvor spesifiserte søkekriteriene som kan benyttes må være. Også her er det imidlertid et viktig poeng at regelverket ikke kan inneholde et detaljnivå som går på bekostning av behovet for hemmelighold. Desto viktigere blir da kontrollen med E-tjenestens søkeaktivitet som en garanti mot misbruk.[106]

Videre ligger det i utenlandsetterretningens formål at det vil bli nødvendig å dele informasjon og etterretningsanalyser med tredjeparter, og da særlig nasjonale myndigheter som E-tjenesten handler på oppdrag for.[107] All den tid utlevering av informasjon til tredjeparter kan utgjøre et selvstendig inngrep overfor den informasjonen gjelder, har EMD understreket at skjønnsadgangen til utlevering ikke bør angis for vidt.[108] En vid adgang til utlevering vil også kunne påvirke hvorvidt bruken av kommunikasjonsdata holdes innenfor

[102] Høringsnotat – Forslag til ny lov om etterretningstjenesten, s. 278-280.
[103] Se kapittel 2.3.2.
[104] Høringsnotat – Forslag til ny lov om etterretningstjenesten, s. 286.
[105] Jf. Lovforslagets § 7-8; Høringsnotatet, s. 386.
[106] Behovet for kontroll med myndighetenes bruk av søkekriterier er også understreket i *Big Brother Watch and others vs. The United Kingdom*, avsnitt 340: *"the search criteria and selectors used to filter intercepted communications should be subject to independent oversight".*
[107] Høringsnotat – Forslag til ny lov om etterretningstjenesten, s. 337-338.
[108] *Centrum för Rättvisa v. Sweden,* avsnitt 150.

rammene av formålsbegrensningen. Sentralt i så måte er det at lovreguleringen tydelig angir for hvilke «etterretningsformål» utlevering kan finne sted, for å hindre formålsutglidning.[109]

Etter lovforslaget følger det videre at innhentende personopplysninger skal slettes når de ikke lenger er nødvendig.[110] Dette kavet til sletting når formålet ikke lenger foreligger eller den øvre grensen er nådd, er et naturlig utslag av forholdsmessighetskravet som stilles til lovgivning som autoriserer overvåkningstiltak.[111] Etter lovforslagets § 1-4 nr. 11 er personopplysninger definert som «enhver opplysning og vurdering som med enkle midler kan knyttes til en identifisert eller identifiserbar fysisk person». Dette vil innebære at kun opplysninger som med enkle midler kan knyttes til en identifiserbar person, vil slettes etter bestemmelsen. Det er usikkert hva som vil kreves for at eksempelvis metadata om kommunikasjon med enkle midler kan knyttes til en person. Det er følgelig uklart hva som skal til for at ulike kommunikasjonsdata vil bli omfattet av sletteplikten. I lys av at kravet om sletting er en sentral komponent for å holde innhenting og lagring innenfor grensene av det som er forholdsmessig, vil denne uklarheten

4.3 Formålskravet

4.3.1 Formålskravets innhold

I Høyesterettspraksis er det slått fast at inngrep i Grl. § 102 må ivareta et legitimt formål. Tilsvarende formålsbegrensning finnes i EMK art. 8, hvor "national security" er eksplisitt angitt som et av de legitime formål som kan begrunne et inngrep. Det er anerkjent at grenseoverskridende terrorisme utgjør en alvorlig trussel mot samfunnssikkerheten, og således faller innenfor formålet om å ivareta nasjonal sikkerhet.[112]

Hvilket formål som angis for et innhentingsregime er av sentral betydning, da dette formålet fungerer som den saklige rammen for hvilke argumenter som kan begrunne innføring av en ordning som tilrettelagt innhenting.[113] Dette ble illustrert i utvisningssaken i C.G mot Bulgaria, hvor EMD la til grunn at utvisning som følge av narkotikakriminalitet ikke kan

[109] Se lovforslagets § 10-5, s. 391.
[110] Lovforslagets § 9-9, s. 319.
[111] Rt. 2014 s. 1105, avsnitt 28.
[112] [*Big Brother Watch and others vs. The United Kingdom*]
[113] Bertelsen, *EMK. Kommentarer til bestemmelsene om individets rettigheter og friheter* (2011), s. 267.

begrunnes i nasjonale sikkerhetsinteresser. Med henblikk på det naturlige meningsinnhold i «national security», ble det uttalt at narkotikakriminalitet ikke kunne utgjøre en trussel mot nasjonal sikkerhet som sådan.[114] Det må følgelig trekkes en grense mot kriminalitet som ikke truer nasjonal sikkerhet. Ren kriminalitetsbekjempelse vil da ikke kunne begrunne E-tjenestens innhentingstiltak, da dette ville innebære en formålsutglidning som vil være uforenelig med innhentingens begrunnelse. Formålsangivelsen for E-tjenestens innhentingstiltak blir derav viktig for å avgrense innhentingsadgangen til det som er i tråd med «the legitimate aim pursued». [115]

Kravet om formålsmessighet gjelder også for den etterfølgende bruken av innhentet informasjon.[116] I så måte er det sentralt at lagring, søk, analyse og deling av informasjon også er begrunnet i vern av den nasjonale sikkerhet. Det er særlig ved videreformidling av informasjon til andre myndigheter at faren for etterfølgende bruk til andre formål enn nasjonale sikkerhetsinteresser vil kunne oppstå.[117] Det er likevel understreket av EMD at "the purpose of signals intelligence **naturally demands that it may be reported to concerned national authorities**».[118] Det vil følgelig anses som formålsmessig at informasjon formidles til relevante myndigheter, såfremt delingsadgangen ikke er angitt så vidt at det åpner for uforholdsmessig deling eller misbrukspotensiale.[119]

4.4 Forholdsmessighetskravet

4.4.1 Nødvendig i et demokratisk samfunn

Forholdsmessighetskravet fremkommer ikke eksplisitt av ordlyden i Grl. § 102. Det er likevel lagt til grunn i Høyesterettspraksis om Grl. § 102 at det gjelder en alminnelig forholdsmessighetsbegrensning også for lovhjemlede og legitimt begrunnede inngrep.[120] Dette forholdsmessighetskravet er også nedfelt i EMK art. 8 (2), som et krav om at inngrep må være «necessary in a democratic society» for å oppnå det angitte formål. Det sentrale

[114] *C.G and others v. Bulgaria*, avsnitt 43.
[115] *Centrum för Rättvisa v. Sweden,* avsnitt 119-120.
[116] *Centrum för Rättvisa v. Sweden,* avsnitt 144: *"personal data treated also has to be adequate and relevant* ***in relation to the purpose of the treatment****".*
[117] Høringsnotatet, s. 258-260.
[118] *Centrum för Rättvisa v. Sweden,* avsnitt 150.
[119] *Centrum för Rättvisa v. Sweden,* avsnitt 150.
[120] HR. 2014 s. 1105, avsnitt 28. Se kapittel 3.

formålet i denne forbindelse er nasjonal sikkerhet. En lovfesting av elektronisk kommunikasjonsinnhenting i etterretningsøyemed, må følgelig være nødvendig i et demokratisk samfunn for å ivareta nasjonal sikkerhet.

Dette nødvendighetskravet består av flere elementer. For at et tiltak som gjør inngrep i privatlivet skal anses nødvendig, må tiltaket være egnet til å ivareta det formål som saklig begrunner inngrepet.[121] Det må også påvises at det foreligger proporsjonalitet mellom det inngrep tiltaket utgjør og det formål det søker å oppnå.[122] I den forbindelse må det også tas hensyn til den skjønnsmargin som statene anerkjennes i overvåkningskontekst.

Et sentralt spørsmål er hvilken grad av nødvendighet som kreves for at et inngrep skal anses forholdsmessig. I Szabó og Vissy mot Ungarn la EMD til grunn et strengt nødvendighetskrav, under henvisning til domstolens tidligere avgjørelse i Klass mot Tyskland.[123] Domstolen la til grunn at skjult overvåkning av borgerne måtte være strengt nødvendig for å ivareta demokratiske institusjoner, dersom vilkåret skulle anses oppfylt.[124] Et slikt skjerpet krav til nødvendighet er imidlertid ikke fulgt opp i EMDs nyere avgjørelser om skjult overvåkning. I både Centrum för Rättvisa mot Sverige og Big Brother Watch mot Storbritannia ble det lagt til grunn at det var tilstrekkelig å påvise at innhentingstiltakene var nødvendig for å ivareta nasjonal sikkerhet.[125] Domstolen gir ikke noen nærmere begrunnelse for at den har lagt til grunn ulike terskler for skjulte overvåkningsregimer. Samtidig omhandlet både Szabó og Vissy mot Ungarn og Klass mot Tyskland mer eller mindre målrettede overvåkningstiltak. Derimot omhandlet både Centrum för Rättvisa og Big Brother Wacth mer generell bulkinnsamling. Det kan dermed tenkes at det skjerpede kravet ble stilt på bakgrunn av innhentingsmetoden som ble benyttet. I så måte vil det skjerpede nødvendighetskravet først og fremst få betydning ved målrettet innhenting.

4.4.2 Egnet for å oppnå formålet om nasjonal sikkerhet

Videre er det et krav om at tiltaket er egnet for å oppnå formålet om å ivareta nasjonal sikkerhet. Dette innebærer at tiltaket må være effektivt for å ivareta nasjonal sikkerhet,

---

[121] HR-2018-104-A, avsnitt 23.
[122] *Big Brother Watch and others vs. The United Kingdom*, avsnitt 384.
[123] *Szabó and Vissy vs. Hungary,* avsnitt 54.
[124] [*Szabó and Vissy vs. Hungary,* avsnitt 54] og [*Klass and others vs. Germany*, avsnitt 42].
[125] [*Centrum för Rättvisa v. Sweden,* avsnitt 104] og [*Big Brother Watch and others vs. The United Kingdom*, avsnitt 315].

herunder for å motvirke grenseoverskridende terrorisme. All den tid mye av E-tjenestens virksomhet er underlagt hemmelighold, vil det være vanskelig å bedømme den reelle effektiviteten av et innhentingsregime.[126]

Etterretningstjenestens arbeid går ut på å kartlegge og analysere utenlandske trusler mot rikets sikkerhet, som et ledd i utarbeidelsen av etterretningsanalyser som senere skal benyttes av myndighetene for å ivareta nasjonale sikkerhetsinteresser. Effektiviteten av tilrettelagt innhenting må således sees i lys av at tiltaket i seg selv ikke avverger trusler mot rikets sikkerhet, men utgjør en sentral komponent i myndighetenes avvergelse.[127] Selv om det på forhånd kan være vanskelig å bedømme hvor effektivt digital innhenting vil være for å avverge trusler mot samfunnssikkerheten, er det uomtvistet at tilrettelagt innhenting også vil tilgjengeliggjøre elektronisk informasjon om potensielle trusselaktører.[128] Således vil tiltaket ha en etterretningsmessig nytteverdi, som i lys av etterretningstjenestens oppgaver og formål også vil kunne nytte til å oppdage og motvirke trusler og således ivareta nasjonale sikkerhetsinteresser.

En alternativ mulighet vil være å innføre tilrettelagt innhenting der både metadata og innholdsdata innhentes mer eller mindre målrettet mot allerede kjente aktører. Forsvarsdepartementet har i lovforslaget betegnet dette som en «lettversjon».[129] Det sentrale karaktertrekk med denne innhentingsmodellen er at metadata vil innhentes ved positiv filtrering basert på kjente selektorer, fremfor innsamling i bulk.[130] En slik variant av tilrettelagt innhenting forutsetter at E-tjenesten allerede besitter informasjon om kjente og relevante aktører. Etter forsvarsdepartementets vurdering vil dette redusere nytteverdien av tilrettelagt innhenting – særlig i relasjon til kontraterrorformålet - ettersom det vil utelukke målsøkingsaktivitet som kan knytte terroraktørenes ulike digitale identiteter og terrornettverk sammen.[131] EMD har også anerkjent nytteverdien i bulkinnsamling av kommunikasjonsdata for sikkerhetsformål, ettersom bulkinnsamling gir muligheten til å treffe proaktive tiltak ved å søke etter og identifisere ukjente trusselaktører.[132] Det sentrale

[126] Likeledes; NIM (2019), *Høringsuttalelse om forslag til ny lov om Etterretningstjenesten*, s. 4.
[127] Høringsnotatet, s. 37.
[128] Dette er også lagt til grunn i høringsuttalelse fra NIM (2019), s. 4.
[129] Høringsnotatet, s. 197.
[130] Høringsnotatet, s. 197.
[131] Høringsnotatet, s. 198.
[132] [*Big Brother Watch and others vs. The United Kingdom*, avsnitt 384-386] og [*Centrum för Rättvisa v. Sweden,* avsnitt 179]

blir således hvorvidt den foreslåtte utforming av tilrettelagt innhenting kan sies å være forholdsmessig ut ifra nasjonale sikkerhetsinteresser.

4.4.3 Proporsjonalitet mellom tilrettelagt innhenting og formålet om terroravvergelse

Proporsjonalitetsvurderingen tar sikte på å balansere de konkurrerende interesser, som i overvåkningskontekst knytter seg til "the interest of the respondent State in **protecting its national security through secret surveillance measures against the seriousness of the interference** with an applicant's right to respect for his or her private life".[133]

4.4.4. Statens skjønnsmargin i overvåkningskontekst

Der staten iverksetter tiltak som gjør inngrep i borgernes menneskerettigheter, tilkjennes statene likevel en viss skjønnsmargin til å bedømme hvilke tiltak som er nødvendige i et demokratisk samfunn.[134] Denne skjønnsmarginen bunner i en betraktning om at statlige myndigheter selv er best egnet til å vurdere hvilke tiltak som er nødvendige for å oppnå de formål staten selv bedømmer vesentlige for nasjonen.[135] I forbindelse med innføring av skjulte overvåkningstiltak for å ivareta nasjonal sikkerhet, har EMD gitt uttrykk for at «national authorities enjoy a certain margin of appreciation in **choosing the means** for achieving the legitimate aim of protecting national security».[136] Dette gir statene en skjønnsmargin til å beslutte hvilken innhentingsform som er nødvendig å innføre for å ivareta nasjonal sikkerhet.

Samtidig understreket Domstolen i Big Brother Watch at «the discretion afforded to [national authorities] in **operating an interception regime must necessarily be narrower**».[137] Selve utformingen av et innhentingsregime vil dermed være gjenstand for en mer inngående forholdsmessighetsprøving. Dette gjenspeiles av EMD i utviklingen av krav til nasjonale kontrollmekanismer for den kommunikasjonsinnhenting som finner sted. Nærmere bestemt må det foreligge "adequate and effective guarantees against abuse", som er egnet til å holde tiltaket innenfor rammene av det som er nødvendig.[138] Domstolen har i

---

[133] [*Szabó and Vissy vs. Hungary,* avsnitt 57] og [*Big Brother Watch and others vs. The United Kingdom*, avsnitt 308].
[134] Skoghøy (2011), s. 189.
[135] Skoghøy (2011), s. 189.
[136] *Big Brother Watch and others vs. The United Kingdom*, avsnitt 308. (Forfatters utheving).
[137] *Big Brother Watch and others vs. The United Kingdom*, avsnitt 315.
[138] [*Szabó and Vissy vs. Hungary,* avsnitt 57] og [*Big Brother Watch and others vs. The United Kingdom*, avsnitt 308].

flere saker om skjult kommunikasjonsovervåkning gitt uttrykk for at denne vurderingen beror på;

> "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."[139]

Disse momenter danner grunnlaget for å vurdere hvilke rettssikkerhetstiltak som må foreligge for å sikre at etterretningsregimet vil være proporsjonalt med inngrepsgraden. Det må foreligge kontrollmekanismer som er i stand til å sikre en effektiv beskyttelse mot misbruk, i lys av de nevnte momenter. Især vil karakteren og rekkevidden av tilrettelagt innhenting, samt vilkårene for å iverksette innhenting, være av betydning for hvorvidt de foreslåtte kontrollmekanismer kan anses tilstrekkelige til å utjevne det inngrep ordningen innebærer.

4.4.5 Kontrollmekanismer for tilrettelagt innhenting

I sin praksis om skjulte overvåkningstiltak har EMD gitt uttrykk for at judisiell autorisasjon er en vesentlig rettssikkerhetsgaranti mot vilkårlighet.[140] Judisiell autoriseringskompetanse anses dermed som ønskelig for å sikre institusjonelt uavhengig og upartisk kontroll, all den tid bruken av skjulte overvåkningstiltak oftest utelukker at den som er utsatt for overvåkning på eget initiativ kan gjøre bruk av rettsmidler.[141] En følge av de berørtes manglende kontradiksjonsmuligheter, er at det bør stilles strengere krav til selve saksbehandlingen.[142] Det er likevel ikke ansett som en absolutt nødvendighet å innføre juridisk forhåndsgodkjenning. I Big Brother Watch mot Storbritannia ble det akseptert at det forelå andre uavhengige klageorganer som utgjorde effektive rettsmidler, selv det ikke forelå judisielle kontrollinstanser for autorisering.[143] Det sentrale er dermed hvorvidt det vil implementeres kontrollmekanismer som sett i sammenheng vil gi en tilstrekkelig uavhengig

---

[139] [*Szabó and Vissy vs. Hungary,* avsnitt 57] og [*Big Brother Watch and others vs. The United Kingdom*, avsnitt 308].
[140] *Big Brother Watch and others vs. The United Kingdom*, avsnitt 318.
[141] *Big Brother Watch and others vs. The United Kingdom*, avsnitt 318.
[142] Dette synspunkt er blant annet fremført av Norges institusjon for Menneskerettigheter i sitt høringssvar til lovforslaget: «*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»,* s. 24.
[143] *Big Brother Watch and others vs. The United Kingdom*, avsnitt 381.

og effektiv garanti mot myndighetsmisbruk. I vurderingen må det også tas i betraktning den foreslåtte utforming av innhentingssystemet i sin helhet, og da især rekkevidden av tilrettelagt innhenting som nevnt ovenfor.

4.4.5.1 Forhåndsautorisering

Forsvarsdepartementet foreslår for det første at det innføres en ordning med uavhengig forhåndsautorisasjon, for alle søk i datagrunnlaget som blir tilgjengelig via tilrettelagt innhenting.[144] Denne forhåndsautorisasjonsordningen omfatter etter lovforslagets kapittel 8 både innhenting ved målsøking og målrettet innhenting.[145] Dette innebærer at søk i lagrede metadata, samt innhenting av innholdsdata, vil kreve forutgående domstolskontroll.

Denne domstolskontrollen er foreslått tillagt Oslo Tingrett.[146] Alternativet som ble drøftet av Lysne II-utvalget, er å opprette en egen særdomstol for behandling av saker om e-tjenestens innhenting. Ettersom Norge ikke har tradisjon for bruk av særdomstoler, har det blitt fremhevet at å legge autorisasjonskompetansen til alminnelige domstoler er det alternativ som i størst mulig grad vil ivareta borgernes tillit.[147] Dette underbygges også av at hensynet til uavhengig og upartisk kontroll regelmessig anses ivaretatt av de alminnelige domstoler.[148]

Saksbehandlingen i domstolene vil i hovedsak bestå i en prøving av vilkårene for å iverksette målsøking eller målrettet innhenting. Dette skjer etter lovforslagets kapittel 8 på begjæring fra E-tjenesten, med skriftlige opplysninger om det faktiske og rettslige grunnlaget for innhentingsbegjæringen.[149] Videre er det foreslått at begjæringene skal kunne omfatte hele sakskompleks, for å begrense omfanget av begjæringer som fremmes.[150]

En legalitetskontroll av tilrettelagt innhenting vil knytte seg til hvorvidt grunnvilkårene for innhenting er oppfylt. Med målsøking for øyet må det foreligge «grunn til å undersøke» om det kan frembringes relevant informasjon, mens det for målrettet innhenting må

---

[144] Høringsnotatet – Forslag til ny lov om etterretningstjenesten, s. 180-181.
[145] Høringsnotatet – Forslag til ny lov om etterretningstjenesten, s. 388.
[146] Høringsnotatet – Forslag til ny lov om etterretningstjenesten, s. 237.
[147] Se bla: NIM (2017), *Høringsuttalelse til forsvarsdepartementet om Lysne II-utvalgets utredning Digitalt grenseforsvar (DGF),* s. 3.
[148] [NIM (2019), *Høringsuttalelse om forslag til ny lov om Etterretningstjenesten*, s. 24.] og [Domstoladministrasjonen, *Høringssvar – Forslag til ny lov om Etterretningstjenesten*, s. 1-2].
[149] Høringsnotatet – Forslag til ny lov om etterretningstjenesten, s. 387.
[150] Høringsnotatet – Forslag til ny lov om etterretningstjenesten, s. 299.

konstateres «konkrete holdepunkter» for at det foreligger grunn til å undersøke om slik informasjon kan frembringes.[151] Dette er vidt formulerte kriterier, som medfører at det vil være vanskelig å trekke grensen for hva som skal regnes som relevant informasjon og ikke.[152] I forlengelsen av dette vil det da også bli utfordrende å vurdere nødvendigheten eller forholdsmessigheten av et innhentingstiltak, som er et vilkår etter lovforslagets § 5-4. Det er da nærliggende å anta at bedømmelsen vil bære preg av særlig erfaringsbaserte og etterretningsfaglige vurderinger. Evnen til å foreta slike vurderinger vil da bero på den aktuelle domstol og dommeres kompetanse innenfor etterretningsfeltet.

I den forbindelse har EMD understreket at kontrollinstanser må ha «sufficient powers and **competence to exercise an effective and continuous control**».[153] Ved å tillegge autorisasjonskompetansen til en alminnelig domstol, blir det nødvendig med en viss form for dommerspesialisering eller bistand til dommerne fra fagkyndige, for at prøvingen av de etterretningsfaglige standarder skal være reell og effektiv. Bistand fra fagkyndige er foreslått besørget av E-tjenesten selv. Dette forslag har vakt reaksjoner i flere høringsinstanser. Særlig har det blitt fremholdt at dersom legalitetskontrollen blir avhengig av bistand fra E-tjenestens egne fagkyndige, er dette egnet til å svekke tilliten til domstolenes uavhengige og upartiske prøving. [154] Ut ifra dette standpunkt synes det nødvendig å innhente eventuell bistand fra andre fagmiljøer, og etablere et eget fagmiljø med spesialisering i domstolen selv.

Videre vil domstolens kapasitet og omfanget av begjæringer være av betydning for hvor effektiv den rettslige prøving i praksis vil være. I lys av de vagt utformede kriteriene som vanskeliggjør den rettslige prøvingen, må det tas høyde for at en sikkerhetsklarert behandling av begjæringer blir arbeidskrevende. Dette gjelder også dersom det fremmes hele sakskompleks i hver enkelt begjæring. I Centum för Rättvisa la EMD særskilt vekt på at det måtte fremmes begæring «in respect of **each intelligence collection mission**», og at begjæringen «must specify [...] also the signal carriers to which access is needed and the

---

[151] Høringsnotatet – Forslag til ny lov om etterretningstjenesten, s. 382-383. Se også kapittel 4.2.2.1 ovenfor.
[152] I samme retning: *Høringsuttalelse fra Datatilsynet om forslag til ny lov om Etterretningstjenesten*, s. 40.
[153] *Centrum för Rättvisa v. Sweden,* avsnitt 153.
[154] Se bla. [*Høringsuttalelse fra Datatilsynet om forslag til ny lov om Etterretningstjenesten*, s. 41], [Domstoladministrasjonen, *Høringssvar – Forslag til ny lov om Etterretningstjenesten*, s. 1-2] og [NIM (2019), *Høringsuttalelse om forslag til ny lov om Etterretningstjenesten*, s. 27].

search terms – or **at least the categories of search terms** – that will be used».[155] Dette er ikke til hinder for at det fremmes hele sakskompleks, men det fordrer en viss grad av spesifisering av de enkelte innhentingstiltak, med dets begrunnelse og virkninger. Dersom slik spesifisering uteblir, står det i fare for å etterlate forholdsmessighetsvurderingen overfladisk og uten reelt innhold.

Det vil også være et sentralt poeng at ordningen med forhåndsautorisasjon ikke er foreslått innført for bulkinnhentingen av metadata, mens først på stadiet for søk i datagrunnlaget - samt innhenting og lagring av innholdsdata. Det vil følgelig kunne innhentes store mengder dekrypterte (og riktignok filtrerte) metadata gjennom tilretteleggingsplikten, før det foretas noen form for legalitetskontroll fra domstolene.[156] Det ble både i Centrum för Rättvisa og Big Brother Watch lagt vekt på at forhåndsautorisasjon av selve bulkinnsamlingen er en viktig mekanisme for å begrense innsamlingens omfang til det som er nødvendig.[157] Et annet poeng er at det da heller ikke vil forekomme noen judisiell legalitetskontroll av den dekryptering som eventuelt gjennomføres via tilretteleggingsplikten. Dette kan anses betenkelig i lys av den mengden personopplysninger innhentede data kan inneholde.[158]

Ordningen med forhåndsgodkjenning fra domstolen må imidlertid sees i sammenheng med de øvrige kontrollmekanismer for tilrettelagt innhenting, ettersom det er det helhetlige bildet av rettssikkerhetsgarantier som er avgjørende. Av særlig relevans er den løpende og etterfølgende kontroll med innhentingen, som er foreslått tillagt EOS-utvalget.[159]

4.4.5.2 Løpende og etterfølgende kontroll

Foruten forhåndsautorisasjon har EMD lagt vekt på eksistensen og graden av kontroll med etterretningsjenestens gjennomføring av innhentingstiltak, samt etterfølgende kontroll.[160] Kontroll med at innhentingen utføres i tråd med tillatelsene og lovverket, er en sentral mekanisme for å hindre maktmisbruk og således ivareta borgernes tillit til systemet.[161] Det

[155] *Centrum för Rättvisa v. Sweden,* avsnitt 139.
[156] Se kapittel 2.1 for nærmere redegjørelse av bulkinnsamling og tilretteleggingspliktens innhold.
[157] [*Big Brother Watch and others vs. The United Kingdom*, avsnitt 376] og [*Centrum för Rättvisa v. Sweden,* avsnitt 139-141].
[158] Se kapittel 2.3 om hvilke opplysninger metadata kan inneholde.
[159] Se Høringsnotatet, punkt 11.12.
[160] [*Big Brother Watch and others vs. The United Kingdom*, avsnitt 379] og [*Centrum för Rättvisa v. Sweden,* avsnitt 105-106].
[161] *Roman Zakharov v. Russia*, avsnitt 273.

er videre lagt til grunn at også løpende og etterfølgende kontroll må tillegges et uavhengig og upartisk organ, som gis «sufficient powers and competence to exercise an effective and continuous control».[162]

I lovforslagets § 7-11 er det lagt opp til at EOS-utvalget skal føre «styrket kontroll» med E-tjenestens innhentingstiltak etter ordningen med tilrettelagt innhenting.[163] Dette omfatter både kontroll med gjennomføringen av innhenting, samt etterfølgende kontroll med avsluttede innhentingstiltak.[164] Denne fullmakten vil innebære en utvidelse av utvalgets oppdrag, som i dag bare omfatter etterfølgende kontroll. Ved utøvelsen av kontrollvirksomhet skal utvalget etter § 7-11 ha tilgang på all informasjon, utstyr, logger mv. som benyttes ved tilrettelagt innhenting.

Som nevnt ovenfor er det ikke noe absolutt krav at kontrollmyndighet tillegges et rettslig organ. At kontrollfunksjonene som foreslås organiseres innenfor det parlamentariske EOS-utvalget, er dermed ikke prinsipielt i strid med kravene utpenslet av EMD. Det sentrale vil uansett være at kontrollfunksjonene tillegges et organ som er organisatorisk og faglig uavhengig, slik at det ikke oppstår noen form for identifikasjon mellom kontrolløren og den kontrollerte.[165] I så måte er det positivt at EOS-utvalget er et statlig kontrollorgan for etterretning, overvåkning og sikkerhet, som er organisatorisk uavhengig fra E-tjenesten.

Den løpende kontroll vil i hovedsak bestå av tilsyn med at søk og innhenting utføres i tråd med domstolens tillatelser, og de materielle og prosessuelle regler i lovverket.[166] Særlig viktig for å ivareta proporsjonalitet, blir kontrollen med at innhentingen holder seg innenfor forholdsmessighetsgrensen i lovforslaget. De grunnvilkår som er foreslått bærer som nevnt preg av å være vage og vide standarder, noe som er mindre egnet for etterprøving.[167] Behovet for etterretningsfaglig kompetanse for å kunne utøve reell og effektiv kontroll innhentingsvirksomhet etter tilrettelagt innhenting, gjør seg følgelig også gjeldene for EOS-utvalgets kontroll. Kontrolloperatørene må være kompetent til å foreta de tekniske og faglige vurderinger som er nødvendig for å avgjøre om elektronisk innhenting, filtrering,

---

[162] *Centrum för Rättvisa v. Sweden,* avsnitt 153.
[163] Høringsnotatet – Forslag til ny lov om etterretningstjenesten, s. 387.
[164] Høringsnotatet – Forslag til ny lov om etterretningstjenesten, s. 257.
[165] Dette element er også fremhevet av Forsvarsdepartementet selv, se høringsnotatet punkt 11.12.7, s. 256.
[166] Høringsnotatet – Forslag til ny lov om etterretningstjenesten, s. 248.
[167] Se kapittel 4.2.2.1 Rekkevidden av innhentingstiltakene og 4.4.5.1 Forhåndsautorisering.

søkeprosesser, deling, sletting mv. utføres i samsvar med tillatelsene og regelverket for øvrig. EOS-utvalget har i så måte gitt uttrykk for at det må foretas en styrking av personalets tekniske og etterretningsfaglige kompetanse, for at den kontrollen som utøves skal ha substans.[168]

Det er i den forbindelse sentralt at kontrollorganet tilkjennes tilstrekkelig fullmakt til å kunne utføre løpende kontroll. Av flere høringsinstanser er behovet for kontinuitet fremhevet, slik at kontrollen ikke begrenses til sporadisk stikkprøvekontroll.[169] Dette fremgår også av EMDs krav til «continuous control».[170] Tilgang til all informasjon på kontrollorganets forespørsel, er i så måte et viktig element. Det må likevel kreves tilstrekkelig personell til at kontroll opprettholdes stabilt og jevnlig. Videre foreslås det tillagt kontrollorganet å drive kontroll med de fiberoptiske kabler som selekteres for innhenting, samt filtreringen av innhentede metadata.[171] Kontroll med at det ikke selekteres kabler som i hovedsak inneholder norsk kommunikasjon, er vesentlig for at selve bulkinnhentingen begrenses til det som er nødvendig.

Videre er det relevant å se hen til hvilken kontrollmodell som er nødvendig for å kunne utøve effektiv kontroll. I 2016 ble EOS-utvalgets virksomhet og rammebetingelser evaluert, etter beslutning fra Stortinget.[172] Evalueringsutvalget fremhevet da at dagens utvalgsmodell innebærer at kapasiteten i organet er begrenset, og at en utvalgsmodell derav vil være mindre egnet ved en eventuell utvidelse av EOS-utvalgets kontrollfunksjon.[173] Dette kommer av at en utvalgsmodell ikke legger opp til at kontrolloppgaver utøves som et fulltidsarbeid. Hvorvidt en utvalgsmodell vil være forenelig med kravene til effektive kontrollmekanismer, vil da i stor grad bero på at dets kapasitet er tilpasset et relativt omfattende innhentingsregime. Dette vil kreve at kontrollmodellen styrkes både faglig sett og ressursmessig. Et kontrollorgan som EOS-utvalget må da tildeles de nødvendige ressurser for en slik utvidelse i kapasitet, for å kunne opprettholde noen form for stabil løpende kontroll.

---

[168] EOS-utvalget (2019), *Høringssvar fra EOS-utvalget*, s. 12-13.
[169] Se bl.a.: NIM (2019), *Høringsuttalelse om forslag til ny lov om Etterretningstjenesten*, s. 30.
[170] *Centrum för Rättvisa v. Sweden,* avsnitt 153.
[171] Høringsnotatet – Forslag til ny lov om etterretningstjenesten, s. 247-248.
[172] Dokument 16 (2015-2016), *Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste.*
[173] Dokument 16 (2015-2016), s. 127.

Uten slike tilpassinger vil det være fare for at kontrollen i realiteten bare blir begrenset til en etterfølgende kontroll.

I Centrum för Rättvisa ble det fremhevet at «the supervisory body's powers with respect to any breaches detected», er et viktig element for kontrollens effektivitet.[174] Det sentrale er da hvilken avgjørelsesmyndighet som tillegges kontrollinstansen. EOS-utvalget er ikke foreslått tillagt myndighet til å avsi bindende vedtak om tjenestens innhenting, søk eller sletting.[175] Selv om utvalgets uttalelser i forbindelse med kontroll av E-tjenestens innhentingstiltak vil tillegges sentral betydning, vil det likevel være Etterretningstjenestens beslutning å ta det til følge. Å tillegge denne kompetansen til E-tjenesten alene, kan medføre at kontrollen i realiteten blir illusorisk.

4.4.5.3 Særlig om kravet til effektive rettsmidler

Kravet til effektive rettsmidler etter EMK art. 8 er nært forbundet med retten til effektive rettsmidler etter EMK art. 13. I overvåkningssammenheng synes EMD å ha lagt til grunn at det vil foretas en samlet vurdering av de rettsmidler som vil være tilgjengelig for borgerne.[176]

I relasjon til etterfølgende kontroll og tilgang til effektive rettsmidler, ble det i Centrum för Rättvisa understreket at «subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies».[177] Det ble likevel lagt til grunn at et system som alternativt gir enhver som mistenker at de har blitt rammet av innhentingstiltak en tilgang til å benytte klagemulighet i et passende kontrollorgan, vil kunne anses tilstrekkelig.[178] Kontrollorganets avgjørelsesmyndighet i slike saker vil da være sentralt. EOS-utvalget er imidlertid ikke tiltenkt kompetanse til å treffe rettslig bindende avgjørelser eller bindende vedtak overfor Etterretningstjenesten forøvrig.[179]

---

[174] *Centrum för Rättvisa v. Sweden,* avsnitt 155.
[175] Høringsnotatet – Forslag til ny lov om etterretningstjenesten, s. 62-63.
[176] *Centrum för Rättvisa v. Sweden,* avsnitt 176.
[177] *Centrum för Rättvisa v. Sweden,* avsnitt 106.
[178] *Centrum för Rättvisa v. Sweden,* avsnitt 106.
[179] Høringsnotatet – Forslag til ny lov om etterretningstjenesten, s. 62-63.

Behovet for hemmelighold og manglende notifikasjon til den overvåkede, vanskeliggjør også muligheten for å forfølge sitt krav i tradisjonelle rettsmidler som domstolene. Ytterligere vil bevisforbudet mot opplysninger som hemmeligholdes av hensyn til rikets sikkerhet i tvisteloven § 22-1, vanskeliggjøre en reell domstolsprøving. På dette punkt kommer betenkelighetene med at EOS-utvalget ikke er et rettslig organ med myndighet til å avsi bindende avgjørelser eller tilkjenne erstatning, i større grad frem. Den reelle adgangen til effektive rettsmidler kan da best betegnes som mangelfull. Denne situasjonen vil forsterke ubalansen i maktforholdet mellom myndighet og borgere, som oppstår ved den informasjonstilgangen staten får ved implementeringen av et innhentingsregime.[180]

4.5 Er det proporsjonalitet mellom tilrettelagt innhenting og inngrepets størrelse?

Proporsjonalitetsvurderingen går som nevnt ut på å balansere de konkurrerende interesser. Denne balanseringen vil staten naturlig nok ha en viss skjønnsmargin til å foreta. Forsvarsdepartementet har selv fremholdt at behovet for å holde tritt med trusselbildet i det digitale rom, er den sentrale interesse for å implementere et innhentingssystem. En innhentingshjemmel vil i seg selv ikke ivareta nasjonal sikkerhet og motvirke grenseoverskridende terrorisme, men er en forutsetning for at E-tjenesten kan drive elektronisk informasjonsinnhenting i utførelsen av sitt samfunnsoppdrag.[181] At det kan foreligge et økende behov for å innføre elektronisk kommunikasjonsinnhenting, synes rettferdiggjort i lys av den stadig økende bruk av internett for å spre, rekruttere og planlegge grenseoverskridende terrorvirksomhet.[182]

Som utpenslet i det foregående vil den foreslåtte utformingen av tilrettelagt innhenting medføre at store mengder rene norske kommunikasjonsdata vil innhentes ved bulkinnsamling. Ytterligere er det foreslått adgang til å foreta søk mot identifiserte nordmenn såfremt det ikke har overvåkningshensikt. Dette fremgår heller ikke av en naturlig fortolkning av innhentingsforbudet og dets unntak. Hvorvidt det foreligger overvåkningshensikt ved innhentingen, vil være vanskelig å kontrollere. Retten til å selv råde over egne personopplysninger og friheten fra å få sin kommunikasjon overvåket, er ansett

[180] Lignende synspunkter er fremmet av bl.a. St.Vincent (2017), s. 371.
[181] Se kapittel 1.3.2.
[182] Se kapittel 1.3.1.

som sentrale rettsstatlige verdier som er karakteristisk for et demokrati.[183] Således kan et innhentingssystem for elektronisk kommunikasjon som i det foreliggende, ikke bare være et vesentlig inngrep overfor den enkelte som rammes, men også utgjøre en overhengende overvåkningstrussel som utfordrer rettsstatsidealene.

4.6 Beskyttelse av andres rettigheter?

At tiltak som implementeres for å ivareta nasjonal sikkerhet også fungerer til å beskytte borgernes øvrige menneskerettigheter mot terrorkrenkelser, innebærer ikke nødvendigvis at tiltaket benyttes til et annet formål enn det angitte «nasjonal sikkerhet». All den tid beskyttelse av samfunnet og borgernes sikkerhet mot terrortrusler er en naturlig del av å ivareta nasjonal sikkerhet, vil det falle innenfor rammene av det meningsinnhold som kan tilskrives «national security».[184] I lys av at formålsangivelsen danner den saklige rammen for argumenter som kan begrunne et tiltak, vil også beskyttelse av borgernes sikkerhet kunne fremføres som begrunnelse for tiltaket. Nasjonale myndigheter kan bruke etterretningsanalysene til å eksempelvis iverksette tiltak for beskyttelse av borgernes sikkerhet, uten at dette anses å være i strid med formålet for at informasjon ble innhentet i utgangspunktet – såfremt utleveringen ikke går lenger enn nødvendig for å ivareta nasjonal sikkerhet.[185] Det kan derfor spørres om et system som tilrettelagt innhenting kan anses som en preventiv forpliktelse for staten. I så fall kan det tenkes at en slik forpliktelse kan nytte som argument av betydning for forholdsmessighetsvurderingen etter art. 8.

Kapittel 5: En preventiv plikt til å forebygge grenseoverskridende terrorisme?

5.1 Innledning

I dette kapittel vil det foretas en analyse av hvorvidt et innhentingssystem som tilrettelagt innhenting kan inngå som en del av statens preventive forpliktelser mot grenseoverskridende terrorisme. For det første må det poengteres at de preventive forpliktelser som kan utledes av menneskerettighetene påhviler statens myndigheter mer

[183] Se kapittel 3.1.
[184] *Klass and others v. Germany*, avsnitt 48.
[185] *Centrum för Rättvisa v. Sweden,* avsnitt 150.

generelt, og ikke nødvendigvis vil knyttes til utenlandsetterretning eller E-tjenesten spesifikt. Analysen forsøker ikke å besvare spørsmål knyttet til innenlandske overvåkningstiltak (m.a.o. overvåkningstiltak rettet mot egne borgere for å oppdage nasjonale terrortrusler). Ettersom det ikke eksisterer eksplisitte bestemmelser som hjemler en rett på vern mot terrorisme, vil det tas utgangspunkt i de forpliktelser som kan utledes fra de mer generelle bestemmelser om retten til liv i Grl. § 93 og EMK art. 2.

5.2 Eksistensen av en preventiv forpliktelse til å beskytte retten til liv

Det er i Grunnloven § 93 første ledd stadfestet at enhver har «rett til liv». I Grl. § 93 fjerde ledd er det videre presisert at «statens myndigheter skal beskytte retten til liv».[186] I forarbeidene til grunnlovsrevisjonen er det understreket at dette innebærer en positiv forpliktelse «til å iverksette øvrige tiltak som kan forhindre at overgrep finner sted».[187] Dette er også i tråd med den generelle plikt til å sikre de enkelte menneskerettighetene, som fremgår av Grl. § 92.[188] At en preventiv forpliktelse kan foreligge også der det er tale om mellom-private krenkelser, ble lagt til grunn av Høyesterett i Rt. 2013 s. 588.[189]
Det nærmere innholdet i denne forpliktelsen til å iverksette tiltak vil måtte tolkes i lys av EMK art. 2.[190]

Bestemmelsen har sin konvensjonsrettslige parallell i EMK art. 2 (1), som fastslår at «everyone's right to life shall be protected by law».[191] Etter ordlyden er det inntatt en plikt til å beskytte retten til liv ved lov, men bestemmelsen gir ikke anvisning på noen positive forpliktelser ut over dette. I praksis tilknyttet bestemmelsen har EMD imidlertid fremhevet behovet for å tolke vernet i lys av statenes alminnelige sikreplikt etter EMK art. 1, for å sikre et effektivt vern av retten til liv.[192] Statens ansvar baseres i slike tilfeller på unnlatelsen av å beskytte menneskerettighetene i tråd med den positive sikreplikten, som gjelder i situasjoner der staten kan påvirke begivenhetene som leder frem til krenkelse.[193]

---

[186] Grunnloven § 93 (4).
[187] Dok.nr.16 (2011–2012), s. 112.
[188] Grunnloven § 92.
[189] Rt. 2013 s. 588.
[190] Behovet for å tolke Grl. § 93 og dens innhold presiserende i lys av EMK art. 2, er bl.a. fremhevet i forarbeidene til grunnlovsrevisjonen: Dok.nr.16 (2011–2012), s. 106.
[191] EMK artikkel 2 (1) jf. menneskerettighetsloven § 2.
[192] *Osman v. The United Kingdom*, avsnitt 116.
[193] Bertelsen, *EMK. Kommentarer til bestemmelsene om individets rettigheter og friheter*, 2011, s. 50

De gjeldende retningslinjer for statens forpliktelser der trusselen mot liv stammer fra privates handlinger, fremgår av Osman mot Storbritannia.[194] For å etablere ansvar oppstilte EMD krav om at staten «knew or ought to have known» at det forelå en «real and immediate risk to the life of identified individuals», og at staten «failed to take measures within the scope of their powers which, judged reasonably, might have been expected to avoid that risk».[195] På bakgrunn av de nevnte kriterier kan staten ha plikt til å benytte preventive virkemidler for å beskytte liv i livstruende situasjoner forårsaket av private aktører. Testen er derfor relevant ved vurderingen av statens plikt til å benytte proaktive tiltak som elektronisk innhenting, til forebyggelse av internasjonal terrorisme som utgjør en trussel mot liv.

5.3 Reell og umiddelbar fare

For det første må det konstateres at det foreligger en «real and immediate risk to the life», som nødvendiggjør en reaksjon.[196] I teorien er det blir fremhevet at denne risikoen «must clearly be capable of causing death», og at sannsynligheten for at risikoen materialiserer seg må «at least be compelling».[197] Grenseoverskridende terrorangrep er klart nok et fenomen som er i stand til å ta flere menneskeliv. Sannsynligheten for at risikoen materialiserer seg vil derimot måtte avgjøres i det konkrete tilfelle, ut ifra hvilken trussel som foreligger.

I relasjon til preventive forpliktelser er det da et sentralt poeng at risikoen enda ikke har materialisert seg i en krenkelse. Det oppstår dermed et spørsmål om når risikoen kan sies å være reell og umiddelbar.[198] Dette er avgjørende for når en preventiv forpliktelse kan sies å inntre. Særlig vanskelig er denne avgjørelsen i tilknytning til proaktive tiltak for å hindre at risikoen materialiserer seg, og det avgjørende vil i slike tilfeller være hvilken kunnskap staten har om trusselen og dens karakter.

5.4 Individualiseringen

[194] *Osman v. The United Kingdom*. Kriteriene er også omtalt som «Osman-testen», se bl.a. Aall (2018), s. 77.
[195] *Osman v. The United Kingdom*, avsnitt 116.
[196] *Osman v. The United Kingdom*, avsnitt 116.
[197] Se McBride (1999), s. 45-46.
[198] Se McBride (1999), s. 45.

Etter Osman mot Storbritannia er det krav om at den aktuelle risikoen for tap av liv kan knyttes til «identified individuals».[199] I lys av at grenseoverskridende terrorangrep ofte rammer tilfeldig og bredt, kan det være vanskelig å på forhånd identifisere hvem som vil rammes. Nyere praksis har imidlertid vist en utvikling av dette kravet. I Tagayeva mot Russland tok domstolen stilling til preventive forpliktelser etter EMK art. 2 i relasjon til terrorfare. EMD uttalte i forbindelse med preventive tiltak mot terrorangrep at:

> "Such a positive obligation may apply not only to situations concerning the requirement of personal protection of one or more individuals identifiable in advance as the potential target of a lethal act, but also in cases raising the obligation **to afford general protection to society"**.[200]

Med andre ord vil det kunne inntre en preventiv forpliktelse i de tilfeller det foreligger en reell og umiddelbar fare «to life for members of the public at large».[201] Et poeng er da at kravet til individualisering primært har betydning for at den risikoen som foreligger skal være identifiserbar i forkant av en krenkelse.[202] Dette kommer av at staten ikke kan holdes ansvarlig for en unnlatelse dersom det ikke er mulig å identifisere risikoens adresse, og således iverksette beskyttelsestiltak. Når den aktuelle risiko er terrorisme, er det mulig å påregne at sivilbefolkning generelt vil være risikoens adressat.[203] Selv om det nok vil kreves at det er mulig å foreta en nærmere identifisering av aktuelle målområder, kan det tenkes at det sentrale slike tilfeller blir muligheten for indentifisering av selve risikokilden.[204]

5.5 Kunnskapskravet

Videre er eksistensen av en preventiv forpliktelse er betinget av at staten «**knew or ought to have known** at the time of the excistence of a real and immediate risk».[205] Domstolens formulering av kunnskapskravet innebærer imidlertid at det er tilstrekkelig at staten «ought to have known» om risikoen, for at betingelsen skal anses oppfylt.[206] Staten vil dermed

---

[199] *Osman v. The United Kingdom*, avsnitt 116.
[200] *Tagayeva v. Russia*, avsnitt 482. (Forfatters utheving).
[201] *Mastromatteo v. Italy*, avsnitt 74.
[202] Se *Tagayeva v. Russia*, avsnitt 482: «*identifiable in advance as the potential target of a lethal act".*
[203] Se kapittel 1.3 om grenseoverskridende terrorisme.
[204] I Stoyanova (2018) er det fremhevet at det i enkelte tilfeller *"might be enough to demonstrate that the state knew or ought to have known about the source of the harm",* s. 314-315.
[205] *Osman v. The United Kingdom*, avsnitt 116. (Forfatters utheving).
[206] *Osman v. The United Kingdom,* avsnitt 116.

kunne holdes ansvarlig for å ikke utvise tilstrekkelig aktsomhet i forbindelse med potensiell risiko for tap av liv.

Det avgjørende for at en preventiv forpliktelse skal inntre blir da spørsmålet når staten «ought to have known» om en trussel. Hvilken grad av aktsomhet som kreves kan variere med konteksten og omstendighetene forpliktelsen oppstår i.[207] Statens ansvar for unnlatelser snevres likevel inn ved at kravet til aktsomhet knyttes opp mot eksistensen av «a real and immediate risk to the life of an identified individual or individuals».[208] Dette utgangspunktet modifiseres noe av at domstolen har også har anerkjent eksistensen av en preventiv forpliktelse «to afford general protection to society».[209] Statens aktsomhet må da omfatte eksistensen av en konkrete risiko for tap av sivile liv, samt aktuelle terrormål som behøver beskyttelsestiltak.[210]

En interessant avgjørelse om kunnskapskravet er K.U mot Finland, hvor EMD uttalte at «it was well-known that the Internet, precisely because of its anonymous character, could be used for criminal purposes».[211] Sammenholdt med at misbruk av barn var et velkjent fenomen, tilsa denne kunnskapen av staten kunne utviklet ordninger for å beskytte barn mot pedofile på internett.[212] I teorien har denne avgjørelsen blitt tatt til inntekt for at «the state may not remain passive: it requires active anticipation».[213] Dette poenget gjelder særlig for kjente utfordninger og trusler som følger med utviklingen av internett.

Et annet poeng fremhevet av EMD er «the more predictable the hazard, the greater obligation to protect against it".[214] Spørsmålet er da hvor forutberegnelig terrortrusselen og dens materialisering vil være for myndighetene. Et særtrekk ved bulkinnsamling er at datagrunnlaget i stor grad inneholder irrelevant informasjon, og innhentingsmetoden brukes i stor grad til å finne ukjente aktører.[215] Forsvarsdepartementet har selv gitt uttrykk for at denne formen for innhenting innebærer at man gis «tilgang til høystakken for å finne nålen».

---

[207] Stoyanova (2018), s. 314.
[208] *Osman v. The United Kingdom*, avsnitt 116.
[209] [*Tagayeva v. Russia*, avsnitt 482] og [*Mastromatteo v. Italy*, avsnitt 69].
[210] Lavrysen (2014), s. 92.
[211] *K.U v. Finland,* avsnitt 48.
[212] *K.U v. Finland,* avsnitt 48.
[213] Lavrysen (2014), s. 93.
[214] *Finogenov and others v. Russia*, avsnitt 243.
[215] *Big Brother Watch and others vs. The United Kingdom*, avsnitt 384-386. Se også kapittel 2.1.

Dette må da være begrunnet i en vid proaktiv undersøkelsesplikt fra myndighetenes side. En slik plikt kan imidlertid ikke oppstilles der det ikke foreligger tegn på fare eller kunnskap om trusselaktører.

5.6 Rimelige tiltak

Den nærmere rekkevidden av statens preventive forpliktelse beror på hvorvidt det/de aktuelle virkemiddel er «measures within the scope of their powers which, **judged reasonably**, might have been expected to avoid that risk».[216] Domstolen har understreket at «reasonable measures» må tolkes slik at forpliktelsen ikke utgjør "an impossible or disproportionate burden on the authorities".[217] I dette ligger det at innholdet i de tiltak staten pålegges å iverksette må være realistisk ut ifra statens ressurser, og samtidig tilfredsstille det minimum av effektivitet som må kreves for å beskytte retten til liv.[218] I den forbindelse tilkjennes konvensjonsstatene en viss skjønnsmargin til å beslutte hvilke operative virkemiddel som skal benyttes for å beskytte liv mot terror.[219]

5.6.1 Kausalitetskravet

I Osman-saken oppstilte EMD som kriterium for ansvar at aktuelle tiltak «might have been expected to **avoid that risk**».[220] EMD legger her opp til et krav om at tiltaket faktisk ville forhindret en krenkelse. Ansvar er dermed betinget av at det foreligger en kausal sammenheng mellom statens unnlatelse og risikoens materialisering.[221]

Domstolen har i majoriteten av saker om positive forpliktelser tydd til en lempeligere forståelse av kausalitetskravet.[222] Avklarende i så måte er E m. flere mot Storbritannia, hvor det uttales at det vil være tilstrekkelig at tiltaket har «a real prospect of altering the outcome or mitigating the harm".[223] Dette er fulgt opp i Tagayeva mot Russland, hvor domstolen understreket at myndighetene kunne forventes å treffe tiltak som «at least mitigate this

[216] *Osman v. The United Kingdom*, avsnitt 116. (Forfatters utheving).
[217] *Osman v. The United Kingdom*, avsnitt 116.
[218] Xenos (2012), s. 106.
[219] *Tagayeva v. Russia*, avsnitt 492.
[220] *Osman v. The United Kingdom*, avsnitt 119.
[221] Lavrysen (2018), s. 710-711.
[222] Lavrysen (2018), s. 717.
[223] *E. and others v. the United Kingdom,* avsnitt 99.

risk».[224] Kravet om kausalitet kan følgelig forstås som at det vil foreligge tilstrekkelig sammenheng mellom en preventiv forpliktelse og risikoens materialisering, dersom det aktuelle tiltak ville minimert risikoen. I tilfeller hvor det er tale om preventive tiltak forut en krenkelse, får denne kausalitetsvurderingen et hypotetisk preg. Dersom en tar utgangspunkt i det premiss at digital informasjonsinnhenting er en sentral forutsetning for å oppdage og således avverge terrorfare, vil dette tyde på at innhentingen faktisk vil minimere risikoen.

5.6.2 Statens skjønnsmargin

Videre er myndighetene tilkjent en skjønnsmargin til å velge hvilke operative virkemiddel som skal iverksettes, all den tid myndighetene selv står nærmest til å vurdere hvilke beskyttelsestiltak som er best egnet for å avverge tap av liv.[225] I Tagayeva mot Russland uttaler EMD eksplisitt at «this is **especially so in respect of counter-terrorist activity**, where the authorities often face organised and highly secretive networks".[226] Dette taler for at staten kan velge å benytte digital informasjonsinnhenting som et tiltak for å oppdage og motvirke terrorisme. Et sentralt spørsmål imidlertid er hvilken skjønnsmargin staten vil tilkjennes ved balanseringen av de rettigheter som konkurrerer om beskyttelse, som i denne forbindelse er retten til liv og privatliv etter EMK art.2 og art. 8.[227] Dette kommer særlig på spissen i relasjon til bulkinnsamling, da dette generelt er et inngripende tiltak.[228] Balanseringen av de to rettigheter er krevende, særlig i lys av at retten til liv er tillagt grunnleggende betydning - og det derav vil være snevrere margin til å vekte rettighetene mot hverandre.[229] Det sentrale må i alle tilfeller være at bulkinnhenting og målrettet innhenting må utføres i tråd med de retningslinjer utledet av EMK art. 8, som utpenslet ovenfor.[230]

5.6.3 Er kommunikasjonsinnhenting et rimelig tiltak?

---

[224] *Tagayeva v. Russia*, avsnitt 491.
[225] *Tagayeva v. Russia*, avsnitt 492.
[226] *Tagayeva v. Russia*, avsnitt 492.
[227] Behovet for en balansering av konkurrerende rettigheter er understreket i K.U v. Finland, hvor EMD fremhevet *"the need to ensure that powers to prevent […] crime are exercised in a manner which fully respects [...] the guarantees contained in Articles 8 and 10 of the Convention*", avsnitt 48.
[228] Bulkinnsamling er et tiltak som rammer bredt. Se kapittel 2.
[229] Lavrysen (2016), s. 173-174 og 193-194.
[230] Se kapittel 4.

Hva gjelder tiltakets effektivitet, er det et viktig poeng at informasjonsinnsamling i seg selv ikke kan avverge terrorisme. Således vil informasjonsinnhenting ikke i seg selv kan være et tilstrekkelig virkemiddel for å beskytte liv. Effektivitetskravet må samtidig forstås dithen at staten ikke kan holdes ansvarlig for tiltak som uansett ikke ville gjort en forskjell.[231]
Det er anerkjent av EMD at både bulkinnsamling og målrettet innhenting er verdifulle virkemidler for å oppdage terrortrusler, ettersom terrorister gjør stadig mer sofistikert bruk av internett for terrorformål.[232] I relasjon til bulkinnsamling er det særlig fremhevet at denne formen for innhenting muliggjør en proaktiv tilnærming for å oppdage ukjente trusler.[233] Dette tyder på at innhentingens nytteverdi i kampen mot terror er anerkjent, selv om den faktiske effektiviteten er vanskelig å overskue.[234] For at kommunikasjonsinnhenting kan anses effektivt for å beskytte liv fordrer det likevel at innhentet informasjon formidles til relevant myndighet, som kan iverksette nødvendige tiltak.

Videre er det et poeng at graden av kunnskap staten kan tilskrives er av betydning for hvilke tiltak som kan anses rimelig å kreve iverksatt.[235] For å iverksette målrettet innhenting vil trusselaktøren gjerne være kjent for myndighetene.[236] Det vil derfor være nærliggende at myndighetenes grad av kjennskap til trusselaktørene vil være av betydning for hvorvidt det kan pålegges en plikt til kommunikasjonsinnhenting. Vanskeligere vil det da være å ilegge staten en plikt til å iverksette bulkinnsamling, ettersom datagrunnlaget da i større grad vil være av betydning for å finne ukjente trusselaktører.[237] Dette forsterkes av at datainnhenting og de tilhørende prosedyrer er ressurskrevende arbeid, hvilket innebærer en prioritetsvurdering staten selv er nærmest å foreta.

En plikt til å innhente informasjon kan da best beskrives som en undersøkelsesplikt fra myndighetenes side, som må kombineres med ytterligere beskyttelsestiltak. At kravet til rimelige eller adekvate tiltak kan innebære en plikt til å treffe flere sammensatte tiltak, synes lagt til grunn av EMD.[238] For å avgjøre rekkevidden av tiltak som kan kreves, er det sett hen

---

[231] Lavrysen (2018), s. 716.
[232] *Big Brother Watch and others vs. The United Kingdom*, avsnitt 384-386.
[233] *Big Brother Watch and others vs. The United Kingdom*, avsnitt 385-386.
[234] Se kapittel 4.4.3.
[235] Lavrysen (2018), s. 713.
[236] Høringsnotatet, s. 145.
[237] Se kapittel 2.
[238] *Tagayeva v. Russia,* avsnitt 491: *«Although some measures were taken, in general the preventive measures in the present case could be characterised as inadequate».*

til statens kontroll over situasjonen.[239] I så måte er det et poeng at statens kontroll har betydning for hvilke tiltak som kreves, samtidig som elementer som terrorfarens aktualitet, forutsigbarhet og statens kunnskap kan kreve mer kontroll.[240] Dersom staten skulle velge å implementere bulkinnhenting og/eller målrettet innhenting, kan denne kontrollen tilsi at staten i større grad vil holdes ansvarlig for å iverksette adekvat respons på terrorfare.

En viktig erkjennelse er at argumentasjonen i sikkerhetstilfellene fort blir sirkulær, da det både kan argumenteres for at statens kjennskap til den generelle terrorfaren som utspiller seg via internett nødvendiggjør elektronisk kommunikasjonsinnhenting, samtidig som statens kommunikasjonsinnhenting i sin tur kan gi en nærhet til risikoen som utvider rekkevidden av preventive forpliktelser staten kan pålegges. Dette er per dags dato et uavklart område.

5.7 Konklusjon

En proaktiv plikt til å benytte digitale innhentingstiltak i forebyggende øyemed, kan ikke leses ut av EMDs praksis i dag. Kunnskapskravet vil sjelden vil være innfridd ved bruk av tiltak som bulkinnsamling, da myndighetene ikke rimelig kan forventes å forutse hittil ukjente trusselaktører ved målsøking, selv om staten skulle velge å anvende tiltaket. I slike tilfeller vil det sjelden foreligge tilstrekkelige tegn på fare.

Dersom staten regelmessig velger å innføre og anvende tiltak som målrettet innhenting overfor allerede kjente trusselaktører, er det mer nærliggende å vurdere ansvar. Dette fordrer imidlertid etter kunnskapskravet at staten allerede besitter tilstrekkelig informasjon som tilsier at aktøren utgjør en aktuell trussel, som det bør innhentes informasjon om i lys av en aktsomhetsplikt. Selv om ansvar i disse tilfellene kan tenkes, er det svært usikkert om EMD vil anse det rimelig å pålegge staten en plikt til å aktivt forutse enhver terrortrussel som er aktuell, selv om staten skulle velge å innføre innhentingstiltak. Å konstituere ansvar vil da bero på hvilken kunnskap staten har om trusselaktørens hensikt, trusselens umiddelbarhet, målets identifiserbarhet og rimeligheten i det konkrete tilfellet. Det kan følgelig ikke anses å

[239] *Tagayeva v. Russia,* avsnitt 491.
[240] Stoyanova (2018), s. 324.

eksistere en alminnelig plikt til implementering av digitale innhentingstiltak som preventivt virkemiddel.

Kapittel 6: Konklusjon og avsluttende bemerkninger

Med det utgangspunkt at internasjonale domstoler synes å akseptere at både bulkinnsamling av data og målrettet innhenting faller innenfor statens skjønnsmargin å implementere, vil det være nærliggende å legge til grunn at det vil være mulig å innføre slike innhentingsmetoder også i Norge.[241] Det er likevel med forbehold om at et innhentingsregime oppfyller de krav til utforming og utførelse som stilles etter Norges konstitusjons- og konvensjonsforpliktelser. Særlig sentralt i så måte er de kvalitetskrav som stilles til en lovregulering av bulkinnsamling og målrettet innhenting, samt de krav som stilles til rettssikkerhetsgarantier og kontrollmekanismer av slike innhentingsmetoder.

Det vesentlige er at lovreguleringen i seg selv utgjør en rettsikkerhetsgaranti, ved å fastsette presise vilkår som ikke legger opp til en uforholdsmessig vid skjønnsadgang for E-tjenesten. I lys av lovforslagets vide formuleringer av grunnvilkår og formålsbestemmelser, kan den foreslåtte lovreguleringen karakteriseres som mangelfull og uforholdsmessig i så måte.[242] All den tid lovgivningen av hensyn til hemmelighold ikke kan utformes for detaljert, kan slike mangler avhjelpes ved at det iverksettes uavhengige og effektive kontrollmekanismer.

En sentral kontrollmekanisme i så måte er forhåndsautorisering ved domstolene. Dette fordrer imidlertid at domstolen ved behandling av saker til forutgående kontroll får tilstrekkelig spesifikke opplysninger til å foreta en reell nødvendighetsvurdering og prøving av vilkårene for søk og innhenting.[243] Ved fremleggelsen av hele sakskompleks må det dermed kreves en viss spesifikasjon. Videre må det kreves en høyere grad av etterretningsfaglig kompetanse enn det som foreligger ved domstolene i dag.

Den løpende kontrollen må også være uavhengig og effektiv. En utvalgsmodell er mindre egnet til å drive effektiv kontroll, i lys av den kapasitetsbegrensningen som ligger iboende en

[241] Se kapittel 4.4.4.
[242] Se kapittel 4.1.
[243] Se kapittel 4.4.5.1.

utvalgsmodell. Også medlemmenes deltidsarbeidsform vil skape ressursmessige utfordringer for at kontrollen faktisk kan utføres løpende og stabilt.[244]

I relasjon til den etterfølgende kontroll er det lagt opp til en kontrollmodell der organet kun har veiledende myndighet. Den mest fremtredende konsekvensen av å operere et kontrollsystem som ikke har bindende avgjørelseskompetanse, eller gode muligheter for domstolsprøving, er at rettsmidlene vil ha mangelfull effektivitet og pålitelighet. Dette vil ikke bare anses uforenelig med kravene til rettsmidler etter EMK art.8, men også utfordre retten til effektive rettsmidler i EMK art. 13.[245] I forlengelsen av dette vil rettsmidlenes mangelfulle effektivitet ha betydning for det overordnede kravet om forholdsmessighet, ved at kravet til «adequate and effective safeguards against abuse» ikke kan anses oppfylt.[246]

Slik innhentingssystemet tilrettelagt innhenting er foreslått utformet og utført i dag, vil det følgelig ikke være forenelig med retten til privatliv etter Grunnloven § 102 og EMK art. 8. En implementering i tråd med retten til privatliv, vil fordre at det utformes kontrollmekanismer som har en tilstrekkelig grad av faglig og teknisk kompetanse, ressurser og avgjørelsesmyndighet til å oppfylle kravene til effektiv kontroll og effektive rettsmidler. Videre vil selve lovreguleringen måtte utformes med tilstrekkelig presisjon i relasjon til sentrale begrensninger som formålet for innhenting, vilkårene for innhenting, deling og sletting av lagrede data. Dette kan i lys av ikke sies å foreligge på nåværende tidspunkt.

[244] Se kapittel 4.4.5.2.
[245] Se kapittel 4.4.5.3.
[246] Se kapittel 4.4.4 og 4.4.5.

7. Litteraturliste

7.1 Lover

Ekomloven (2003)	Lov 4. juli nr. 83 om elektronisk kommunikasjon (Ekomloven – e-koml).
Etterretningstjenesteloven (1998)	Lov 20. mars 1998 nr. 11 om Etterretningstjenesten (Etterretningstjenesteloven).
Grunnloven (1814)	Lov 17. mai 1814 Kongeriket Norges Grunnlov (Grunnloven – Grl.)
Menneskerettighetsloven (1999)	Lov 21. mai nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (Menneskerettsloven – mrl)

7.2 Konvensjoner

EMK (1950)	Den europeiske menneskerettskonvensjon, Roma 4. november 1950. (EMK)

7.3 Forarbeider

(Sitert fra lovdata)

Dok.nr.16 (2011–2012)	Dok.nr.16 (2011–2012) Rapport fra Menneskerettighetsutvalget om menneskerettigheter i Grunnloven. 19.12.2011.

7.4 Rettspraksis

7.4.1 Rettspraksis fra Høyesterett

HR-2018-104-A

Rt. 2015 s. 93

Rt. 2014 s. 1105

Rt. 2013 s. 588

7.4.2 Rettspraksis fra EMD

(Sitert fra https://hudoc.echr.coe.int/)

Big Brother Watch and others v. The United Kingdom	Case of Big Brother Watch and others v. The United Kingdom. (Applications nos. 58170/13, 62322/14 and 24960/15). 13.09.2018. (Ikke rettskraftig)
Centrum för Rättvisa v. Sweden	Case of Centrum för Rättvisa v. Sweden. (Application no. 35252/08). 19.06.2018. (Ikke rettskraftig)
C.G and others v. Bulgaria	Case of C.G and others v. Bulgaria. (Application Number 1365/07). 24.04.2008.
E. and others v. the United Kingdom	Case of E. and others v. the United Kingdom. (Application no. 33218/96). 26.11.2002.
Finogenov and others v. Russia	Case of Finogenov and others v. Russia. (Applications nos. 18299/03 and 27311/03). 20.12.2011.
Klass and others vs. Germany	Case of Klass and others vs. Germany. (Application no. 5029/71). 06.09.1978.
K.U v. Finland	Case of K.U v. Finland. (Application no. 2872/02). 02.12.2008.
Leander v. Sweden	Case of Leander v. Sweden. (Application no. 9248/81). 26.03.1987.
Mastromatteo v. Italy	Case of Mastromatteo v. Italy. (Application no. 37703/97). 24.10.2002.
Osman v. The United Kingdom	Case of Osman v. The United Kingdom. (Application No(s). 23452/94). 28.10.1998.

Roman Zakharov v. Russia	Case of Roman Zakharov v. Russia. (Application no. 47143/06). 4.12.2015.
Rotaru v. Romania	Case of Rotaru v. Romania. (Application no. 28341/95). 04.05.2000.
Szabó and Vissy vs. Hungary	Case of Szabó and Vissy vs. Hungary. (Application no. 37138/14). 12.01.2016.
Tagayeva v. Russia	Case of Tagayeva and others v. Russia. (App. No(s). 26562/07, 14755/08, 49339/08, 49380/08, 51313/08, 21294/11, 37096/11). 13.04.2017.
Weber and Saravia v. Germany	Case of Weber and Saravia v. Germany (Application no. 54934/00). 29.06.2006.

7.5 Høringsnotat og høringsuttalelser

Forsvarsdepartementet (2018)	Forsvarsdepartementet. *Høringsnotat – forslag til ny lov om Etterretningstjenesten.* 12.11.2018. https://www.regjeringen.no/contentassets/556459ec77bd448f828af034dd573e11/horingsnotat---forslag-til-ny-lov-om-etterretningstjenesten.pdf
Datatilsynet (2019)	Datatilsynet. *Høringsuttalelse fra Datatilsynet om forslag til ny lov om Etterretningstjenesten.* 2019. https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=e0b87829-2c74-4f2c-8066-c75801bcd0d5
Domstoladministrasjonen (2019)	Domstoladministrasjonen. *Høringssvar – Forslag til ny lov om Etterretningstjenesten.*2019. https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=262c51c1-f24c-4b41-a29a-a60bbbe0be7e

EOS-utvalget (2019) EOS-utvalget. *Høringssvar fra EOS-utvalget – høring om forslag til ny lov om Etterretningstjenesten*. 2019. https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=7fb7c142-e17d-4ca4-bf49-3f7afb1ee1fc

NIM (2019) Norges nasjonale institusjon for menneskerettigheter. *Høringsuttalelse om forslag til ny lov om Etterretningstjenesten.* 2019. https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=1b03fe18-1d1e-4be5-a7ce-5f1dc785695a

NIM (2017) Norges nasjonale institusjon for menneskerettigheter. *Høringsuttalelse til forsvarsdepartementet om Lysne II-utvalgets utredning Digitalt grenseforsvar (DGF).* 2017. https://www.regjeringen.no/contentassets/84a90462cf9b4aebb310d97052083d26/norges-nasjonale-institusjon-for-menneskerettigheter_dgf.pdf?uid=Norges_nasjonale_institusjon_for_menneskerettigheter

7.6 Juridisk litteratur

7.6.1 Bøker

Aall (2018) Aall, Jørgen. *Rettsstat og menneskerettigheter*, 5. utg, Bergen, 2018.

Bertelsen (2011) Bertelsen, Thor Ehlers. *EMK. Kommentarer til bestemmelsene om individets rettigheter og friheter,* 1. utg, Oslo, 2011. (Sitert fra Rettsdata).

Lavrysen, L. (2014) Lavrysen, Laurens. *Protection by the Law: The Positive Obligation to Develop a Legal Framework to Adequately Protect ECHR Rights*. Human Rights and Civil Liberties in the 21st Century. Y. Haeck and E. Brems. Dordrecht, Springer Netherlands**:** 69-129, 2014. https://doi.org/10.1007/978-94-007-7599-2_4

Lavrysen, L. (2016)	Lavrysen, Laurens. *Human Rights in a Positive State: Rethinking the relationship between positive and negative obligations under the European Convention on Human Rights,* Cambridge, 2016.
National Research Council (2015)	National Research Council. *Bulk Collection of Signals Intelligence: Technical Options.* Washington DC, The National Academies Press, 2015. https://doi.org/10.17226/19414
Macdonald og Mair (2015)	Macdonald, Stuart og David Mair. *Terrorism online: A new strategic environment.* Terrorism Online. Jarvis, Lee, Macdonald, Stuart og Thomas M. Chen, London, 2015.
Rubinstein, Nojeim, Lee (2017)	Rubinstein, Ira, Nojeim, Gregory og Ronald Lee. *Systematic Government Access to Private-Sector Data: A Comparative Analysis*. Bulk collection: systematic government access to private-sector data. Cate, F. H. and J. X. Dempsey, New York, Oxford University Press, 2017. DOI:10.1093/oso/9780190685515.001.0001
Strand og Larsen (2016)	Strand, Vibeke Blaker og Larsen, Kjetil Mujezinovic. *Menneskerettigheter i et nøtteskall,* 1.utg, Oslo, 2016.
St. Vincent (2017)	St. Vincent, Sarah. *Preventing the Police State: International Human Rights Laws Concerning Systematic Government Access to Communications Held or Transmitted by the Private Sector.* Bulk collection: systematic government access to private-sector data. Cate, F. H. and J. X. Dempsey, New York, Oxford University Press, 2017. DOI:10.1093/oso/9780190685515.001.0001
Xenos (2012)	Xenos, Dimitris. *The Positive Obligations of the State under the European Convention on Human Rights,* London, 2012.

7.6.2 Artikler

Blandhol, Tøssebro og Skotheim (2015)	Blandhol, Sverre, Tøssebro, Henriette N. & Skotheim, Øystein, 2015. Innføring i juridisk metode. *Jussens Venner*, (06), pp.310–345. (Sitert fra Idunn).
Lavrysen (2018)	Lavrysen, Laurens. Causation and Positive Obligations under the European Convention on Human Rights: A Reply to Vladislava Stoyanova. *Human Rights Law Review*, 18(4), pp.705–718. 2018. https://doi-org.pva.uib.no/10.1093/hrlr/ngy027
McBride (1999)	McBride, Jeremy, 1999. Protecting life: a positive obligation to help. *European Law Review*, 24, pp.43–54.
Skoghøy (2011)	Skoghøy, Jens Edvin A. 2011. Nasjonal skjønnsmargin etter EMK. *Lov og Rett*, (04), pp.189–190. (Sitert fra Idunn).
Stoyanova (2018)	Stoyanova, Vladislava. Causation between State Omission and Harm within the Framework of Positive Obligations Under the ECHR. *Human Rights Law Review*, 18(2), pp.Human Rights Law Review, 2018, Vol.18(2). http://dx.doi.org/10.2139/ssrn.3001446
Tzanou (2013)	Tzanou, Maria. *"Is Data Protection the same as Privacy? An Analysis of Telecommunications Metadata Retention Measures", Journal of Internet Law, vol. 17, no. 3, pp. 21-34.* 2013. https://search-proquest-com.pva.uib.no/docview/1432699544?accountid=8579

7.7 Offentlige dokumenter og rapporter

Dokument 16 (2015-2016)	Dokument 16 (2015-2016), *Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-Utvalget)*. 29.02.2016. https://www.stortinget.no/globalassets/pdf/dokumentserien/2015-2016/dok16-201516.pdf

Lysne II-utvalget (2016) Lysne II-utvalget. *Digitalt Grenseforsvar (DGF).* 26.08.2016 https://www.regjeringen.no/contentassets/ca1f705dbebd48cb9a61889d4cfee6bf/digitalt-grenseforsvar-lysne-ii-utvalget.pdf

Mayer, Mutchler, Mitchell (2016) Mayer, J., Mutchler, P. & Mitchell, J., 2016. Evaluating the privacy properties of telephone metadata. *Proceedings of the National Academy of Sciences of the United States of America*,p.5536. https://doi.org/10.1073/pnas.1508081113