

FORSVARSDEPARTEMENTET
Postboks 8126 DEP
0032 OSLO

Deres referanse
2016/2773-5/FD
II/HVA

Vår referanse
18/03707-2/JHN

Dato
06.02.2019

Høringsuttalelse fra Datatilsynet - Forslag til ny lov om etterretningstjenesten

Datatilsynet viser til høringsnotat fra Forsvarsdepartementet datert 12.11.2018 om forslag til ny lov om Etterretningstjenesten.

Datatilsynet støtter i utgangspunktet forslaget om at det gis en særskilt lov om behandling av personopplysninger på dette området, men vi har mange spørsmål og merknader.

Datatilsynet mener at metoden «tilrettelagt innhenting», tidligere omtalt som digitalt grenseforsvar, er altfor inngripende og ikke bør innføres. Det er et for stort inngrep i retten til privatliv. Slik ordningen er foreslått og skissert er den heller ikke i tråd med våre menneskerettslige forpliktelser.

Siden lovforslaget er svært omfattende har vi i vårt arbeid med lovforslaget lagt vekt på den delen av forslaget som omhandler overvåking av elektronisk kommunikasjon gjennom tilrettelagt innhenting. Vi vil imidlertid også kommentere enkelte andre sider av forslaget. Vi tar forbehold om at det kan være sider ved forslaget som vi ikke er enige i, men som vi på grunn av kapasitetshensyn og den svært korte høringsfristen ikke har hatt mulighet til å gå inn i.

Datatilsynet fører som kjent ikke kontroll med Etterretningstjenesten. Vi har vurdert lovforslaget i egenskap av vår ombudsrolle, hvor en av våre oppgaver er å identifisere farer for personvernet i samfunnet, og å gi råd om hvordan farene kan unngås eller begrenses.

Vårt hørings svar er ganske omfattende, og vi har derfor innledningsvis i vårt svar laget et sammendrag over våre synspunkter og anbefalinger.

Vedlagt er vår høringsuttalelse til forslag om ny lov om etterretningstjenesten.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Jan Henrik Nielsen
seniorrådgiver

Høringsuttalelse fra Datatilsynet – forslag til ny lov om Etterretningstjenesten

1 Sammendrag av Datatilsynets merknader til lovforslaget

“a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it”

Den Europeiske menneskerettighetsdomstolen, 29. Juni 2006, no. 54934/00, para. 106

Datatilsynet er imot digital masseovervåking gjennom «tilrettelagt innhenting»

Datatilsynet støtter i utgangspunktet forslaget om at det gis en særskilt lov om behandling av personopplysninger på dette området.

Når det gjelder metoden «Tilrettelagt innhenting», tidligere omtalt som digitalt grenseforsvar, mener vi det ikke bør innføres.

Personvern og retten til privatliv er en grunnleggende forutsetning for et demokratisk samfunn. Selv om Etterretningstjenestens arbeid er rettet mot utenlandske trusler, vil tiltaket ramme de fleste brukere av telefoni og internett i Norge. Tiltaket innebærer i praksis overvåking av oss alle. Det er et altfor stort inngrep i retten til privatliv og det vil også rkke ved vårt demokratiske fundament

Overvåking vil for de fleste gi en følelse av ubehag. En åpenbar konsekvens av overvåking er at det har en nedkjølende effekt på ytringsfriheten fordi muligheten for å bli overvåket og usikkerheten hos borgerne vil medføre at mange vegrer seg for å kommunisere og innhente informasjon.

Overvåking av privat kommunikasjon er altså ikke bare et spørsmål om personvern i snever forstand. Det er også et spørsmål om maktforholdet mellom innbygger og stat, og om vilkårene for utvikling av meninger og perspektiver som utfordrer det bestående i et demokrati.

Departementet omtaler nedkjølingseffekt i høringsnotatet, men vi oppfatter at det uttrykkes tvil om nedkjølingseffekten er reell, blant annet ved å stille spørsmål ved forskningen som gjelder denne problematikken. Det er det ingen grunn til, nedkjølingseffekten har blitt påvist i en rekke studier og lagt til grunn av både EU-domstolen og Den europeiske menneskerettighetsdomstolen (EMD).

Et viktig aspekt, som det er helt nødvendig at regjering og Storting tar inn i vurderingen av dette lovforslaget, er at metoden tilrettelagt innhenting med stor sannsynlighet bli langt mer inngripende enn det regjering og Storting i denne omgang skal ta stilling til. Kombinasjonen

av de enorme mengdene data, en stadig utvikling av søkemetoder og kunstig intelligens gjør potensialet for formålsutglidning stort.

Vi mener at Regjeringen og Stortinget ved å innføre dette regimet vil krysse en prinsipiell linje som ikke bør krysses. Vår klare anbefaling er derfor at regjeringen ikke går videre med forslaget.

Lovforslaget er ikke i tråd med våre menneskerettslige forpliktelser

Vi mener at lovforslaget ikke er i tråd med våre menneskerettslige forpliktelser, og at det derfor ikke kan vedtas i sin nåværende form.

Ifølge Den europeiske menneskerettskonvensjonen (EMK) art. 8 må et inngrep være i *samsvar med loven og nødvendig i et demokratisk samfunn*. EMD har etablert en rekke minimumskrav som må være oppfylt for at bulkinnhenting av kommunikasjonsdata skal være i tråd med menneskerettighetene. Etter vårt syn fyller ikke lovforslaget disse kravene.

Vi mener forslaget utgjør et mye større inngrep i norske borgerens privatliv enn det departementet gir uttrykk for, og at det vil innebære et skadepotensiale for vårt demokratiske samfunn.

På grunn av vag begrepsbruk i lovforslaget, samt uklarheter om hvem som omfattes av tilretteleggingsplikten, rekkevidden av forpliktelsen til dekryptering, og effekten av filtrene, er det stor usikkerhet knyttet til hvem som faktisk rammes og hva slags opplysninger som vil bli innhentet. Kravet om klarhet i lov gjør seg enda sterkere gjeldene i en lov om etterretningen fordi praktisering av loven vil i stor grad (nødvendigvis) være hemmelig. Vi mener at kravet til klarhet og forutberegnelighet ikke kan sies å være oppfylt.

Etter vårt syn er heller ikke kravet om at systemet i sin helhet må anses som proporsjonalt og «nødvendig i et demokratisk samfunn» oppfylt. For at et lovforslag kan anses som proporsjonalt, må det vurderes hvorvidt den skaden som inngrepet kan medføre blir begrenset ved egnede tiltak som reduserer virkningen av skaden.

Hvorvidt proporsjonalitetskravet er oppfylt beror på en vurdering av hvorvidt systemet i sin helhet er omfattet av nødvendige garantier mot misbruk, og garanterer effektive rettsmidler. Kontrollsystemet ved forutgående domstolskontroll, løpende kontroll og etterkontroll må altså ses i sammenheng. En samlet vurdering av alle disse mekanismene må tilfredsstillende kravene i EMK art. 8 og 13.

Forhåndskontroll ved domstolsprøving vil sannsynligvis være lite reell på grunn av manglende etterretningsfaglige kunnskaper hos dommerne som skal overprøve Etterretningstjenestens vurderinger og på grunn av den vide oppgavebeskrivelsen til Etterretningstjenesten.

Vi er bekymret for at den løpende kontrollen, omtalt i forslaget som «styrket kontroll», vil bli lite effektiv, siden det ikke bevilges nok ressurser til EOS-utvalget. I tillegg er det ikke foreslått tekniske løsninger for å gjøre kontrollen mer praktisk gjennomførbart.

Når det gjelder kontroll i etterkant, gjør de samme bekymringen om manglende ressurser seg gjeldende. I tillegg er det problematisk at EOS-utvalget ikke har vedtakskompetanse. Dette er særlig en svakhet når det gjelder klagemekanismen, som allerede er svak på grunn av fritaket fra kravet om underretning til de som har vært gjenstand for urett.

Muligheten for oppreisning vil i praksis være fraværende siden EOS-utvalget bare vil kunne uttale seg med en anbefaling. Domstolsprøvingen vil være begrenset på grunn av dagens bevisforbud. Dette betyr at hverken hver for seg, eller sett i sammenheng, vil klagemuligheten til EOS-utvalget og domstolsprøving utgjøre et effektivt rettsmiddel etter EMK art. 13

Når man tar alt dette i betraktning, er det vanskelig å se at kontrollmekanismene, i sin helhet, er gode nok til å motvirke misbruk. Konsekvensen av dette er at forslaget ikke er i tråd med våre internasjonale forpliktelser.

Selv om kontrollmekanismen hadde vært innrettet på en måte som kunne anses som robust nok til å motvirke de negative konsekvensene ved innføring av et slikt system, kreves det at det må foretas en avveining mellom *samfunnets/statens interesse* og *inngrepet* i retten til privatliv. Det må derfor vurderes både fordeler og ulemper ved tiltaket i et større samfunnsperspektiv. Forslaget mangler tilstrekkelig kartlegging og vurdering av alle samfunnsmessige fordeler og ulemper.

Dette vil gjøre det vanskelig for regjeringen og Stortinget å ta stilling til om forslaget er proporsjonalt, slik EMK krever at de skal gjøre.

Sammenlignet med forslaget i Lysne II-rapporten er dette lovforslaget et enda større inngrep og har svakere kontrollmekanismer. Lysne II antydte at selv små endringer i deres forslag ville føre til at tiltaket ikke lenger ville være i tråd med menneskerettighetene.

På bakgrunn av det overnevnte mener vi det er klart at dette forslaget ikke er i tråd med våre menneskerettslige forpliktelser.

Regjeringen bør avvente Personvernkommisjonens arbeid

Vi mener at departementet i høringsnotatet bruker uforholdsmessig mye plass på å prøve å overbevise om at tiltaket er innenfor de rettslige rammene oppstilt av Menneskerettighetsdomstolen og altfor lite på å gjøre rede for de samfunnsmessige konsekvensene av forslaget.

Vi mener det er svært viktig å se på konsekvensene av forslaget for samfunnet som helhet. Det er lite spor i høringsnotatet av at slike vurderinger er gjort. Kapittelet om «samfunnsmessige konsekvenser» utgjør en halv side, i et høringsnotat på til sammen 395 sider.

Konsekvensene dette forslaget vil kunne ha for samfunnet som helhet er det naturlig å belyse i arbeidet som den planlagte Personvernkommisjonen skal gjøre. Det er derfor svært uheldig at departementet har kommet med sitt lovforslag før kommisjonen har ferdigstilt sitt arbeid.

Et uklart lovforslag, en altfor kort høringsfrist og det vi opplever som en generell bagatellisering av konsekvensene av forslaget fra departementets side, gjør at det sannsynligvis vil bli vanskelig å oppnå den samfunnsdebatten som dette forslaget trenger.

Vi frykter at verken befolkningen eller Stortinget blir gjort i stand til å forstå fullt ut hva som er i ferd med å skje før loven er innført. Dette er høyst problematisk.

Våre anbefalinger dersom regjeringen går videre med lovforslaget

Vår klare anbefaling er, som det fremgår ovenfor, er at regjeringen ikke går videre med lovforslaget om tilrettelagt innhenting. Dersom regjeringen likevel velger å gjøre det, har vi en rekke anbefalinger.

Samfunnsmessige konsekvenser må utredes

- De samfunnsmessige konsekvensene av forslaget må utredes, herunder må det vurderes mer omfattende hvordan forslaget vil påvirke eller endre vårt demokratiske samfunn
- Innføring av lovforslaget bør avvende personvernkommisjonens arbeid
- Innføring av forslaget må ikke forhastes, det må være tid og rom for opplyste og prinsipielle samfunnsdebatter
- Regjeringen bør i sitt videre arbeid med lovforslaget i langt større grad erkjenne at dette er overvåking av befolkningen og være åpen i sin kommunikasjon
- Regjeringen bør i større grad anerkjenne nedkjølingseffekten og faren for formålsutglidning
- Det bør besluttes at loven skal evalueres etter 1 år, og senere med regelmessige intervaller. Det må utarbeides parametere for å vurdere effektiviteten av «tilrettelagt innhenting»

Omfanget av inngrepet må begrenses

- Lovforslagene om territoriell begrensnig og filtrering bør klargjøres slik at det blir tydeligere hvem som er berørt av loven
- Tilretteleggingsplikten må klargjøres og det må avklares hvilken plikt tilbyderne har til å oppheve kryptering. Ordenene «eller lignende kryptering» i § 7-2 d må strykes
- Stortingsrepresentanter bør inkluderes i kategorien av særskilte yrkesutøvere. Terskelen for når det kan behandle slik informasjon bør også være langt høyere enn det som er foreslått
- Reglene for personopplysninger i kapitel 9 må gis anvendelse for registre som omhandler innhenting av opplysninger fra åpne kilder, jf. § 4-1 og 4-2
- Begrepene «tilrettelagt innhenting» og «innhenting av rådata i bulk» bør endres slik at de reflekterer hva som faktisk skjer
- Definisjonen av personopplysninger i § 1-4 nr. 11 må endres slik at den sammenfaller med personvernforordningen, og tolkningen av den må klargjøres

Adgangen til å dele informasjon må spesifiseres bedre

- Reglene for deling av informasjon gjennom internasjonalt samarbeid bør inkludere en momentliste, for eksempel krav til vurdering av mottakerstatens demokratiske kontroll av tjenesten, etterlevelsen av menneskerettigheter i landet det skal samarbeides med, tjenestens profesjonalitet og pålitelighet, lovpålagte oppgaver og kompetanse, inklusiv kontrollmekanismer, og måten personopplysninger behandles og beskyttes på
- Bestemmelsen om unntak fra taushetsplikt for offentlige bør tas ut

Kontrollmekanismene må forbedres

- Lovforslagets rettsikkerhetsmekanismer bør ikke skille mellom metadata og innholdsdata
- Det bør innføres en ordning med forhåndsgodkjenning for behandling av opplysninger om særskilte yrkesutøvere
- Det må stilles ytterligere krav til innholdet av begjæring og kjennelse under domstolskontrollen. Blant annet bør det stilles krav om hvilke signaler/kilder/tilbydere man behøver adgang til, søkebegrep eller kategorier av søkebegrep, en vurdering av om innhenting kan foretas på en mindre inngripende måten og om søket antas å gi informasjon som er av klart større verdi enn den integritetskrenkelse inngrepet er
- Innhenting av rådata i bulk bør underlegges de samme rettsikkerhetsmekanismer som tilrettelagt innhenting
- Det bør innføres en klageordning for tilbyderne som pålegges tilretteleggingsplikt.
- Det innføres en spesifisert rapporteringsplikt for Etterretningstjenesten som ledd i løpende kontroll
- Det må innføres en varslingshjemmel i loven og sikre varslingsmekanismer direkte til EOS-utvalget
- Loven bør pålegge en plikt til å innføre automatiserte mekanismer for å gjøre internkontroll og løpende kontroll enklere
- EOS-utvalget må gis kompetanse til å fatte bindende vedtak om stans, sletting og oppreisning
- Det bør innta en plikt til å underrette registrerte som har vært gjenstand for informasjonsinnhenting i strid med loven, med nødvendige unntak
- Det må bevilges betydelig mer ressurser til kontrollorganet som skal føre løpende kontroll
- Vi anbefaler at det igangsettes et arbeid med sikte på å foreta en helhetlig gjennomgang og vurdering av kontrollmekanismen, slik at kvaliteten i kontrollmekanismen øker i takt med utvidelsen av etterretningstjenesters oppgaver

Personvernprinsipper må innebygges

- Krav til kontinuerlig vurdering av personvernkonsekvenser og innebygget personvern bør inntas i loven
- Åpenhet er et viktig personvernprinsipp. Etterretningstjenesten bør i større grad etterstrebe å implementere dette prinsippet i sitt arbeid og kommunikasjon til allmenheten. Dette vil ivareta samfunnets tillit i tjenesten.
- Personvernrådgiver bør endres til personvernombud og det bør stilles krav til ressurser

Innhold

1	Sammendrag av Datatilsynets merknader til lovforslaget	1
2	Vår forståelse av lovforslaget om ny lov om etterretningen	9
2.1	Innledning	9
2.2	Ny lov om Etterretningstjenesten	9
2.3	Hva er «tilrettelagt innhenting»?	10
2.4	Hva er «midtpunktinnhenting» og «rådata i bulk»?	12
2.5	Den foreslåtte kontrollmekanismen	12
3	Personvern og retten til privatliv er grunnleggende forutsetninger for demokratiet	13
4	Forslaget om tilrettelagt innhenting er et vesentlig inngrep i borgernes privatliv og vårt demokratiske samfunn	14
4.1	Innledning	14
4.2	Forslaget om tilrettelagt innhenting må anses som overvåking	15
4.3	Nedkjølingseffekten	17
4.3.1	Nedkjølingseffekt for særlige yrkesutøvere og på særskilte samfunnsområder	21
4.4	Formålsutglidning må påregnes	22
5	Rettslige rammer for forslaget	24
5.1	Innledning	24
5.2	Den europeiske menneskerettskonvensjonen (EMK) art. 8	24
5.3	Praksis fra EU-domstolen	26
5.4	Personopplysningsvern	27
6	Kravet til klarhet i loven	28
6.1	Innledning	28
6.2	Territoriell begrensning	29
6.3	Hva slags data kan innhentes? Forskjellen på metadata og innholdsdata	29
6.4	Hvem blir det behandlet opplysninger om?	31
6.4.1	Nærmere om personselektorer	31
6.4.2	Nærmere om modusselektorer	32
6.4.3	Lovbestemmelse om filtrering	33
6.5	Omfanget av tilretteleggingsplikten er uklar	33
6.5.1	Omfatter tilretteleggingsplikten lag 2-kryptering?	34
6.6	Lovforslaget oppfyller ikke kravet til klarhet	35
7	Prosedyrene for behandling av personopplysninger	35
7.1	Innledning	35
7.2	Personopplysningsbegrepet	35

7.3	Behandling av fortrolig kommunikasjon med særlige yrkesutøvere	37
8	Krav til klare regler for utlevering av data.....	37
8.1	Innledning.....	37
8.2	Nasjonal informasjonsdeling	38
8.3	Internasjonal informasjonsdeling.....	38
8.4	Utlevering fra offentlige myndigheter til Etterretningstjenesten	39
9	Forhåndskontroll ved domstolsprøving	39
9.1	Innledning.....	39
9.2	Forhåndskontroll- ingen reell prøving av at vilkårene er oppfylt.....	40
9.3	Begrenset forhåndskontroll.....	41
9.4	Datatilsynets samlede syn på kontrollmekanismen forhåndskontroll.....	42
10	Kontrollmekanismer	43
10.1	Innledning.....	43
10.2	Løpende kontroll gjennom «styrket kontroll»	43
10.3	Etterkontroll	45
10.4	Nærmere om EOS-utvalget- uavhengighet og ressurser	46
10.4.1	Utvalgets uavhengighet.....	46
10.4.2	Utvalgets ressurser	46
11	Klagemulighet og mulighet for oppreisning.....	47
11.1	Innledning.....	47
11.2	Manglende underretning til de berørte	48
11.3	EOS-utvalgets behandling av klager fra individer.....	50
11.4	Domstolsprøving	51
11.5	Behov for grundigere vurdering av kontrollmekanismen	52
12	Proporsjonalitetsvurderingen	54
13	Lovforslaget om «tilrettelagt innhenting» bør ikke vedtas.....	56
14	Andre merknader	57
14.1	Krav til utredning av personvernkonsekvenser og krav til innebygget personvern.....	57
14.2	Krav til personvernrådgiver	58
14.3	Varslingskanal.....	59

2 Vår forståelse av lovforslaget om ny lov om etterretningen

2.1 Innledning

Høringsnotatet om ny lov om Etterretningstjenesten, inkludert forslag om tilrettelagt innhenting, er svært omfattende og krevende å sette seg inn. Vi har derfor valgt å ta inn i vårt høringssvar en beskrivelse av hvordan vi forstår forslaget om «tilrettelagt innhenting» og hva vi oppfatter at «midtpunktinnhenting» og «rådata i bulk» er.

Dette kan kanskje være nyttig for andre aktører som skal sette seg inn i forslaget, samtidig som det gjør det tydelig under hvilke forutsetninger vi har gitt våre merknader. Først vil vi si noe kort om lovforslaget i sin helhet.

2.2 Ny lov om Etterretningstjenesten

Forsvarsdepartementet mener at det er behov for en gjennomgang av gjeldende lov fra 1998, og foreslår en helt ny lov om Etterretningstjenesten. Dette er blant annet basert på anmodningsvedtak fra Stortinget, på bakgrunn av melding fra EOS-utvalget til Stortinget om rettsgrunnlaget for Etterretningstjenestens overvåkingsvirksomhet. Loven er ikke ment å endre Etterretningstjenestens oppgaver eller samfunnsoppdrag, men skal sørge for at disse har en sikker rettslig forankring, særlig med hensyn til rettsutviklingen innen menneskerettigheter og personvern.

Departementet skriver at lovforslaget i stor utstrekning kodifiserer gjeldende regelverk og praksis, men det er også noen nyvinninger. Den metodebruken som etterretningen benytter, og som innebærer et inngrep overfor enkeltpersoner, er foreslått lovfestet. Loven skiller mellom innhenting av informasjon, og den videre behandlingen av (person)opplysningene. Loven oppstiller grunnvilkår for innhenting, og nærmere vilkår for de ulike metodene som etterretningen benytter.

Loven er ment å regulere uttømmende hva som er etterretningens oppgaver, i tillegg til at den gir regler om organisering, styring og kontroll, mv. Det foreslås også regler om behandling av personopplysninger, tilpasset etterretningens virksomhet. Per i dag gjelder lov om behandling av personopplysninger (personopplysningsloven) av 2000, som er en overgangsordning i påvente av ny lov om etterretningen. Ny personvernforordning (GDPR)¹, gjennomført i Norge gjennom personopplysningsloven av 2018, gjelder ikke for behandling av personopplysninger som skjer i nasjonal sikkerhets øyemed.

Det som er helt nytt i loven er at det foreslås å gi etterretningen «tilrettelagt tilgang til grenseoverskridende elektronisk kommunikasjon», omtalt som «tilrettelagt innhenting» og tidligere omtalt som «Digitalt grenseforsvar».

Dette gir etterretningen hjemmel til å lagre metadata om elektronisk kommunikasjon som passerer landegrensen, se nærmere om denne metoden nedenfor. Loven legger også til rette for innhenting av informasjon gjennom elektronisk kommunikasjon på andre måter

¹ [EUROPAPARLAMENTS- OG RÅDSFORORDNING \(EU\) 2016/679](#) av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning).

enn gjennom «tilrettelagt innhenting». Dette omtales om «midtpunktinnhenting», og er ikke underlagt særreglene om «tilrettelagt innhenting».

2.3 Hva er «tilrettelagt innhenting»?

Tilrettelagt innhenting er, ifølge lovforslaget, «innhenting av elektronisk kommunikasjon som transporteres over den norske landegrense». Hovedformålet med tilrettelagt innhenting er at Etterretningstjenesten skal kunne gjøre søk i de lagrede dataene som er hentet inn.

Etterretningstjenestens tilgang til grenseoverskridende elektronisk kommunikasjon starter med tilretteleggingsplikten. Denne plikten innebærer at tilbydere av kommunikasjons- og meldingstjenester skal legge til rette for at Etterretningstjenesten kan installere teknisk utstyr på steder som kontrolleres av tilbyderne. Gjennom dette utstyret vil Etterretningstjenesten få speilet ut all kommunikasjon som passerer landegrensene.

Tilretteleggingsplikten vil gjelde for alle som regnes som tilbydere etter definisjonen i lov om elektronisk kommunikasjon (ekomloven) §1-5 nr. 16, for eksempel teleoperatører. I tillegg vil den gjelde for tilbydere av innholdstjenester som ikke er omfattet av denne definisjonen, såkalte «over the top-tjenester» (OTT-tjenester). OTT-tjenester er tjenester som leveres på toppen av et internettbasert kommunikasjonsnett, for eksempel ulike eposttjenester og Facebook Messenger. Tilretteleggingsplikten inkluderer også en plikt til å sørge for tilgang til kommunikasjon uten hinder av linkkryptering eller liknende kryptering.

Selv om Etterretningstjenestens arbeid er rettet mot utenlandske trusler, så vil tiltaket i praksis omfatte de fleste norske brukere av telefoni og internett. Grunnen til det er at norsk trafikk går inn og ut av landet gjennom kabler som krysser landegrensen, selv om kommunikasjonen er mellom personer som begge oppholder seg i Norge.

Den speilede kommunikasjonen vil deretter passere gjennom ulike filtreringsmekanismer, som best mulig skal hindre at det samles inn og lagres data som faller utenfor Etterretningstjenestens ansvarsområde. Det mest åpenbare tilfellet er kommunikasjon mellom en avsender og mottaker som befinner seg i Norge. I høringsnotatet nevnes norske telefonnumre som et mulig filtreringsparameter.

En utfordring er at mye av dagens internettbaserte kommunikasjon skjer uten bruk av slike avgrensede identifikatorer. Det fremgår av høringsnotatet, pkt 11.14.3, som at det er «ikke til å komme ifra at det vil lagres ikke ubetydelige mengder metadata om kommunikasjon mellom norske borgere».

Filtreringssystemet vil bestå av tre filtre:

Filter 1

Filteret har som oppgave å redusere mengden av data som flyter inn i systemet. Dette kan være kommunikasjon som ikke er relevant for Etterretningstjenesten, for eksempel trafikk fra store strømmetjenester. Filtrering vil i stor grad skje gjennom negativ filtrering, ved at det identifiseres hva som skal filtreres bort. Nye kommunikasjonsformer som ikke tidligere er identifisert, vil slippe gjennom dette filteret.

Filter 2

Filteret har som oppgave å filtrere bort alle innholdsdata. For å hindre at det lagres innholdsdata, skal Etterretningstjenesten opprette og vedlikeholde en liste som spesifiserer hvilke typer data som regnes som metadata. Filteret skal også i størst mulig grad filtrere ut metadata som ligger utenfor Etterretningstjenestens område, for eksempel norsk-norsk kommunikasjon.

Filter 3

Filteret har som oppgave å slippe gjennom innholdsdata knyttet til spesifiserte objekter som er godkjent av domstolen.

Systemet vil bestå av tre forskjellige datalager:

Korttidslageret

Lageret skal inneholde korte tidsintervaller med ufiltrert kommunikasjon, og dataene vil dermed ikke passere noen av filtrene som er nevnt over. Lageret vil inneholde både metadata og innholdsdata, men avviker fra de andre lagrene ved at det utelukkende kan benyttes for teknisk understøttelse. Dette er spesifisert i lovutkastets² § 7-6:

«Testinnhenting og testanalyser skal aldri benyttes for etterretningsformål, men utelukkende for teknisk å muliggjøre utvalg, filtrering, lagring og søk i lagrede data, reprosessering av data, forståelse av signalmiljø og gjenkjenning av tjenester og dataformater».

Et uttrekk av ufiltrert kommunikasjon skal ikke overstige 30 sekunder, og det kan maksimalt gjøres uttrekk en gang per time.

Metadatalageret

Dette lageret er den mest sentrale komponenten i den foreslåtte løsningen, og data vil lagres her etter å ha passert filter 2. Metadata er i lovutkastet § 7-7 andre ledd definert som «data som beskriver annen data eller som inneholder ekstra informasjon knyttet til data», for eksempel informasjon om avsender, mottaker, tidspunkt og lokasjon. Lageret vil inneholde 18 måneder med kommunikasjon som passerer landegrensen.

Søk i metadatalageret vil kreve rettens godkjenning, jf. lovforslagets kapittel 8, og skal baseres på en såkalt *personselektor* eller en *modusselektor*, jf. § 7-8. Typiske personselektorer er telefonnumre, epostadresser og identiteter knyttet til ulike meldingstjenester.

En modusselektor er i § 1-4 nr. 7 definert som «et søkebegrep eller søkestreng som beskriver et bestemt mønster eller avgrensning, herunder handlingsmønster eller geografisk område». Høringsnotatet går ikke i detalj på hvordan en modusselektor typisk vil bli utformet. Det er heller ikke beskrevet hvordan et søk vil innrettes rent teknisk eller hvilke verktøy eller teknologier som vil bli brukt.

Innholdslageret

Lageret vil inneholde innholdsdata med tilhørende metadata, og data vil lagres her etter å ha

² Alle lovhenvisninger hvor lov ikke er angitt viser til forslaget vedlagt høringsnotat om ny lov om Etterretningstjenesten.

passert Filter 3. Dette skal være målrettet mot spesifisert objekt, jf. § 7-9, og lagring skal kun skje etter godkjenning fra domstolen.

2.4 Hva er «midtpunktinnhenting» og «rådata i bulk»?

I tillegg til «tilrettelagt innhenting», gir lovforslaget hjemmel for innhenting av elektronisk kommunikasjon ved såkalt midtpunktinnhenting. I lovforslaget er midtpunktinnhenting forklart som «innhenting av elektronisk kommunikasjon og kartlegging av kommunikasjonsinfrastruktur». Lovforslaget gir også hjemmel for å innhente rådata i bulk «når det er nødvendig for å få tilgang til et relevant og tilstrekkelig informasjonsgrunnlag i den hensikt å gjennomføre målsøking eller målrettet innhenting i dette informasjonsgrunnlaget».

Innhenting av rådata i bulk innebærer en ufiltrert innsamling av både innholdsdata og metadata fra det som er omtalt som generelle datastrømmer, blant annet overvåking av satellittkommunikasjon. Datatilsynet forstår dette som den innhenting av informasjon som er omtalt i en rekke artikler om manglende lovhjemmel for innhenting av satellittkommunikasjon³, og i EOS-utvalgets særskilte melding til Stortinget om rettsgrunnlaget for Etterretningstjenestens overvåkingsvirksomhet.⁴ Dette er altså en metode som benyttes i dag.

Midtpunktinnhenting vil i hovedsak inneholde informasjon om utenlandske forhold, men det er i forslaget opplyst at det også vil innhentes opplysninger om norske borgere i Norge. Innhenting er ikke omfattet av reglene om filtrering og vil innebære en lagring av informasjon i 15 år. Etterretningen vil være underlagt tilsyn fra EOS-utvalget.

2.5 Den foreslåtte kontrollmekanismen

Slik vi forstår det, er de to metodene «tilrettelagt innhenting» og «midtpunktinnhenting» i prinsippet like, men fordi førstnevnte metode vil innebære et større inngrep i personvernet er det underlagt særlige regler. Det fremgår av høringsnotatet pkt. 10.5.2:

«Innhenting av grenseoverskridende elektronisk kommunikasjon som transporteres over den norske landegrensen faller i utgangspunktet inn under metoden «midtpunktinnhenting». Denne tilgangen bør etter departementets syn underlegges særskilte lovreguleringer og autorisasjons- og kontrollmekanismer».

Kontrollregimet for tilrettelagt innhenting skal bestå av tre hovedkomponenter. Søk i lagrede metadata, og innhenting og lagring av innholdsdata vil kreve forutgående domstolskontroll ved Oslo tingrett. EOS-utvalget skal føre løpende kontroll gjennom såkalt «styrket kontroll». I denne forbindelse er det foreslått å styrke EOS-Utvalgets sekretariats ressurser med 4 årsverk. Søk som gjøres i materialet som blir innhentet gjennom rådata i bulk trenger ikke rettens kjennelse.

Videre skal EOS-utvalget, som i dag, føre etterkontroll og behandle eventuelle klager fra individer. I den forbindelse vil EOS-utvalget få kompetanse til å uttale seg om grunnlag for

³ NRK, "[Antennene som samler inn data om norske borgere](#)", Skille, Hansen, Døvik, Lied og Jansson, 01.03.2018

⁴ EOS-utvalget, Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste, [Særskilt melding til Stortinget om rettsgrunnlaget for Etterretningstjenestens overvåkingsvirksomhet](#), 17.06.2016

erstatningsansvar for det offentlige overfor klageren gjennom en endring i lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste(EOS-kontrollloven). Forslaget viderefører ellers i stor grad de eksisterende øvrige kontrollordninger.⁵

3 Personvern og retten til privatliv er grunnleggende forutsetninger for demokratiet

Retten til privatliv, ytringsfrihet og personvern er grunnleggende verdier som er nødvendige forutsetninger for et demokratisk samfunn

Personvern handler om ivaretagelse av den personlige integritet, herunder mulighet for privatliv, selvbestemmelse og selvutfoldelse. Personvern og retten til privatliv er en rett som blant annet begrenser offentlige myndigheters mulighet til å innhente og lagre visse former for informasjon om sine borgere.

Personvern er også viktig for å sikre felles goder i et demokratisk samfunn. Uten retten til å ha et privatliv vil det ikke være mulig for det enkelte menneske å skape seg et rom til å utvikle refleksjoner og vurderinger på et selvstendig grunnlag, uten å bli forstyrret eller kontrollert av andre.⁶

Den enkelte vil kunne oppleve et inngrep fra myndighetene i den private sfære som en svekkelse i maktbalansen mellom en selv som individ og omgivelsene. «Kunnskap er makt»⁷ er et allment akseptert uttrykk i samfunnsforskningen for å forstå maktforholdet mellom staten og borgerne. Det at staten har kunnskap om sine borgere kan virke disiplinerende og innebære at borgerne avstår fra lovlige aktiviteter de normalt ville ha foretatt seg⁸.

Et tiltak hvor store deler av borgernes kommunikasjon er gjenstand for lagring og søk innebærer at borgeren aldri fullt ut kjenner sitt publikum. Dette synet henter blant annet støtte fra sosiologiske teorier som sier at menneskers kommunikasjon med hverandre er kontekstuell, det vil si at hvem budskapet er ment for er avgjørende for form og innhold. Mennesker måler sitt publikum og tilpasser budskapet etter hvem som lytter. En utenforstående og potensiell "medlytter" endrer samhandlingens forutsetninger, også selv om samtalepartene "ikke har noe å skjule".⁹

Meningsdannelse skjer ikke bare i den offentlige debatt, den skjer også i den private sfære.

⁵ Høringsnotatet beskriver i kapittel 6.6 og 6.7 også de øvrige kontrollmekanismene som etterretningstjenesten er underlagt.

⁶ NOU 2009: 1 [Individ og integritet— Personvern i det digitale samfunnet](#), utredning fra Personvernkomisjonen

⁷ Begrepet som opprinnelig ble formulert av Francis Bacon har blitt benyttet av blant annet av Michel Foucault og har blitt benyttet i teorien om det panoptiske samfunnet.

⁸ Hannemyr, G. (2002) [Foucault i kyberrommet](#), I: Digital Makt, (Red., Tore Slaatta) Gyldendal Akademisk, Oslo, pp. 41-63.

⁹ SNL, [Erving Goffman](#) og den «dramaturgiske metaforen»

Den private sfære er derfor en viktig ressurs i et fungerende demokrati. Drøftelser rundt middagsbordet, mellom venner, kollegaer, studenter og i foreninger er med å forme den enkeltes politiske forståelse og engasjement. Ettersom stadig mer av samhandlingen i den private sfære flyttes over på elektroniske møteplasser, er det viktigere å verne om privatlivet i slike sammenhenger. Den private sfære er ofte et arnested for kritiske tanker, utvikling av holdninger og perspektiver som kan utfordre hva som der og da er alminnelig aksepter - på godt og vondt.

Om usikkerhet eller frykt for å bli overvåket påvirker hva som kommuniseres, vedrører det vilkårene for meningsdannelse i den private sfære. Overvåking av privat kommunikasjon er derfor ikke bare et spørsmål om personvern i snever forstand, som avgrenset til integritetskrenkelse på et individnivå. Det er også et spørsmål om maktforholdet mellom innbygger og stat, og om vilkårene for utvikling av normer og perspektiver som utfordrer det bestående i et demokrati. Frykten er at overvåkingstiltak kan legge en demper på noe som i ettertid viser seg å være viktig for samfunnets utvikling. Brudd på etablerte konvensjoner kan drive samfunnet fremover.

Vi lever våre liv på internett, og overvåking av internett vil kunne medføre at vi unngår å søke kunnskap eller delta i fellesskap fordi vi er usikre på hvordan vi blir oppfattet. Dette kan påvirke vår mulighet til å utvikle oss og kan begrense vår utfoldelse.

Overvåking vil for de fleste gi en følelse av ubehag. Dette kan begrense muligheten til å danne forhold til andre personer gjennom fortrolighet, samt at det gjør det mulig å utvikle oss som autonome individer. En forutsetning er at samfunnet gir rom og plass for at man kan velge å trekke seg tilbake og føle seg fri fra andres blikk.

4 Forslaget om tilrettelagt innhenting er et vesentlig inngrep i borgernes privatliv og vårt demokratiske samfunn

4.1 Innledning

Forslaget om tilrettelagt innhenting innebærer at det vil bli behandlet personopplysninger om nesten alle norske borgere uten hensyn til om de er mistenkt for, eller involvert i, aktiviteter som Etterretningstjenesten arbeider mot. Lagringen av personopplysninger baserer seg på en massiv innhenting av opplysninger om elektronisk kommunikasjon.

Selv om Etterretningstjenestens arbeid er rettet mot utenlandske trusler, vil tiltaket ramme de fleste brukere av telefoni og internett i Norge. Grunnen til det er at norsk datatrafikk går inn og ut av landet, uavhengig av om kommunikasjonen er mellom personer som begge oppholder seg i Norge.

Dette har sin bakgrunn i de IP-baserte kommunikasjonsplattformene, hvor personer og virksomheter i økende grad tar i bruk tjenester hvor den tekniske infrastrukturen befinner

seg utenfor Norge. Eksempler på dette er tjenester som Facebook Messenger, Gmail, Snapchat og andre typer nettbaserte tjenester som gjøres tilgjengelig via en skyplattform i utlandet. Mobiloperatørene har gått over fra vanlig tale og SMS til IP-baserte tjenester med etableringen av Rich Communication Services (RCS). Felles for disse tjenestene er at datatrafikken vil gå via servere i utlandet og fanges opp, selv når kommunikasjonen foregår mellom to personer i Norge.

Som nevnt over regulerer lovforslaget to former for innhenting av opplysninger fra elektronisk kommunikasjon, tilrettelagt innhenting og innhenting av rådata i bulk, gjennom det som i lovforslaget beskrives som midtpunktinnhenting. Til sammen åpner dette for en nærmest ubegrenset adgang til å innhente kommunikasjonsdata hvor det ikke er spesifisert tilstrekkelig klart i lovforslaget hvem som rammes.

Departementet slår i høringsnotatet fast det åpenbare, nemlig at lovforslaget om tilrettelagt innhenting innebærer et inngrep i retten til privatliv. Vi mener imidlertid at departementet ikke har beskrevet godt nok hvor omfattende inngrepet er, samt at de negative konsekvensene av forslaget underkommuniseres.

I det følgende vil vi beskrive nærmere hvorfor vi mener «tilrettelagt innhenting», er å anse som overvåking, gjøre rede for vårt syn på den potensielle nedkjølingseffekten forslaget vil ha og betydningen av faren for formålsutglidning.

4.2 Forslaget om tilrettelagt innhenting må anses som overvåking

I lovforslaget og høringsnotatet blir det brukt et språk som er egnet til å tilsløre hva forslaget innebærer. Begrepet «tilrettelagt innhenting» er uklart og ikke egnet til å beskrive hva som faktisk skjer. Begrepet «digitalt grenseforsvar», som ble brukt i Lysne II-utvalgets rapport¹⁰, var heller ikke treffende.

Det er ikke likegyldig hvilket språk som benyttes når et tiltak skal beskrives, og departementet bør forsøke å bruke et klart språk som gjør det mulig å forstå hva dette handler om.

Begrepet tilrettelagt innhenting er ikke definert i forslaget, men det må forstås som «innhenting av elektronisk kommunikasjon som transporteres over den norske landegrense» jf. lovutkastets § 7-1. Rent språklig så kan «tilrettelagt innhenting» oppfattes som en målrettet eller begrenset innhenting, mens det faktisk vil være en tilnærmet ubegrenset lagring av internettrafikk og telefoni. Dette begrepet burde i det minste vært definert i loven.

For å kunne ta stilling til hvor inngripende tiltaket er, er det nødvendig at det formidles klart hva som faktisk skjer, med vekt på hva som er viktig for borgerne å vite. I høringsnotatet pkt. 11.3 er det argumentert for en teknologinøytral betegnelse i loven, men det er ikke hvilken teknologi som er brukt, for eksempel om det er innhenting fra kabel eller satellitt, som er det mest sentrale. Det viktigste for å kunne vurdere inngrepets størrelse er hva slags informasjon som faktisk innhentes.

¹⁰ [Digitalt grenseforsvar \(DGF\)](#), Lysne II-utvalget, 26.08.2016

EMD bruker, blant annet i *Big Brother Watch and others v. UK*¹¹ begrepet, «bulk surveillance» som kan oversettes med masseovervåking.

I høringsnotatet pkt. 11.13.8.3 understreker departementet «at tilrettelagt innhenting etter forslaget ikke med rimelighet kan karakteriseres som «overvåking» av alle som befinner seg i Norge».

Det argumenteres med at materialet ligger uberørt med mindre en operatør aktivt søker etter «informasjonen og henter den ut av rådatamaterialet» og at personvern hensyn ikke gjør seg sterkt gjeldende.

Dette bygger på en uriktig forståelse av retten til personvern og hvilken betydning inngrepet i borgernes privatliv har for maktforholdet mellom stat og borger. Vi mener at den innhenting av informasjon som lovforslaget åpner for klart må anses som overvåking.

Inngrepet i personvernet oppstår allerede ved innhenting, som lovforslagets tilretteleggingsplikt legger til rette for. Det er i potensialet for myndighetsutøvelse og kontroll at inngrepet i personvernet oppstår. «Dette gjelder også i tilfeller der myndighetsutøvelse foreligger som en mulighet (som ikke nødvendigvis vil bli benyttet)»¹². Om det lagrede materiale senere blir gjenstand for viderebehandling, for eksempel ved søk, er det uten betydning for det at selve innhenting er et inngrep.¹³

Dette er også lagt til grunn av EMD i en rekke avgjørelser, blant annet *Leander v. Sweden*¹⁴ hvor lagringen av informasjon om Leanders privatliv i et hemmelig politiregister ble ansett som et inngrep i art. 8 om retten til privatliv.

I *Tele2/Watson*¹⁵-dommen påpeker EU-domstolen at selve lagringen av trafikk- og lokasjonsdata kan ha innvirkning på bruken av elektroniske kommunikasjonsmidler og på brukernes ytringsfrihet. Et annet perspektiv som kommer frem er følelsen av å være konstant overvåket.

«The fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance»¹⁶

Det avgjørende er altså at selve maktforskyvning skjer ved lagringen.

I rapporten *Datalagring og Menneskerettighetene*¹⁷ benyttes begrepet overvåking om datalagring. Det vises også til andre samfunnsområder hvor begrepet overvåket har fått

¹¹ ECHR, [Big Brother Watch and others v. The United Kingdom](#), no. 58170/13, 62322/14 og 24960/15, 13.09.2018

¹² "Overvåking i en rettsstat", *Wiese Schartum*, 2010, side 21.

¹³ "Putting Privacy to the Test: How Counter-Terrorism Technology is Challenging Article 8 of the European Convention on Human Rights", van der Hilst, 2013, s 62-64.

¹⁴ ECHR, [Leander v. Sweden](#), no. 9248/81, 26.03.1987

¹⁵ ECJ, *Tele2/Watson*, Joined Cases C-203/15 and C-698/15, European Court of Justice, 21.12.16, p. 101

¹⁶ ECJ, *Tele2/Watson*, Joined Cases C-203/15 and C-698/15, European Court of Justice, 21.12.16, p. 100

¹⁷ [Datalagring og menneskerettighetene](#), Utredning til Justisdepartementet og Samferdselsdepartementet, Petter Graver, Henning Harborg, 01.10.15

anvendelse. Dette har Høyesterett lagt til grunn i flere saker, blant annet i forbindelse med overvåkning i arbeidslivet. I Rt. 2013 s. 143¹⁸ avsnitt 56 sier førstvoterende:

«Som lagmannsretten understreker, vil kontrolltiltak ikke bare kunne være en ulempe for den som har noe å skjule, men også for den som ikke har noe å skjule. At generell overvåkning i arbeidslivet vil være en belastning, understrekes i NOU 2009:1 Individ og integritet side 22, hvor det heter:

«Personvernkommisjonen mener at det å bli overvåket i sitt daglige virke vil oppfattes som en belastning av de fleste. Dersom opplysningene som innhentes ved slik overvåkning i tillegg blir brukt til andre formål enn de opprinnelig var beregnet for, og andre formål enn dem man har fått informasjon om, øker dette belastningen og følelsen av overtramp mot den personlige integritet.»

Dette kan jeg på generelt grunnlag slutte meg til.»

Datatilsynet mener at det mest treffende begrepet å bruke om «tilrettelagt innhenting» er digital masseovervåkning.

For øvrig må det bemerkes at høringsnotatet er svært omfattende, noe som gjør det krevende å sette seg inn i lovforslaget. Det blir da særlig viktig at forslaget kommuniseres utad på en lett forståelig måte slik at alle gis mulighet til å sette seg inn i forslaget og ytre seg. Dette for å gi lovforslaget nødvendig legitimitet, slik at samfunnets tillit til Etterretningstjenesten opprettholdes.

Når forsvarsminister Frank Bakke-Jensen sier i en kronikk¹⁹ at Etterretningstjenesten ikke har lov til og heller ingen interesse av å følge vanlige folks aktiviteter på internett, så er det misvisende. Videre sies det: «Betyr dette at Etterretningstjenesten vil lese e-posten til vanlige norske borgere? Svaret er nei.» Dette er ikke nødvendigvis riktig.

Det er alarmerende at Forsvarsministeren allerede i høringen må gå ut å påpeke det selvsagte at Etterretningstjenesten ikke skal overvåke norske borgere, når man i realiteten ved innføring av det nye regimet med tilrettelagt innhenting, gjør Etterretningen i stand til å overvåke kommunikasjonen til hele den norske befolkningen.

Det er svært viktig at departementet legger til rette for en god samfunnsdebatt. Vi mener at det er problematisk at departementet i sin kommunikasjon omkring forslaget så langt har valgt å tone ned inngrepets størrelse og de konsekvensene inngrepet vil ha for samfunnet.²⁰

4.3 Nedkjølingseffekten

Majoriteten av Norges befolkning opplever å ikke være av interesse for Etterretningstjenesten. De fleste vil tenke at etterretningstiltak er rettet mot grupper de ikke tilhører eller har befatning med. Er tiltakene imidlertid ikke avgrenset til spesielle

¹⁸ Rt. 2013 s. 143

¹⁹ Adresseavisen, "[Feilslutning om digitalt grenseforsvar](#)", Bakke-Jensen, 23.11.2018

²⁰ Se f.eks. Aftenposten, «Frykter du overvåkingssamfunnet? Utkastet til ny e-lov bør berolige deg», Morten Haga Lunde, 05.02.2019.

målgrupper, men innebærer lagring av nesten all kommunikasjon som passerer et kommunikasjonsknutepunkt, endres denne forutsetningen.

Vil vissheten om at kommunikasjonen kan fanges opp av myndighetene påvirke hvem vi kommuniserer med, hva vi kommuniserer om, våre valg av ord og formuleringer og hvorvidt vi kommuniserer i det hele tatt? Og i så fall, vil en slik visshet påvirke adferden vår?

Datatilsynet tror svaret er ja. Vi er bekymret for at forslaget vil medføre en nedkjølingseffekt som begrenser ytringsfriheten, den offentlige samtalen og individets selvutfoldelse.

Nedkjølingseffekten innebærer at enkeltpersoner avstår fra å ytre noe de ellers ville gjort, eventuelt modifierer eller sensurerer egne ytringer, på grunn av frykten for eller kunnskapen om at ytringene overvåkes. Nedkjølingseffekt er en opplevelse eller følelse som oppstår hos den enkelte og som påvirker den enkeltes mulighet for utfoldelse.

Nedkjølingseffekten er noe alle har opplevd i forskjellige sammenhenger, på skolen eller i arbeidslivet, eller i møte med helsevesenet. Hvem som lytter og hvordan informasjonen blir behandlet påvirker hva vi ønsker å dele.

Sett i en større sammenheng får nedkjølingseffekten for den enkelte konsekvenser for hele samfunnet. Se kapittel 3 om dette.

Vi oppfatter at departementet i høringsnotatet trekker i tvil at nedkjølingseffekten faktisk finnes, blant annet ved å stille spørsmål ved forskning på nedkjølingseffekten. I høringsnotatets punkt 11.13.8.3 argumenteres det for at spørsmål om «vurderingen av en eventuell nedkjølingseffekt (må) ta utgangspunkt i et informert kunnskapsgrunnlag knyttet til hva Etterretningstjenesten lovlig kan og ikke kan gjøre.».

Vi mener det har noe begrenset betydning for nedkjølingseffekten hva etterretningen rent juridisk har lov til. Det at Norge krysser den grensen det innebærer å innføre dette tiltaket vil i seg selv vil få stor betydning for nedkjølingseffekten. Dette kan et stykke på vei avhjelpes ved klar lovgivning, men kan ikke unngås helt.

Så lenge det er uklart hva slags informasjon som innhentes og fra hvem og på hvilken måte, vil det kunne ha en nedkjølende effekt. Det sentrale poenget er at når borgere i praksis ikke kan være sikre på hvem som inkluderes i sitt publikum, vil mange ta sine forbehold. Både usikkerheten og realiteten vil kunne påvirke borgerens frimodighet.

På grunn av omfanget og usikkerheten omkring hvem som rammes vil vi i en verden hvor tanker, meninger og drømmer flyter fritt for den enkelte mellom skytjenester, mobiltelefoner, datamaskiner og sosiale medier kunne stå igjen med det som George Orwell sa i 1984: «Hvis du vil holde på en hemmelighet, så må du også gjemme den for deg selv.»

Nedkjølingseffekten har blitt påvist i en rekke studier og lagt til grunn av både EU-domstolen og EMD. Blant annet i *Goodwin v. UK*²¹, hvor det i høringsnotatet også er pekt på nedkjølingseffekten, og senest i *Big Brother Watch and others v. UK*²², hvor man fant at

²¹ ECHR, [Goodwin v. The United Kingdom](#), no. 17488/90, 27.03.1996

²² ECHR, [Big Brother Watch and others v. The United Kingdom](#), no. 58170/13, 62322/14 og 24960/15, 13.09.2018

bulkinnhenting var i strid med art. 10 om ytringsfrihet fordi, i lys av en potensiell nedkjølingseffekt på pressefriheten, så vil et inngrep i kommunikasjon mellom journalister og kilder kreve åpne mekanismer for kontroll av Etterretningstjenesten.

I Tele2/Watson²³-dommen påpeker EU-domstolen at selve lagringen av trafikk- og lokasjonsdata kan ha en innvirkning på bruken av elektroniske kommunikasjonsmidler og på brukernes ytringsfrihet.

Også Norsk Høyesterett har vist til nedkjølingseffekten blant annet i Rt. 2015 s. 2308²⁴ hvor spørsmålet var om kildevernet stod sterkere enn PSTs rett til beslag i upublisert materiale.

Man har også sett tegn til en nedkjølingseffekt etter Snowden-avsløringene.²⁵

Nedkjølingseffekten i tilknytning til overvåkning av kommunikasjonsdata er påvist i en rekke studier. En studie²⁶ viser hvordan søk i Wikipedia endret seg etter avsløringen av amerikanske myndigheters elektroniske overvåkning. En annen studie tar for seg hvordan minoriteters bruk av Facebook har endret seg²⁷. Vi viser også til rapport fra blant annet PEN²⁸ som påpeker hvordan klimaet for ytringer stadig blir dårligere.

I Fritt Ords rapport «Status for ytringsfriheten i Norge»²⁹ blir paradokset mellom den økte muligheten for deltakelse i den offentlige debatten, som har blitt mulig gjennom digitalisering, og myndighetenes mulighet for kontroll drøftet. Det påpekes i rapporten at det ligger et spesielt potensiale for nedkjøling ved innføring av masseovervåkning ved at informasjonstilgangen er så stor. Det konkluderes med:

«Mens den publisistiske friheten er blitt styrket, og nå i liten grad utgjør noen skranke for ytringsfriheten, er informasjonsfriheten blitt sterkt svekket gjennom endringer i retten til overvåkning av norske borgeres kommunikasjon. En mulig konsekvens av denne utviklingen er at pressens adgang til ulike former for informasjon svekkes, siden kilder vil vegre seg for å uttale seg, og at individer blir mer forsiktige med å ytre seg gjennom sosiale medier og i andre fora som registreres digitalt – en såkalt nedkjølingseffekt. Denne utviklingen gir oss en sterk påminnelse om at jussen i stor grad kan påvirke normer og adferd i bred forstand. Utviklingen minner oss også om en annen type spenning mellom frihet og regulering som ligger i digitaliseringen enn den vi for øvrig har diskutert i denne rapporten. På den ene siden gir digitaliseringen økt mulighet og frihet til ytring for individene. På den andre siden øker mulighetene for kontroll og overvåkning, både fra statlige og private aktører.»

Datatilsynet er spesielt bekymret for nedkjølingseffekten når det gjelder Etterretningstjenestens arbeid mot påvirkningsoperasjoner, valgpåvirkning, desinformasjon, jf. lovutkastets § 3-1 bokstav e «fremmede sabotasje- og påvirkningsoperasjoner».

²³ ECJ, Tele2/Watson, Joined Cases C-203/15 and C-698/15, European Court of Justice, 21.12.16, p. 101

²⁴ [Rt. 2015 s. 2308](#)

²⁵ [Personvern – Tilstand og trender 2014](#), Datatilsynet og Personvernrådet, Oslo, januar 2014

²⁶ Berkeley Technology Law Journal, Vol 31, Issue 1, Article 5, 06.01.2016 - Chilling Effects: Online Surveillance and Wikipedia Use by Jonathon W. Penney

²⁷ Journalism & Mass Communication Quarterly 1 –16, 2016 - Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring By Elizabeth Stoycheff

²⁸ Pen America 2014: [Global Chilling: The Impact of Mass Surveillance on International Writers](#)

²⁹ Fritt Ord, ["Status for ytringsfriheten i Norge"](#), 2014, ISBN trykt versjon: 978-82-7763-452-4

Eksempler på påvirkningsoperasjoner er at utenlandske krefter har forsøkt å påvirke utfallet av f.eks. amerikanske valg³⁰ og Brexit-avstemningen³¹. Det er også forskning som viser at påvirkningsoperasjoner som har til hensikt å forstyrre den offentlige samtalen ved å polarisere og minske tilliten til pressen. Dette har man sett i tilknytning til skepsisen mot vaksine³² og konkrete saker som forgiftningen av Skripal i Storbritannia³³.

Påvirkningsoperasjoner pågår i stor grad på sosiale medier. At Etterretningstjenesten skal bidra til å avdekke og motvirke dette, kan gi inntrykk av at Etterretningstjenesten vil følge med på politiske debatter i sosiale medier, noe som i seg selv kan føre til at nedkjølingseffekten forsterkes.

Dette er et område som er spesielt sårbart da ytring av politiske meninger må ha særlig vern, og det vil være de som har meninger som kan betraktes som ytterliggående som vil kunne være spesielt utsatt.

Det er de marginale som trenger vern. De som Jens Bjørneboe omtaler i sin hyllest til den franske forfatteren Jean Genet, Blomster for Genet (*Hommage à Jean Genet*)

I. CANTO

*Maria, alle smerters moder
Nevn vårt navn i dine bønner!
Vi er alle tornekronet
Vi er alle dine sønner!*

*Halliker og sodomitter
Blottere og transvestitter
Pederaster, fetisjister
Diktere og masochister
Drankere og morfinister –
Jomfru, alle smerters moder
Trøst Genet, vår stakkars
broder!*

Også han er tornekronet.

*Tyver, horer og Genet –
Vi som hang på begge sider
Av din sønn på smertens tre –
Vet hva Verdens Frelser lider.*

*Jomfrumoder, bare vi
Vet hva nådens kalk vil si:*

Kronens torner blir til roser.

Diktet forteller oss at også det stygge, frastøtende og kontroversielle kan i det lange løp bli til noe samfunnet anser som verdifullt og i dette ligger det vanskeligste i ytringsfriheten – vernet av meninger man ikke liker. Diktet kan også illustrere at samfunnets syn på hva som er riktig og galt forandrer seg på noen områder. I Kina har man forbudt Ole Brumm og bokstaven N³⁴, fordi bruk av dem kan innebære regimekritikk, og fra vår egen historie vet vi at selv en binders³⁵ kan inneholde et klart politisk budskap.

³⁰ CNN, "[Russian troll threat hasn't gone away as election day nears](#)", O'Sullivan, Sands, 20.10.2018

³¹ The Guardian, "[Russia used hundreds of fake accounts to tweet about Brexit, data shows](#)", Booth, Weaver, Hern, Smith, Walker, 14.11.2017

³² American Journal of Public Health, "[Weaponized Health Communication: Twitter Bots and Russian trolls Amplify the Vaccine Debate](#)" Broniatowski, M. Jamison, Qi SM, AlKulaib, Chen, Benton, Quinn, Dredze, 12.09.2018

³³ Washington Post, "[Agent of doubt](#)", Warrick, Troianovski, 10.12.2018,

³⁴ NYTimes, "China's Censors Ban Winnie the Pooh and the Letter 'N' After Xi's Power Grab", Javier C. Hernández, 28.02.2018

³⁵ Digitalskolen, Norsk motstand under andre verdenskrig, Individuell motstand, Historisk institutt, Universitetet i Bergen ved Olaug Engesæter

Nedkjølingseffekten er reell, men virkningen av den viser seg ikke nødvendigvis på kort sikt. Ved bruk av kvantitative metoder kan det påvises endringer på sosiale medier og begrensning av ytringer. Den totale negative effekten av nedkjøling for demokratiet er imidlertid vanskelig å påvise ved bruk av slike metoder. Som kjent er det mange land hvor ytringsfriheten er begrenset og dette har ført til svekket lovgivning, korrupte domstoler, indoktrinerende undervisning og en stilnet samfunnsdebatt.

4.3.1 Nedkjølingseffekt for særlige yrkesutøvere og på særskilte samfunnsområder

Nedkjølingseffekten vil kunne ramme sterkere i enkelte sektorer enn andre, for eksempel helse, politikk, journalistikk og forskning. I verste fall kan forslaget innebære at enkelte vil kunne vegre seg for å kontakte helsevesenet eller være tilstrekkelig åpne. I sin ytterste konsekvens vil nedkjølingseffekten kunne ødelegge den nødvendige tilliten som borgene må ha for at det store norske digitaliseringsprosjektet som pågår skal bli vellykket.

Dette er problemstillinger som ble nevnt i Lysne-II rapporten³⁶, men det er ikke ytterligere utredet.³⁷ Se nærmere om dette nedenfor i pkt. 7.3.

I forslaget § 9-6 er det foreslått et nødvendighetskrav for behandling av fortrolig kommunikasjon med særlige yrkesutøvere blant annet journalist og kilde. Men hva er en journalist? I høringsnotatet pkt. 12.10.6.3 er det angitt en formalistisk tilnærming til problemet – at det må ha blitt formidlet *fortrolig kommunikasjon* til en person som faller inn under kategorien *særlig yrkesutøver*. Med denne definisjonen vil vernet være formelt og ikke funksjonelt. Det er vist til at det vil ha betydning om «den særlige yrkesutøveren opererer i tråd med de profesjonelle og yrkesetiske krav som bærer det særlige vernet», og det konkluderes med at ikke enhver blogger eller driver av et nettsted skal kunne likestilles med en journalist.

Det er egnet til å skape uklarhet og forsterke nedkjølingseffekten, for det er ytringers innhold som trenger vern. I Rt. 2015 s. 2308³⁸, hvor spørsmålet var om kildevernet stod sterkere enn PSTs rett til beslag i upublisert materiale, var det harddisker hjemme hos en dokumentarfilmskaper som var gjenstand for beslag. Men i en digital verden vil alle aspekter ved den aktuelle personen bli berørt fordi kommunikasjonen ofte kan være vanskelig å skille. Den aktuelle filmskaperen er også kjent som regissør og filmanmelder og medlem av Arbeiderpartiets demokrati- og medieutvalg,³⁹ og når vil et prosjekt nytte godt av kildevernet? På et tidlig tidspunkt som frilanser, eller er det kun «fortrolig informasjon» til en «særlig yrkesutøver» som vernes?

Om betydningen av kildevernet uttaler Høyesterett i avsnitt 70:

«Etter min vurdering er (...) filmprosjekt i kjernen av undersøkende journalistikk; det griper fatt i et sentralt og presserende samfunnsproblem hvor allmenheten og myndighetene har behov for kunnskap og innsikt. Undersøkelsene er gjort mulig fordi (...) har en særlig og tillitsbasert

³⁶ [Digitalt grenseforsvar \(DGF\)](#), Lysne II-utvalget, 26.08.2016

³⁷ [Høringssvar Digitalt grenseforsvar, Direktoratet for e-helse](#), 06.01.2017

³⁸ [Rt. 2015 s. 2308](#)

³⁹ Journalisten, "[Vil sikre mediernes fremtid](#)", Huseby Jensen, 17.10.2014

tilgang til et lukket islamistisk miljø. Jeg legger til grunn at et effektivt kildevern er helt avgjørende for at filmen kan realiseres.”

Departementet har omtalt denne problemstillingen i høringsnotatet og har foreslått en særskilt bestemmelse om særlige yrkesutøvere i § 9-6. Se vår kommentar til denne i pkt. 7.3.

Vi vil for øvrig bemerke at bestemmelsen om vern av særlige yrkesutøvere kun omfatter en begrenset personkrets.

Kommunikasjon mellom stortingsrepresentanter, regjeringsmedlemmer og dommere er ikke foreslått å få et særskilt vern. Dette mener Datatilsynet er uheldig. Det er viktig at særlig stortingsrepresentanter kan kommunisere fritt for å ivareta sine forpliktelser som folkevalgte. I Storbritannia er medlemmer av parlamentet i loven sikret et særlig vern. Denne problemstillingen er ikke omtalt i høringsnotatet.

4.4 Formålsutglidning må påregnes

Tiltaket om tilrettelagt innhenting vil med stor sannsynlighet bli mer inngripende enn det høringsnotatet synliggjør. Det er et viktig aspekt som regjering og Storting må ta inn i vurderingen av lovforslaget.

Med formålsutglidning menes en situasjon der hvor personopplysninger som er innhentet til et bestemt formål senere benyttes til et annet, nytt formål. Et sentralt personvernprinsipp er formålsbegrensningsprinsippet. Prinsippet er todelt. For det første skal personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål. For det andre skal ikke opplysningene viderebehandles på en måte som er uforenlig med disse formålene. Prinsippet er begrunnet i kravet til forutberegnelighet, åpenhet og tillit.

Formålsutglidning kan skje gradvis gjennom praksis og en utvidende tolkning av gjeldende rett eller gjennom lovvedtak vedtatt av Stortinget.

Et eksempel på formålsutglidning uten lovendring er en sak i Høyesterett⁴⁰ der bruk av DNA-informasjon fra politiregistre ble benyttet i en farskapssak. I denne saken hadde mor bedt om dom på at den tidligere ektemannen ikke er barnets far. Ettersom mannen mest sannsynlig befant seg i Tsjetsjenia, hadde kvinnen bedt om å få benytte den DNA-prøven som ble lagret da mannen ble straffedømt i 2014. I politiregisterloven § 12 står det at «opplysningene i registeret skal kun brukes i strafferettspleien». Høyesteretts ankeutvalg kom til at paragrafen skal tolkes innskrenkende, og at barneloven § 24 skal gis forrang.

Når det gjelder formålsutglidning som følge av Stortingsvedtak, så finnes det mange eksempler på det. Et eksempel er reglene for dataavlesing som ble innført i nytt kapittel 16 d i lov om rettergangsmåte i straffesaker (straffeprosessloven) ved lov 17. juni 2016 nr. 5. I lovproposisjonen Prop. 68 L (2015-2016) Endringer i straffeprosessloven mv. (skjulte tvangsmidler), ⁴¹uttaler departementet under pkt. 14.8.9, side 273 høyre spalte:

⁴⁰ [HR-2018-2241-U](#)

⁴¹ Prop. 68 L (2015-2016), [Endringer i straffeprosessloven mv. \(skjulte tvangsmidler\)](#)

«Videre foreslår departementet at straffeprosessloven § 216 om taushetsplikt og bruk av opplysninger som fremkommer ved kommunikasjonskontroll (og ved romavlytting, jf. § 216 m) skal gjelde tilsvarende for opplysninger som fremkommer ved dataavlesing».

Denne bestemmelsen regulerer til hvilke formål politiet kan bruke informasjon innhentet ved skjulte tvangsmidler og setter altså begrensninger i adgangen til å bruke opplysningene utad.

Rett i forkant av vedtakelsen av loven, ble et forslag om endring av straffeprosessloven § 216 (i) og lov om politiet § 17 f sendt på høring. Forslaget gikk ut på at PST skulle kunne utlevere informasjon fra skjulte tvangsmidler (herunder dataavlesing) til Etterretningstjenesten. Forslaget ble vedtatt 16. juni 2017, altså ganske nøyaktig et år etter at man innførte den nye metoden dataavlesing. Dette er et eksempel på at nye metoder som innføres, og som i utgangspunktet underlegges strenge restriksjoner på bruk, etter en ny runde i Stortinget, åpner opp for nye formål.

Det er en utfordring at forslaget inneholder to ulike regimer for deling av overskuddsinformasjon. I lovutkastets § 10-8 er det foreslått at overskuddsinformasjon kan deles med norske offentlige myndigheter når vilkårene etter § 10-5 er oppfylt, med unntak av vilkåret om at Etterretningstjenesten kan behandle opplysningene etter kapittel 9, mens overskuddsinformasjon som fremkommer gjennom innhenting etter kapittel 7 reguleres av § 7-12 som begrenser utlevering av overskuddsinformasjon. Overskuddsinformasjon som er fortrolig kommunikasjon etter § 9-6 kan ikke utleveres.

Vi tror det i praksis trolig vil bli vanskelig å til enhver tid vite hvor informasjonen i en konkret sak kommer fra, noe som gjør kontroll med utlevering vanskelig.

Disse foreslåtte bestemmelsene er på ingen måte en garanti for at opplysningene som er innhentet ikke vil bli brukt til nye formål. Vi mener det ikke kan være noen tvil om at spørsmål omkring videre bruk til nye formål før eller senere vil komme opp. Som det også fremgår av høringsnotatet, var politiet ute med en gang Lysne II-rapporten ⁴²ble sendt på høring og krevde at opplysningene også måtte kunne brukes til kriminalitetsbekjempelse.

Avgjørelsen om å ikke benytte slik overskuddsinformasjon til å forhindre kriminalitet eller andre skadelige hendelser vil bli et etisk dilemma. Både for lovgiver generelt og den enkelte medarbeider i konkrete situasjoner. For eksempel der en medarbeider kommer over informasjon om et planlagt ran. I høringsnotatet er det drøftet hvorvidt nødrettsbetraktninger og eventuelle positive forpliktelser etter Grunnloven og EMK innebærer at staten får en handlingsplikt som går foran begrensningen i § 7-12. Dette viser at det er grunnlag for reelle bekymringer og at erfaring viser at det vil komme situasjoner hvor forbudet vil bli utfordret. På samme måte vil politikere komme under press til å endre loven, dersom det i forbindelse med en konkret hendelse kommer frem at etterretningstjenesten hadde tilgang til informasjon som kunne forhindre forbrytelsen.

For at Stortinget skal bestemme at overskuddsinformasjon innhentet gjennom tilrettelagt innhenting skal brukes til andre formål, og deles på en måte som avviker fra den vedtatte

⁴² [Digitalt grenseforsvar \(DGF\)](#), Lysne II-utvalget, 26.08.2016

loven, må det foretas en ny forholdsmessighetsvurdering og vurdering opp mot de menneskerettslige skrankene som ligger til grunn for lovligheten. En endring vil helt klart kunne forrykke denne balansen. Det vil i så fall være nødvendig å vurdere hele systemet og kontrollmekanismene på nytt.

Det kan for øvrig stilles spørsmål ved forholdet til lov om straff (straffeloven) § 287, om forsømmelse av hjelpeplikt. Dette bør avklares mer presist.

Forbudet gjelder ikke straffbar handling som omfattes av straffeloven kapittel 17 om vern av Norges selvstendighet og andre grunnleggende nasjonale interesser eller kapittel 18 om terrorhandlinger og terrorrelaterte handlinger og som kan avverges. Det ligger et potensiale for formålsutglidning i denne avvergingsplikten.

Kombinasjonen av den enorme mengden av data, en stadig utvikling av søkemetoder og kunstig intelligens gjør potensialet for formålsutglidning stort. Det vil alltid være gode formål som vil tale for å bruke opplysningene på nye måter. En slik utglidning vil kunne bringe oss stadig nærmere et totalt overvåkingssamfunn.

Den overhengende muligheten for formålsutglidning gjør det vanskelig å forutberegne konsekvensene av tiltaket og anslå omfanget av inngrepet. Det beste vernet mot formålsutglidning er å ikke samle inn opplysningene i første omgang, eller begrense innsamlingen til mer målrettede tiltak.

5 Rettslige rammer for forslaget

5.1 Innledning

Vi vil i dette kapitlet gjøre rede for de rettslige rammene for å kunne innføre et tiltak om «tilrettelagt innhenting», før vi i de etterfølgende kapitlene kommer med våre merknader til de delene av lovforslaget som vi mener er mest problematiske.

Retten til privatliv er en grunnleggende forutsetning for et fritt demokratisk samfunn. Rettigheten er nedfelt i Grunnloven § 102, EMK art. 8 og FNs internasjonale konvensjon om sivile og politiske rettigheter (SP) art. 17.

Retten til privatlivet er ikke absolutt, men rettigheten kan ikke innskrenkes i den grad at kjernen til retten og dens *raison d'être* ikke lenger er tilstede. I noen tilfeller er det akseptabelt og ønskelig at myndighetene, av hensyn til samfunnet, innfører tiltak som begrenser individers privatliv, for eksempel for å beskytte nasjonal sikkerhet. De menneskerettslige reglene som verner privatlivet inneholder derfor også regler som regulerer under hvilke omstendigheter et inngrep i privatlivet kan finne sted.

5.2 Den europeiske menneskerettskonvensjonen (EMK) art. 8

EMK art. 8 oppstiller skranker for hvilke inngrep staten kan gjøre i borgernes privatliv. Inngrep i denne rettigheten må tilfredsstille de krav som følger av disse bestemmelsene og praksis i Den europeiske menneskerettsdomstol (EMD).

«Art 8. Retten til respekt for privatliv og familieliv,

1. Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.

2. Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.»

Staten må vurdere om tiltaket vil medføre et inngrep, og i så fall om inngrepet er i samsvar med loven, og om det er nødvendig i et demokratisk samfunn

Helt sentralt står lovskravet som krever at inngrepet i retten til respekt for privatliv må være hjemlet i nasjonal lov. Lovskravet innebærer ikke bare at det skal foreligge en nasjonal lov som regulerer inngrepet, men innebærer også et kvalitetskrav til loven: lovgivningen må være tilstrekkelig klar og forutberegnelig. Dette kravet har som formål å verne mot vilkårlige inngrep fra myndighetene. Jo større inngrepet er, jo strengere må kravet tolkes. Loven må altså være klar og forståelig nok slik at den gjengse borger, om enn med rådgivning, kan forutse sin rettsposisjon.

Et inngrep må også forfølge legitime formål⁴³ og være nødvendig i et demokratisk samfunn.

Bestemmelsen krever at det må foretas en avveining mellom *samfunnets/statens interesse* og *inngrepet* i retten til privatliv. Det må derfor vurderes både fordeler og ulemper ved tiltaket. Dette for å fastslå om inngrepet i privatlivet er forholdsmessig.

I dette ligger et krav om å vurdere hvorvidt den skaden som er gjort ved inngrepet er begrenset ved egnede tiltak som reduserer virkningen av skaden. I vurderingen av om dette kravet er oppfylt, må man se hen til hvordan dette er regulert i lov, men også hvordan dette fungerer (eller vil komme til å fungere) i praksis.

Myndighetene må passe på at de ikke undergraver demokratiet i sin streben etter å beskytte det.

«Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate effective guarantees against abuse [...].”⁴⁴

I denne sammenhengen betyr dette at det er nødvendig å forsikre seg om at det finnes effektive kontrollmekanismer som sørger for at etterretningstjenester ikke bruker sin makt på en ulovlig og utilbørlig måte. Kontroll av Etterretningstjenesten må foregå før tiltaket iverksettes, og under og etter at tiltaket er avsluttet.

Det er en nær sammenheng mellom kravet om tilfredsstillende og effektive garantier mot misbruk i EMK art. 8 og art. 13. EMK art. 13 gjelder retten til et effektivt rettsmiddel. Enhver

⁴³ EMD-praksis krever at også en vurdering av hvorvidt loven forfølger et legitimt formål, og hvorvidt tiltaket er nødvendig, og i dette ligger også et krav om å velge det minst inngripende tiltaket dersom man med dette kan oppnå det samme resultatet. Vi har ikke kompetanse til å etterprøve departementets vurderinger på disse punktene, så vi legger deres vurderinger til grunn. Vi vil derfor ikke gå nærmere inn på disse temaene. Se departementets vurdering av legitimitet i høringsnotatet pkt. 11.8.2.3.

⁴⁴ ECHR, [Weber and Saravia v. Germany](#), no. 54934/00, 29.06.2006 p. 106

som har fått de rettigheter og friheter som er fastlagt i konvensjonen krenket, skal ha en effektiv prøvningsrett hos en nasjonal myndighet.

I saker som omhandler statlig overvåking har EMD gjennom sin praksis derfor etablert en rekke minimumskrav som må være oppfylt for at bulkinnhenting av kommunikasjonsdata skal være i tråd med menneskerettighetene.

Kravene som omtales som Weber-kriteriene ble først omtalt i *Weber and Saravia v. Germany*⁴⁵ og deretter utviklet i *Zakharov v. Russia*⁴⁶, *Szabó and Vissy v. Hungary*⁴⁷, og har blitt tilpasset bulkinnhenting av kommunikasjonsdata i *Centrum för rättvisa v. Sweden*⁴⁸, og *Big Brother Watch and others v. UK*.⁴⁹

Weber-kriteriene kan sammenfattes som krav til:⁵⁰

- den nasjonale loven som lovfester inngrepet må være tilgjengelig, herunder er det et krav til tilstrekkelig klar beskrivelse av hvilke forhold som kan begrunne innhenting og lagring av opplysninger, og en angivelse av hvilke personer eller grupper som kan bli gjenstand for tiltaket
- prosedyre for forhåndsgodkjenning
- prosedyrene for lagring, tilgang, bruk, deling og sletting av data
- kontrollmekanismer, herunder underretning til den registrerte
- krav til et effektivt rettsmiddel

Kravene i EMK art. 8 er kumulative, det vil si at *alle* kravene må være oppfylt for at et inngrep kan anses å være innenfor de rettslige skranker. Samtidig er det viktig å poengtere at det må foretas en helhetsvurdering av alle kravene for å fastslå om et inngrep er berettiget. Dersom et av kravene ikke er tilstrekkelig ivaretatt, vil det kunne avhjelpes ved sterkere oppfyllelse av et av de andre kravene. Det er totale det forslaget som må vurderes på en helhetlig rettslig og samfunnsmessig måte.

5.3 Praksis fra EU-domstolen

I tillegg til EMD, har EU-domstolen avsagt flere dommer som er relevante for temaet. Selv om EU-domstolens avgjørelser om EUs pakt over fundamentale rettigheter ikke er bindende

⁴⁵ ECHR, [Weber and Saravia v. Germany](#), no. 54934/00, 29.06.2006

⁴⁶ ECHR, [Zakharov v. Russia](#), no. 47143/06, 04.12.2015

⁴⁷ ECHR, [Szabó and Vissy v. Hungary](#), no. 37138/14, 12.01.2016

⁴⁸ ECHR, [Centrum för Rättvisa v. Sverige](#) no. 35252/08, 10.06.2018, ikke endelig. Saken skal behandles i EMDs storkammer.

⁴⁹ I dommene skilles det ikke mellom metode for innhenting eller geografiske begrensninger. Det sentrale er at selve inngrepet i privatlivet må tilfredsstillende minimumsvilkårene.

De to sistnevnte dommene som ble avsagt i 2018 omhandler bulkinnhenting av etterretningsinformasjon i Sverige og Storbritannia. I den svenske dommen kom domstolen til at FRAs signalspaning oppfylte minimumskravene, mens i dommen mot England fant domstolen brudd på flere bestemmelser. Selv om det kan argumenteres for EMD åpner for digital masseovervåking, så er det viktig å påpeke at vurderingen er konkret.

⁵⁰ De 'tradisjonelle' Weber og Saravia kriteriene for hemmelig overvåking ble tilpasset til bulk innsamling i EMDs dom i [Centrum for Rättvisa v. Sverige](#) p. 114.

for Norge, så peker de på viktige prinsipper for å ivareta borgernes rettigheter i et demokratisk samfunn.

Når det gjelder Tele2/Watson-dommen,⁵¹ er denne særlig relevant siden den oppstiller krav om målretting og den klargjør en rekke minimumsvilkår for at lagring av kommunikasjonsopplysninger kan anses akseptabelt. Domstolen slår fast at en generell og uddifferensiert innsamling og lagring av kommunikasjonsopplysninger er i strid med de grunnleggende rettighetene. En målrettet innhenting av trafikk- og lokaliseringsdata kan være akseptabelt dersom lagringen begrenses til det som er strengt nødvendig når det gjelder kategorier av data, hvilke kommunikasjonsmidler, de berørte personer og varigheten av lagringen.

Spørsmålet om dommen også får anvendelse på innhenting av kommunikasjonsdata i bulk for ivaretagelse av nasjonal sikkerhet er forelagt EU-domstolen i sak C-623/17 (Privacy International).⁵² Saken er per i dag ikke avgjort.

Selv om tilrettelagt innhenting og innhenting av rådata i bulk retter seg mot utenlandske trusler, så vil realiteten i forslaget være en tilnærmet ubegrenset innhenting av kommunikasjonsopplysninger om norske borgere, og prinsippet om målrettethet som er etablert i denne dommen må da vektlegges.

5.4 Personopplysningsvern

Personopplysningsvern kan ses på som en underkategori av personvern som omhandler normer og regler for behandling av personopplysninger, med sikte på å verne om personlig integritet, autonomi og privatlivets fred. Med noen unntak skal enkeltpersoner ha mulighet til å bestemme selv hva andre skal få vite om han eller hennes personlige forhold.

Personopplysningsvernet er underlagt omfattende lovregulering. Internasjonaliseringen på dette området har fått stadig større betydning for norsk praksis og regelverksutforming, senest ved ny personvernforordning i EU, som i 2018 ble gjort til norsk lov gjennom ny personopplysningslov. Personopplysningsvern kan ikke ses på løsrevet fra retten til privatliv etter SP art. 17 og EMK art. 8. Både EU-domstolen og EMD anerkjenner vern av personopplysninger som en del av retten til privatliv.

EUs personvernforordning er den mest sentrale og viktigste folkerettslige forpliktelsen på dette området. Kjernen i regelverket oppsummeres i personvernforordningen art. 5 om grunnprinsipper. Prinsippet om lovlighet, rettferdighet og åpenhet legger grunnlaget for den tillit som er nødvendig i et demokratisk samfunn. De andre personvernprinsippene handler om formålsbegrensning, dataminimering, at opplysningene skal være korrekte og om nødvendig oppdaterte, lagringsbegrensning, integritet og konfidensialitet.

⁵¹ECJ, Tele2/Watson, Joined Cases C-203/15 and C-698/15, European Court of Justice, 21.12.16

⁵² Prejudisiell framlegging fra en britisk domstol. Saken gjelder hvordan trygghets- og etterretningstjenesters innhenting av kommunikasjonsdata i «bulk» for ivaretagelse av nasjonal tryggleik faller innenfor EU-rettens virkeområde, herunder direktiv 2002/58/EC (e-privacy). Videre er det reist spørsmål om hvilke avgrensninger som i så fall følger av EU-retten, herunder om «Watson-kriteriene» kommer til anvendelse.

Personvernforordningen gjelder ikke for behandling av personopplysninger som skjer i nasjonal sikkerhets øyemed, men den gir likevel veiledning om hvordan regelverk som omhandler personopplysninger kan utformes. Det bør være et ideal at den nye loven om Etterretningstjenesten i størst mulig grad følger personopplysningsprinsippene.

I forordningens art. 23 gis det regler for hvilke hensyn som bør vektlegges når man fastsetter begrensninger i rettighetene som forordningen skal beskytte, noe som dette lovforslaget i realiteten vil innebære. Eventuelle begrensninger må overholde det vesentligste innholdet i de grunnleggende rettighetene og frihetene, og være et nødvendig og forholdsmessig tiltak i et demokratisk samfunn. I tillegg må loven, når det er relevant, inneholde særlige bestemmelser om blant annet garantiene for å unngå misbruk eller ulovlig tilgang eller overføring, risikoene for de registrertes rettigheter og friheter og de registrertes rett til å bli underrettet om begrensningen, med mindre dette kan skade formålet med begrensningen.

Dette bør være naturlige utgangspunkter for en vurdering av bestemmelsene om personopplysninger i forslaget.

6 Kravet til klarhet i loven

6.1 Innledning

Som nevnt over oppstiller EMDs praksis krav til en tilstrekkelig klar beskrivelse av hvilke forhold som kan begrunne innhenting og lagring av opplysninger, og en definering av hvilke personer eller grupper som kan bli gjenstand for tiltaket. Dette handler om at loven må være forutberegnelig.

Forutberegnelighet er et viktig rettsstatsprinsipp.⁵³ Når det gjelder hemmelig overvåking er kravet til forutberegnelighet i loven noe lavere enn ellers. Det er ikke ønskelig at detaljer rundt Etterretningstjenestens virksomhet blir offentliggjort dersom dette fører til at tjenestens kapasiteter blir avslørt. Det er heller ikke meningen at borgerne i hvert eneste tilfelle skal være klar over at de blir overvåket. Dette vil kunne føre til at de endrer sin adferd, og dermed blir den etterretningsfaglige verdien av overvåkingen begrenset.

Likevel må loven klargjøre rekkevidden av Etterretningstjenestens myndighet, slik at det ikke gjøres vilkårlige eller utilbørlige inngrep i borgenes privatliv. Manglende oppfyllelse av kravet til forutberegnelighet har ikke bare en rettslig side. Det er også et viktig poeng at uklarhet og manglende forutberegnelighet skaper en større nedkjølingseffekt og et samfunn med mindre tillit til myndighetene. Se nærmere om det i punkt. 4.3.

Datatilsynet mener at omfanget av tiltaket «tilrettelagt innhenting» på en rekke områder er uklart. Vi vil i det følgende si noe om de delene av forslaget som vi mener er særlig uklare.

⁵³ ECHR, [Sunday Times, v. The United Kingdom](#), no. 6538/74 26.04.1979, para 49

6.2 Territoriell begrensning

Lovforslaget inneholder et forbud mot innhenting rettet mot personer og virksomheter som befinner seg i Norge i § 4-1, med en rekke unntak i § 4-2.

Som det fremgår i kapittel 3 er det problematisk at selv om selve etterretningsinnhentingene tilsynelatende er begrenset, så omfatter innsamlingen opplysninger gjennom elektronisk kommunikasjon i realiteten nesten samtlige personer som oppholder seg i Norge, i og med at de fleste benytter internett og mobiltelefon.

Den territorielle begrensningen i § 4-1, jf. § 4-2, som skal sørge for at Etterretningstjenesten ikke skal drive overvåkningsvirksomhet av personer som befinner seg i Norge, er formulert på en uklar måte. Utfra hovedregelen i § 4-1 vil den jevne borger forvente at Etterretningstjenesten ikke skal lagre informasjon om kommunikasjon som går mellom personer som befinner seg i Norge. Det fremgår imidlertid av unntakene i § 4-2 at informasjon (metadata) om borgernes kommunikasjon i Norge likevel kan innhentes og lagres over en lang periode.

Det er for øvrig et spørsmål om hvorfor norske borgere som oppholder seg i utlandet ikke skal ha samme beskyttelse som de som befinner seg i Norge. Dette handler om rekkevidden av staters menneskerettslige forpliktelser, men vi kan ikke se noen god begrunnelse for at retten til privatliv ikke skal være lik, uavhengig av hvor man oppholder seg.

Dette skaper en uklarhet som gjør det vanskelig å forutberegne om man blir utsatt for overvåking eller ikke.

Innhenting og søk i rådata i bulk ved midtpunktinnhenting er ikke underlagt forbudet mot innhenting av informasjon og personer i Norge, jf. § 4-1, jf. § 4-2 sjette og syvende ledd. Søk kan da ta utgangspunkt i personer eller virksomheter i Norge.

I høringsnotatet pkt. 8.6.2 anføres det at informasjon som innhentes og lagres om fysiske og juridiske personer i Norge ved å innhente metadata ikke rammes av innhenningsforbudet i § 4-1 fordi innhentingene ikke har overvåknings*hensikt*.

Dette fremstår for oss som en retorisk øvelse. Vi mener at det vil være uvesentlig (for den som berøres av innhentingene) hvorvidt det foreligger overvåknings*hensikt* eller om man anser innhentingene som rettet mot en annen person. Faktum er at Etterretningstjenesten ved denne metoden vil innhente og lagre informasjon om personer som befinner seg i Norge og kommunisere innenfor landet. Dette går ikke klart frem av loven.

6.3 Hva slags data kan innhentes? Forskjellen på metadata og innholdsdata

I lovforslaget gjøres det et skille mellom metadata og innholdsdata. Det foreslås forskjellige krav til lagring, sletting og rettsikkerhetsgarantier for det som beskrives som ulike typer data.

Vi mener at det ikke er grunn til å behandle metadata og innholdsdata forskjellig, og at det er uheldig at betydningen av lagring av metadata nedtones, slik at inngrepet fremstår som mindre enn det faktisk er.

Det er i dag ingen prinsipiell eller rettslig forskjell på innholdsdata og metadata⁵⁴. Metadata kan inneholde store mengder personopplysninger. Metadata er lettere å strukturere og analysere enn innholdsdata. På grunn av disse egenskapene er metadata, i minst like stor grad som innholdsdata, egnet til å avsløre intime detaljer om en persons privatliv. Dette betyr at behandling (inkludert lagring) av metadata medfører et stort inngrep i retten til privatliv.

Metadata inneholder blant annet informasjon om tilbyder av kommunikasjonstjeneste, kilden til kommunikasjon og bestemmelsessted, geografisk plassering, dato, klokkeslett, varighet, type kommunikasjonsutstyr, navn, adresse, abonnement, telefonnummer, IP-adresse, brukernavn og gjør det mulig å identifisere hvem som har kommunisert, hvorfra og med hvilken hyppighet. Fra en smarttelefon vil det i dag gå en kontinuerlig strøm av metadata til og fra ulike apper, som vil kunne gi en detaljert kartlegging av en persons liv.

Opplysninger om hvor en mobilsamtale blir koplet opp vil kunne være mye mer inngripende enn selve innholdet i samtalen. Eksempelvis vil metadataene omkring en samtale med en venn om spillet FIFA 2018 som starter ved SUSS (Senteret for ungdomshelse, samliv og seksualitet), avsluttes på legevakten og gjenopptas på apoteket, være minst like inngripende eller mer inngripende enn selve innholdet av samtalen.

Også i Etterretningstjenestens historie er dette et vesentlig poeng som kan illustreres med det kjente bildet fra Treholt-saken, hvor Arne Treholt i 1983 blir fotografert i samtale med KGB-generalen Gennadij Titov i Wien. Her blir selve møtet en sentral del av saken, uten at det nødvendigvis er kjent hva samtalen dreide seg om.⁵⁵

Det er klart at systemet vil kunne fange opp informasjon som ved misbruk vil kunne gjøre skade eller skape frykt for skade, og som i andre regimer kan bli brukt som pressmiddel.⁵⁶ Dette sier noen om den maktforskyvning systemet innebærer og potensialet for skade ved misbruk.

Det er i forslaget og i kommunikasjon fra departementet forsøkt å nedtone betydningen av metadata. Senest i Forsvarsministerens nyttårstale 7. januar 2019⁵⁷, gjentas en uriktig fremstilling av metadata: «*Metadata er data om data – altså ikke innholdsdata. Det er som å fotografere utsiden av en konvolutt – uten å åpne den.*»

Dette er ikke riktig. Gjennom analyse og sammenstilling av metadata er det er mulig å skaffe seg detaljert informasjon om enkeltpersoner⁵⁸, også der hvor informasjonen i utgangspunktet er anonymisert.

⁵⁴ ECJ, Tele2/Watson - Joined Cases C-203/15 and C-698/15, European Court of Justice, 21.12.16, p. 98 og 99.

⁵⁵ NRK, "[Treholt-bildene du ikke fikk se](#)", Hansen, Andersen, 11.03.2014

⁵⁶ "The Mitrokhin Archive: the KGB in Europe and in the West", Andrew, Mitrokhin, Penguin UK, 2015

⁵⁷ Regjeringen, [Forsvarsministerens nyttårstale i Oslo militære samfund](#), Bakke-Jensen, 07.01.2019

⁵⁸ NYTimes, "[Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret](#)", Valentino-Devries, Singer, Keller, Krolic, 10.12.2018

På grunn av omfanget av metadata vil lagring og søk i dette kunne være svært personverninnngripende. Vi anbefaler derfor at, i likhet med nederlandsk lov, at det ikke gjøres forskjell på innholdsdata og metadata når det gjelder lagring av data.⁵⁹

I tillegg følger det av forslaget § 6-2 at Etterretningstjenesten kan innhente informasjon fra åpne kilder, og at dette kan gjøres mot personer og virksomheter i Norge jf. § 4-2 åttende ledd. Det kan hentes informasjon fra blant annet sosiale profiler, hjemmesider eller liknende.

Dette er potensielt svært personverninnngripende, ettersom omfanget av personopplysninger som deles på nettet er enormt.

6.4 Hvem blir det behandlet opplysninger om?

Tilrettelagt innhenting av grenseoverskridende kommunikasjon er i lovutkastets § 7-1 omtalt som «elektronisk kommunikasjon som transporteres over den norske landegrensen» og begrenset til innhenting hvor tilrettelegging av tilgang til elektronisk kommunikasjon er nødvendig etter § 7-2.

Det er problematisk at loven tilsynelatende er begrenset til etterretningsinnhenting som omhandler grenseoverskridende kommunikasjon. Dette tåkelegger at den tekniske virkeligheten er at innsamlingen vil omfatte nesten samtlige personer som oppholder seg i Norge, i og med at de fleste benytter internett og mobil, hvor kommunikasjon som regel vil transporteres over den norske landegrensen.

Forslaget innebærer at det vil bli foretatt søk i metadatalageret basert på *personselektorer* og *modusselektorer*. Med personselektorer menes en identifikator tilknyttet en bestemt person eller virksomhet, jf. § 1-4 nr. 12. Med modusselektorer menes et søkebegrep eller søkestreng som beskriver et bestemt mønster eller avgrensning, herunder handlingsmønster eller geografisk område, jf. § 1-4 nr. 7.

Vi mener at det i lovforslaget og høringsnotatet ikke kommer klart frem hvor omfattende søkene i realiteten vil være. Slik Datatilsynet forstår det, så vil det innsamlede materialet bli utsatt for en kontinuerlig behandling gjennom ulike former for søk basert på de selektorene man til enhver tid benytter. Som et bilde på det kan man si at ved et søk etter et sort får i en saueflokk, så vil en datamaskin måtte vurdere alle sauene og vil ikke kunne identifisere den sorte uten at de andre sauene vurderes.

6.4.1 Nærmere om personselektorer

I forslaget del som omhandler tilrettelagt innhenting er det i § 7-8 åpnet for at søk basert på personselektor kan inkludere to ledd ut i personens kommunikasjonskjede, en begrensnig som ikke finnes for innhenting av rådata i bulk. Dette medfører at et stort antall personer som oppholder seg i Norge kan bli gransket av Etterretningstjenesten bare på grunnlag av at de har kommunisert med en person som er av interesse for Etterretningstjenesten.

⁵⁹ “[Upping the Ante on Bulk Surveillance - An International Compendium of Good Legal Safeguards and Oversight Innovations](#)”, Wetzling, Vieth, Böll-Stiftung, VOLUME 50, 2018, s.57

Høringsnotatet viser til en undersøkelse gjort på Stanford i 2016⁶⁰ som indikerer at et søk på en person som inkluderer to ledd ut potensielt kan ramme 25 000 personer. Selv om det i høringsnotatet anerkjennes at søk to ledd ut er problematisk av personvern hensyn, åpnes det for at retten kan åpne for søk i enda flere ledd.

Departementet opplyser at det ikke vil bli gjort søk i metadata, og laget nettverkskart av norske kontakter til en norsk kontakt av etterretningsmålet. Dette skal filtreres bort så langt det er praktisk mulig.

6.4.2 Nærmere om modusselektorer

Når det gjelder søk på modusselektor beskrives det som søk på et bestemt mønster eller avgrensning, herunder handlingsmønster eller geografisk mønster. Det opplyses at et søk med modusselektor vil være mindre finmasket enn personselektor søk, men det er vanskelig å få tak i hvilken begrensning grunnvilkåret om forholdsmessighet setter.

Forslaget beskriver målsøking i pkt. 8.7.1.1:

«Under målsøking benyttes blant annet såkalte metadatasøk, som innebærer søk i store rådatagrunnlag som tjenesten lovlig har innhentet ved hjelp av tekniske kapasiteter. Slike søk er i sin natur kartleggende og avgjørende for å avdekke nye og ukjente trusselaktører. Aktiviteten finner sted før et etterretningsmål er identifisert som relevant og målrettet fordekt innsamling mot vedkommende iverksettes. Betydningen av slike metadata, det vil si data som beskriver typen eller formatet av innholdet, hvem som er avsender og mottaker, størrelse, tidspunkt og varighet av kommunikasjon, har blitt stadig viktigere i etterretningsarbeidet de senere år.»

Og i 12.6.5.3:

«Etterretningstjenesten er avhengig av å kunne innsamle og lagre store mengder rådata som tjenesten gjennom komplekse søk, og med tjenstlig behov, kan få tilgang til for deretter å hente ut de data som har størst etterretningsmessig verdi. (...)

Dette synliggjøres blant annet gjennom metodikken som benyttes for å finne relevant etterretningsinformasjon. Man ser etter mønstre i store datamengder som er innsamlet over lengre tid, for å finne det etterretningsrelevante.»

Et søk med modusselektor vil gjennomføres i alle data som er lagret. Verktøyene for søk i stor-data blir stadig mer avanserte og mønstergjenkjennelse åpner for å finne sammenhenger som man ikke tidligere klarte. En økt bruk av kunstig intelligens gjør at svart-boks problematikken⁶¹, hvor programvaren produserer resultater som ikke er kontrollerbare⁶², skaper rom for feil.

Det er uklart hva som kan danne utgangspunkt for et søk. Det som i utgangspunktet kan være et legitimt søk kan få uforutsette virkninger fordi omfanget av opplysninger er så stort og ethvert søk vil kunne ramme alle.

⁶⁰ PNAS, [Evaluating the privacy properties of telephone metadata](#), Mayer, Mutchler, C. Mitchell, 16.05.2016

⁶¹ Datatilsynets rapport om [Kunstig intelligens og personvern](#), januar 2018.

⁶² MIT Technology Review, «Intelligent Machines -The Dark Secret at the Heart of AI», Will Knight 11.04.2017

6.4.3 Lovbestemmelse om filtrering

Systemet baserer seg på en filtrering som skal frembringe mest mulig etterretningsfaglig relevant informasjon og forsøksvis filtrerer bort informasjon som er sendt mellom avsender og mottaker hvor begge befinner seg i Norge, jf. § 7-5. Dette for å størst mulig grad unnta norske borgere fra etterretningens søkelys.

At det er vanskelig å filtrere bort overskuddsinformasjon er åpenbart. Det vises til høringsnotatets pkt. 8.6.3, hvor det argumenteres med at det ikke finnes «realistiske alternativer for å filtrere ut ikke-relevant informasjon fra datasettene.» fra informasjon som er innhentet gjennom tilrettelagt innhenting.

Metodene for filtrering beskrives ved å vise til et eksempel om å filtrere bort samtaler fra + 47 til + 47. Dette vil trolig få begrenset betydning, sett hen til hvordan kommunikasjon foregår på ulike plattformer i dag.

Lovforslagets bestemmelse om filtrering er uklart formulert, og kan gi et uriktig inntrykk av filtrenes effektivitet. Dette gjør det vanskelig å overskue hvem som i praksis vil kunne bli gjenstand for søk.

I den forbindelse viser vi til Nederlands lov, som ikke skiller mellom innenlandsk eller utenlands data. Dette fordi de mener det ikke er teknisk mulig å gjøre en effektiv filtrering. De har derfor gjort et prinsipielt valg om beskytte all data, som om det var innenlands og har dermed gitt all data høyest mulig vern.

6.5 Omfanget av tilretteleggingsplikten er uklar

Det er uklart for oss hvilke aktører som omfattes av tilretteleggingsplikten.

Etter § 7-2 omfatter tilretteleggingsplikten «ekomloven § 1-5 nr. 16 og tilbydere av internettbaserte kommunikasjons- eller meldingstjenester som er tilgjengelige for allmennheten»

For de tilbydere som er omfattet av ekomloven § 1-5 nr. 16, jf. forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften) § 1-2, vil det foreligge et regelsett og en liste over tilbydere. Dette er en relativt omfattende liste, som i tillegg til Telenor og Telia, inneholder tilbydere som f.eks. Oslo kommune, Kvam Kraftverk, Rana kommune drifts- og anleggskontoret, Hålogaland Kraftproduksjon osv.

Tilretteleggingsplikten omfatter dessuten også «tilbydere av internettbaserte kommunikasjons- eller meldingstjenester som er tilgjengelige for allmennheten». Tilbydere av internettbaserte kommunikasjons- eller meldingstjenester er i høringsnotatet definert som «typisk internettbaserte «over the top-tjenester» (OTT-tjenester), som kan brukes til overføring av tekst, lyd og bilder».

Inkluderingen av OTT-tjenester medfører en kraftig utvidelse av tilretteleggingsplikten sammenliknet med forslaget til Lysne II-utvalget, som foreslo at tilretteleggingsplikten kun skulle gjelde for alle tilbydere som er definert i ekomloven § 1-5. Nå er det ikke lenger bare tilbydere av grensekryssende kabler som får en tilretteleggingsplikt, men også alle som leverer grensekryssende kommunikasjonstjenester til allmenheten på toppen av disse.

Det er vanskelig å se rekkevidden av denne plikten, men vi oppfatter at den vil kunne inkludere en rekke norske tjenesteleverandører. Er for eksempel Finn.no en «internettbasert kommunikasjons- eller meldingstjeneste som er tilgjengelig for allmennheten», med sine 8 millioner annonser i året og 6,3 millioner unike brukere i uken? Vi mener samtidig at høringsnotatet er uklart mht. om plikten kun vil gjelde for norske OTT-tjenesteleverandører, eller om plikten også vil omfatte enhver som leverer OTT-tjenester til allmennheten i Norge. Dersom det sistnevnte er tilfelle, vil plikten også kunne gjelde for tjenesteleverandører som Facebook, Grindr, Skype og Whatsapp? Dette vil i så fall gjøre forslaget lang mer inngripende.

For øvrig er det i § 7-2 kun angitt en plikt til å tilrettelegge, men det angis ingen klageordning for tilbydere. Tradisjonelt vil et pålegg om tilretteleggingsplikt være å regne som et enkeltvedtak og kunne påklages etter lov om behandlingsmåten i forvaltningssaker (forvaltningsloven), men denne loven er ikke gitt anvendelse for Etterretningstjenesten jf. § 11-7.

Datatilsynet anbefaler, dersom man går videre med lovforslaget, at det inntas en klagerett for de aktuelle virksomhetene i loven, hvor det også gis mulighet for domstolskontroll av vedtaket. Det vises til at tilretteleggingsplikten vil kunne få både praktiske, økonomiske og omdømmemessige konsekvenser for tilbydere som blir pålagt en tilretteleggingsplikt.

6.5.1 Omfatter tilretteleggingsplikten lag 2-kryptering?

I Lysne II-utvalgets rapport ⁶³omtales tilrettelegging av ukryptert kommunikasjon slik:

«Tilretteleggingsplikten for teletilbyderne må derfor omfatte leveranse av datastrøm uten linkkryptering dersom dette er implementert på den grensekryssende forbindelsen. Tilretteleggingsplikten bør imidlertid ikke inneholde krav om støtte til omgåelse av krypto utover dette.»

Datatilsynet oppfatter at det her menes en omgåelse av såkalt lag 2-kryptering i utstyr som er direkte tilkoblet den grensekryssende kabelen, og at omgåelsen skal gjøres av den operatoren som eier eller har ansvar for kabelen. Professor Olav Lysne har selv bekreftet at dette var hans mening i en artikkel på digi.no⁶⁴

I høringsnotatet pkt. 11.15.3. står det at «tilretteleggingsplikten inkluderer en plikt til å sørge for tilgang til kommunikasjon uten hinder av linkkryptering *eller liknende* kryptering som tilbyder kontrollerer».

Det er svært uklart hva som menes med «liknende kryptering som tilbyder kontrollerer». Uklarheten forsterkes ytterligere av at tilretteleggingsplikten nå vil omfatte OTT-tjenesteleverandører, som i mange tilfeller vil ha implementert egen kryptering i sine applikasjoner og tjenester. Det er opplagt at tilbydere av OTT-tjenester vil kontrollere kryptering i sine egne tjenester, også der hvor det brukes ende-til-ende kryptering

Krypteringsteknologi gjør det mulig for personer å ha meninger og å bruke sin ytringsfrihet på internett uten fare for tilfeldige eller ulovlige inngrep. Teknologien er mye brukt over hele

⁶³ [Digitalt grenseforsvar \(DGF\)](#), Lysne II-utvalget, 26.08.2016

⁶⁴ [Digi.no, «Lysne II, digitalt grenseforsvar og kryptering»](#), Lysne, 18.12.18

verden, blant annet av menneskerettighetsforsvarere, journalister, varslere og politiske dissidenter som står overfor forfølgelse og trakassering. Dersom tilretteleggingsplikten medfører en svekkelse av krypteringen, vil det true personvernet til alle brukere og eksponere dem for ulovlige inngrep. Ikke bare av stater, men også av ikke-statlige aktører og kriminelle nettverk. En slik utbredt og ikke-diskriminerende effekt vil ikke være forenlig med proporsjonalitetsprinsippet som FNs høykommissær påpeker i sin rapport «The right to privacy in the digital age»⁶⁵

Vi mener derfor at loven må være tydelig på at tilretteleggingsplikten ikke skal medføre en svekkelse av krypteringen, og at den ikke skal omfatte annen omgåelse av kryptering enn det som gjøres direkte på den grensekryssende kabelen.

6.6 Lovforslaget oppfyller ikke kravet til klarhet

Lovforslagets bestemmelser er uklart formulert, slik at det ikke kommer tydelig frem hvem sine data som blir lagret, og under hvilke omstendigheter disse kan bli gjenstand for søk. I tillegg er det uklart hvem som er omfattet av tilretteleggingsplikten, og ordene «eller lignede kryptering» skaper stor uvisshet om hvilke data som egentlig vil være tilgjengelige for Etterretningstjenesten.

På grunn av disse uklarhetene i lovforslaget, anser vi at kravet om forutberegnelighet gjennom klarhet i lov ikke er oppfylt.

7 Prosedyrene for behandling av personopplysninger

7.1 Innledning

I følge EMDs praksis må prosedyrene for hvordan personopplysninger skal behandles fremgå i lov.⁶⁶ For eksempel bør det gå klart frem av loven hvor lenge opplysninger skal oppbevares, hvem som kan bestemme at lagrede data kan tas i bruk, og til hvilke formål. Lovens bestemmelser må basere prosedyrene på alminnelige personvernprinsipper.

Personvernprinsippene omtalt i pkt. 5.4 er grunnleggende, og utgjør målestokken for et godt personvern. Dette gjelder uavhengig av om personopplysningsloven og forordningen gjelder, men med de begrensninger som følger av de spesielle hensynene som må tas i Etterretningstjenesten. Det er en klar forbedring sammenlignet med gjeldende lov at loven inneholder et eget kapittel om hvordan personopplysninger skal behandles. Vi har imidlertid noen bemerkninger. I det følgende vil vi problematisere tre temaer som vi mener bør forbedres.

7.2 Personopplysningsbegrepet

Definisjonen av hva som er å regne som en personopplysning er helt sentralt for å vurdere inngrepets størrelse og dets betydning for retten til privatliv. Det har også en side mot

⁶⁵ A/HRC/39/29, [The Right to Privacy in the Digital Age](#), Report of the United Nations High Commissioner for Human Rights, 03.08.2018

⁶⁶ ECHR, [Zakharov v. Russia](#), no. 47143/06, 04.12.2015 og ECHR, [Centrum för rättvisa v. Sweden](#), no. 35252/08, 10.06.2018

hvordan konsekvensene av forslaget kommuniseres til de som rammes. Med et snevert personopplysningsbegrep vil man kunne hevde at inngrepet er mindre enn det faktisk er.

En definisjon av personopplysninger bør derfor ta utgangspunkt i en allment akseptert definisjon som er i bruk på flere samfunnsområder.

Det naturlige utgangspunkt er da personvernforordningens definisjon i art. 4 nr. 1:

«enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet» (...)

I forslaget § 1-4 nr. 11 er det foreslått:

«enhver opplysning og vurdering som med enkle midler kan knyttes til en identifisert eller identifiserbar fysisk person.»

I høringsnotatet pkt. 12.4.2 så anføres det at «Departementets forslag tilsvarer materielt sett legaldefinisjon i EUs-personvernforordning 2016 artikkel 4». Dette mener vi ikke er riktig.

For de første avviker definisjonen språklig fra personvernforordningens, noe som i seg selv åpner for uklarheter, men den er også innholdsmessig forskjellig på et vesentlig punkt: I forslaget snevres definisjonen inn ved at det kun er opplysninger som med *enkle midler* kan knyttes til en person som er omfattet av definisjonen. Dette endrer altså kravet til hvor mye som skal til for å si at en opplysning er å regne som en personopplysning.

I fortalen til personvernforordningen pkt. 26 er det uttalt:

«Når det skal fastslås om en fysisk person er identifiserbar, bør det tas hensyn til alle midler som det med rimelighet kan tenkes at den behandlingsansvarlige eller en annen person kan ta i bruk for å identifisere vedkommende direkte eller indirekte, f.eks. utpeking. For å fastslå om midler med rimelighet kan tenkes å bli tatt bruk for å identifisere den fysiske personen bør det tas hensyn til alle objektive faktorer, f.eks. kostnadene for og tiden som er nødvendig for å foreta identifikasjonen, idet det tas hensyn til teknologien som er tilgjengelig på behandlingstidspunktet, samt den teknologiske utvikling.»

I en verden med stadig utvikling av analyse og søkeverktøy, er det vanskelig å si hva enkle midler er. I tillegg besitter Etterretningstjenesten formodentlig teknologisk kompetanse og kapasitet langt utover det som er vanlig hos andre behandlingsansvarlige. Det som er «enkle midler» for dem er ikke det samme som for oss andre.

I høringsnotatet pkt. 12.4.1 argumenteres det også for at IP-nummer knyttet til en datamaskin med flere brukere (dynamisk IP-adresse) ikke skal falle inn under definisjonen fordi informasjonen ikke kan knyttes til en konkret enkeltperson.

Dette er ikke korrekt. Dynamiske IP-adresser kan knyttes til enkeltpersoner noe også EU-domstolen har kommet til i saken Patrick Breyer v Bundesrepublik Deutschland⁶⁷. Der ble det slått fast at dynamiske IP-adresser skal regnes som personopplysninger i gitte tilfeller, blant annet der brukeren bak IP-adressen ved hjelp av tilleggsinformasjon fra internettleverandøren kan identifiseres.

Datatilsynet mener forslagets definisjon av personopplysninger må endres slik at det sammenfaller med personvernforordningens.

7.3 Behandling av fortrolig kommunikasjon med særlige yrkesutøvere

I lovforslagets § 9-6 er det foreslått et nødvendighetskrav for behandling av fortrolig kommunikasjon med særlige yrkesutøvere. Etterretningstjenesten skal ikke behandle opplysninger som er fortrolig kommunikasjon mellom advokat og klient, helsepersonell og pasient, journalist og kilde eller tilsvarende fortrolig kommunikasjon som nyter særlig menneskerettslig vern, med mindre vektige samfunnshensyn gjør behandlingen strengt nødvendig.

Beslutning om å behandle opplysninger skal etter bestemmelsens første ledd treffes av sjefen for Etterretningstjenesten, med mindre beslutning tilligger departementet etter § 2-7. Vi mener at det ikke er tillitsvekkende at etterretningen skal foreta denne avveiningen av motstridene hensyn selv og mener at beslutningen bør tas av en uavhengig instans, og aller helst underlegges en domstolsprøving. Til sammenligning kreves kjennelse fra retten når politiet skal benytte tvangsmidler ved kommunikasjonskontroll, jf. straffeprosessloven kapittel 16 a.

Vi mener det er svært viktig at særlige yrkesutøvere sikres et særlig vern. Her vil nedkjølingseffekten kunne være særlig skadelig. Om tanken på at man er overvåket, er berettiget eller ikke, er det svært problematisk om innbyggernes tillit til sentrale tjenester og instanser i samfunnet svekkes. Se for øvrig omtale av betydningen av nedkjølingseffekt på dette området i pkt. 4.3.1.

Vi mener at den foreslåtte bestemmelsen ikke gir tilstrekkelige vern for de aktuelle yrkesgruppene. Vi mener terskelen «strengt nødvendig» for behandling av slike opplysninger er for lav. Bruk av slike opplysninger bør bare strengt unntaksvis kunne benyttes, og et krav om rettskjennelser før behandlingen settes i gang vil kunne styrke tillit og minske den potensielle nedkjølingseffekten.

8 Krav til klare regler for utlevering av data

8.1 Innledning

Kravet til forutsigbar og tilgjengelig lovgivning innebærer at lovgiver må utforme klare regler om utlevering av data.

⁶⁷ ECJ, Case C-582/14, [Patrick Breyer v Bundesrepublik Deutschland](#)

Datatilsynet støtter en kodifisering av praksis og en samling av kravene til utlevering i en lovbestemmelse. Spørsmålet er imidlertid om den foreslåtte bestemmelsen er klar nok.

Det er bra at det er inntatt et krav til notoritet. Notoritet er nødvendig for at EOS-utvalget skal kunne overprøve lovligheten av utleveringer. Vi legger til grunn at departementet har foretatt en vurdering av om det fremgår tilstrekkelig klart av EOS-kontrolloven at dette er en oppgave som påligger utvalget. Dersom det er noen tvil om dette, mener vi det bør inntas en presisering av dette i loven.

I høringsnotatet pkt.13.3 fremgår det at departementet har vurdert hvem som bør tillegges beslutningskompetanse. Vi kan midlertid ikke se at det er foreslått noen regler om dette. Slik vi ser det bør vurderinger knyttet til utlevering gjøres av personer som er særlig utpekt, slik at det kan fungere som en sikkerhetsmekanisme.

8.2 Nasjonal informasjonsdeling

Vi savner en nærmere redegjørelse for *hvem* det er aktuelt å utlevere til, særlig gjelder det hvem som er aktuelle «andre offentlige myndigheter». Dette er i høringsnotatet forklart på en for overfladisk måte, med få konkrete eksempler.

Ordlyden i § 10-5 første ledd bokstav a, «fremme mottakerens oppgaver eller for å forhindre at virksomhet blir utøvd på en uforsvarlig måte», er temmelig vag og skaper dårlig forutberegnelighet. Nærmere regler om hvem det kan utleveres til og på hvilke vilkår kan med fordel fremgå i en forskrift. Se for eksempel politiregisterforskriften § 9-6, jf. politiregisterloven § 30.

8.3 Internasjonal informasjonsdeling

Etterretningen har et omfattende samarbeid med andre land om deling av informasjon. Det er viktig å ha klare regler om dette for å unngå en omgåelse av reglene om privatliv ved at alle stater fritt overvåker andre lands borgere, for så å dele informasjon med hverandre.⁶⁸

Et av vilkårene for utlevering er at utlevering skjer i overenstemmelse med forbudet i forslaget § 1-3 annet ledd. Vi foreslår at dette presiseres ved at det listes opp nærmere kriterier for vurderingen. I tilsvarende lov i Nederland er disse vurderingsmomentene uttrykkelig nevnt i loven. Jf. art. 88 Wet op de inlichtingen-en veiligheidsdienst 2017 (Wiv 2017), og blant annet følgende må vurderes: Den demokratiske 'embedding' av tjenesten (hvorvidt tjenesten er en del av en demokratisk rettstat), etterlevelsen av menneskerettigheter i landet det skal samarbeides med, profesjonalitet og pålitelighet av tjenesten, lovpålagte oppgaver og kompetanse, inklusiv kontrollmekanismer, og måten personopplysninger behandles og beskyttes på.⁶⁹

⁶⁸ Se også A/HRC/39/29, [The Right to Privacy in the Digital Age](#), Report of the United Nations High Commissioner for Human Rights, p. 21.

⁶⁹ [Wet op de inlichtingen- en veiligheidsdienst](#), (tilgjengelig på nederlandsk)

Å synliggjøre vurderingskriteriene i loven kan avhjelpe mangel av gjennomsiktighet på dette området. Dette er et område der det er høyere risikopotensiale enn andre områder, på grunn av manglende kontrollmekanismer.⁷⁰

8.4 Utlevering fra offentlige myndigheter til Etterretningstjenesten

Departementet viser til det de omtaler som «buyer beware»-prinsippet, altså at det er den som etterspør eller mottar informasjon som må vurdere om dens eget rettsgrunnlag tillater å etterspørre og behandle den aktuelle informasjonen.⁷¹ Dette mener vi er en for passiv tilnærming, sett hen til at det vil kunne være utlevering av opplysninger av sensitiv karakter.

Departementet foreslår en ny bestemmelse om at lovbestemt taushetsplikt ikke er til hinder for at offentlige myndigheter utleverer informasjon som er nødvendig innenfor etterretningens oppgaver.

Datatilsynet støtter ikke dette forslaget. Vi mener regler om opphevelse av taushetsplikt i størst mulig grad bør fremgå av lovgivningen som regulerer den aktuelle offentlige myndigheten. Dette for å skape forutberegnelighet og klarhet. Det bør gjøres konkrete avveininger knyttet til de konkrete myndighetens taushetsplikt og ikke i form av en generell opphevelse av taushetsplikt slik det er foreslått.

Vår erfaring er at offentlige etater enkelte ganger tror opphevelse av taushetsplikt er det samme som behandlingsgrunnlag for utlevering av opplysninger etter personopplysningsregelverket. Vi frykter derfor at den foreslåtte bestemmelse vil kunne bli oppfattet som en generell bestemmelse om rettslig grunnlag for utlevering, uten at det foretas en nærmere vurdering i det enkelte tilfelle.

Dersom forslaget opprettholdes bør det inntas en henvisning til § 9-6 om særskilte yrkesutøvere.

9 Forhåndskontroll ved domstolsprøving

9.1 Innledning

Departementet foreslår at kontrollregimet for tilrettelagt innhenting skal bestå av tre komponenter, forutgående domstolskontroll, løpende kontroll gjennom «styrket kontroll» og etterfølgende kontroll. Løpende og etterfølgende kontroll er det EOS-utvalget som skal stå for. Se nærmere om dette i kapittel 10. I dette kapitlet vil vi gi vår vurdering av forslaget om forhåndskontroll ved domstolsprøving.

Som tidligere nevnt er spørsmålet om systemet i sin helhet kan anses som proporsjonalt og «nødvendig i et demokratisk samfunn», avhengig av hvorvidt systemet omfatter nødvendige garantier mot misbruk og garanterer effektive rettsmidler. Forutgående domstolskontroll, og

⁷⁰ Å synliggjøre vurderingskriteriene i loven er også fremhevet som 'best practice' i "[Upping the Ante on Bulk Surveillance - An International Compendium of Good Legal Safeguards and Oversight Innovations](#)", Wetzling, Vieth, Böll-Stiftung, VOLUME 50, 2018, s.31

⁷¹ Høringsnotatet pkt. 13.3.2.1.

tilsyns- og kontrollsystemet må altså ses i sammenheng. En samlet vurdering av alle disse mekanismene må tilfredsstille kravene i EMK art. 8 og 13.

Krav til forhåndsgodkjenning (ex-ante kontroll) ved innsamling av data kan bidra til å begrense Etterretningstjenestens skjønnsutøvelse, og bidra til at tjenestenes maktutøvelse ikke går utover de rettslige rammene som lovgiver har satt. Et viktig kriterium for at forhåndskontroll skal fungere etter sin hensikt er at den er uavhengig.

Forhåndsgodkjenning ved en rettslig instans kan i seg selv ikke være en avgjørende eller tilstrekkelig form for kontroll, men det er et viktig element i et kontrollregime. Det vil også kunne styrke tilliten til at systemet ikke blir misbrukt.⁷² Forhåndskontroll er derfor ett av flere ulike kontrollelementer som til sammen må sørge for at Etterretningstjenesten holder seg innenfor sine fastsatte rammer.

Slik domstolskontrollen er utformet i forslaget vil den innebære en hemmelig forhåndskontroll ved Oslo tingrett. Behandlingen i sakene og kjennelsene vil ikke bli offentliggjort. Dette innebærer store utfordringer med hensyn til offentlighetens tillit til at det faktisk skjer en kontroll. Det må derfor stilles ekstra store krav til de prosessuelle og materielle reglene som skal gjelde for domstolskontrollen.

Tilrettelagt innhenting er underlagt domstolskontroll etter lovutkastets kapittel 8. Dette innebærer at søk i metadatalageret etter § 7-8 og innhenting og lagring av innholdsdata etter § 7-9 skal forhåndsgodkjennes av retten, jf. § 8-1. Det er videre foreslått bestemmelser om krav til kontroll av at søkene ikke innebærer brudd på lovens regler om diskrimineringsforbud mv, samt krav til skriftlig saksbehandling.

Datatilsynet ser grunn til å stille flere spørsmål ved forhåndskontrollordningen som foreslått.

9.2 Forhåndskontroll- ingen reell prøving av at vilkårene er oppfylt

Vi stiller spørsmål ved hvorvidt domstolen i praksis vil være i stand til å foreta en reell prøvelse. Loven stiller krav til hva retten skal prøve, men vurderingsmomentene er veldig vidt formulert.

Dette må ses i sammenheng med Etterretningstjenestens upresise/vide oppgaver.

Lovforslaget kapittel 3 angir Etterretningstjenestens oppgaver. Disse fremstår som veldig vidt angitt, og særlig oppgavene listet opp i § 3-2 er lite presise. I tillegg er grunnvilkårene for innhenting i § 5-1 og § 5-2 så vidt formulerte at det er vanskelig å tenke seg en reell prøving av om vilkårene er tilstede. Grunnvilkåret for målsøking, jf. § 5-1, er at det foreligger grunn til å undersøke om innhenting kan bidra til å frembringe informasjon som er relevant for etterretningsformål. Etterretningstjenesten kan altså gjøre søk dersom det i det hele tatt er en mulighet for at selve innhenting kan bidra til informasjon som kan være relevant for etterretningsformål. Med så vide oppgaver, og så vide hjemler for søk, vil det være vanskelig å si hva som er relevant informasjon eller ikke.

⁷² ECHR, [Big Brother Watch and others v. The United Kingdom](#), no. 58170/13, 62322/14 og 24960/15, 13.09.2018

Videre stiller lovforslaget svært få krav til begjæringen. Utover at denne må være skriftlig, stilles det kun krav om at den må angi hva eller hvem innhentingene retter seg mot og opplyse om det rettslige og faktiske grunnlaget for innhentingene.

Siden vilkårene er vidt formulert vil det kreve høy kompetanse hos dommerne for å kunne etterprøve nødvendighet og forholdsmessighet av tiltaket som det bes om godkjenning til. Dette krever igjen grundig innsikt og kunnskap i den etterretningsfaglige verdien som søkes oppnådd ved søk i informasjon og/eller lagring av innholdsdata.

Videre vil domstolen måtte foreta en vurdering av forholdsmessighet som innebærer at dommere må kunne overskue konsekvensene av det aktuelle tiltaket. Dette krever god kunnskap om de tekniske løsninger for å vite hvordan og hvem som vil bli rammet av tiltaket. Med de tekniske innretninger som er foreslått i høringsnotatet er vi bekymret for at kompleksiteten overstiger kompetansen til den jevnlig dommer i Oslo tingrett, selv om det blir en slik spesialisering som departementet foreslår.⁷³

Vi stiller spørsmål ved hvor realistisk disse kompetansekrav til dommerne er, og er bekymret for at de fleste dommere ikke vil ha de kunnskaper som kreves for å foreta en reel avveining av disse momentene. Dette vil i realiteten innebære en uthuling av domstolskontrollen.

I forslaget er det forsøkt å avdempe mangelfull teknisk ekspertise hos dommerne ved å åpne for at retten kan beslutte muntlige forhandlinger for å opplyse saken, og Etterretningstjeneste kan i så fall stille med fagkyndige, som antageligvis vil kunne belyse hva de tekniske løsninger vil innebære i praksis.

Dersom dette i praksis fører til at domstolen, for sin oppgaveløsning, vil være forbeholden bistand fra Etterretningstjenestens fagkyndige, er vi bekymret for at denne løsningen vil svekke domstolens uavhengighet.

Det vises for øvrig til at liknende ordninger har fått kritikk. Kritikken av rettens prøving i forbindelse med kommunikasjonskontroll har gått ut på at prøvingen fremstår som lite reell. I 2016 ble det brukt kommunikasjonskontroll i 135 saker. I to saker avslo tingretten politiets begjæring. I begge sakene ble det gitt tillatelse etter anke.

9.3 Begrenset forhåndskontroll

Vi stiller spørsmål ved at forhåndskontrollen er avgrenset til behandling av personopplysninger fremskaffet gjennom tilrettelagt innhenting, og at det ikke stilles krav til den samme type behandling av personopplysninger fremskaffet på annet vis. Etterretningstjenesten vil gjøre mange av de samme behandlingene av opplysninger (søk, lagring, bearbeiding) av informasjon fremskaffet ved andre innhentingsmetoder, som for eksempel ved midtpunktsinnhenting (rådata i bulk).

Vi ser ingen prinsipiell grunn til å forskjellsbehandle behandling av personopplysninger på basis av hvordan opplysninger teknisk sett er fremskaffet, og mener derfor at metodebruken

⁷³ Høringsnotatet pkt. 11.11.4.2

beskrevet i lovutkastets § 6-7 bør underlegges den samme forhåndskontrollmekanismen. Vi kan ikke se at argumentet med at dette ville blitt ressurskrevende kan tillegges særlig vekt.

Vi stiller videre spørsmål ved hvorfor nødvendighetskravet for behandling av fortrolig kommunikasjon med særlige yrkesutøvere etter § 9-6 ikke er gjenstand for forhåndskontroll.

Slik Datatilsynet forstår det, er ikke søk i fortrolig kommunikasjon omfattet av domstolskontrollen i kapittel 8. I § 8-4 som bestemmer hva retten skal prøve er ikke vilkårene i § 9-6 inkludert. Derimot er § 9-4 inkludert, noe som støtter tolkningen av at § 9-6 ikke skal prøves av retten. Det ville vært naturlig å inkludere bestemmelsen hvis man mente at den skulle kunne prøves.

Nødvendighetsvurderingen etter § 9-6 skal derfor foretas etter at søk har blitt gjennomført, og er foreslått overlatt til Etterretningstjenestens sjef. Se for øvrig pkt. 7.3

Dette innebærer at domstolen ikke kan ta stilling til om søket berører fortrolig kommunikasjon. Et eksempel vil kunne være søk rettet mot norske journalister som oppholder seg i utlandet, og dermed ikke er omfattet av den territoriale begrensningen i § 4-1.

Vi mener at denne gruppen har et særskilt beskyttelsesbehov som taler for at bruken av denne type opplysninger burde være underlagt forhåndsgodkjenning ved domstolskontroll.

9.4 Datatilsynets samlede syn på kontrollmekanismen forhåndskontroll

Departementet advarer, med god grunn, mot urealistiske forestillinger om hvor høy rettssikkerhet og godt personvern som kan oppnås ved å kreve at domstolen på forhånd må gi tillatelsen til metodebruken. De understreker også at den forutgående domstolskontrollen må sees i sammenheng med tilsyn- og kontrollsystem for øvrig. Noe som vi vil kommentere ytterligere i de neste to kapitlene. Likevel er det viktig at forhåndskontrollmekanismen innrettes på best mulig måte.

Datatilsynet mener det må være et absolutt krav om forhåndsgodkjenning av en domstol både ved søk i materiale som er innhentet etter tilrettelagt innhenting, men også ved midtpunktsinnhenting (rådata i bulk).

Videre mener vi at de aktuelle lovbestemmelsene bør gjennomgås med sikte på å klargjøre hvilke momenter og vilkår Etterretningstjenesten og domstolene skal foreta sine vurderinger etter, slik at bestemmelsene blir mindre skjønnsmessige.

I den forbindelse vil Datatilsynet peke på at det i den svenske lag om signalspaning § 4 a⁷⁴ stilles strengere krav til begjæringens innhold, blant annet stilles det krav om hvilke signaler/kilder/tilbydere man behøver adgang til, søkebegrep eller kategorier av søkebegrep og tidsrom for søkene.

⁷⁴ Lag (2008:717) [om signalspaning i försvarsunderrättelseverksamhet](#)

I lag om signalspaning § 5 a⁷⁵ stilles det også krav til selve kjennelsen som blant annet skal inneholde krav til tiltak for å begrense integritetskrenkelsen.

Vi mener at lignende krav som i den svenske lov bør inntas på en klarere måte i den norske loven.

Presiseringen i loven angående vurderingmomentene, som for eksempel finnes i den svenske loven, vil også være mer i tråd med 'best practice' på dette området.⁷⁶

10 Kontrollmekanismer

10.1 Innledning

Forslaget innebærer en videreføring av EOS-utvalgets opprinnelige oppgaver etter EOS-loven, men de har altså fått utvidede oppgaver ved det som omtales som styrket kontroll av tilrettelagt innhenting, jf. lovutkastets § 7-11. Utvalget får også kompetanse til å uttale seg om grunnlag for erstatningsansvar for det offentlige ovenfor klageren gjennom en endring i EOS-kontrollloven § 15.

I høringsnotatet er det gjort en grundig gjennomgang av de krav som EMK art 13 oppstiller med hensyn til uavhengighet, kompetanse til å prøve det materielle innholdet, krav til å sikre at en krenkelse opphører og mulighet til å gi en passende oppreisning. Vi har likevel mange merknader knyttet til de ulike delene av kontrollmekanismen.

Før vi kommenterer EOS-utvalgets egnethet til å inneha disse oppgaver, vil vi gå nærmere inn på noen av bekymringene vi har rundt selve kontrolloppgavene. Til slutt vil vi har vi merknader knyttet til spørsmål om ressurser og uavhengighet.

10.2 Løpende kontroll gjennom «styrket kontroll»

Departementet foreslår i § 7-11 at det skal føres «styrket kontroll» med at Etterretningstjenesten bare gjennomfører søk i henhold til rettens kjennelser, at korttidslageret og testdata ikke benyttes til etterretningsformål, og at de øvrige bestemmelsene i kapittel 7 etterleves.

EOS-utvalget skal ha uhindret adgang til all informasjon, interne retningslinjer og prosedyrer, lokaler, utstyr, programvarer, filteroppdateringer, aktivitetslogger og annet som benyttes for gjennomføring av virksomhet etter kapittelets 7.

Departementet skriver i høringsnotatet at de antar at denne styrkende kontrollen som foreslås er egnet til å motvirke nedkjølingspotensialet av tilrettelagt innhenting.

Bestemmelsen foreslått i høringsnotatet fraviker i betydelig grad fra den type løpende kontroll som ble foreslått i forbindelse med Lysne II-utvalgets rapport om digitalt

⁷⁵ Lag (2008:717) [om signalspaning i försvarsunderrättelseverksamhet](#)

⁷⁶ Overseeing Information Collection, L. Hutton, i "Overseeing Intelligence Services, A Toolkit". H. Born, A.Wills, DCAF, 2012, s.100

grenseforsvar. I Lysne II-rapporten ⁷⁷ble det foreslått opprettelse av et «DGF-tilsyn» utenfor EOS-utvalget. Det ble foreslått at DGF-tilsynet skulle ha følgende oppgaver:

- I nær sanntid motta all informasjon om alle søk som gjøres i alle datasamlinger i DGF-systemet, motta alle avgjørelser fra DGF-domstolen, ha tilgang til all informasjon om hvordan filtrene er implementert og konfigurert, og ha tilgang til all informasjon om hvordan interne retningslinjer og avgjørelser fra domstolen er oversatt til søkeprivilegier.
- Rapportere avvik til EOS-utvalget og for øvrig rapportere regelmessig til EOS-utvalget, Forsvarsdepartementet og Samferdselsdepartementet. Avvik skal i den sammenheng være brukt av DGF-systemet som ikke er hjemlet i lov om Etterretningstjenesten (etterretningstjenesteloven), domstolens avgjørelser, eventuelle forskrifter og interne retningslinjer.
- Føre tilsyn med at datasikkerheten i DGF-systemet er så høy som teknologisk og praktisk mulig.

Datatilsynet, på samme linje som forslaget i Lyse II, mener det er avgjørende for å opprettholde tillitt at det føres et *kontinuerlig* tilsyn og en tilstrekkelig kontroll med innhenting og søk i elektronisk kommunikasjon.

Forslagets § 7-11 om EOS-utvalgets styrkede kontroll gir ikke den nødvendige kompetansen til å føre et tilstrekkelig tilsyn. Det er også uheldig at ordningen med «styrket kontroll» ikke omfatter innhenting av rådata i bulk. Slik bestemmelsen er utformet innebærer den i realiteten kun etterkontroll ved at EOS-utvalget gis uhindret adgang, men Etterretningstjenesten pålegges ikke en løpende rapporteringsplikt. I høringsnotatet 11.12.8 presiseres det at adgang skal gis etter «forespørsel». Forskjellen på løpende og etterfølgende kontroll vil da kun være om tiltaket fortsatt pågår eller ikke, og kontrollen vil basere seg på hva EOS-utvalget ber om. Lysne II foreslo at informasjon skal mottas «i nær sanntid» noe som er et viktig element for å forhindre misbruk, men dette er ikke fulgt opp i lovforslaget.

Etter vårt syn ivaretar ikke loven kravet til løpende kontroll og selv med en betydelig personellmessig styrking av EOS-utvalget, vil ikke dette være tilstrekkelig. Kontrollen bør innrettes ved at Etterretningstjenesten pålegges en plikt til å opprette systemer og rutiner for kontinuerlig rapportering. Dette vil kunne bidra til å forhindre misbruk, og rapporteringsplikten vil fremme kravet til åpenhet og kontroll kontinuerlig i arbeidet. Dette er spesielt viktig når kontrollrutinene og resultat ikke er tilgjengelig for offentligheten.

Vi anbefaler videre at det gjøres en grundigere vurdering av muligheten for tekniske løsninger som tilrettelegger for mer effektiv løpende kontroll, gjennom en kombinasjon av manuell og automatisert maskinell kontroll.

I denne vurdering bør det tas hensyn til personvernprinsippet om «innebygd personvern». Dette prinsippet betyr at når det skal utformes et nytt system, skal det tenkes personvern helt fra starten av ved utarbeidelsen av kravspesifikasjoner. I dette tilfellet betyr det at det

⁷⁷ [Digitalt grenseforsvar \(DGF\)](#), Lysne II-utvalget, 26.08.2016

må stilles krav til kontrollfunksjonalitet på lik linje med operasjonell funksjonalitet, slik at kravet om effektiv kontroll (ved EOS-Utvalget) gjennom notoritet kan etterleves.

I denne forbindelse minner vi også om oppfordringen som ble gitt i rapporten til Evalueringsutvalget for EOS-utvalget. Det må vurderes muligheter på et *teknologisk nivå* for tilrettelegging for kontroll som integreres i prosessene knyttet til vurdering og implementering av nye metoder i tjenestene.⁷⁸ Dersom kontrollfunksjonen tillegges i etterkant vil dette sannsynligvis være langt mindre effektivt enn dersom det er en del av det opprinnelige konseptet. I tillegg har dette en økonomisk aspekt, ved at det vil være langt mer kostbar å legge inn kontrollfunksjoner i ettertid.⁷⁹

Kun gjennom en lovfestet plikt til å tilrettelegge kontrollen gjennom tekniske løsninger vil den løpende kontroll kunne være meningsfull og effektiv. Slik forslaget er utformet per i dag, er tilretteleggingsplikten for løpende kontroll av Etterretningstjenesten ikke klart nok beskrevet.

Teknisk tilrettelegging for løpende kontroll har for øvrig en sterk sammenheng med øvrige spørsmål om EOS-utvalgets ressurser som vi vil kommentere nedenfor i pkt. 10.4.

10.3 Etterkontroll

I tillegg til løpende kontroll, er etterkontroll et viktig element i den totale kontrollmekanismen. Etterkontroll vil i hovedsak skje i to spor, gjennom tilsyn og gjennom klagebehandling.

Når det gjelder tilsyn, foreslår departementet i § 7-10 at det skal føres aktivitetslogger for kontrollformål. Etterretningstjenestes informasjonssystemer skal ha en funksjonalitet som sikrer at alle søk skal kunne kontrolleres i ettertid gjennom aktivitetslogger. Aktivitetsloggene skal oppbevares i 10 år, og skal til enhver tid være tilgjengelig for kontroll.

Etter vår forståelse (også basert på dagens praksis) må dette betegnes som en stikkprøvekontroll. Selv om det er ikke mulig, og heller ikke ønskelig, at et kontrollorgan har full kontroll over sine kontrollobjekter, må det stilles spørsmål ved hvor effektiv denne stikkprøvekontrollen vil være. Dersom det viser seg at bruk av stikkprøvekontroller fører til at kun 3 prosent av etterretningsvirksomheten blir kontrollert, vil dette svekke tilliten til kontrollsystemet.

For etterkontroll gjør mange av de samme bekymringene seg gjeldende som for løpende kontroll. At bestemmelsen nevner aktivitetslogger spesifikt er et bra utgangspunkt, men det er også her behov for tekniske løsninger som kan automatisere og effektivisere analyse av loggene, og dermed gjøre det lettere å oppdage avvik og eventuelt misbruk.

Videre er et viktig element i vurderingen av kontrollmekanismens effektivitet hvorvidt kontrollorganet er i stand til å sikre at en krenkelse opphører. Kontrollmyndigheten bør ha myndighet til å sikre at, dersom de kommer til at inngrepet var ulovlig, inngrepet avsluttes

⁷⁸ EOS Evalueringsrapport, [Dokument 16](#), 2015-2016, s. 11

⁷⁹ EOS Evalueringsrapport, [Dokument 16](#), 2015-2016, s. 152

og at ulovlig materiale slettes. Dette kravet må være oppfylt i lov, så vel som i praksis. Vi vil omtale dette nærmere under vår vurdering av klagemuligheter.

10.4 Nærmere om EOS-utvalget- uavhengighet og ressurser

I følge lovforslaget er det EOS-utvalget som skal gjennomføre både den løpende kontrollen, etterfølgende kontroll og behandle klager. EOS-utvalget vil være et viktig, om ikke det viktigste, elementet i kontrollmekanismen som skal motvirke misbruk.

EOS-utvalget har nylig blitt evaluert, og selv om mandatet til evalueringsutvalget har vært begrenset, vil vi ikke overprøve deres funn. Likevel mener vi at de nye oppgavene som EOS-utvalget vil bli satt til å gjøre, inviterer til refleksjon på noen viktige punkter.

10.4.1 Utvalgets uavhengighet

Det er ingen tvil om at EOS-utvalget, med sin forankring i Stortinget, oppfyller kravet til uavhengighet. Vi mener imidlertid at det er grunn til å påpeke at de utvidende oppgavene og funksjonene som dette lovforslaget legger opp til, vil sette EOS-utvalgets uavhengighet under press.

Når det gjelder utvalgets sammensetning stiller loven ikke noen særlige kompetansekrav til utvalgets medlemmer. Hvorvidt dette er ønskelig har blitt drøftet i rapporten til Evalueringsutvalget om EOS-Utvalget. I rapporten ble det forslått å lovfeste at minst tre medlemmer (av syv) bør ha sterk juridisk, teknologisk og EOS—eller sikkerhetsfaglig innsikt.⁸⁰ Denne anbefalingen ble dessverre ikke fulgt opp i endringsloven av 21. juni 2017 nr. 95.

De systemene som EOS-utvalget skal føre kontroll med er særdeles spesialisert og såpass komplekse at det kreves en svært god teknologiforståelse av utvalgets medlemmer. Kontroll med om søkekriteria er i henhold til domstolens kjennelse vil sannsynligvis i stor grad være basert på en høyteknologisk øvelse, i tillegg til det juridiske. I praksis vil tilsyn derfor i stor grad være avhengig av tekniske eksperter, som det per i dag ikke stilles krav til i utvalgets sammensetting.

Problemene med manglende teknologisk (og for så vidt juridisk) kompetanse i EOS utvalget, er til dels kompensert gjennom et faglig sterkt sekretariat, hvor det blant annet har blitt opprettet en teknologisk enhet. Likevel minner vi om at sekretariatet ikke har den samme uavhengigheten som utvalgets medlemmer. Dersom utvalgets medlemmer i for stor grad blir avhengig av den juridiske og teknologiske kompetansen i sekretariatet, kan det sås tvil om utvalgets uavhengighet er troverdig.

10.4.2 Utvalgets ressurser

For at kontrollen i realiteten skal kunne være effektiv, er det strengt nødvendig å bevilge de tiltrengte ressurser som denne viktige oppgaven trenger.

I denne forbindelse vil vi påpeke at med de ressurser som EOS-utvalget per i dag har til disposisjon, vil kontrollen betegnes som stikkprøvebasert. Det må vurderes om

⁸⁰ EOS Evalueringsrapport, [Dokument 16](#), 2015- 2016, kapittel 37.1

stikkprøvekontroll vil være tilstrekkelig når fullmaktene og datamengdene som Etterretningstjenesten behandler vokser betydelig.

I vurderingene rundt økonomiske og administrative konsekvenser knyttet til kontrollmekanismen, anslår departementet at en styrking av EOS-utvalgets sekretariat med fire årsverk vil være tilstrekkelig for å ivareta de nye kontrollfunksjonene.⁸¹ Etter vårt syn vil en økning med fire stillinger neppe være nok.

For det første fordi EOS-utvalgets oppgaver per i dag kreve at sekretariatet styrkes for å løse deres kontrolloppgaver på en mer tilfredsstillende måte enn stikkprøvekontroll. Dette anses som høyst nødvendig for å bevare tilliten til at misbruk faktisk oppdages.

For det andre fordi den nye oppgave med «styrket kontroll» vil kreve mye tilstedeværelse. I denne forbindelse minner vi også om at i Lysne II om DGF forslaget, ble det ansett som nødvendig at et helt eget organ fører en nesten kontinuerlig kontroll.

Til slutt mener vi at det vil være naturlig å forvente at EOS-utvalget vil motta flere klager, simpelthen på grunn av den åpenhet om metodebruk denne loven gir og manglende krav på underretning, som vil føre til at flere personer vil føle seg nødt til å sende inn en klage for å få avdekket om det har blitt gjort urett mot dem.

Vi mener at departementets anslag om behov for fire ekstra stillinger ikke er realistisk, sett i lys av de viktige oppgavene EOS-utvalget har og vil få. Dersom det organet som skal utgjøre en sentral del av kontrollmekanismen ikke gis de nødvendige ressurser til å i praksis kunne være effektive, er vi sterkt i tvil om kravet om effektiv kontroll vil kunne anses oppfylt.

11 Klagemulighet og mulighet for oppreisning

11.1 Innledning

I tillegg til krav om etterfølgende kontroll gjennom tilsyn, følger det av en samlet tolkning av EMK art.8 og 13, at den som mener seg utsatt for en krenkelse skal kunne klage til en uavhengig kontrollinstans. Dette omtales som et krav til effektivt rettsmiddel.

For at et rettsmiddel skal kunne anses som effektivt, må flere kriterier være oppfylt: kontrollinstansen må være uavhengig, den må ha kompetanse til å prøve det materielle innholdet i klagen og den må kunne sikre at en krenkelse opphører. For hvert enkelt rettsmiddel må disse tre hovedkriteriene være tilstede, både i lov og i praksis, for at rettsmiddelet kan anses som effektivt.⁸²

⁸¹ Høringsnotatet pkt. 11.16.6.3.

⁸² ECHR, [Segerstedt-Wiberg and others v Sweden](#), no 62332/00, 06.06.2006 para 120-122. Se også United Nations Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including their oversight. United Nations document A/HRC/14/16 (17 May 2010). s.11

Før vi går nærmere inn på en vurdering av de institusjonelle aspektene ved klagebehandling, vil vi si noe om «retten til underretning», som er et viktig moment i vurderingen av hvor effektivt et kontrollsystem, og særlig klagebehandling, vil være.

11.2 Manglende underretning til de berørte

Et sentralt personvernprinsipp er åpenhet, noe som stiller krav til informasjon til den registrerte om hva som har blitt registrert. Dette gjør den registrerte i stand til å ta i bruk sine rettigheter, til for eksempel å klage på etterretningstjenesters praksis. Det er tross alt vanskelig å klage på noe man ikke vet har skjedd.

Selv om disse rettighetene ikke kan gjøres fullt ut gjeldende på grunn av Etterretningstjenestens nødvendigvis skjulte metoder, så bør man tilstrebe å gjøre dette på best mulig måte.

Ved bruk av skjulte tvangsmidler krever EMD at den det gjelder blir underrettet om tiltaket i etterkant, så snart dette kan skje uten å skade det formålet som tiltaket hadde.⁸³

Departementet hevder i høringsnotatet at retten til underretting er et vurderingsmoment, og ikke en absolutt rettighet etter EMK art. 8. På den bakgrunnen foreslår departementet i § 11-8 at den som har vært gjenstand for informasjonsinnhenting, som kan innebære inngrep i dennes menneskerettigheter, ikke har krav på underretning om inngrepet.

Det er riktig at EMD i noen tilfeller har funnet at mangelfulle underretning *i praksis* var akseptabelt. Avgjørende i disse sakene var en vurdering av hvorvidt det finnes gode løsninger som gjør at klageordningen likevel kan fungere uten underretning. For eksempel ved å gi vid adgang til å klage og at organet som behandler klagen er i stand til å få krenkelsen til å opphøre eller sikre passende oppreisning.

Sammenholdt med unntakene fra lov om rett til innsyn i dokument i offentlig verksemd (offentleglova) § 11-6, innebærer § 11-8 en nærmest total begrensning av retten til innsyn og underrettelse. Selv om det foreligger en mulighet til å klage til EOS-utvalget uten å måtte påvise den konkrete urettmessigheten, er dette svært uheldig fordi dette fritar Etterretningstjenesten fra enhver forpliktelse til å vurdere åpenhet fra sak til sak.

Vi foreslår at innretningen i bestemmelsen snus, slik at den formuleres som en rettighetsbestemmelse, men med noen klare unntak. Altså at underretning skal skje, med mindre gode, spesifikke og lovfestede grunner tilsier at det må gjøres unntak.

En slik unntaksbestemmelse vil være snevrere og mer spesifikk enn en bestemmelse om fullstendig fritak, siden den forplikter Etterretningstjenesten til å rettferdiggjøre fra sak til sak hvorfor retten til underretning ikke burde gjelde i det spesifikke tilfellet. Dette vil gi en helt annen signaleffekt og øke tilliten til tjenesten.

En kontinuerlig vurdering av om underretning skal gis, og en plikt til å underrette der hvor Etterretningstjenesten behov ikke medfører hemmelighold, vil bidra til en bevisstgjøring hos

⁸³ ECHR, [Centrum för rättvisa v. Sweden](#), no. 35252/08, 10.06.2018

tjenesten. Vurderingen om underretning kan i så fall også være gjenstand for kontroll ved EOS-utvalget, noe som igjen kan bidra til å øke tilliten utad ytterligere.

Departementet antyder videre at det å ikke underrette er i overensstemmelse med etablert praksis for de fleste sammenlignbare utenlandske etterretningstjenester.⁸⁴ Departementet klargjør ikke hvilke lands praksis det sikter til. Land som vi mener det er naturlig å sammenligne oss med, for eksempel, Sverige, Nederland og Tyskland⁸⁵, har ikke fullstendig fritak fra underretningsplikten fastsatt i lov.

Tvert imot pålegger for eksempel den svenske lag om signalspaning §§ 11 a og b⁸⁶ en plikt til å underrette en fysisk person hvor det har blitt benyttet et søkebegrep som direkte kan knyttes til denne personen. Underretning skal sendes snarest, eller senest 1 måned etter at innhenting er avsluttet og skal inneholde opplysninger om når innhenting skjedde og formålet med den. Underrettelse skal ikke sendes dersom det er til skade for Etterretningstjenestens virksomhet.

I Nederland gir art. 59 Wiv 2017 pålegg om at det skal vurderes om det kan gis informasjon til en berørt om bruk av tvangsmidler fem år etter tiltaket opphører. Hovedregelen er at informasjon skal gis dersom dette er mulig og ikke er til hinder for at etterretningstjenesters kilder, samarbeidspartner eller spesifikke metoder vil bli avslørt. Dersom vurderingen tilsier at informasjon ikke kan gis, må dette begrunnes skriftlig og meddeles til kontrollorganet. Videre må denne vurderingen gjøres på nytt hvert år.

Selv om retten til underrettelse etter disse bestemmelsene er begrenset, så tilfører de en viktig rettsikkerhetsmekanisme som vi mener mangler i det norske forslaget.

I denne forbindelse minner vi på fortellinger som kom etter at Lund-rapporten⁸⁷ ble publisert. Det kom frem hvordan overvåkingen hadde påvirket den enkelte og gitt enkelte en følelse av paranoia som først ble forløst ved informasjon om at de faktisk hadde blitt overvåket.⁸⁸

Vi er klar over at selv med en slik unntaksbestemmelse, vil underretning *i praksis* ofte ikke skje. Det kan argumenteres med at denne erkjennelsen i seg selv taler for en fritaksbestemmelse slik departementet har foreslått, altså at en unntaksbestemmelse bare vil bli illusorisk.

Likevel mener vi at en unntaksbestemmelse i tråd med eksemplene over vil kunne ha en oppdragende og tillitsvekkende effekt, og at dette veier opp for ulempene av den forventete begrensede gjennomføring i praksis.

⁸⁴ Høringsnotatet pkt.14.9.3

⁸⁵ For en henvisning til Tysk lov, se *Overseeing Intelligence Services, a Toolkit*, s.116

⁸⁶ Lag (2008:717) [om signalspaning i försvarsunderrättelseverksamhet](#)

⁸⁷ Dokument nr. 15 (1995–96) – Rapport til Stortinget fra kommisjonen som ble nedsatt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere

⁸⁸ Nordlys, "[Overvåket i årevis](#)", Jangås, 30.06.2003

I tillegg er en unntaksbestemmelse kun tillat dersom et effektivt kontrollsystem er på plass. I det følgende kapitelet vil vi vurdere hvorvidt dette er tilfellet.

11.3 EOS-utvalgets behandling av klager fra individer

EOS-utvalget kan behandle klager fra individer. Departementet foreslår å endre EOS-kontrolloven § 5 femte ledd, slik at utvalgets kontrolloppgaver skal omfatte enhver person, uavhengig av bosted eller statsborgerskap, som er underlagt norsk jurisdiksjon. Dette vil sørge for at det både rettslig og reelt sett vil være en vid klageadgang.

Det skal ikke stilles noen materielle krav til klagens innhold, slik at det ikke skal være nødvendig å vise til en konkret krenkelse for å fremme en klage. At klageadgangen er vid og at det er ingen materielle krav til klagens innhold, er en tvingende nødvendig konsekvens av den manglende underretning til den berørte.

Om adgangen til å fremme en klage er vid eller ikke, har ingen betydning dersom behandlingen av klagen ikke kan anses å være et effektivt rettsmiddel. Igjen må altså alle tre kriteriene om uavhengighet, kompetanse til å prøve det materielle innholdet og kompetanse til å sikre at en krenkelse opphører, være oppfylt.

Det er ingen tvil om at EOS-utvalget, når de mottar en klage, vil være i stand til å prøve det materielle innholdet i klagen. Vi har, utover noen bemerkninger nedenfor i pkt. 10.4.1 heller ingen bemerkninger til EOS-utvalgets uavhengighet. Vi stiller imidlertid spørsmålstegn ved EOS-utvalgets kompetanse til å kunne sikre at en krenkelse opphører.

EOS-utvalget har kun «rett til å uttale sin mening», jf. EOS-kontrolloven § 14 første ledd, og kan ikke fatte juridisk bindende vedtak. Det er ikke foreslått å gi utvalget slik kompetanse heller. Departementet foreslår derimot en endring i EOS-kontrolloven § 15, slik at EOS-utvalget skal få myndighet til, i tillegg til å uttale seg om en klage har gitt grunn til kritikk eller ikke, å uttale seg om utvalget mener det er grunnlag for erstatningsansvar fra det offentlige overfor klageren.

I de forbindelsene bemerker Departementet at EOS-utvalgets kontroll i praksis alltid følges opp av EOS-tjenestene og at en sak i ytterste konsekvens kan bli håndtert i de formelle prosessene mellom Stortinget og Regjeringer.⁸⁹ Departementet anser derfor at kravet om at klageorganet skal kunne sørge for at menneskerettskrenkelser opphører er ivaretatt.

Vi er usikre på om dette er riktig.

Om en anbefaling fra EOS-utvalget om sletting av opplysninger eller oppreisning i en enkelt klagesak følges opp eller ikke, vil være opp til den utøvende makt. Selv om EOS-utvalgets anbefalinger tidligere har blitt fulgt i praksis, er dette ingen garanti for at dette vil vedvare i fremtiden. Mangelfull oppfølging vil meddeles utvalget, men ikke nødvendigvis den person klagen gjelder. EOS-utvalget kan, når det selv bestemmer, informere Stortinget om saken.

⁸⁹ Høringsnotatet pkt. 4.3.6.

Vi anser det imidlertid som lite sannsynlig at Stortinget i så fall vil stille et statsråd til ansvar for manglende oppfølging i en enkelt sak. Vi mener derfor at EOS-utvalgets kompetanse til å sikre at en krenkelse opphører hverken rettslig eller i praksis vil være tilstede.

11.4 Domstolsprøving

Kravet om effektive rettsmidler etter EMK art. 13 vil også kunne være oppfylt med en effektiv klageadgang for domstolene. Det kan tenkes at en klager som har fått medhold fra EOS-utvalget og som har uttalt seg om en anbefalt erstatning, ønsker å gå til en domstol for å få sin sivile sak prøvd for retten.

Når det gjelder kravet om uavhengighet og kravet til å kunne sikre at en krenkelse opphører, har vi ingen bemerkninger. Vi har imidlertid store bekymringer knyttet til domstolens kompetanse til å prøve det materielle innholdet i saken.

Grunnloven § 95 sier at enhver har rett til å få sin sak avgjort av en uavhengig og upartisk domstol innen rimelig tid. De nærmere villkårene for å kunne fremme en sivil sak for domstolene er regulert i lov om mekling og rettergang i sivile tvister (tvisteloven) § 1-3.

Som departementet anerkjenner, vil tvisteloven § 22-1 kunne være til hinder for en reell domstolsprøving. I henhold til denne bestemmelsen kan det ikke føres bevis om noe som holdes hemmelig av hensyn til rikets sikkerhet eller forholdet til fremmed stat. Føring av slik bevis krever samtykke fra Kongen. Det kan dermed hevdes at regjeringen kan blokkere at viktige bevis føres for retten. Dette vil kunne være et hinder for domstolsprøvingen av saker som omhandler Etterretningstjenesten, siden deres virksomhet utvilsomt vil måtte være hemmelig.

Departementet antyder i høringsnotatet at dette er et rent hypotetisk problem, og at det må forventes at regjeringen i praksis vil vurdere hver forespørsel konkret.⁹⁰ Departementet mener derfor at bevisforbudsregelen ikke i seg selv betyr at adgangen til domstolen er stengt og dermed ikke fyller kravet til et effektivt rettsmiddel.

En vurdering av effektiviteten av et rettsmiddel må vurderes utfra både den praktiske og den rettslige tilstanden. Selv om, som departementet skriver, det i praksis *kan* skje at domstolen gjør en materiell vurdering, vil dette etter vårt syn ikke være det samme som å inneha full kompetanse til å prøve det materielle innholdet. Domstolens kompetanse vil i denne sammenhengen være avhengig av den utøvende makts beslutning til å frigi bevis i en konkret sak.

På grunn av bevisavskjæringsproblematikken oppfyller domstolen ikke kravet til å ha rettslig kompetanse til å prøve det materielle innhold. Domstolsprøving oppfyller derfor kun to av de tre kriteriene, og kan dermed, slik vi ser det, ikke anses som et effektivt rettsmiddel.

Departementet hevder at det at domstolen kanskje ikke kan anses som et effektivt rettsmiddel ikke vil være problematisk, fordi EOS-utvalgets klagebehandling alene kan anses som et tilstrekkelig effektivt rettsmiddel.⁹¹ Som vi har påpekt ovenfor kan EOS-utvalgets

⁹⁰ Høringsnotatet pkt. 4.3.6.

⁹¹ Høringsnotatet pkt. 4.3.6.1.

klagebehandling neppe alene anses som et effektivt rettsmiddel, fordi EOS-utvalget som nevnt mangler kompetanse til å sikre at en krenkelse opphører.

Departementet kommer, etter en helhetsvurdering, til at kravene om et effektivt rettsmiddel er oppfylt.⁹² Vi kan ikke se hvordan, når verken domstolsprøving eller EOS-utvalgets klagebehandling hver for seg kan anses som tilfredsstillende. Disse to mekanismene tilsammen vil oppfylle kravet om et effektivt rettsmiddel. I dette tilfellet gjelder ikke regelen om at mangler ved et rettsmiddel kan kompenseres ved et annet mangelfullt rettsmiddel. To ineffektive rettsmidler blir ikke effektive fordi de ses i sammenheng.

11.5 Behov for grundigere vurdering av kontrollmekanismen

Problemstillingen om EOS-utvalgets manglende vedtakskompetanse ble drøftet i evalueringsrapporten om EOS-utvalget⁹³. Evalueringsutvalget viste til at i professor Husabøs utredning om grunnlovens og EMKs krav til etterfølgende kontroll er det pekt på at, blant annet på grunn av EOS-utvalget manglende vedtakskompetanse, er det usikkert om EOS-utvalgets klagebehandling i seg selv er nok til å oppfylle kravene til et effektivt rettsmiddel.

Evalueringsutvalget hadde imidlertid ikke anledning til å gå nærmere inn på disse spørsmålene, og peker på at en bredere evaluering av det *samlede kontrollsystemet* som EOS-tjenestene er underlagt er nødvendig og «bør vurderes og integreres i eventuelle fremtidige prosesser knytte til utvikling av EOS-tjenestenes fullmakter og virksomhet.»⁹⁴

Det er altså sterke holdepunkter for å si at dagens kontrollsystem ikke oppfyller kravene som stilles til effektiv klagebehandling. Dersom det er tilfellet, mener vi at det hadde vært naturlig å se på mulighetene for å revurdere eller forbedre dagens kontrollmekanismer i forbindelse med dette lovforslaget.

Departementet bemerker at «Dersom man skulle mene at kravene til effektiv rettergang etter EMK art. 13 ikke er oppfylt antar departementet at hele kontrollsystemet som sådan må settes under lupen.» Dette vil kreve en bred evaluering av det norske kontrollsystemet. Noe som, gitt EOS-utvalgets forankring, etter departementets syn må initieres av Stortinget.⁹⁵

Det er skuffende at det nå, etter arbeidet fra evalueringsutvalget i 2016 og det omfattende høringsnotatet som departementet har presentert, må enda et utredningsarbeid til for å finne en løsning som vil tilfredsstillende kravene i art. 13.

Vi kan ikke se at det er noe i veien for at departementet kan gjøre en slik vurdering. Tvert imot mener vi at det hadde vært riktig tidspunkt å foreta denne vurderingen i forbindelse med dette lovforslaget, ettersom en utvidelse av Etterretningstjenestes myndighet/kapasitet krever at tilfredsstillende kontrollmekanismer øker i samme takt. Etter vår mening er dette to sider av samme sak.

⁹² Høringsnotatet pkt. 4.3.6.5.

⁹³ EOS Evalueringsrapport, [Dokument 16](#), 2015- 2016, særlig Vedlegg 4.

⁹⁴ EOS Evalueringsrapport, [Dokument 16](#), 2015- 2016, s. 129

⁹⁵ Høringsnotatet pkt. 4.3.6.3

For eksempel kunne en tilnærming ha vært å søke å forbedre domstolsprøvingen ved å vurdere hvorvidt problemstillingen med bevisavskjæring kunne løses ved en eventuell lovendring. Som professor Husabø bemerket i sin utredning, finnes det eksempler på at endringer i domstolprosessen kan gjøre det mulig å få til en reell mulighet for overprøving i saker som involverer gradert informasjon.⁹⁶ Vi kan ikke se at departementet har vurdert dette i høringsnotatet.

Når det gjelder forbedring av eller utvidelse av EOS-utvalgets kompetanse, viser departementet i høringsnotatet pkt. 4.3.6.3. til evalueringsrapporten og begrunner hvorfor departementet mener at EOS-utvalget ikke bør ha vedtakskompetansen ovenfor Etterretningstjenesten. De mener dette ville «rokke ved grunnleggende prinsipper i vårt statsrettslige system og maktfordeling mellom regjering og Stortinget.»⁹⁷

Dersom departementet fastholder at EOS-utvalget ikke *kan* ha vedtakskompetanse på grunn av konstitusjonelle forhold, mener vi at det er nødvendig å vurdere om et kontrollsystem med forankring i Stortinget virkelig er det beste virkemiddelet for å ivareta den enkelte borgernes rettigheter.

Departementet har ikke foretatt en slik vurdering⁹⁸, og har heller ikke foreslått forbedringer som gjør at dagens kontrollsystem oppfyller kravene i art. 8 og 13 EMK. Dette mener vi er høyst problematisk.

Etter vårt syn er det derfor (fortsatt) nødvendig å revurdere kontrollsystemet i sin helhet. Et naturlig utgangspunkt for denne vurderingen er å først fastsette hvilke kriterier som må oppfylles. Etter EMDs praksis er det som nevnt tre hovedkriterier, at kontrollinstansene er uavhengige, har kompetanse til å prøve det materielle innholdet, og at de må kunne sikre at en krenkelse opphører.

FNs spesialrapportør har også understreket behovet for at et uavhengig organ har tilgang til alt materiale relatert til tjenestenes virksomhet og har myndighet til å beslutte at informasjon skal gis til berørte personer, samt myndighet til å beordre sletting av informasjon.⁹⁹ Videre er det hensiktsmessig å se hen til praksis i andre land. For eksempel har både Nederland¹⁰⁰ og Sverige¹⁰¹ uavhengige organer med vedtakskompetanse.

⁹⁶ EOS Evalueringsrapport, [Dokument 16](#), 2015- 2016, Vedlegg 4 s.260

⁹⁷ Høringsnotatet pkt. 4.3.6.3

⁹⁸ Departementet har gitt en beskrivelse av de forskjellige elementer i kontrollsystemet i kapittel 6.7 og 4.3. men har kun gjort en vurdering av alternative kontrollmekanismer når det gjelder løpende kontroll for tilrettelagt innhenting.

⁹⁹ United Nations Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including their oversight. United Nations document A/HRC/14/16 (17 May 2010). S.22 (Practice 25).

¹⁰⁰ [Wet op de inlichtingen- en veiligheidsdiensten](#), artikkel 124, (tilgjengelig på nederlandsk)

¹⁰¹ I Sverige har kontrollorganet vedtakskompetanse til å beordre at innhenting eller søk skal opphøre eller at data skal slettes. Vedtakskompetansen gjelder ikke oppreisning.

Et viktig argument for at dette systemet av klagebehandling likevel ble vurdert som et effektivt rettsmiddel er at oppreisning kunne søkes gjennom domstolene eller gjennom «Chancellor of Justice». Se ECHR, [Centrum för rättvisa v. Sweden](#), no. 35252/08, 10.06.2018

Vi mener at et kontrollsystem må skisseres ut fra nevnte tre kriterier. Det fremstår som at det i høringsnotatet ikke har vært kriteriene som har vært utgangspunktet, men i stedet har man tatt utgangspunkt i de eksisterende kontrollmekanismer, for så å prøve å forsvare at kriteriene er oppfylt. Dette er etter vårt syn å begynne i feil ende.

Vi anbefaler at det igangsettes et arbeid med sikte på å foreta en helhetlig gjennomgang og vurdering av kontrollmekanismen, slik at kvaliteten i kontrollmekanismen øker i takt med utvidelsen av etterretningstjenesters oppgaver.

12 Proporsjonalitetsvurderingen

For at et lovforslag kan anses som proporsjonelt, og dermed innenfor de menneskerettslige skranker, må det vurderes hvorvidt den skaden som er gjort ved inngrepet er minsket ved egnede tiltak som reduserer virkningen av skaden. Jo større inngrepet er, desto mer robust må tiltakene være for å avdempe ulempene ved at et slikt system innføres.

Før man kan vurdere om tiltakene er gode nok, må man ha en klar forståelse av hvor stort inngrepet egentlig er.

I henhold til EMDs praksis oppstår inngrepet i personvernet allerede ved selve innhenting, uavhengig av videre bruk eller søk i opplysninger. Det er også på dette tidspunktet at de skadelige effekter, som for eksempel nedkjølingseffekten, oppstår.

Som vi skriver i kapittel 4 mener vi at høringsnotatet og departementets uttalelser i den offentlige debatten, synes å bagatellisere de negative konsekvensene. Vi mener forslaget utgjør et betydelig større inngrep i norske borgeres privatliv enn det departementet gir uttrykk for, og at skadepotensialet for vårt demokratiske samfunn utvilsomt er tilstede.

I tillegg blir de negative konsekvensene for personvernet forsterket av en uklar beskrivelse av tiltakene. Ut fra den tekniske beskrivelsen vil systemet i praksis sannsynligvis ramme nesten hele Norges befolkning.

På grunn av vagt begrepsbruk i lovforslaget, samt uklarheter om hvem som omfattes av tilretteleggingsplikten og effekten av filtrene, er det stor usikkerhet rundt hvem som faktisk rammes. Dette gjør at Datatilsynet mener at kravet til klarhet og forutberegnelighet neppe er oppfylt.

Siden kravene i EMK art. 8.2 er kumulative, er den manglende oppfyllelsen av lovkravet i seg selv nok til å konkludere med at lovforslaget, slik det er formulert, ikke vil være i tråd med Norges menneskerettslige forpliktelser.

Likevel mener vi at det er hensiktsmessig å foreta en vurdering av det siste kravet, nemlig om systemet i sin helhet kan anses som proporsjonalt og «nødvendig i et demokratisk samfunn». Dette beror på en vurdering av hvorvidt systemet i sin helhet er omfattet av nødvendige garantier mot misbruk, og garanterer effektive rettsmidler. Kontrollsystemet

ved forutgående domstolskontroll, tilsyns- og kontrollsystemet må altså ses i sammenheng. En samlet vurdering av all disse mekanismene må tilfredsstillende kravene i EMK art. 8 og 13.

Formålet med kontrollen er å forhindre misbruk og opprettholde tilliten befolkningen har til de hemmelige tjenestene, noe som er avgjørende for å begrense de negative konsekvensene av masseovervåkning.

Departementet mener at den samlede kontrollen, bestående av (hemmelig) domstolsprøving for tilrettelagt innhenting og bruk, «styrket kontroll» (i.e. løpende kontroll) og etterkontroll ved EOS utvalget, samlet sett er et robust nok system for å verne mot misbruk og garanterer effektive rettsmidler.

Når det gjelder kontroll før tiltaket iverksettes, så vil vi påpeke at det er en betydelig svakhet ved lovforslaget at det kun er tilrettelagt innhenting og søk etter kapittel 7 som er underlagt domstolskontroll og ikke søk etter innhenting av rådata i bulk. Videre vil prøvingen sannsynligvis være lite reell. Både på grunn av manglende etterretningsfaglige kunnskap hos dommerne som skal overprøve etterretningens vurderinger, og på grunn av den vide oppgavebeskrivelsen til Etterretningstjenesten. Tilsammen gjør dette at nødvendighet og forholdsmessighet trolig vil være nærmest umulig å vurdere.

Når det gjelder løpende kontroll (eller styrket kontroll), vil dette som nevnt falle inn under EOS-utvalgets ansvar. Den nye funksjon «styrket kontroll» og etterfølgende kontroll som utføres av EOS-utvalget, betyr at de ville måtte tilføres betydelige ressurser for å øke sin kapasitet og kompetanse. Her har vi store bekymringer knyttet til om hvorvidt departementet klarer å løse utvalgets problem med mangel på teknisk kompetanse, og sekretariatets manglende kapasitet. De fire årsverk som departementet foreslår, er etter all sannsynlighet ikke nok til å fylle dette behovet. I realiteten vil dette etter vår mening bety at den løpende kontrollen vil bli lite effektiv og reell.

Når det gjelder kontroll i etterkant, gjør de samme bekymringer om kompetanse og ressurser seg gjeldende. I tillegg er ikke EOS-utvalget bemyndiget med vedtakskompetanse. Dette er særlig en svakhet når det gjelder klagemekanismen, som allerede er svak på grunn av fritaket fra kravet om underretning. Det er usikkert om EOS-utvalgets klagebehandling i seg selv er nok til å oppfylle kravene til et effektivt rettsmiddel.

Muligheten for oppreisning vil i praksis være fraværende siden EOS-utvalget bare vil kunne uttale seg med en anbefaling, og hvor det ellers er lagt opp til domstolsprøving som vil være begrenset på grunn av dagens bevisforbud. Dette betyr at hverken hver for seg, eller sett i sammenheng, vil klagemuligheten til EOS-utvalget og domstolsprøving utgjøre et effektivt rettsmiddel etter EMK art. 13

Når man tar alt dette i betraktning, er det vanskelig å se hvordan departementet kan komme fram til at kontrollmekanismene, i sin helhet, vil være gode nok til å motvirke misbruk.

Etter vår vurdering er kontrollsystemet så svakt at det ikke kan anses å veie opp mot det store inngrepet i retten til privatliv som dette lovforslaget er. Konsekvensen av dette er at forslaget ikke er i tråd med våre internasjonale forpliktelser.

Selv om kontrollmekanismen hadde vært innrettet på en måte som kunne anses som robust nok til å motvirke de negative konsekvensene ved innføring av et slikt system, kreves det at det må foretas en avveining mellom *samfunnets/statens interesse* og *inngrepet* i retten til privatliv. Det må derfor vurderes både fordeler og ulemper ved tiltaket i et større samfunnsperspektiv.

Som departementet påpeker i høringsnotatet har statene en viss skjønnsmargin når de skal gjøre denne vurderingen. I kraft av i sin rolle som domstol, overprøver EMD denne vurderingen sjeldent, og gir derfor heller ikke noen føringer for minimumskrav til denne vurderingen. Dette betyr likevel ikke at statene kan unnlate å gjøre den.

Denne kartleggingen av alle samfunnsmessige fordeler og ulemper ved forslaget mener vi mangler. Dette gjør at det er vanskelig å kunne konkludere med om forslaget er proporsjonalt.

13 Lovforslaget om «tilrettelagt innhenting» bør ikke vedtas

Vi mener at de nødvendige vurderingene av hvilke konsekvenser dette regimet vil kunne ha for samfunnet ikke er gjort og at det foreliggende lovforslaget ikke er bra nok til at det kan vedtas. Det er en rekke uklarheter i forslaget og kontrollmekanismene er ikke tilstrekkelige. Dette gjør at forslaget i sin nåværende form ikke oppfyller kravene i våre menneskerettslige forpliktelser.

Samtidig erkjenner Datatilsynet at en type etterretningsregime som lovforslaget om tilrettelagt innhenting legger til rette for, vil kunne være lovlig etter våre folkerettslige forpliktelser dersom alle nødvendige vurderinger er gjort, tilstrekkelige kontrollmekanismer er på plass, osv. Likevel mener vi at det at det eventuelt rettslig sett *kan* innføres, ikke er det samme som at det *bør* innføres.

Vi mener at departementet i høringsnotatet bruker uforholdsmessig mye plass på å overbevise om at tiltaket er innenfor de rettslige rammene oppstilt av EMD og altfor lite plass på å gjøre rede for de samfunnsmessige konsekvensene av forslaget.

Vi har forståelse for at etterretningen har behov for effektive metoder for å utføre sine oppgaver, og at dette også er viktig for at Norge skal være en attraktiv samarbeidspartner for andre lands etterretningsmyndigheter. Samtidig har forslaget helt klare negative og uante konsekvenser for vårt demokratiske samfunn, som nedkjølingseffekt som følge av at mange vil føle ubehag ved å være overvåket og stor fare for formålsutglidning.

Innføring av tiltaket er i første rekke en politisk beslutning om hvordan vi vil at det norske samfunnet skal se ut. I den debatten kan EMDs minimumskrav neppe være målet man skal strekke seg til.

I den forbindelse minner vi om hva Norge har gitt uttrykk for internasjonalt om dette temaet, senest i november 2018 ved å være medforlagsstiller av FNs Generalforsamlings

resolusjon A/RES/73/179.¹⁰² Denne Resolusjonen anser innhenting av kommunikasjonsdata som en 'highly intrusive act', og oppfordrer alle land til å ivareta sine menneskerettslige forpliktelser i denne forbindelse. Vi oppfordrer regjeringen, som medforslagsstiller til denne resolusjonen, om å følge sin egen anbefaling.

Vi er bekymret for om regjeringen har gjort grundige nok vurderinger, og om den har foretatt den nødvendige avveiningen av de fordeler og ulemper lovforslaget medfører for samfunnet som helhet. Det er lite spor i høringsnotatet av at slike vurderinger er gjort. Vi viser til at kapittelet om «samfunnsmessige konsekvenser» utgjør en halv side, i et høringsnotat på til sammen 395 sider.

Dette handler om våre grunnverdier som demokratisk samfunn, og om vårt samfunn blir bedre eller verre som følge av innføringen av et slikt system som forslaget legger opp til. I den forbindelse er det svært uheldig at regjeringen legger frem sitt lovforslag før Personvernkommisjon har ferdigstilt sitt arbeid.

Dette gjør at det sannsynligvis blir vanskelig å oppnå den samfunnsdebatten som dette forslaget trenger. Et uklart lovforslag, en altfor kort høringsfrist og departementets generelle bagatellisering av konsekvensene understreker ytterligere behovet for en grundig gjennomgang av de tiltakene som forslaget legger opp til, og virkningene av dem. Vi frykter at verken befolkningen eller Stortinget er gjort i stand til å forstå fullt ut hva som er i ferd med å skje før det er for sent. Dette er høyst problematisk.

Vi mener at Regjeringen og Stortinget ved å innføre dette regimet vil krysse en prinsipiell linje som ikke bør krysses. Vår klare anbefaling er derfor at regjeringen ikke går videre med forslaget.

14 Andre merknader

14.1 Krav til utredning av personvernkonsekvenser og krav til innebygget personvern

Det viktigste og nyeste regelverket for personvern er EUs personvernforordning, som gjelder som norsk lov gjennom personopplysningsloven av 2018. I forordningen fremgår personvernprinsippene og nærmere bestemmelser om de ulike pliktene og rettighetene som til sammen utgjør personopplysningsvernet.

I forordningen tydeliggjøres pliktene til den behandlingsansvarlige sammenlignet med personopplysningsloven av 2000. Lovgiver har gått bort fra krav til forhåndskontroll av tilsynsmyndighetene, men innfører i stedet nye mekanismer og presiserer at ansvaret for å følge personvernprinsippene ligger hos den behandlingsansvarlige. Nye forpliktelser er art. 35, som gjelder metode for utredning av personvernkonsekvenser, særlig ved bruk av ny

¹⁰² FNs Generalforsamlings resolusjon [A/RES/73/179](#), The Right to Privacy in the Digital Age, 21. januar 2019.

teknologi, og art. 25, om krav til innebygget personvern og personvern som standardinnstillinger.

Selv om EU-forordningen ikke gjelder for etterretningen er den et uttrykk for en mer moderne måte å tenke personvern på som bør gjenspeiles i all nasjonal lovgiving om behandling av personopplysninger.

Datatilsynet mener departementet ikke i tilstrekkelig grad har tatt inn over seg denne utviklingen og de krav til personvern på systemnivå som forordningen stiller. Lov om etterretningen er ment å uttømmende regulere behandling av personopplysninger på dette området og bør gi føringer utover behandling i de enkelte sakene. Vi kan ikke se hvorfor det skal være lavere krav til slike vurderinger på dette området enn på forordningens virkeområde. Det kan her nevnes at politiregisterforskriften § 41-1 oppstiller krav til personvernkonsekvensvurderinger ved ny type behandling av personopplysninger på politiregisterloven virkeområde. Dette kom inn i forskriften som en konsekvens av nytt EU-regelverk.

Vi mener departementet må vurdere å ta inn bestemmelser om krav til innebygget personvern og krav til konsekvensutredninger, for eksempel ved innføring av ny teknologi i lov om Etterretningstjenesten, for å sikre at det ved innføring av nye tiltak gjøres gode personvernkonsekvensutredninger og at hensynet til personvernet vektlegges allerede når man starter planleggingen av et tiltak eller en tjeneste eller et produkt skal utvikles. Personvern hensyn skal ikke være noe man utkvitterer etter at en tjeneste er ferdig utviklet og alle valg er tatt.

Selv om plikten til å utrede personvernkonsekvenser delvis også fremgår av utredningsinstruksen, mener vi det at dette også fremgår av loven. I tillegg til at det vil pålegge etterretningen en forpliktelse, vil det være et viktig pedagogisk grep som også har stor symbolverdi.

For øvrig er det noe uklart hvem som i realiteten er behandlingsansvarlig, altså hvem som er ansvarlig for at lovens bestemmelser følges, siden dette begrepet ikke brukes i loven. Det er ikke åpenbart hvilken instans som er ansvarlig, siden det er Norges nasjonale utenlandsetterretningstjeneste som er den som innhenter og behandler opplysningene, mens det er departementet som formulerer oppdrag og foretar prioriteringer. Vi viser til at det i høringsnotatet er presisert at Etterretningstjenesten aldri innhenter informasjon for sin egen del, men for sine oppdragsgivere, samtidig som det er etterretningen som i hovedsak er pålagt tydelige plikter. Hvem som har ansvaret for de ulike forpliktelsene etter loven vil være sentralt for EOS-utvalget som kontrollorgan og kan med fordel klargjøres, enten i loven eller i lovens forarbeider.

14.2 Krav til personvernrådgiver

Datatilsynet støtter forslaget i § 9-2 om at etterretningen i egen organisasjon skal ha personvernrådgiver.

Vi foreslår at begrepet det benyttes begrepet personvernombud, i stedet for personvernrådgiver. Dette er begrepet som benyttes i personopplysningsloven og EU-

forordningen, og er et begrep som har blitt innarbeidet i norsk praksis og regelverk gjennom mer enn 15 år. Begrepet personvernombud signaliserer selvstendighet og autoritet, noe som er en viktig kvalitet ved rollen.

Videre mener vi at det bør fremgå av lovbestemmelsen at sjef for Etterretningstjenesten plikter å stille til rådighet de ressurser som er nødvendige for å utføre sine oppgaver. Se til sammenligning forordningen art. 38 nr. 2. Dette er en sentral forutsetning for at ordningen skal kunne ha noen effekt i praksis.

14.3 Varslingskanal

I forbindelse med utformingen av loven bør det være en målsetning å lage det beste systemet for kontroll og rettsikkerhet. Det innebærer at man må tenke utover de minimumskravene som følger av EMK og forsøke å tenke på løsninger som i størst mulig grad sikrer den tilliten borgerne må ha til systemet.

Det finnes litteratur om rettssikkerhet omkring digital masseovervåking¹⁰³ på området som tar for seg hvordan denne typen systemer bør utformes, blant annet om varsling.

Varsling er en viktig mekanisme for å sikre regeletterlevelse og forhindre misbruk. I de siste årene har rutiner for varsling og regelverk blitt utviklet, og man har for eksempel fått regler om varsling i lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven) kapittel 2. I reglene ligger det en rett til å varsle til aktuell tilsynsmyndighet. Dette er for å sikre konfidensialitet og en behandling av varselet der hvor interne forhold ikke gjør det mulig. Det gir også varsleren en større trygghet mot gjengjeldelse.

I lovutkastets § 9-12 er det åpnet for at brudd og avvik kan rapporteres til personvernrådsgiveren, men det er ikke gitt regler for hva personvernrådsgiveren skal gjøre med eventuelle varsel. Datatilsynet forstår det slik at det er utarbeidet interne retningslinjer for varsling, men klarer ikke å finne mer informasjon om hva de går ut på. Forholdet til arbeidsmiljøloven og Forsvarets varslingskanal er heller ikke omtalt.

Slik varslingsmekanismen er utformet i forslaget, er det tvilsomt om den i tilstrekkelig grad ivaretar hensynene til varslers rettigheter. Den innebærer også utfordringer for personvernrådsgiverens uavhengighet. En sentral del av personvernombudenes oppgaver under personvernforordningen er å være kontaktpunkter for tilsynsmyndighet, noe som vil trenge en avklaring av rollen i regelverket.

Datatilsynet foreslår at det etableres en sikker varslingskanal for alle direkte til EOS-utvalget, og at regler om dette inntas i loven.

¹⁰³ [“Upping the Ante on Bulk Surveillance - An International Compendium of Good Legal Safeguards and Oversight Innovations”](#), Wetzling, Vieth, Böll-Stiftung, VOLUME 50, 2018