OSLO TINGRETT

DOM

Avsagt:	26.03.2025 i Oslo tingrett, Oslo
Saksnr.:	24-038001TVI-TOSL/04
Dommer:	Tingrettsdommer Yngvild Thue
Saken gjelder:	Vilkårlig og ulovlig digital masseovervåkning og bulkinnsamling av elektronisk kommunikasjon

Stiftelsen Tinius	Advokat Jon Wessel-Aas og advokat Emanuel Feinberg Rettslig medhjelper advokatfullmektig Elmira Oshnavie
Tom Erik Thorsen	Advokat Jon Wessel-Aas og advokat Emanuel Feinberg Rettslig medhjelper advokatfullmektig Elmira Oshnavie

mot

Staten v/Forsvarsdepartementet	Advokat Ida Thue Rettslig medhjelper advokat Kaija Marie Folkestad Bjelland

DOM

Saken gjelder spørsmålet om reglene om tilrettelagt innhenting (TI) etter etterretningstjenesteloven kapittel 7 er i strid med Grunnlovens § 102, EMK artikkel 8 og 10 samt EUs kommunikasjonsverndirektiv.

1. Oversikt over saken

Etterretningstjenesten (E-tjenesten) er Norges nasjonale utenlandsetterretning. Tjenesten er en del av Forsvaret og er underlagt forsvarssjefens kommando, jf. e-tjenesteloven § 2-1 (1). E-tjenesten har som hovedoppgave å innhente informasjon om utenlandske trusler og andre forhold av betydning for rikets sikkerhet.

Ny lov om Etterretningstjenesten (e-tjenesteloven) ble vedtatt 19. juni 2020. Hoveddelen av loven trådte i kraft 1. januar 2021. Stortinget vedtok 6. juni 2023 endringer i e-tjenesteloven om tilrettelagt innhenting (TI) samt prosedyrer for domstolskontroll med dette. Gjennom disse reglene får E-tjenesten adgang til å innhente, lagre, søke i og analysere elektronisk kommunikasjon som krysser Norges grenser. Reglene har også blitt kalt «digitalt grenseforsvar».

Det er enighet om at mye av den elektroniske kommunikasjonen mellom personer i Norge av tekniske årsaker går via utlandet, blant annet via utenlandske servere. Dette betyr at kommunikasjonen mellom en sender og en mottaker som befinner seg i Norge i mange tilfeller krysser landegrensen. Denne kommunikasjonen vil kunne omfattes av E-tjenestens innhenting av grensekryssende kommunikasjon etter TI.

Saksøkerne, Stiftelsen Tinius og Tom Erik Thorsen (heretter samlet «Stiftelsen»), har gjort gjeldende at E-tjenestens innsamling, lagring og behandling av elektroniske kommunikasjonsdata i realiteten innebærer en omfattende og vilkårlig masseovervåkning av personer i Norge. Store deler av norske borgeres digitale liv vil kunne bli hentet inn og lagret av norske myndigheter. Dette er i strid med retten til privatliv, herunder kommunikasjon og personvern, slik disse rettighetene er beskyttet i henholdsvis Grunnlovens § 102 og EMK artikkel 8. Retten til privatliv henger nært sammen med pressens kildevern ettersom hvem som helst kan være pressens kilder. Stiftelsen har også vist til at den omfattende digitale overvåkningen fører til at det ikke lenger er mulig å ha tillit til at digital kommunikasjon med journalister er fortrolig. Dette vil ha en nedkjølende effekt på ytringsfriheten og TI innebærer derfor også et inngrep i ytringsfriheten og krenker kildevernet etter Grunnlovens § 100 og EMK artikkel 10. Endelig mener Stiftelsen at reglene om tilrettelagt innhenting er i strid med EUs kommunikasjonsverndirektiv og dermed også i strid med EØS-retten.

Staten er ikke enig i at TI krenker de nevnte rettighetene. Ifølge staten er TI nødvendig for å ivareta grunnleggende hensyn knyttet til rikets sikkerhet og reglene om tilrettelagt innhenting ligger godt innenfor rammene av Grunnloven, EMK og EØS-retten.

Søksmålet omfatter også andre oppgaver som er tillagt E-tjenesten i loven. Dette gjelder lovens bestemmelser i §§ 6-9 og 6-10 om henholdsvis midtpunktinnhenting og endepunktinnhenting. Staten har krevd at dette kravet avvises på grunn av manglende rettslig interesse, subsidiært at staten frifinnes.

1.1 Lovens regulering av TI

E-tjenesteloven § 7-1 fastsetter de generelle vilkårene og virkeområdet for TI. Bestemmelsen lyder:

> Etterretningstjenesten kan for etterretningsformål innhente elektronisk kommunikasjon som transporteres over den norske grensen når grunnvilkårene etter kapittel 5 er oppfylt, bestemmelsene i kapittel 7 og 8 følges, og innhenting ikke strider mot loven for øvrig.
>
> Bestemmelsene i kapittel 7 og 8 kommer bare til anvendelse der det er nødvendig at tilbydere som nevnt i § 7-2 legger til rette for innhentingen.

Bestemmelsen fastsetter at E-tjenesten kan «innhente elektronisk kommunikasjon som transporteres over den norske grensen». Forutsetningene for dette er at slik innhenting skjer innenfor de rammer og vilkår som følger av loven som helhet, herunder at grunnvilkårene i kapittel 5 og de særskilte vilkårene for bestemte tiltak i kapittel 7 er oppfylt. Kapittel 7 suppleres videre av kapittel 8 om forutgående domstolskontroll for slike tiltak.

Kravet til at kommunikasjonsstrømmen må krysse landegrensen innebærer for det første at det ikke kan innhentes kommunikasjon som utelukkende transporteres i et norsk nettverk. Det er imidlertid ikke uenighet om at deler av norsk innenlandsk kommunikasjon også i mange tilfeller vil krysse den norske grensen som følge av at informasjonen rutes via utlandet eller at den er lagret på en server som befinner seg i utlandet.

For det andre må kommunikasjonsdataene «transporteres». Bestemmelsen gir dermed ikke hjemmel for innhenting av lagrede data som ikke er i transitt.

Lovens kapittel 6 gjelder ulike innhentingsmetoder som E-tjenesten kan benytte. I denne saken er det særlig skillet mellom midtpunktinnhenting, jf. lovens § 6-9, og endepunktinnhenting, jf. lovens § 6-10, som er av betydning. Ved midtpunktinnhenting kan E-tjenesten innhente kommunikasjonssignaler som er under transport, eksempelvis via radio, satellitt eller internett, jf. spesialmerknadene til bestemmelsen i Prop. 80 L (2019-2020) side 211. Med endepunktinnhenting menes innhenting av ikke åpent tilgjengelig

elektronisk kommunikasjon i et datasystem eller lignende. Det er her ikke tale om kommunikasjon i transitt, men informasjon som er tilgjengelig i selve endepunktet, eksempelvis en mobiltelefon eller en datamaskin.

E-tjenesteloven § 7-1 er en særskilt form for midtpunktinnhenting som reguleres i lovens kapittel 7 og 8. Den skiller seg fra midtpunktinnhenting etter § 6-9 ved at innhentingen skjer ved tilrettelegging fra tilbydere av elektroniske tjenester. Etter lovens § 6-9 er det E-tjenesten selv som forestår innhentingen. Begrunnelsen for denne særreguleringen er at innhentingen i stor grad vil berøre norsk innenlandsk kommunikasjon som av tekniske årsaker krysser grensen, jf. Prop.80 L (2019-2020) side 213.

Det følger av forarbeidene at det i dagens situasjon normalt vil være tale om å innhente kommunikasjon som transporteres i fiberoptiske kabler, men at bestemmelsen er utformet på en teknologinøytral måte. Bestemmelsen gjelder både kommunikasjon mellom flere parter og ensidig overføring av kommunikasjon.

Innhenting kan bare skje «for etterretningsformål». Dette innebærer at innhentingen må begrunnes i en av E-tjenestens oppgaver i kapittel 3, jf. e-tjenesteloven § 1-3 bokstav c). Hvilke formål som omfattes er nærmere utdypet nedenfor i punkt 3.4.3.2.

Lovens kapittel 4 oppstiller ulike forbud mot innhenting. Sentralt i denne sammenheng er § 4-1 om forbud mot innhenting i Norge og § 4-8 som setter forbud mot å innhente informasjon for politiformål.

TI må videre oppfylle grunnvilkårene som er fastsatt i lovens kapittel 5. Her oppstilles det grunnvilkår for blant annet målrettet innhenting (§ 5-2) og grunnvilkår for innhenting av og søk i rådata i bulk (§ 5-3). Retten kommer nærmere tilbake til innholdet av disse vilkårene, men nevner at disse vil ha betydning som inngangsvilkår for tilrettelagt innhenting etter kapittel 7.

En viktig begrensning i adgangen til å iverksette innhenting av elektronisk kommunikasjon er kravet til forholdsmessighet som er nedfelt i lovens § 5-4. Etter denne bestemmelsen skal:

> Innhenting og utlevering av informasjon [skal] ikke gjennomføres dersom det vil være et uforholdsmessig inngrep overfor den enkelte. Ved vurderingen skal det tas hensyn til om mindre inngripende tiltak i tilstrekkelig grad kan ivareta formålet, inngrepets virkning for den som rammes, sakens betydning og forholdene ellers.

Kravet innebærer at «tiltaket må være nødvendig for å oppnå formålet, herunder at det er egnet og at formålet ikke kan oppnås med mindre inngripende tiltak. Det må også foretas en samlet avveining av de beskyttede individuelle interessene og det legitime

samfunnsbehovet for informasjonsinnhenting», jf. Prop. 80 L (2019-2020) punkt 9.5.3. Dette må avgjøres konkret i den enkelte sak. Kravet er nærmere behandlet nedenfor.

Endelig må bestemmelsene i lovens kapitler 7 og 8 følges, jf. nedenfor.

1.1.1 TI er en trinnvis prosess

Innhenting av informasjon gjennom TI er en prosess i flere trinn. E-tjenesten må først få en forhåndsgodkjennelse fra retten for å innhente («speile») ufiltrerte kommunikasjonsstrømmer som krysser grensen, jf. § 7-3. De speilede dataene skal filtreres etter e-tjenesteloven § 7-6 før de lagres i bulk i et metadatalager. For å få tilgang til dataene gjennom søk og senere bruk, må E-tjenesten få en ny forhåndsgodkjennelse fra retten, jf. §§ 7-8, 7-9 jf. § 8-1, og domstolen må godkjenne hvilke søkebegreper som kan benyttes. Når disse søkene er foretatt, kan E-tjenestene bruke dataene til etterretningsproduksjon.

1.1.1.1 Speiling av kommunikasjonsstrømmer

E-tjenesten kan etter tillatelse fra retten gi tilbydere av elektroniske tjenester pålegg om å speile kommunikasjon som krysser den norske grensen, jf. § 7-3 (1):

> Elektronisk kommunikasjon som transporteres over den norske grensen kan speiles som grunnlag for søk i lagrede metadata etter § 7-8 og målrettet innhenting og lagring av innholdsdata etter § 7-9, når det er nødvendig for å etablere et informasjonsgrunnlag for etterretningsformål. Tillatelse til å gi pålegg om slik speiling gis av retten ved kjennelse etter reglene i kapittel 8. Pålegget gis av sjefen for Etterretningstjenesten.

Uttrykket «speiling» er ikke nærmere definert i loven. Retten forstår uttrykket slik at kommunikasjonsstrømmene gjøres tilgjengelige for E-tjenesten gjennom en form for kopiering/duplisering mens dataene fortsatt er i transitt. Dataene lagres ikke.

Speiling etter § 7-3 er en type innhenting av rådata i bulk, jf. e-tjenesteloven § 1-3 (i) og § 5-3. Formålet med speilingen er å etablere et informasjonsgrunnlag som senere kan brukes til etterretningsproduksjon. Speilingen kan bare tillates når det er «nødvendig» for å etablere «et informasjonsgrunnlag for etterretningsformål». Uttrykket «nødvendig» rommer både et krav til «egnethet, formålsmessighet og forholdsmessighet», jf. Prop. 92 L (2022-2023) side 57. Det er blant annet en forutsetning at formålet ikke kan oppnås med mindre inngripende tiltak. Et krav om forholdsmessighet er også nedfelt i loven § 5-4 og retten legger til grunn at vurderingsnormen er den samme etter denne bestemmelsen, jf. avgradert kjennelse fra Borgarting lagmannsrett side 5.

E-tjenesten må fremme en begjæring om speiling for retten. Denne begjæringen skal redegjøre for det faktiske og rettslige grunnlaget for speilingen og hvor lenge tiltaket bør

vare. Begjæringen må også angi hvilke kommunikasjonsstrømmer og hvilke tilbydere som skal omfattes av speilingen, jf. e-tjenesteloven § 8-2.

Domstolen behandler deretter begjæringen, jf. § 8-1 (1). Ved denne behandlingen skal retten kontrollere at alle vilkårene er oppfylt, jf. § 8-4. Dette innebærer blant annet at retten skal ta stilling til om speilingen i den konkrete saken ligger innenfor E-tjenestens formål, om noen av innhentingsforbudene er til hinder for speilingen samt at grunnvilkårene i kapittel 5, herunder kravet til forholdsmessighet, er oppfylt. Det oppnevnes en særskilt advokat som skal ivareta «den enkeltes rettigheter og samfunnets interesser» og rettens avgjørelse kan ankes, jf. §§ 8-5 og 8-9.

Innenfor rammen av rettens tillatelse kan E-tjenesten deretter gi pålegg om speiling for tilbydere av elektronisk kommunikasjon (ekom-tilbydere) etter lovens § 7-2.

Grenseoverskridende kommunikasjon kan etter bestemmelsens annet ledd også speiles for å gjennomføre tekniske analyser. Dette er nærmere behandlet under punkt 3.4.4.

1.1.1.2 Filtrering og lagring

Loven skiller mellom innholdsdata og metadata. Metadata er nærmere definert i lovens § 7-7 (1) 2. punktum:

> Med metadata menes data som beskriver annen data eller som inneholder ekstra informasjon knyttet til data, blant annet data som beskriver formatet på innholdet, hvem som er avsender og mottaker, eller kommunikasjonens størrelse, posisjon, tidspunkt eller varighet.

Innholdsdata avgrenses negativt til «data som ikke er metadata». Et forenklet eksempel på forskjellen mellom metadata og innholdsdata er at adressat, avsender og datostempel på en konvolutt er metadata, mens innholdet i konvolutten kan betegnes som innholdsdata.

Retten legger etter bevisførselen til grunn at det kan være en glidende overgang mellom metadata og innholdsdata og at også metadata kan inneholde svært mye informasjon om den enkelte. Førsteamanuensis Inga Strümke har forklart at det er vanskelig å definere eksakt hva metadata er, og at en mer dekkende betegnelse er «atferdsdata». Denne informasjonen sier noe om hvordan vi oppfører oss, hvor vi befinner oss og hva vi gjør når vi befinner oss på et gitt sted. Atferdsdata kan brukes til å finne ut sensitiv informasjon både hver for seg og ikke minst når informasjonen settes i sammenheng. Dette gjelder også informasjon om forhold som ikke fremgår eksplisitt av dataene. Kjøpshistorikk kan eksempelvis brukes til å finne ut om noen var gravid, data om sosiale nettverk vil kunne si noe om seksuell orientering, etnisitet og sivilstatus mv. Ved hjelp av avanserte analysemetoder kan historiske atferdsdata også benyttes til å predikere fremtidig atferd. Vi produserer mer og mer metadata samtidig som tilgjengeligheten av andre data, eksempelvis

statistikk, øker og analyseverktøyene er i rask utvikling. Dette medfører at man med større presisjon kan forutsi fremtidig atferd.

De speilede dataene filtreres av E-tjenesten før dataene lagres i et metadatalager.

Etter lovens § 7-6 skal E-tjenesten «søke å hindre» lagring av metadata om kommunikasjon mellom personer i Norge. Så langt det er teknisk mulig skal E-tjenesten filtrere ut de norske dataene. Retten legger imidlertid til grunn at det i dag ikke er teknisk mulig å hindre lagring av store mengder norsk innenlandsk kommunikasjon. Metadata som ikke filtreres bort, sendes videre til prosessering og lagring i bulk i et metadatalager, jf. lovens § 7-7. I denne prosessen filtreres også innholdsdata ut av kommunikasjonsstrømmen. Filtreringen skjer gjennom automatiserte maskinelle prosesser og E-tjenesten kan ved lagringen verken se eller bruke dataene til etterretningsproduksjon.

Lovens § 7-7 (3) oppstiller et krav om sletting av lagrede metadata senest etter 18 måneder.

1.1.1.3 Søk og analyse av innhentede data

E-tjenesten kan fremme ny begjæring for retten om tillatelse til å iverksette søk i lagrede metadata eller målrettet innhenting og lagring av innholdsdata, jf. lovens §§ 7-8, 7-9 jf. § 8-1 (1) b) og c).

Slike søk baseres på søkekriterier som er egnet til å finne relevante data, jf. § 5-3. Søkekriterier kan knytte seg til en person (personselektor), eksempelvis et telefonnummer, en e-postadresse eller et brukernavn på en tjeneste, eller til et bestemt mønster eller avgrensning (modusselektor), eksempelvis et geografisk område eller trafikk til og fra en bestemt digital enhet. Modusselektoren vil ofte bestå av en kombinasjon av søkebegreper. Den vil normalt være mindre finmasket enn en personselektor, jf. Prop. 80 L (2019-2020) side 216.

Retten behandler begjæringen i medhold av lovens § 8-1 (1) b) og c) og retten kan vurdere samtlige vilkår i loven, jf. § 8-4. Først etter at retten har gitt tillatelse til å foreta avgrensede søk kan E-tjenestene behandle dataene til etterretningsproduksjon. I dette ligger det at E-tjenesten kan analysere og sammenstille opplysningene til et etterretningsprodukt som kan danne grunnlag for varsel til norske myndigheter.

1.1.1.4 Kontroll

Etterretningstjenestens virksomhet kontrolleres av flere instanser.

Den forvaltningsmessige kontrollen av E-tjenesten ivaretas av forsvarssjefen som etatssjef og departementet på vegne av forsvarsministeren. EOS-utvalget ivaretar den uavhengige kontrollen av samtlige etterretnings- og sikkerhetstjenester på vegne av Stortinget, og

Riksrevisjonen ivaretar på vegne av Stortinget revisjon og kontroll av E-tjenesten. I tillegg til ekstern kontroll gjennomfører E-tjenesten internkontroll.

I forbindelse med reglene om tilrettelagt innhenting er det særlig den uavhengige kontrollen som utføres av EOS-utvalget som er relevant.

Hovedformålet med EOS-utvalgets kontroll er å ivareta den enkeltes rettsikkerhet og utvalget gjennomfører etterfølgende kontroller av E-tjenesten i medhold av EOS-kontrolloven § 6. I tillegg skal EOS-utvalget etter e-tjenesteloven § 7-11 føre løpende kontroll med E-tjenestens etterlevelse av reglene om tilrettelagt innhenting, blant annet at søk bare gjennomføres i tråd med rettens kjennelser. Dette er nærmere utdypet nedenfor i punkt 3.4.6.1.

1.2 Lovgivningsprosessen

E-tjenesteloven bygger på et grundig lovarbeid.

Bakgrunnen for lovarbeidet var rapporten «Et felles løft» av 28. april 2015 fra Ekspertgruppen for forsvaret av Norge. Ekspertgruppen pekte blant annet på trusler i det digitale rom, og behovet for å kunne følge med på relevant internett-trafikk for å kunne oppdage, varsle og håndtere utenlandske trusler som terror, spionasje og digitale angrep. Gruppen anbefalte å etablere et digitalt grenseforsvar.

Regjeringen nedsatte i juni 2014 et utvalg for å kartlegge samfunnets digitale sårbarheter. I NOU 2015:13 «Digital sårbarhet – sikkert samfunn» (Lysne I) ble det gitt uttrykk for forståelse av det etterretningsfaglige behovet, men at en slik digital grenseovervåkning ikke bør innføres uten en forutgående utredning og offentlig debatt. Utvalget foreslo å sette ned et eget utvalg for å utrede dette nærmere.

EOS-utvalget avga 17. juni 2016 en særskilt melding til Stortinget om rettsgrunnlaget for etterretningstjenestens overvåkningsvirksomhet og reiste spørsmål om rettsgrunnlaget for E-tjenesten var tilstrekkelig oppdatert og påpekte et mulig behov for lovendringer for å sikre at tjenesten har hjemmelsgrunnlag for sin aktivitet.

Stortinget fattet anmodningsvedtak 21. februar 2017 om at regjeringen skulle legge frem forslag til ny lov for E-tjenesten.

Lysne II-utvalget leverte sin rapport «Digitalt grenseforsvar» 26. august 2016. Utvalget anbefalte å etablere et digitalt grenseforsvar som ga E-tjenesten tilgang til digitale datastrømmer som krysser landegrensene. Forutsetningen for anbefalingen var et strengt kontrollregime i flere ledd i tillegg til strenge begrensninger for bruken av informasjonen fra tilgangen.

Rapporten ble sendt på offentlig høring høsten 2016 og rapporten ble gjenstand for en bred offentlig debatt. På bakgrunn av dette startet departementet arbeidet med en ny e-tjenestelov i 2017 og departementets høringsnotat ble sendt på høring 12. november 2018.

Høringsnotatet inneholdt en bred drøftelse av de rettslige rammene for TI og forhold til menneskerettighetene og EØS-avtalen. Det innkom om lag 85 høringsuttalelser fra ulike parter.

Lovproposisjonen (Prop. 80 L (2019-2020)) ble fremlagt for Stortinget i april 2020. Proposisjonen inneholdt flere endringer etter innspill fra høringen.

Utenriks- og forsvarskomiteen på Stortinget besluttet å avholde høring i saken og komiteen mottok flere skriftlige innspill. Det ble også avholdt en åpen og en lukket høring i mai 2020 og Stortinget vedtok ny etterretningstjenestelov 19. juni 2020.

Loven trådte i kraft 1. januar 2021 med unntak av lovens kapittel 7 og 8 som omhandler tilrettelagt innhenting. Ikrafttredelsen av disse kapitlene ble utsatt for å avvente en vurdering av dommer fra EMD og EU-domstolen.

I oktober 2020 avsa EU-domstolen dom i forente saker C-511/18, C-512/18 og C-520, La Quadrature du Net, og C-623/17, Privacy International, om tolkningen av EUs kommunikasjonsvernsdirektiv.

I mai 2021 avsa EMD i storkammer avgjørelsene Centrum för Rättvisa vs. Sverige (35252/08) og Big Brother Watch m.fl. vs. Storbritannia (58170/13, 62322/14 og 24690/15) som omhandlet bulkinnhentingsregimer. I begge sakene ble det konstatert brudd på EMK.

Det ble nedsatt en interdepartemental arbeidsgruppe som utarbeidet en felles rettslig analyse for å vurdere behovet for endring/justering av lovens kapittel 7 og 8 som følge av disse avgjørelsene. Arbeidsgruppen konkluderte med at TI-reglene i all hovedsak var i tråd med både EMK og EØS-avtalen, men anbefalte en nærmere utredning av spørsmål knyttet til lovens § 7-3 og pressens kildevern.

Lovens kapittel 7 og 8 trådte i kraft 1. januar 2022 med unntak av § 7-3 om vilkår og beslutningskompetanse i saker om tilrettelegging.

I juni 2022 fremla Forsvarsdepartementet et nytt høringsnotat hvor det ble foreslått endringer om at beslutningskompetansen etter § 7-3 skal legges til Oslo tingrett, samt enkelte presiseringer av bestemmelsene om blant annet kildevern for å sikre bedre samsvar med kriteriene oppstilt i EU-domstolens avgjørelse i La Quadrature du Net (LQN).

Høringsnotatet ble sendt på høring og lovproposisjonen Prop. 92 L (2022-2023) ble lagt frem 31. mars 2023. Her ble det foreslått å flytte beslutningskompetansen for speiling etter § 7-3 fra sjefen for E-tjenesten til Oslo tingrett, samt krav om forhåndsgodkjennelse fra domstolen for målrettet innhenting etter § 5-2 og bruk av kildeidentifiserende opplysninger.

Utenriks- og forsvarskomiteen avholdt ny høring i saken og endringsloven ble vedtatt 16. juni 2023 med ikrafttredelse av endringsloven 1. oktober 2023.

1.3 Saksbehandlingen for tingretten

Ved stevning 6. mars 2024 tok Stiftelsen Tinius og Tom Erik Thorsen ut søksmål mot staten ved Forsvarsdepartementet med krav om at

1. Staten v/Forsvarets etterretningstjeneste er uberettiget til å innhente, lagre og behandle elektronisk kommunikasjon ved tilrettelagt innhenting etter kapittel 7 i Lov om Etterretningstjenesten.
2. Staten v/Forsvarets etterretningstjeneste pålegges å slette all elektronisk kommunikasjon som er innhentet ved tilrettelagt innhenting etter kapittel 7 i Lov om Etterretningstjenesten.
3. Staten v/Forsvarets etterretningstjeneste er uberettiget til å innhente, lagre og behandle elektronisk kommunikasjon ved midpunktinnhenting og endepunktinnhenting innhenting etter paragrafene henholdsvis 6-9 og 6-10 i Lov om Etterretningstjenesten.
4. Staten v/Forsvarets etterretningstjeneste pålegges å slette all elektronisk kommunikasjon som er innhentet etter paragrafene henholdsvis 6-9 og 6-10 i Lov om Etterretningstjenesten.
5. Staten v/Forsvarets etterretningstjeneste er uberettiget til å behandle og lagre kommunikasjonsdata etter kjøp av metadata i bulk.
6. Staten v/Forsvarets etterretningstjeneste pålegges å slette all lagret kommunikasjonsdata etter kjøp av metadata i bulk.
7. Staten v/Forsvarets etterretningstjeneste pålegges å erstatte Stiftelsen Tinius' og Tom Erik Thorsens sakskostnader.

Saksøkernes påstand er senere endret, jf. påstanden gjengitt ovenfor.

Norsk Redaktørforening, Norsk Presseforbund, Norsk Journalistlag, Mediebedriftenes Landsforening, Den norske Forleggerforening, Norsk Pen og Norsk faglitterær forfatter- og oversetterforening erklærte partshjelp til søksmålet samme dag.

Staten ved Forsvarsdepartementet har til rett tid inngitt tilsvar i saken og det ble nedlagt påstand om frifinnelse.

Hovedforhandling i saken ble avholdt i Oslo tingrett over fem rettsdager fra 2. til 6. desember 2024. Begge parter møtte, og retten mottok forklaringer fra saksøkerne og representanter for partshjelperne. I tillegg mottok retten forklaring fra tre vitner, herunder to sakkyndige vitner. Om bevisførselen for øvrig viser retten til rettsboken.

2. Partenes syn på saken

2.1 Saksøkerne, Stiftelsen Tinius m.fl., har overordnet gjort gjeldende:

Ved den nye e-tjenesteloven lovfestet staten for første gang omfattende vilkårlig masseovervåkning – innhenting, lagring og behandling i bulk – av befolkningens digitale kommunikasjon.

Det klare utgangspunktet er at slik vilkårlig masseovervåkning er ulovlig etter EØS-retten, etter EMK og etter Grunnloven.

Borgernes tillit til at de har et reelt privatliv og et vern av sin private kommunikasjon er en sentral forutsetning for fri meningsbrytning. Reell trygghet for at kommunikasjon også kan skje i fortrolighet, ikke minst uten statens innsyn, er også et avgjørende premiss for reell opposisjon og kritikk av makten generelt og for pressens arbeid og tilgang på informasjon fra kilder.

På denne bakgrunn ble europeiske staters forsøk på å innføre masseovervåkning til bruk i kriminalitetsbekjempelse, underkjent av EU-domstolen og EMD.

Til tross for dette innførte flere stater masseovervåkningssystemer til bruk for å ivareta nasjonale sikkerhetsinteresser. Også slike systemer har blitt underkjent både av EU-domstolen og EMD. Begge domstolene har likevel åpnet for at denne typen masseovervåkning unntaksvis kan aksepteres for å ivareta nasjonal sikkerhet, forutsatt at formålet er tilstrekkelig konkret og tungtveiende (reelle nasjonale sikkerhetsinteresser) og at rettssikkerhetsgarantiene er gode nok. Som uttrykt av EMD i storkammerdommen i Big Brother Watch mot Storbritannia avsnitt 339:

> In view of the risk that a system of secret surveillance set up to protect national security (and other essential national interests) may undermine or even destroy the proper functioning of democratic processes under the cloak of defending them, the Court must be satisfied that there are adequate and effective guarantees against abuse.

Saksøkerne gjør gjeldende at det norske systemet åpner for masseovervåkning begrunnet i for generelle og for svake hensyn. Saksøkerne gjør også gjeldende at rettssikkerhetsgarantiene er utilstrekkelige.

Søksmålet gjelder for det første de nye reglene i etterretningstjenesteloven kapittel 7 om tilrettelagt innhenting (TI).

E-tjenestens innsamling, lagring og behandling av elektroniske kommunikasjonsdata etter etterretningstjenesteloven kapittel 7, er i strid med retten til ytringsfriheten og retten til privatliv og personvern, slik disse rettighetene er beskyttet i henholdsvis EØS-retten, Grunnloven §§ 100 og 102 og EMK artikkel 8 og 10.

På EØS-rettslig grunnlag anføres særlig at formålene som kan begrunne TI er for vide og at terskelen for å tillate TI er for lav. Etter loven kan samtlige oppgaver i e-tjenesteloven kapittel 3 begrunne masseovervåkning, selv om flere av disse oppgavene/formålene ikke er tungtveiende nasjonale sikkerhetsinteresser. Vilkårene i loven er også så vage/uspesifiserte at de åpner for kontinuerlig masseovervåkning til enhver tid.

Etter EMK og Grunnloven er det, i tillegg til de nevnte innvendingene, de samlede svakhetene i rettssikkerhetsgarantiene som påberopes. I denne vurderingen er det sentralt at systemet har vesentlige svakheter knyttet til mangel på domstolskontroll, regler om lagringstid og sletting, regler om deling av overvåkningsmateriale og til reell uavhengig kontroll.

Under EMK og Grunnloven er også risikoen for at pressens kilder avsløres som følge av overvåkningen, og den avkjølende effekten dette fører med seg, sentralt.

For det andre gjelder søksmålet etterretningstjenesteloven § 6-9 om midtpunktinnhenting og 6-10 om endepunktinnhenting.

Paragraf 6-9 gir E-tjenesten adgang til å «innhente elektronisk kommunikasjon i transitt». Dette innebærer (i motsetning til TI, som forutsetter tilrettelegging fra relevante tjenesteytere) at E-tjenesten innhenter kommunikasjonen selv, direkte fra luft, kabel eller hvilket som helst annet overføringsmedium og uavhengig av teknologi, mens kommunikasjonen er i transitt mellom avsender og mottaker. Slik innhenting vil også kunne omfatte bulkinnhenting av kommunikasjonsdata.

Paragraf 6-10 gir E-tjenesten adgang til å «observere og innhente ikke åpent tilgjengelig elektronisk informasjon i datasystemer eller lignende systemer eller tjenester som etterretningsmål besitter eller antas å ville benytte». Dette innebærer å avlytte eller avlese informasjon direkte fra en kommunikasjonsenhet, datamaskin eller annet system hvor relevante etterretningsdata ligger lagret eller blir behandlet. Dette til forskjell fra midtpunktinnhenting, hvor informasjonen hentes inn under transport. Også paragraf 6-10 kan brukes til bulkinnhenting av kommunikasjonsdata.

Både gjennom §§ 6-9 og 6-10 hver for seg og i kombinasjon, kan etterretningstjenesten gjennomføre vilkårlig masseovervåkning i egenregi uten domstolskontroll eller andre reelle rettsikkerhetsgarantier. De strengere rettssikkerhetsgarantiene i kapittel 7 kommer kun inn dersom E-tjenesten er avhengig av tilrettelegging fra private aktører. Det er imidlertid ingenting som tilsier at ikke EMK og Grunnloven også krever reelle rettssikkerhetsgarantier der overvåkningen skjer i statens egenregi. Det er derfor en alvorlig svakhet i loven at dette ikke er sikret.

Det ble nedlagt følgende påstand:

1. Staten v/Forsvarsdepartementet er uberettiget til å innhente, lagre og behandle elektronisk kommunikasjon ved tilrettelagt innhenting etter kapittel 7 i Lov om Etterretningstjenesten.
2. Staten v/Forsvarsdepartementet er uberettiget til å innhente, lagre og behandle elektronisk kommunikasjon innhentet i bulk ved midpunktinnhenting og endepunktinnhenting etter paragrafene henholdsvis 6-9 og 6-10 i Lov om Etterretningstjenesten.
3. Staten v/Forsvarsdepartementet pålegges å erstatte Stiftelsen Tinius' og Tom Erik Thorsens sakskostnader.

2.2 Saksøkte, Staten ved Forsvarsdepartementet, har i det vesentlige gjort gjeldende:

TI er et system for innhenting av elektronisk kommunikasjon som krysser den norske grensen, og hvor innhentingen krever tilrettelegging fra tilbydere av elektroniske tjenester, se e-tjenesteloven § 7-1. Med TI vil E-tjenesten for eksempel kunne avdekke at en kjent terrorleder i utlandet kommuniserer med ukjente personer i Norge, eller at andre stater driver digital spionasje mot norske mål.

TI er en type midtpunktinnhenting, det vil si innhenting av kommunikasjon i transitt mellom to endepunkter, jf. e-tjenesteloven § 6-9. TI fungerer slik at man først må samle inn og lagre store datasett, for å senere søke i og bruke de lagrede dataene til utenlandsetterretningsformål. Det som skiller TI fra andre typer midtpunktinnhenting, er at den også berører norske data fordi det i dag er teknisk umulig å filtrere ut all intern norsk kommunikasjon. Dersom dette blir mulig i framtida med teknologiske framskritt, har E-tjenesten en plikt til å filtrere ut slike data, jf. § 7-6.

Saksøkernes redegjørelse for TI-reglene bygger på flere juridiske og tekniske misforståelser. De legger blant annet til grunn at E-tjenesten kan masselagre innholdsdata. Dette er ikke riktig, se e-loven § 7-7 og 7-9. Saksøkerne har dessuten misforstått e-loven § 7-3, og synes å legge til grunn at E-tjenesten kan omgå kravet til rettens forhåndsgodkjennelse ved å bruke e-loven § 7-5 om tekniske tester eller 7-3 (2) om speiling for teknisk analyse. Dette er uriktig. E-tjenesteloven § 7-3 (1) annet punktum bestemmer at all speiling av data for etterretningsformål må godkjennes av retten. Dette

gjelder uten unntak. Speilingen for teknisk analyse etter 7-3 (2) gir kun tilgang til overordnede data om tilbydernes tekniske løsninger. Tekniske tester etter § 7-5 skjer i data som er speilet med rettens godkjennelse etter § 7-3 (1).

TI blir strengt kontrollert. EOS-utvalget fører en løpende kontroll i sanntid, og kan be retten om å stanse innhenting, se e-tjenesteloven § 7-12. E-tjenesten trenger domstolenes tillatelse både til å hente og lagre metadataene og for søk og analyse til etterretningsproduksjon. Innholdet i kommunikasjonen (innholdsdata) blir ikke lagret.

TI-reglene ivaretar retten til privatliv etter EMK og Grunnloven.

Det er på det rene at bulkinnhentingssystemer, hvor E-tjenesten gis muligheten til å søke i metadata som er samlet inn og lagret i forkant av søket (retrospektive søk) ikke i seg selv er i strid med EMK. Spørsmålet er om den nærmere utformingen av TI-reglene er «nødvendig i et demokratisk samfunn», jf. EMK artikkel 8 nr. 2. Her må det avgjørende være at EMD har vurdert det svenske TI-systemet og funnet at dette i all hovedsak tilfredsstille kravene etter EMK, se Centrum för rättvisa mot Sverige avsnitt 373. EMD påpekte enkelte svakheter som samlet sett gjorde at domstolen konstaterte krenkelse av retten til privatliv, blant annet at deling med andre stater var mangelfullt regulert, og at det ikke var gitt regler om stansing der vilkårene for innhenting ikke lenger gjorde seg gjeldende. Disse svakhetene gjør seg ikke gjeldende i det norske systemet, se e-tjenesteloven § 10-3 (1) a, jf. § 10-2 (1) d, e og f, 8-6 (2) og 5-4.

TI-reglene ivaretar kildevernet.

Saksøkernes argumentasjon synes å bygge på at TI i seg selv strider mot kildevernet. EMD har slått fast at det ikke er tilfelle, se Big Brother Watch mot Storbritannia avsnitt 431 og 446. Kravene EMD stilte til bruk av kildeidentifiserende materiale er oppfylt ved e-loven § 9-6 (3), jf. Prop. 92 L (2022–2023) punkt 4.4.4 og 4.5.

Det er for øvrig spørsmål om saksøkerne (en norsk privatperson og en norsk stiftelse) i det hele tatt kan påberope utenlands aktørers evt. rettigheter etter EMK, jf. også pkt. 2.5 under.

TI er forenelig med kommunikasjonsverndirektivet.

Kommunikasjonsverndirektivet beskytter fortrolighet for kommunikasjon (artikkel 5), men gir statene adgang til begrensinger så lenge disse er nødvendige, egnete og forholdsmessige i et demokratisk samfunn av hensyn til nasjonal sikkerhet (artikkel 15).

E-tjenesteloven § 7-3 første ledd er i tråd med kommunikasjonsverndirektivet som tolket i La Quadrature du Net. TI kan brukes når det er tilstrekkelig konkrete omstendigheter til at det er mulig å anta at det foreligger en alvorlig trussel mot den nasjonale sikkerhet som er

reell og aktuell eller som kan forutses. Det er tilstrekkelig med en generell trusselsituasjon av en bestemt art. Det er ikke nødvendig med mistanke om at bestemte personer vil foreta konkrete handlinger som kan skade nasjonal sikkerhet. Det er derfor slik lagring av metadata kalles «preventiv», jf. avsnitt 138.

At det er tilstrekkelig med en generell trusselsituasjon, kommer videre til uttrykk gjennom at en tillatelse til speiling kan gis for en lengre periode, og om nødvendig fornyes. Det er også av den grunn at det ikke gjelder et absolutt krav om at den aktuelle trusselen er reell og aktuell, men at det er tilstrekkelig at den kan forutses.

Saksøkernes krav om midt- og endepunktinnhenting i bulk må avvises.

Staten mener at saksøkerne mangler tilknytning til kravet, jf. tvl. § 1-3 (2). Metodene kan bare rettes mot utenlandske mål og forhold, og vil (i motsetning til TI) i svært begrenset grad kunne berøre innenlands kommunikasjon.

Subsidiært bestrides saksøkernes anførsler. Det er ingen holdepunkter for at de kravene som EMD har oppstilt for TI-systemer, kan overføres til etterretningstjenestens øvrige virksomhet. Staten kjenner ikke til at andre stater bruker TI-kravene på annen etterretningsvirksomhet.

Et forslag om generell forhåndsautorisering av E-tjenestens metoder ble vurdert og forkastet (høringsnotat 12. november 2018 punkt 10.6.2 og Prop. 80 L (2019–2020) punkt 11.11.4.1.

Det ble nedlagt følgende påstand:

1. Kravet i saksøkernes påstand pkt. 2 avvises.
2. For øvrig frifinnes staten v/Forsvarsdepartementet.
3. Staten v/Forsvarsdepartementet tilkjennes sakskostnader.

Påstandsgrunnlagene er nærmere utdypet under de enkelte punktene nedenfor.

3. Rettens vurdering

3.1 Innledning

Søksmålet er generelt anlagt og gjelder overprøving av Stortingets lovvedtak om endringer av e-tjenesteloven 6. juni 2023 i forhold til de rammer EMD og EU-domstolen har satt for bulkinnsamlingssystemer.

Påstandsgrunnlagene som er gjort gjeldende under henholdsvis EMK og EØS-retten er i hovedsak de samme, og retten behandler først forholdet til EMK og deretter EØS-retten.

3.2 Rettslig interesse

Saksøkerne har fremmet to krav i saken. For det første kreves det fastsettelsesdom for at staten er uberettiget til å innhente, lagre og behandle elektronisk kommunikasjon ved tilrettelagt innhenting, jf. e-tjenesteloven kapittel 7. For det andre kreves det fastsettelsesdom for at staten er uberettiget til å innhente, lagre og behandle elektronisk kommunikasjon innhentet i bulk ved midtpunktinnheting og endepunktinnheting etter e-tjenesteloven §§ 6-9 og 6-10. Begge kravene er således av generell karakter.

Saksøkerne i saken er Stiftelsen Tinius og Tom Erik Thorsen.

Stiftelsen Tinius ble etablert i 1996 og kontrollerer den største aksjeposten i Schibsted gjennom det heleide selskapet Blommenholm Industrier AS. Schibsted omfatter en rekke store medier i Norge, herunder Aftenposten. Verdens Gang og Bergens Tidende. I tillegg har Schibsted eierandeler i Aftonbladet og Svenska Dagbladet i Sverige. Etter vedtektene § 3 er Stiftelsens formål blant annet:

> Schibstedkonsernet skal drives på en måte som sikrer frie og uavhengige redaksjoner i
> konsernets aviser og øvrige datterselskaper med redaksjonell virksomhet.
>
> Schibstedkonsernets utgivelser skal tilstrebe kvalitet og troverdighet. De skal forsvare
> verdier som trosfrihet, toleranse, menneskerettigheter og demokratiske prinsipper.
> (…)
> Stiftelsen skal ved behov arbeide for og støtte prosjekter som påvirker de rammebetingelser som er vesentlige for å sikre frie og uavhengige redaksjoner.

Det er gjort gjeldende at saksøkerne er direkte berørt av TI som følge av at Stiftelsens egen kommunikasjon omfattes av tiltakene saken gjelder. I tillegg ligger søksmålet innenfor Stiftelsens formål. Tiltakene som angripes har dessuten vesentlig negative virkninger for ytringsfriheten generelt og redaksjoners adgang til å virke fritt.

Saksøker nr. 2, Tom Erik Thorsen, er bosatt i Norge og er ansvarlig redaktør i avisen Varden. Det er anført at han berøres av overvåkningen både i egenskap av å være norsk borger og som redaktør.

I tillegg har organisasjonene Norsk Redaktørforening, Norsk presseforbund, Norsk Journalistlag, Mediebedriftenes Landsforening, Den norske Forleggerforening, Norske Pen og Norsk faglitterær forfatter- og oversetterforening erklært partshjelp i saken etter tvisteloven § 15-7. Felles for disse organisasjonene er at de arbeider for å fremme ytringsfrihet og trykkefrihet og kildevern. Partsrepresentanter for hver av disse organisasjonen har forklart seg under hovedforhandlingen og gitt uttrykk for at de har elektronisk kommunikasjon med kilder både i Norge og i utlandet.

Etter tvisteloven § 1-3 må den som reiser saken «påvise et reelt behov for å få kravet avgjort overfor saksøkte». Hvorvidt dette er tilfellet «avgjøres ut fra en samlet vurdering av kravets aktualitet og partenes tilknytning til det». I uttrykket «reelt behov» ligger det en forutsetning om at en avgjørelse «får betydning for saksøkerens rettsstilling», jf. Ot.prp. nr. 51 (2004-2005) side 365. Det følger videre av Rt-2014-1089 (avsnitt 11) at det ikke kan kreves dom for et krav dersom avgjørelsen ikke vil få umiddelbare rettsvirkninger for dem. Bestemmelsen i § 1-3 suppleres av tvisteloven § 1-4 som fastslår at foreninger og stiftelser kan reise søksmål i eget navn «om forhold som ligger innenfor organisasjonens formål og naturlige virkeområde å ivareta».

Høyesterett har HR-2021-4176-P (Acer) foretatt en grundig gjennomgang av i hvilken utstrekning søksmålsvilkårene åpner for saksanlegg av mer generell karakter. Saken gjaldt søksmål fra organisasjonen Nei til EU mot staten for å stanse gjennomføringen av EUs tredje energimarkedspakke i norsk rett. Høyesterett kom her til at lovens forarbeider ga rettskildemessig grunnlag for at det i en viss utstrekning kan reises søksmål av mer generell karakter, ikke bare konkrete rettstvister. For å kunne fremme et slikt krav må det kreves at det er et særlig behov for avklaring og at rettsspørsmålene egner seg for å bli prøvd i generell form, jf. avsnitt 174. I det konkrete tilfellet fant Høyesterett at det forelå et særlig behov for å få prøvd det prinsipielle og uavklarte rettsspørsmålet i saken, som også egnet seg til avklaring i en mer generell form på det rettslige og faktiske grunnlaget som forelå.

Når det gjelder kravet knyttet til reglene om tilrettelagt innhenting (krav nr. 1) har staten påpekt at det er tale om et søksmål av generell karakter, men staten har ikke bestridt at det foreligger rettslig interesse i å få de rettslige spørsmålene avklart. Retten er enig i denne vurderingen. Retten viser til at kravet reiser uavklarte rettsspørsmål med stor prinsipiell rekkevidde, at saken er godt nok belyst samt at det er begrenset mulighet for å få prøvd disse spørsmålene i en åpen rettsprosess.

Staten har derimot krevd avvisning av Stiftelsens krav om at staten er uberettiget til å innhente, lagre og behandle elektronisk kommunikasjon innhentet i bulk ved midtpunktinnheting og endepunktinnheting etter e-tjenesteloven §§ 6-9 og 6-10. Det er vist til at ingen av saksøkerne er berørt av disse innhentingsmetodene og at en dom i saksøkers favør ikke vil ha noen faktiske eller rettslige virkninger for dem. Saksøkerne vil heller ikke kunne klage til EMD, jf. EMK artikkel 34.

Stiftelsen har anført at det ikke er tvilsomt at Norges forpliktelser etter EMK også gjelder overfor personer (norske og andre) utenfor Norges grenser som kan rammes av etterretningstjenestens innhenting, lagring og behandling av elektronisk kommunikasjon. Stiftelsen har blant annet vist til EMDs avgjørelse i Wieder and Guarnieri mv Storbritannia (12/9-23). Denne avgjørelsen gjaldt spørsmålet om jurisdiksjon og kravet til å være offer for rettighetskrenkelse (offerkravet) når inngrepet skjer i et annet land. Selve inngrepet - innhenting, lagring og behandling av elektronisk kommunikasjon - ble gjennomført i Storbritannia mens klagerne befant seg utenfor Storbritannias grenser. EMD uttalte i avsnitt 99:

> For the purposes of the Article 8 complaint the level of persuasion necessary to establish victim status cannot be unreasonably high. The section 8(4) regime is a bulk interception regime and communications may be intercepted, stored and searched even if neither the sender nor recipient is of interest to the intelligence agencies. Moreover, the nature of electronic communications is such that the sender will not know which countries his communications passed through *en route* to the recipients, and cannot, therefore, know which States' intelligence agencies might have had the opportunity to intercept them. Nonetheless, as the Convention does not provide for the institution of an *actio popularis* or for a review the relevant law and practice in *abstracto* (see *Roman Zakharov*, cited above, § 164), potential applicants must take steps to substantiate their claim that they were potentially at risk of having their communications intercepted, searched and possibly even examined under the impugned surveillance regime.

EMD tok ikke eksplisitt stilling til om de aktuelle klagerne hadde offerstatus da dette ikke var bestridt av britiske myndigheter. EMD la dette til grunn.

Etter rettens syn er ikke situasjonen i vår sak helt sammenlignbar. For det første vil innhenting etter §§ 6-9 og 6-10 foregå utenfor landets grenser og det kan derfor reises spørsmål om kravet til jurisdiksjon er oppfylt, jf. Wieder and Guarnieri avsnitt 87 flg. Dernest omhandlet den refererte saken enkeltpersoner som faktisk ble rammet av inngrepet.

Saksøkerne i vår sak befinner seg i Norge og innhenting av informasjon etter disse metodene er forbudt i Norge, jf. territorialforbudet i lovens § 1-4. Saksøkerne selv kan dermed ikke rammes av et slikt inngrep. Slik retten forstår saksøkernes anførsel mener de

at det faktum at de kommuniserer med personer i utlandet, som kan rammes av et slikt tiltak, er tilstrekkelig for å etablere rettslig interesse. Retten er ikke enig i dette. Retten viser til at en dom i saksøkernes favør ikke vil ha noe faktiske eller rettslige virkninger for dem. En eventuell virkning for noen som befinner seg i utlandet og som saksøkerne kommuniserer med, kan ikke anses å etablere en tilstrekkelig tilknytning til kravet.

Saksøkerne oppfyller etter rettens syn heller ikke offerkravet i relasjon til krav nr. 2, slik dette er beskrevet i Centrum för Rättvisa (avsnitt 167) hvor den såkalte Zakharov-testen gjengis slik:

> Firstly, the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his communications intercepted.

Det oppstilles her to alternative grunnlag for å påvirkes at et tiltak. For det første kan en slik påvirkning følge av at klager tilhører en gruppe som lovgivningen retter seg mot. Alternativt må lovgivningen rette seg mot alle brukere av kommunikasjonstjenestene.

Ingen av disse vilkårene er oppfylt som følge av forbudet i e-tjenesteloven § 1-4 og retten har etter dette kommet til at saksøkernes krav nr. 2 skal avvises.

3.3 TI – forholdet til EMK og Grunnloven

3.3.1 Innledning

Alle som oppholder seg i Norge har rett til respekt for sitt privatliv og sin kommunikasjon. Denne rettigheten følger av både Grunnloven § 102 og EMK artikkel 8.

Etter Grunnloven § 102 første ledd har «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon». Grunnlovens § 102 er utformet blant annet etter forbilde av tilsvarende rettighet etter EMK, og Høyesterett har i flere saker slått fast at Grunnlovens § 102 skal tolkes med utgangspunkt i EMK artikkel 8, jf. blant annet HR-2016-2554-P (Holship) avsnitt 81 med videre henvisninger. Retten viser også til Rt-2015-155 (Rwanda) avsnitt 40 og 41. Retten tar dermed i det følgende utgangspunkt i EMK artikkel 8.

3.3.2 Nærmere om EMK artikkel 8

EMK artikkel 8 nr. 1 oppstiller et generelt vern for privatlivets fred:

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

Vernet omfatter den enkeltes privatliv og familieliv, hjem og korrespondanse. Det er ingen tvil om at kommunikasjon som innhentes ved hjelp av TI omfattes av begrepet «korrespondanse» og at TI i utgangspunktet utgjør et inngrep i denne rettigheten. Den økende digitaliseringen av samfunnet innebærer at bulkinnsamling av kommunikasjonsdata utgjør et tilsvarende sterkere inngrep i disse rettighetene.

Vernet etter artikkel 8 nr. 1 er ikke absolutt. Inngrep i rettighetene kan forsvares dersom tiltaket har tilstrekkelig hjemmel i lov, forfølger et legitimt formål og er «nødvendig i et demokratisk samfunn», jf. EMK artikkel 8 nr. 2. Dette er en unntaksbestemmelse som skal tolkes restriktivt.

Lovkravet er todelt. Et inngrep må for det første ha hjemmel i lov. Reglene om TI fremgår av e-tjenesteloven kap. 7 og 8 og det er ikke tvilsomt at det formelle kravet til lovhjemmel er oppfylt. Det følger videre av EMDs rettspraksis at lovgivningen må være tilgjengelig og utformet på en måte som er klar og forutsigbar for borgerne.

Når det gjelder hemmelig overvåkning har imidlertid kravet til forutberegnelighet et noe annet innhold. EMD har i Centrum för Rättvisa avsnitt 247 uttalt følgende om dette kravet knyttet til hemmelig overvåking:

> 247. The meaning of "foreseeability" in the context of secret surveillance is not the same as in many other fields. In the special context of secret measures of surveillance, such as the interception of communications, "foreseeability" cannot mean that individuals should be able to foresee when the authorities are likely to resort to such measures so that they can adapt their conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on secret surveillance measures, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (…). Moreover, the law must indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (…).

Det følger av dette at lovgivningen må bestå av klare, detaljerte regler for hvilke inngrep som kan iverksettes, hvilke omstendigheter som kan føre til inngrep, omfanget av myndighetens skjønn og hvordan skjønnet kan benyttes.

Det er ikke bestridt at TI systemet er ment å oppfylle et av de legitime formålene som er opplistet i EMK artikkel 8 nr. 2. Formålet med e-tjenesteloven og dermed E-tjenestens

virksomhet er å «bidra til å trygge Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser», jf. E-tjenesteloven § 1-1 a). Reglene om tilrettelagt innhenting skal bidra til at E-tjenesten kan ivareta disse oppgavene.

Det tredje grunnvilkåret er at et inngrep må være «nødvendig i et demokratisk samfunn». Dette betyr at tiltaket må være egnet til å ivareta det definerte legitime formålet og at interessene som begrunner inngrepet samlet sett må være mer tungtveiende enn de interessene som krenkes. Vilkåret gir anvisning på en forholdsmessighetsvurdering på om tiltaket er egnet, nødvendig og forholdsmessig. Ved vurderingen av om et inngrep er «nødvendig i et demokratisk samfunn» og dermed proporsjonalt, er statene tillagt en vid skjønnsmargin med hensyn til valg av hvordan det legitime formålet best kan ivaretas (Centrum för Rättvisa avsnitt 252).

Norge står i dag i en betydelig mer krevende sikkerhetssituasjon enn på mange tiår, blant annet som følge av økt spenningsforhold mellom stormaktene, krigen i Ukraina og konfliktene i Midtøsten. Digitaliseringen av samfunnet har ført til at stadig mer av kommunikasjonen skjer elektronisk. Dette gjelder også for de ulike trusselaktørene.

Sjefen for E-tjenesten, viseadmiral Nils-Andreas Stensønes, har blant annet forklart at Russland anser seg selv for å ha en varig konflikt med Vesten, og at dette blant annet har kommet til uttrykk gjennom ulike påvirkningsaksjoner, sabotasjeaksjoner og cyberangrep i Europa. Han forklarte at videre at muligheten til å innhente grensekryssende kommunikasjon er av stor betydning for E-tjenestens evne til å oppdage, forebygge og avverge utenlandske trusler. Dette gjelder både fremmede militæroperasjoner, terrorplanlegging og fremmede staters påvirknings-aksjoner. Felles for dette er at man kommer over biter av informasjon som må holdes opp mot annen informasjon for å avklare om det foreligger en trussel. Dette krever at E-tjenesten har tilgang til informasjon som er lagret.

Norge som ett av verdens mest digitale samfunn, blant annet innenfor infrastruktur, er svært sårbart for cyberoperasjoner. Ifølge Stensønes vil TI gi et vesentlig styrket bidrag til nasjonal situasjonsforståelse innenfor cybersikkerhet og styrke evnen innenfor kontraterror. Stensønes viste i den forbindelse til at over 50 % av de planlagte terroraksjonene i Europa de senere årene har blitt avverget som følge av etterretningsaksjoner. Stensønes forklarte også at aksjonen mot Sykehuspartner HF/Helse Sørøst i 2018 kunne vært avverget dersom man hadde hatt TI på dette tidspunktet.

Retten legger etter dette til grunn at den informasjonen E-tjenesten får tilgang til gjennom TI vil ha stor etterretningsmessig verdi og at systemet som sådan er egnet. TI er også nødvendig for å oppdage og varsle om trusler som stammer fra utlandet. Uten et slikt system vil E-tjenesten være henvist til å få tilgang til informasjon gjennom samarbeid med andre lands tjenester.

Samfunnsbehovet som begrunner reglene er dermed sterkt og skal sikre at E-tjenesten får tilgang til informasjon som er strengt nødvendig for å oppfylle lovens formål, nemlig vern av nasjonale sikkerhetsinteresser. Inngrep ved bruk av TI vil derfor også etter omstendighetene være forholdsmessige.

EMD har i to storkammeravgjørelser fra 25. mai 2021 trukket opp rammene for bruk av TI og TI-lignende systemer («bulk interception regimes»); nemlig sakene Big Brother Watch m.fl. mot Storbritannia og Centrum för Rättvisa mot Sverige.

EMD har akseptert at et slikt system i seg selv ikke er i strid med EMK (Big Brother Watch avsnitt 340). Dommene oppstiller imidlertid strenge krav for at et bulkinnsamlingssystem av grenseoverskridende elektronisk kommunikasjon kan være forenelig med EMK. Som en følge av hvor omfattende og inngripende systemet er og risikoen for misbruk, må det oppstilles tilstrekkelige rettslige rammer og rettssikkerhetsgarantier for å hindre misbruk og forsikre at inngrepet blir holdt til det som er nødvendig.

Både det britiske og det svenske bulkinnsamlingssystemet ble ansett å være i strid med EMK artikkel 8. I Big Brother Watch ble det også konstatert brudd på EMK artikkel 10.

Centrum för Rättvisa gjelder et bulkinnsamlingssystem som er mest sammenlignbar med det norske TI regimet og retten vil i det følgende ta utgangspunkt i EMDs avgjørelse i denne saken.

3.3.3 Nærmere om EMDs avgjørelse i Centrum för Rättvisa

Avgjørelsen Centrum för Rättvisa gjaldt spørsmålet om det svenske bulkinnhentings-systemet var forenelig med retten til privatliv etter EMK artikkel 8. Klageren i saken, Centrum för Rättvisa, var en organisasjon som blant annet tilbyr rettshjelp til personer som mener at rettighetene deres er krenket. Organisasjonen kommuniserte på daglig basis med personer både i og utenfor Sverige. På bakgrunn av den kontrollfunksjon organisasjonen hadde overfor den svenske staten, mente organisasjonen at de var særlig utsatt for overvåkning.

EMD slår innledningsvis fast at bulkinnhentingssystemer («bulk interception regimes») ikke i seg selv er i strid med EMK artikkel 8 og beskriver bulkinnhenting som en gradvis prosess hvor inngrepet i borgernes rettigheter etter EMK artikkel 8 gradvis øker i styrke jo lengere ut i prosessen man kommer (avsnitt 239). Domstolen deler deretter bulkinnhentingsprosessen inn i fire stadier:

(a) the interception and initial retention of communications and related communications data (that is, the traffic data belonging to the intercepted communications);
Norsk: Innhente og lagre innholds- og metadata
(b) the application of specific selectors to the retained communications/related communications data;
Norsk: Bruk av søkebegreper på lagrede data
(c) the examination of selected communications/related communications data by analysts; and
Norsk: Analyse av lagrede data
(d) the subsequent retention of data and use of the "final product", including the sharing of data with third parties
Norsk: Etterfølgende lagring av data og bruk av sluttproduktet, herunder deling av data med tredjemann.

Domstolen slår fast at EMK artikkel 8 gjelder for alle stadiene i denne prosessen, men at inngrepet og dermed behovet for rettssikkerhetsgarantier og regler mot misbruk, blir sterkere jo lengere ut i prosessen man kommer.

Domstolen fastslo videre at statene har en vid skjønnsmargin når det gjelder å velge hvilken type etterretningsregime som er nødvendig for å ivareta nasjonal sikkerhet (avsnitt 252) og at en beslutning om å innføre et bulkinnhentingssystem faller innenfor denne skjønnsmarginen (avsnitt 254). På grunn av risikoen for misbruk ved et slikt system må lovgivningen inneholde adekvate og tilstrekkelige garantier mot misbruk og dette vil bero på en helhetsvurdering basert på:

> (…) all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. (…) (avsnitt 253)

I tillegg må systemet inneholde tilstrekkelige rettsikkerhetsgarantier («end-to-end-safeguards»). Dette innebærer at det på nasjonalt nivå må foretas en vurdering på hvert trinn i prosessen av om inngrepet er nødvendig og forholdsmessig. Inngrepene skal skje på bakgrunn av tillatelser som skal sikre at det foretas en slik vurdering på ethvert trinn i prosessen. Slike tillatelser må gis av en domstol eller annen uavhengig instans (avsnitt 265) som gis tilstrekkelig informasjon til å kunne foreta en reell vurdering.

Inngrepene må videre være gjenstand for løpende kontroll på ethvert trinn av prosessen for å sikre at innhentingen ikke går ut over hva som er «nødvendig i et demokratisk samfunn». Kontrollorganet må settes i stand til å vurdere om innhentingen er nødvendig og forholdsmessig i forhold til det stadiet i innhentingsprosessen man er. For å sikre en slik overvåkning må etterretningstjenesten utarbeide detaljerte logger/records for hvert steg i prosessen (avsnitt 270). Endelig må det finnes et effektivt rettsmiddel som er tilgjengelig for enhver som mistenker at vedkommende kommunikasjon har blitt innhentet, enten for å

utfordre lovligheten av tiltaket eller for en vurdering av om tiltaket er i samsvar med EMK (avsnitt 271).

På bakgrunn av disse utgangspunktene oppstilte EMD 8 punkter for å vurdere om nasjonal lovgiving inneholder en klar regulering av (avsnitt 275):

1. The grounds on which bulk interception may be authorised
   Norsk: På hvilket grunnlag og for hvilke formål innhenting av rådata i bulk kan autoriseres
2. The circumstances in which an individual's communications may be intercepted;
   Norsk: Hvilke omstendigheter som kan medføre innhenting av enkeltpersoners kommunikasjon
2. The procedure to be followed for granting authorisation;
   Norsk: Hvilke prosedyrer som gjelder for å gi autorisasjon
4. The procedures to be followed for selecting, examining and using intercept material;
   Norsk: Hvilke prosedyrer som gjelder for seleksjon, analyse og bruk av innhentede data
5. The precautions to be taken when communicating the material to other parties;
   Norsk: Hvilke forholdsregler som må tas dersom innhentede data skal overføres til andre
6. The limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
   Norsk: Tidsbegrensninger for innhentingen, lagring av innhentede data og omstendighetene som gjør at innhentede data må slettes
7. The procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
   Norsk: Hvilke prosedyrer som gjelder for uavhengig tilsyn og kontroll, og deres kompetanse til å adressere manglende etterlevelse
8. The procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.
   Norsk: Hvilke prosedyrer som gjelder for uavhengig etterhåndskontroll, og hvilken kompetanse kontrollorganet har til å adressere manglende etterlevelse

I denne vurderingen skal lovkravet og nødvendighetsvurderingen foretas samlet. EMD vil deretter, basert på disse elementene, foreta en samlet vurdering («global assessment») av hvordan regimet fungerer.

I Centrum för Rättvisa fant EMD at det svenske bulkinnsamlingssystemet i hovedsak var i overensstemmelse med konvensjonens krav. Det svenske systemet inneholdt imidlertid tre mangler/svakheter basert på de kriteriene som domstolen hadde oppstilt. For det første pekte Domstolen på at det svenske lovverket ikke inneholdt en klar regel om sletting av overskuddsmateriale som ikke inneholdt personlig informasjon. Her krevde EMD som et minimum at den nasjonale lovgivningen må inneholde en regel om at innsamlet informasjon som ikke lenger var nødvendig for formålet med innsamlingen, må slettes. For det andre mente Domstolen at de svenske reglene om deling av etterretningsinformasjon

med utenlandske tjenester ikke sikret noen vurdering av hensynet til den aktuelle persons privatliv. Dette ble ansett som en alvorlig svakhet ved systemet («significant shortcoming») (avsnitt 330). For det tredje manglet det svenske systemet en ordning for effektiv og uavhengig etterkontroll av overvåkningssystemet. Her ble det særlig lagt vekt på at kontrollinstansen, Statens inspektion för försvarsunderrättelsesverksamheten (SIUN), hadde en dobbeltrolle. Domstolen kom etter en helhetsvurdering til at det på bakgrunn av disse tre manglene at det forelå brudd på EMK artikkel 8.

3.4 Er TI forenelig med EMK?

3.4.1 Oversikt

Stiftelsen Tinius har anført at de norske reglene om TI ikke er i samsvar med de kravene som EMD har oppstilt for bulkinnsamlingssystemer. Det anføres at det er særlig følgende 5 krav som ikke er oppfylt:

1. På hvilket grunnlag og for hvilke formål innhenting av rådata i bulk kan autoriseres
2. Hvilke omstendigheter som kan medføre innhenting av enkeltpersoners kommunikasjon
6. Tidsbegrensninger for innhentingen, lagring av innhentede data og omstendighetene som gjør at innhentede data må slettes
7. Hvilke prosedyrer som gjelder for uavhengig tilsyn og kontroll, og deres kompetanse til å adressere manglende etterlevelse
8. Hvilke prosedyrer som gjelder for uavhengig etterhåndskontroll, og hvilken kompetanse kontrollorganet har til å adressere manglende etterlevelse

Retten legger til grunn at det ikke er innsigelser fra Stiftelsen til de øvrige vilkårene som er oppstilt av EMD.

Staten har anført at den norske loven er godt i samsvar med de krav som er oppstilt av EMD og har i hovedsak vist til EMDs vurdering av det svenske systemet.

Til dette har Stiftelsen anført at det er betydelige forskjeller mellom det norske og det svenske systemet for bulkinnhenting. Ifølge Stiftelsen skjer blant annet speilingen, filtreringen og selektorbasert søk i én operasjon i det svenske systemet (avsnitt 18, 25-29). Dette innebærer at man i Sverige ikke ender opp med et stort metadata-lager slik som i Norge. Staten er uenig i denne anførselen.

Utover det som er gjengitt i EMDs avgjørelse har det ikke vært nærmere bevisførsel om hvordan det svenske systemet er utformet. Etter rettens syn er dette heller ikke nødvendig for å foreta en vurdering av det norske systemet.

Som nevnt ovenfor har EMD oppstilt 8 punkter for en slik vurdering og retten tar i det følgende utgangspunkt i denne oppstillingen.

3.4.2 Vilkår 1: På hvilket grunnlag og til hvilket formål innhenting av rådata kan autoriseres

Dette vilkåret skal bidra til at kravet til forutberegnelighet ivaretas.

Som nevnt ovenfor, har EMD i avsnitt 247 lagt til grunn at det i forbindelse med hemmelig overvåkning ikke kan oppstilles et krav om at personer som er gjenstand for overvåkningen skal kunne forutse at etterretningstjenesten kan igangsette TI og dermed tilpasse sin aktivitet til dette. Det avgjørende for å vurdere forutberegnelighet i denne sammenheng er at lovgivningen inneholder klare og detaljerte regler for å iverksette tiltak. Dette gjelder både når tiltak kan iverksettes og vilkårene for slike tiltak. Formålet må dermed være tilstrekkelig klart definert for å beskytte borgerne mot vilkårlighet (avsnitt 247). Lovligheten av tiltaket er nært knyttet sammen med vurderingen av om tiltaket er «nødvendig i et demokratisk samfunn» og for å sikre effektive garantier for å hindre misbruk (avsnitt 248).

3.4.3 Er formålet for vidt?

3.4.3.1 Partenes anførsler

Stiftelsen Tinius har gjort gjeldende at e-tjenesteloven åpner for masseovervåkning på grunnlag av et for vidt/vagt formål.

E-tjenesten kan i medhold av § 7-1 innhente elektronisk kommunikasjon som transporteres over den norske grensen «for etterretningsformål». Dette omfatter alle oppgavene som E-tjenesten er tillagt etter lovens kapittel 3, jf. § 1-3 bokstav c), og medfører at E-tjenesten er gitt svært vide fullmakter til å benytte seg av denne metoden for informasjonsinnhenting.

Stiftelsen har blant annet vist til at TI kan benyttes for å sikre Norges «politiske og økonomiske handlefrihet», jf. § 3-1 bokstav a) og at e-tjenesteloven § 3-2 omfatter utenlandske forhold som blant annet sikring av «ivaretakelse av prioriterte utenriks-, forsvars- eller sikkerhetspolitiske interesser knyttet til forhold og utviklingstrekk i andre stater og regioner», «alvorlige trusler mot samfunnssikkerheten i Norge», «alvorlige trusler mot norske interesser i utlandet», «nasjonal beredskapsplanlegging», og «episode- og krisehåndtering».

Retten oppfatter at denne anførselen i den skriftlige saksforberedelsen primært er knyttet til spørsmålet om TI er forenelig med EØS-retten hvor det er oppstilt noe mer presise krav enn under EMK. Dette spørsmålet er behandlet under punkt 3.6.3 nedenfor. Retten forstår imidlertid Stiftelsen slik at det i relasjon til EMK anføres at formålet som skal begrunne innhenting og lagring er for vidt formulert i forhold til EMDs kriterier 1 og 2, og at dette innebærer en svakhet ved TI-systemet som inngår i den samlede helhetsvurderingen som skal foretas under EMK.

Staten bestrider at formålene som kan begrunne tilrettelagt innhenting er for vide. Det anføres at det går klart frem av e-tjenesteloven på hvilket grunnlag og for hvilke formål innhenting av rådata i bulk kan autoriseres. E-tjenestelovens bestemmelser om formål og E-tjenestens oppgaver må leses i sammenheng, og TI kan bare benyttes av E-tjenesten for å sikre nasjonale sikkerhetsinteresser. Reglene i Norge og Sverige er ganske like og EMD vurderte de svenske reglene som tilstrekkelig klare, jf. Centrum för Rättvisa avsnitt 367.

3.4.3.2 Rettens vurdering

Ivaretagelse av statens suverenitet og borgernes rettsikkerhet er en grunnleggende oppgave for nasjonalstaten. Dette har blant annet kommet til uttrykk i Grunnlovens § 2 om å sikre «demokratiet, rettsstaten og menneskerettighetene». Dette er i samsvar med E-tjenestens overordnede formål som er beskrevet i e-tjenesteloven § 1-1 a:

> bidra til å trygge Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser, herunder forebygge, avdekke og motvirke utenlandske trusler mot Norge og norske interesser.

Gjennom reglene om TI kan E-tjenesten innhente grenseoverskridende kommunikasjon for «etterretningsformål», jf. e-tjenesteloven § 7-1. «Etterretningsformål» er i lovens § 1-3 bokstav c) definert som «formål om å ivareta en eller flere av Etterretningstjenestens oppgaver etter kapittel 3». Lovens kapittel 3 danner dermed rammen for hva E-tjenesten kan innhente av informasjon. Bestemmelsene må imidlertid leses i sammenheng med lovens øvrige bestemmelser.

E-tjenestens oppgaver og formålet med innhentingen blir for det første avgrenset av innhentingsforbudene i lovens kapittel 4. Etter § 4-1 kan E-tjenesten ikke benytte innhentingsmetoder overfor personer i Norge. Overvåkning og innhenting av informasjon av personer som oppholder seg i Norge kan bare skje i regi av Politiets sikkerhetstjeneste (PST) og Nasjonal Sikkerhetsmyndighet (NSM). Forbudet i § 4-1 er imidlertid ikke til hinder for innhenting mot utenlandske mål hvor det følger med informasjon om personer i Norge (aksessorisk informasjon), jf. § 4-7. Retten nevner også at § 4-8 inneholder et uttrykkelig forbud mot å innhente informasjon for å utføre oppgaver som tilligger politiet eller andre rettshåndhevende myndigheter.

All innhenting må videre oppfylle grunnvilkårene i kapittel 5. Kapittel 5 oppstiller grunnvilkår for målsøking (§ 5-1), målrettet innhenting (§ 5-2) og innhenting av og målsøking i rådata i bulk (§ 5-3). Av særlig betydning er lovens § 5-4 som oppstiller et krav om forholdsmessighet. Kravet til forholdsmessighet utgjør en sentral skranke for E-tjenestens bruk av inngripende metoder. Kravet er nærmere beskrevet i Prop. 80 L (2019-2020) punkt 9.5.3 side 74:

> (…) Kravet innebærer at tiltaket må være nødvendig for å oppnå formålet, herunder at det er egnet og at formålet ikke kan oppnås med mindre inngripende tiltak. Det må også foretas en samlet avveining av de beskyttede individuelle interessene og det legitime samfunnsbehovet for informasjonsinnhenting.
>
> Forholdsmessighetsvurderingen må foretas i lys av den konkrete saken. Alle relevante hensyn kan tas i betraktning. Utgangspunktet for vurderingen vil på den ene siden være *styrken av inngrepet i de beskyttede individuelle interessene* som innhentingen eller utleveringen innebærer, og på den andre siden *sakens betydning*. Styrken av inngrepet i de beskyttede individuelle interessene vil kunne variere avhengig av hvilken metode det er tale om å benytte. Jo mer alvorlig og tidskritisk saken er, jo større inngrep vil være tillatt. Motsatt vil det stilles større krav til fremgangsmåten hvis tjenesten har god tid til rådighet.

I tillegg må E-tjenesten følge særreglene for tilrettelagt innhenting i kapitlene 7 og 8, samt reglene om behandling av personopplysninger etter innhenting i kapittel 9.

Nærmere om e-tjenesten oppgaver etter kapittel 3

Lovens kapittel 3 inneholder 5 ulike kategorier av oppgaver som er tillagt E-tjenesten. Bestemmelsene i § 3-1 om informasjonsinnhenting om utenlandske trusler og § 3-2 om informasjonsinnhenting om andre utenlandske forhold, er de mest sentrale.

Retten nevner for ordens skyld også at kapittel 3 inneholder bestemmelser om okkupasjonsberedskap (§ 3-3), internasjonalt etterretningssamarbeid (§ 3-4) og evneinformasjon (§ 3-5). Retten forstår det imidlertid slik at det i hovedsak er § 3-1 og § 3-2 som Stiftelsens anførsel retter seg mot.

Lovens § 3-1 lyder:

> **3-1.** ***Informasjonsinnhenting om utenlandske trusler***
> Etterretningstjenesten skal innhente og analysere informasjon om utenlandske forhold som kan bidra til å avdekke og motvirke
> a. trusler mot Norges selvstendighet og sikkerhet, territorielle integritet og politiske og økonomiske handlefrihet
> b. alvorlige trusler mot samfunnssikkerheten i Norge
> c. alvorlige trusler mot norske interesser i utlandet
> d. fremmed etterretningsvirksomhet
> e. fremmede sabotasje- og påvirkningsoperasjoner
> f. grenseoverskridende terrorisme
> g. spredning av masseødeleggelsesvåpen og utstyr og materiale for fremstilling av slike våpen
> h. internasjonal våpenhandel som kan utgjøre en alvorlig sikkerhetstrussel
> i. eksport av sanksjonerte, listeførte eller sensitive varer og tjenester.

Bestemmelsen gjelder utenlandske trusler og regulerer uttømmende hvilke utenlandske trusler som er å regne som etterretningsformål. De ulike kategoriene vil i noen grad

overlappe hverandre, men det avgjørende er hvorvidt trusselen ligger innenfor rammene av bestemmelsen, jf. Prop. 80 L (2019-2020) side 199.

Uttrykket «trusler» er ikke nærmere definert i loven. Det fremgår av forarbeidene at spørsmålet om det foreligger en «trussel» må avgjøres konkret og at forholdet må ha en viss alvorlighetsgrad for å kunne utgjøre en trussel, jf. Prop. 80 L (2019-2020) punkt 7.3.4.3.

Bestemmelsen gir E-tjenesten hjemmel til å innhente og analysere informasjon «som kan bidra til å avdekke eller motvirke» disse truslene. Av spesialmerknadene til bestemmelsen, jf. Prop. 80 L (2019-2020) punkt 17, fremgår det at informasjonen som innhentes må «antas å ha en viss relevans for oppgavene». Det oppstilles med andre ord et krav til relevans. Terskelen for informasjonsinnhenting er ment å være lav når det gjelder sannsynligheten for at innhentingen vil frembringe faktisk relevant informasjon. Med «avdekke» siktes det til informasjon som er egnet til å oppdage og kartlegge trusler, mens med «motvirke» siktes det til informasjon som er egnet til å sette beslutningstakere i stand til å treffe nødvendige tiltak ved behov.

Selv om flere av de opplistede formålene også kan være straffbare i Norge, blant annet grenseoverskridende terrorisme (bokstav f) og internasjonal våpenhandel (bokstav i) vil formålet med E-tjenestens informasjonsinnhenting aldri være kriminalitetsbekjempelse, men kun ivaretakelse av nasjonal sikkerhet. Retten nevner også for fullstendighetens skyld bevisforbudet i straffesaker i lovens § 7-14.

Bestemmelsen beskriver de mest alvorlige truslene mot norsk stats- og samfunnssikkerhet med opprinnelse fra utlandet. Retten legger til grunn at ingen av høringsinstansene kommenterte bestemmelsen direkte og at det var bred enighet om at disse oppgavene er en kjerneoppgave for E-tjenesten, jf. Prop. 80 L (2019-2020) punkt 7.3.4.2.

Stiftelsen har imidlertid reist spørsmål om «politiske og økonomiske handlefrihet» inntatt i bokstav a) kan anses som en trussel mot samfunnssikkerheten, jf. ovenfor. Til dette bemerkes at § 3-1 bokstav a) omfatter kjernen av trusler mot statssikkerheten og det er etter rettens syn klart at Norges selvstendighet og integritet ikke kan holdes atskilt fra råderetten over politiske og økonomiske anliggende, jf. også Prop. 80 L (2019-2020) side 197.

Stiftelsen har videre pekt på bokstav b) om alvorlige trusler mot samfunnssikkerheten i Norge og bokstav c) om alvorlige trusler mot norske interesser i utlandet. Det fremgår av spesialmerknadene til bokstav b), jf. Prop.80 L (2019-2010) side 198, at det her kun dreier seg om alvorlige trusler som utfordrer samfunnets grunnleggende funksjonalitet, stabilitet og befolkningens sikkerhet. Når det gjelder utenlandske interesser i utlandet fremgår det at dette kan dreie seg om trusler mot norske borgere i utlandet, slik som eksempelvis

gisselsituasjoner som anslaget mot gasskraftverket ved In Amenas i 2013. Retten legger etter dette til grunn at bestemmelsen kun omfatter svært alvorlige trusler som klart faller innenfor hensynet til nasjonal sikkerhet.

Lovens § 3-2 gjelder andre utenlandske forhold som ikke er å anse som trusler. Det er særlig oppgavene som fremgår av denne bestemmelsen som Stiftelsen har pekt på under anførselen om at formålet med e-tjenesteloven er for vidt. Også flere høringsinstanser mente at lovens § 302 og særlig bokstav a) var for vidt formulert.

Bestemmelsen lyder:

> **3-2.** ***Informasjonsinnhenting om andre utenlandske forhold***
> Etterretningstjenesten skal innhente og analysere informasjon om utenlandske forhold som kan bidra til
> a. ivaretakelse av prioriterte utenriks-, forsvars- eller sikkerhetspolitiske interesser knyttet til forhold og utviklingstrekk i andre stater og regioner
> b. nasjonal beredskapsplanlegging
> c. episode- og krisehåndtering
> d. planlegging og gjennomføring av nasjonale eller internasjonale militære operasjoner.

Med «utenlandske forhold» etter § 3-2 menes militære og sivile forhold utenfor Norges territorium som har betydning for å avdekke eller forstå de truslene som følger av bestemmelsen. Av forarbeidene fremgår det at dette eksempelvis kan omfatte kartlegging av andre staters militære kapasiteter, identifisering av organisasjoner eller enkeltpersoner som er på vei til Norge for å utføre en terrorhandling, eller avdekke digitale angrep eller påvirkningsaksjoner mot Norge fra utlandet, jf. Prop 80 L (2019-2020) side 197.

I Prop. 80 L (2019-2020) punkt 7.3.4.3 er det redegjort nærmere for forholdet mellom § 3-1 og § 3-2.

> (…) Dersom Etterretningstjenesten utelukkende skal innhente informasjon om etablerte trusler og kjent truende aktivitet, vil den ikke evne å avdekke fremtidens trusselbilde. Etterretningsvirksomhet er prediktiv i sin natur, og det å detektere avvik fra normalen er en viktig oppgave. For å kunne varsle om avvik fra det normale, må normaltilstanden være kjent. Forholdet mellom §§ 3-1 og 3-2 kan illustreres med et eksempel fra våre nærområder. Norges forhold til Russland er i stor grad preget av forutsigbarhet. Russland utgjør ingen militær trussel mot Norge i dag. Vår geografiske plassering i forhold til russiske strategiske kapasiteter betyr likevel at utviklingen i Russland og nordområdene har vedvarende stor betydning for norsk og alliert sikkerhet. God og tidsriktig situasjonsforståelse, herunder inngående kunnskap om utviklingen i russisk utenriks- og innenrikspolitikk og om moderniseringen av den russiske militærmakten i våre nærområder, er dermed avgjørende forutsetninger

> for å kunne utforme norsk utenriks-, forsvars- og sikkerhetspolitikk. Uten hjemmel til å innhente informasjon om disse forholdene, som ikke kan karakteriseres som en trussel, men som et prioritert område, vil man ikke besitte den dybdekunnskapen som kreves for å evne å varsle om endringer av betydning. Litt forenklet sagt vil derfor informasjonsinnhenting etter § 3-2 ofte være en avgjørende forutsetning for å kunne innhente informasjon om trusler etter § 3-1.

Stiftelsen har pekt på at § 3-2 bokstav a) om «ivaretakelse av prioriterte utenriks-, forsvars- eller sikkerhetspolitiske interesser knyttet til forhold og utviklingstrekk i andre stater og regioner» er vidt formulert.

Denne bestemmelsen har to hovedelementer. For det første må informasjonen knytte seg til forhold eller utviklingstrekk i andre stater eller regioner. Dette vil eksempelvis kunne bidra til situasjonsforståelse i land og regioner som er viktige for Norge slik som politiske forhold, migrasjonsutfordringer og utvikling av militære eller andre kapasiteter som ikke har manifestert seg som en trussel, jf. Prop. 80 L (2019-2020) side 199. For det andre må forholdet ha relevans for Norges utenriks-, forsvars- eller sikkerhetspolitiske interesser. Hvilke forhold dette kan omfatte må sees i sammenheng med lovens § 2-2 om oppdragsstyring som vil utgjøre en begrensning i tillegg til lovens øvrige bestemmelser, herunder kravet om forholdsmessighet.

Når det gjelder bokstav b) om nasjonal beredskapsplanlegging og bokstav c) om episode- og krisehåndtering, omfatter dette informasjon som bidrar til at den nasjonale beredskapen til enhver tid tilpasses det gjeldende trussel- og risikobildet og informasjon om forhold knyttet til eksempelvis grensekrenkelser eller lignende som krever diplomatisk håndtering, jf. Prop. 80 L (2019-2020) side 199.

Retten er enig med Stiftelsen i at ordlyden i § 3-2 gir E-tjenesten forholdsvis vide fullmakter til å drive informasjonsinnhenting og analyse av forhold som på innhentingsstadiet ikke faller inn under begrepet «trussel». Etterretningsformålene i § 3-2 er imidlertid nært knyttet til formålet om å avdekke og motvirke utenlandske trusler etter § 3-1. Etterretningsvirksomhet innebærer å sette sammen biter av informasjon over tid. For å kunne vurdere om det foreligger en trussel etter § 3-1, må E-tjenesten også vite hva som er normalsituasjonen og ha oversikt over utviklingstrekk. Etter rettens syn vil kunnskap om forhold som nevnt i § 3-2 være avgjørende for å kunne avdekke endrede forhold som kan utvikle seg til en trussel. Retten viser også til Centrum för Rättvisa avsnitt 285 gjengitt nedenfor hvor Domstolen legger vekt på at truslene kan variere og utvikle seg over tid.

Lovens § 3-2 må videre sees i sammenheng med lovens øvrige bestemmelser, herunder bestemmelsen om oppdragsstyring i § 2-2 og kravet til forholdsmessighet i § 5-4. Som det fremgår ovenfor, vil formålet med innhentingen være et sentralt moment i forholdsmessighetsvurderingen. Dette vil igjen ha betydning for hvilke metoder E-

tjenesten kan benytte etter kapittel 6. Jo viktigere formålet er, jo mer inngripende metoder kan benyttes, jf. Prop. 80 L (2019-2020) side 44.

Samlet sett mener retten at e-tjenesteloven §§ 3-1 og 3-2 – lest i sammenheng – gir anvisning på et innbyrdes sammenhengende formål om å innhente informasjon om utenlandske forhold som utfordrer rikets sikkerhet. Bestemmelsene i lovens kapittel 3 er nærmere utdypet i lovens forarbeider og gir etter rettens syn tilstrekkelig klare rammer for hvilke formål som kan begrunne bruk av TI.

De norske reglene som regulerer formålet med innhentingen, er også godt i samsvar med de svenske reglene som ble vurdert av EMD i Centrum för Rättvisa (avsnitt 284):

> 284. As noted by the Chamber, according to the Signals Intelligence Act signals intelligence may be conducted only to monitor:
> 1. external military threats to the country;
> 2. conditions for Swedish participation in international peacekeeping or humanitarian missions or threats to the safety of Swedish interests in the performance of such operations;
> 3. strategic circumstances concerning international terrorism or other serious cross-border crime that may threaten essential national interests;
> 4. the development and proliferation of weapons of mass destruction, military equipment and other similar specified products;
> 5. serious external threats to society's infrastructure;
> 6. foreign conflicts with consequences for international security;
> 7. foreign intelligence operations against Swedish interests; and
> 8. the actions or intentions of a foreign power that are of substantial importance for Swedish foreign, security or defence policy (see paragraph 22 above).

Oppregningen av den svenske reguleringen omfatter både forhold som er regulert i den norske loven § 3-1 («trusler») og forhold som er regulert i § 3-2 «utenlandske forhold» uten noe nærmere skille. Den svenske loven er på enkelte punkter videre formulert enn de norske bestemmelsene. Retten viser særlig til punkt 8 ("the actions or intentions of a foreign power that are of substantial importance for Swedish foreign, security or defence policy") med en generell henvisning til formålsbestemmelsen gjengitt i dommens avsnitt 22. Retten nevner også at den svenske loven gir FRA (Försvarets Radioanstalt) mulighet for å innhente informasjon om «serious cross-border crime». Den norske loven inneholder ikke en tilsvarende bestemmelse.

EMD kom til at formålet i den svenske loven var tilstrekkelig presist definert, jf. avsnitt 285:

> (…) In the Court's view, the level of detail and the terms used circumscribe the area in which bulk interception may be used with sufficient clarity, having regard, in particular, to the fact that the impugned regime aims at uncovering unknown foreign threats whose nature may vary and evolve with time.

EMD påpeker videre at den svenske loven utelukker bruk av reglene i forbindelse med straffesaker i Sverige (avsnitt 286/287). Retten nevner i denne forbindelse at også den norske e-tjenesteloven inneholder forbud mot å innhente informasjon for politiformål, jf. § 4-8, og industrispionasje, jf. § 4-9, jf. nedenfor.

EMD konkluderer i avsnitt 288 at de formålene som kan tillate bulkinnsamling er klare nok til å gi nødvendig kontroll i forbindelse med tillatelsen og etterfølgende kontroll.

Retten har etter dette kommet til at formålsangivelsen i e-tjenesteloven § 3-1 og § 3-2 er tilstrekkelig klart formulert til å kunne kontrolleres i forbindelse med tillatelsen til å speile og den etterfølgende kontroll.

3.4.4 Vilkår 2: Hvilke omstendigheter som kan medføre innhenting av enkeltpersoners kommunikasjon

Stiftelsen har gjort gjeldende at TI innebærer at metadata om store deler av den norske befolkningens digitale kommunikasjon/aktivitet vil bli innsamlet og lagret i E-tjenestens metadatalager. Dette er veldig potent informasjon som kan misbrukes og sammenholdt med at det er tale om hemmelige tjenester må det ikke gis for vide rammer for lovgivningen. Retten kan ikke se at det gjennom saksforberedelsen eller under hovedforhandlingene har kommet konkrete anførsler knyttet til vilkår 2 utover at dette er problematisk, og at dette innebærer en «masseovervåkning».

Staten har anført at den norske reguleringen er i samsvar med EMDs krav.

Etter e-tjenesteloven § 7-1 kan E-tjenesten «innhente elektronisk kommunikasjon som transporteres over den norske grensen».

Bestemmelsen gjelder grenseoverskridende kommunikasjon. Dette innebærer for det første at det ikke kan innhentes kommunikasjon som utelukkende transporteres i et norsk nettverk. Det har ingen betydning om kommunikasjonen transporteres inn eller ut av landet, og det er også likegyldig om kommunikasjonen transporteres via kabel eller luft da bestemmelsen er utformet på en teknologinøytral måte. I dagens situasjon vil det i praksis normalt være tale om transport gjennom fiberoptiske kabler, jf. Prop. 80 L (2019-2020) side 213.

Kommunikasjonen må videre være i transitt. Innhentingen er en form for midtpunkt-innhenting, jf. § 6-9, som reguleres særskilt i kapittel 7 og 8, jf. ovenfor punkt 1.1.

Det er ikke nødvendig at det foreligger kommunikasjon mellom to eller flere parter, også ensidig overføring av lyd, tekst, bilder eller annen data omfattes, jf. Prop. 80 L (2019-2020) side 213.

Innhenting skjer ved at kommunikasjonsstrømmen speiles etter loven § 7-3, jf. ovenfor. Hvor denne speilingen finner sted er ikke avgjørende.

Det følger av e-tjenesteloven § 4-1 at E-tjenesten ikke har adgang til å innhente kommunikasjon etter kapittel 6 mellom sendere og mottakere i Norge. Det er imidlertid på det rene at mye av kommunikasjonen mellom personer i Norge av tekniske årsaker krysser grensen, og at dette også skjer uten at de som kommuniserer er klar over dette. Retten viser til forklaringen til sakkyndig vitne, professor Kristian Gjøsteen.

Som beskrevet ovenfor blir kommunikasjonsstrømmen filtrert før den lagres i metadatalageret. Retten legger imidlertid til grunn at det er vanskelig å skille ut og filtrere ut all kommunikasjon mellom sender og mottaker i Norge. Dette var også tilfellet i den svenske ordningen og ble lagt til grunn ved EMDs vurdering i Centrum för Rättvisa (avsnitt 290) uten at dette ble ytterligere kommentert.

I tillegg kan grenseoverskridende kommunikasjon speiles etter § 7-3 (2) for å gjennomføre tekniske analyser for å avklare om det er grunnlag for å fremme begjæring om rettens tillatelse til speiling etter § 7-3 første ledd. Beslutning om å gjennomføre slik speiling treffes av sjefen for E-tjenesten.

Formålet med en slik speiling er å fremskaffe tekniske opplysninger som sier noe overordnet om hvilken etterretningsmessig verdi kommunikasjonsstrømmene vil kunne ha som søkegrunnlag. Disse analysene skal blant annet bidra til å besvare spørsmål om hva slags trafikk som går gjennom kommunikasjonsstrømmene, hvorvidt kommunikasjonen er grenseoverskridende og hvor speiling og tilgjengeliggjøring skal finne sted. Informasjonen skal videre bidra til at E-tjenesten kan fremme begjæring for retten basert på et riktig faktisk grunnlag, jf. Prop. 92 L (2022-2023) side 33.

De dataene som speiles etter § 7-3 (2) skal holdes adskilt fra annen informasjon som speiles etter kapittel 7 (siste punktum) og den speilede kommunikasjonen kan utelukkende brukes til dette formålet, jf. § 7-3 (2) annen punktum. Dette innebærer at slik kommunikasjon ikke kan brukes i etterretningsproduksjon. E-tjenesteloven inneholder videre detaljerte regler i § 7-5 om gjennomføring og lagring av kommunikasjon etter slik speiling, samt hvilken type personell som kan forestå disse oppgavene.

En tilsvarende mulighet for teknisk analyse ble vurdert av EMD i Centrum för Rättvisa avsnitt 291 flg. EMD mente at en slik innhenting i liten grad representerte et inngrep i artikkel 8, jf. Centrum för Rättvisa avsnitt 292:

> (…) The degree of interference with individuals' Article 8 rights engendered by such activities appears to be of a very low intensity having regard to the fact that the data thereby obtained is not in a form destined to generate intelligence.

Domstolen la videre vekt på at slik informasjon ikke kunne benyttes til etterretnings-produksjon. Tilsvarende gjelder for den norske loven. Dette er videre gjenstand for løpende kontroll av EOS-utvalget etter lovens § 7-11 første ledd, jf. nedenfor.

Domstolen kom til at den svenske lovgivningen var tilstrekkelig klar når det gjelder innhenting av kommunikasjon og retten mener at dette også må gjelder innhenting etter e-tjenesteloven. Retten tilføyer i den forbindelse at e-tjenesteloven kapittel 5 også oppstiller grunnvilkår for ulike typer innhenting. Den svenske loven inneholder ikke tilsvarende bestemmelser.

Retten har etter dette kommet til at de omstendigheter som kan føre til at enkeltpersoners kommunikasjon innhentes ved tilrettelagt innhenting tilfredsstiller kravene til en tilstrekkelig klar og forutberegnelig lovgiving.

3.4.5 Vilkår 6 – Varighet, lagring og sletting

3.4.5.1 Varighet

E-tjenesteloven § 8-6 gir nærmere regler om varigheten av rettens tillatelse:

> Rettens tillatelse etter § 8-1 skal ikke gis for lengre tid enn nødvendig. Gjelder tillatelsen målsøking etter § 7- 8, kan den ikke overstige ett år. Gjelder tillatelsen målrettet innhenting etter § 5-2 andre ledd, § 7-8 eller § 7-9, kan den ikke overstige seks måneder. Gjelder tillatelsen speiling etter § 7-3 første ledd, kan den ikke overstige to år.
>
> Etterretningstjenesten skal avslutte pågående tiltak dersom lovens vilkår ikke lenger er til stede.

Hovedregelen etter første ledd første punktum er at tillatelsen ikke skal gis lengere varighet enn nødvendig. Etter annet punktum gis det lengstefrister for tillatelsen for henholdsvis målsøkning etter 7-8 (ett år), målrettet innhenting etter §§ 5-2, 7-8 og 7-9 (seks måneder). I tredje punktum fastsettes lengstefristen for tilrettelagt innhenting etter § 7-3 til to år. Innenfor rammene av disse fristene skal retten avgjøre tillatelsens varighet etter en konkret vurdering i den enkelte sak.

Begrunnelsen for en lengstefrist på to år for tilrettelagt innhenting fremgår av Prop. 92 L (2002-2023) punkt 6.4.5:

> Departementet har i vurderingen lagt særlig vekt på at utenlandsetterretning er et langsiktig og møysommelig arbeid og at trusselaktørene er meget sikkerhetsbevisste. Etterretningsfaglige og økonomiske hensyn tilsier at speiling og tilgjengeliggjøring av utenlandskommunikasjon ikke må revurderes for ofte. Det har også sammenheng med behovet for lagring av metadata for retrospektive søk. Retrospektive søk er viktige for å avdekke blant annet koblinger mellom trusselaktører, og mellom trusselaktørenes ofte mange digitale identiteter, samt avdekking av cyberoperasjoner fra fremmede stater. For eksempel vil man etter at en hendelse har funnet sted, som en avdekket cyberoperasjon eller forberedelser til terror, kunne bruke informasjon man avdekker i den forbindelse opp mot annen informasjon som man besitter. For å kunne søke å avdekke rekkevidden av cyberoperasjonen eller hvem som deltar i et internasjonalt terrornettverk, må man ha et søkegrunnlag å ta utgangspunkt i, og dette krever lagring av metadata i en lengre tidsperiode. For at speilingen av data skal kunne oppfylle sitt formål som relevant søkegrunnlag må det i vurderingen av tidsavgrensning derfor tas hensyn til at lagringstiden er tilstrekkelig til å gi reell etterretningsmessig verdi.

Av spesialmerknadene til § 8-6 fremgår det at retten skal forholde seg til lengstefristene slik det fremgår av Prop. 80 L (2019-2020) side 222 hvor det uttales følgende om varigheten:

> Varighet til lengstefristen kan være aktuelt når de faktiske forholdene som har betydning for innhentingen, antas å være stabile i denne perioden. Det kan for eksempel være tilfelle hvis det er tale om søk eller innhenting som gjelder statlige aktører. Hvis det er grunn til å anta at faktiske forhold av betydning vil kunne endre seg i løpet av et kortere tidsrom, bør det gis en kortere tillatelse.

I bestemmelsen andre ledd pålegges E-tjenesten å avslutte pågående søk og innhenting dersom vilkårene for dette ikke lenger er til stede, eksempelvis hvis nye faktiske omstendigheter innebærer at fortsatt innhenting må anses uforholdsmessig.

Stiftelsen har anført at den unødvendige og uforholdsmessige lagringstiden av kommunikasjonsdata er i strid med EMKs krav til nødvendighet og forholdsmessighet, jf. Centrum för Rättvisa avsnitt 275.

Staten har gjort gjeldende at det ifølge EMDs praksis er opp til statene å avgjøre varigheten av tiltaket så lenge det er klare rammer for dette, og at konkret varighet derfor er irrelevant.

Retten har kommet til at e-tjenesteloven § 8-6 oppfyller EMDs krav til at varigheten er klart definert.

I Centrum för Rättvisa avsnitt 331 slår EMD fast at det er opp til nasjonale myndigheter å avgjøre varigheten av bulkinnsamlingsoperasjoner, men at lovgivningen må inneholde klare krav til varigheten av tillatelsen til å innhente data, vilkår for fornyelse samt når de innhentede dataene skal slettes:

> The duration of bulk interception operations is, of course, a matter for the domestic authorities to decide. There must, however, be adequate safeguards, such as a clear indication in domestic law of the period after which an interception warrant will expire, the conditions under which a warrant can be renewed and the circumstances in which it must be cancelled (see *Roman Zakharov*, cited above, § 250).

Etter den svenske loven § 5 a) ble en tillatelse gitt for seks måneder av gangen, og kunne fornyes for en periode av 6 måneder med full prøving av vilkårene hver gang. EMD kom til at svensk lovgiving dermed ga en klar regulering av varigheten og vilkårene for fornyelse, jf. avsnitt 332.

Den svenske loven inneholdt imidlertid ingen forpliktelse til å stanse innhentingen når vilkårene ikke lenger var til stede (avsnitt 333). EMD mente at en slik lovbestemt plikt ville medført en klarere regulering av varigheten i den svenske loven (avsnitt 335). Denne svakheten ble imidlertid tillagt begrenset vekt dels fordi lovgivingen inneholdt en mulighet for å be om tilbakekall av tillatelsen og dels eksistensen av overvåkningssystemer med tilgang til all informasjon. EMD kom dermed til at den svenske lovgivningen tilfredsstilte de oppstilte krav med hensyn til varigheten av tiltaket (avsnitt 336).

E-tjenesteloven § 8-2 annet ledd inneholder en plikt om å avslutte innhentingen når vilkårene ikke lenger er til stede, jf. ovenfor.

Etter rettens syn inneholder de norske bestemmelsene en klar regulering av varigheten av inngrepet samt en plikt til å stanse innhentingen før fristen er utløpt dersom vilkårene ikke lenger er oppfylt. Retten mener derfor at den norske reguleringen av varigheten er i samsvar med EMDs krav.

1.3.1.2 Lagring og sletting

Stiftelsen har anført at reglene for lagring og sletting i e-tjenesteloven § 9-8 ikke oppfyller EMDs krav. Det er imidlertid noe uklart for retten hva som er grunnlaget for denne anførselen.

Under den skriftlige saksforberedelsen er det for det første vist til at sletteplikten ikke gjelder for innholdsdata og at det ikke er oppstilt et krav om sletting av data som ikke inneholder personopplysninger eller kildeidentifiserende opplysninger, jf. stevningen side 42 og prosesskriv 6. juni 2024. Staten har under saksforberedelsen vist til at E-tjenesten ikke har hjemmel til å innhente og lagre innholdsdata i bulk, og at dette er årsaken til at sletting av innholdsdata ikke er nevnt i § 9-8 annet ledd. Grunnlaget for anførselen ble ikke nærmere konkretisert under hovedforhandlingen.

Som redegjort for ovenfor, skjer speilingen etter § 7-3 (1) mens kommunikasjonen er i transitt og kommunikasjonsstrømmen blir på dette tidspunktet ikke lagret. Innholdsdata filtreres ut av kommunikasjonsstrømmen før metadata lagres i metadatalageret. Retten viser til avgradert kjennelse fra Borgarting lagmannsrett, som er fremlagt i saken, hvor det fremgår:

> Ut fra det som er opplyst i begjæringen og under rettsmøtet, legger lagmannsretten til grunn at e-tjenesten har gode tekniske systemer for å hindre lagring av metadata fra kommunikasjon i Norge. Den konkrete prosessen med filtrering mv. er beskrevet slik i tingrettens kjennelse (side 8):
>
> > Når det gjelder selve speilingen forklarte kontorsjef (…) at det Etterretningstjenesten speiler er rådata, hvor man først filtrerer ut kommunikasjon fra Norge til Norge, og så tar ut innholdsdata, før resterende metadata sendes videre til prosessering. Dette er den metadata som lagres, og
> > som etter etterretningstjenesteloven § 7-7 tredje ledd skal slettes etter 18 måneder. Dette innebærer at speiling ikke innebærer lagring, men på speilingstidspunktet ennå utgjør data i transport. Først etter filtrering i to omganger lagres resterende metadata («data om data»). Etterretningstjenesten
> > bekreftet at materiale ut over resterende metadata slettes før lagringen.
>
> E-tjenesten har for lagmannsretten bekreftet at denne beskrivelsen er riktig, med den presisering at også uttak av innholdsdata forutsetter prosessering.

Retten legger etter dette til grunn at det er korrekt at innholdsdata ikke lagres etter § 7-3 og at det dermed ikke er behov for en regel om sletting av innholdsdata.

Reglene om sletting er inntatt i lovens § 9-8:

> **9-8.** ***Sletting***
> Personopplysninger, og kildeidentifiserende opplysninger som det er gitt tillatelse til å behandle etter § 9-6 tredje ledd og som ikke er personopplysninger, skal slettes når de ikke lenger er nødvendige for formålet med behandlingen.
>
> Rådata i bulk skal slettes senest 15 år fra lagringstidspunktet, med mindre vesentlige hensyn tilsier at sletting utsettes. Beslutning om utsatt sletting treffes av sjefen for Etterretningstjenesten for ikke mer enn fem år avgangen. Metadata som er innhentet og lagret i bulk i samsvar med § 7-7, skal likevel slettes senest etter 18 måneder, jf. § 7-7 tredje ledd.

Hovedregelen etter denne bestemmelsen er at opplysninger som ikke lenger er nødvendige for formålet med behandlingen skal slettes. Dette gjelder både personopplysninger og kildeidentifiserende opplysninger som ikke er personopplysninger. Kildeidentifiserende opplysninger vil normalt være personopplysninger og skal dermed slettes etter første punktum.

Stiftelsen har påpekt at EMD i Centrum för Rättvisa avsnitt 342 også oppstiller et krav om vern av juridiske personer:

> 342. In the Court's view, while there is clear justification for special requirements regarding the destruction of material containing personal data, there must also be a general legal rule governing the destruction of other material obtained through bulk interception of communications, where keeping it may affect, for example, the right of respect for correspondence under Article 8, including concerning legal persons as the applicant. As a very minimum, as also stressed by the Chamber, there should be a legal requirement to delete intercepted data that has lost pertinence for signals intelligence purposes. (…)

Svensk lovgiving inneholdt ikke en slik bestemmelse og dette var en av svakhetene ved det svenske systemet som førte til at det ble konstatert brudd på EMK artikkel 8.

Det følger av forarbeidene til e-tjenesteloven at uttrykket «kildeidentifiserende opplysninger som ikke er personopplysninger» omfatter blant annet opplysninger som avslører en organisasjon eller annen juridisk person som kilde, jf. Prop. 92 L (2022-2023) punkt 4.6 og spesialmerknadene til bestemmelsen. Innskuddet om kildeidentifiserende opplysninger som ikke er personopplysninger kom inn i loven ved lovendringen 6. juni 2023. Stiftelsens anførsel om at dette ikke omfattes av lovbestemmelsen kan dermed ikke føre frem.

Bestemmelsen i § 9-8 oppstiller et krav om nødvendighet. Kravet innebærer at det som utgangspunkt må foretas en individuell og konkret vurdering i hvert enkelt tilfelle av om det er nødvendig å fortsette behandlingen av opplysningene. Tatt i betraktning at E-tjenesten ofte samler inn store mengder opplysninger, som skal sammenstilles og analyseres, vil det ikke la seg gjøre å vurdere nødvendigheten av her enkelt opplysning. I praksis vil dette i stor grad gjennomføres som samlede vurderinger av hvorvidt større datasett skal slettes, jf. Prop. 80 L (2019-2020) punkt 12.10.4.

Etter bestemmelsens andre ledd skal rådata i bulk, jf. § 1-3 bokstav h) og i), slettes senest 15 år etter opplysningen ble lagret. Utsatt sletting kan bestemmes for fem år av gangen. Beslutning om en slik forlengelse treffes av sjefen for E-tjenesten. Det fremgår av forarbeidene at begrepet «senest» skal forstås slik at dataene skal slettes på et tidligere tidspunkt dersom E-tjenesten vurderer at datasettet ikke lenger har etterretningsmessig verdi, jf. spesialmerknadene til bestemmelsen i Prop. 80 L (2019-2020) side 227.

I andre ledd siste punktum presiseres det at metadata som er innhentet og lagret i bulk i samsvar med § 7-7 likevel skal slettes etter 18 måneder. Det samme fremgår av e-tjenesteloven § 7-7 tredje ledd.

Bestemmelsen fastsetter således først en plikt til å slette dataene basert på en nødvendighetsvurdering og deretter en absolutt frist for sletting av rådata i bulk. Etter rettens syn inneholder e-tjenesteloven tilstrekkelig klare regler om lagring og sletting og at e-tjenesteloven § 9-8 oppfyller de krav til klarhet som er oppstilt av EMD.

Retten nevner for ordens skyld også e-tjenesteloven § 9-2 hvor det fremgår at E-tjenesten bare kan behandle personopplysninger når dette er nødvendig for etterretningsformål. Ved treff på søk etter lovens § 7-8 og § 7-9 som ligger utenfor E-tjenestens oppgaver, eller ved treff på innenlandsk kommunikasjon, vil E-tjenesten mangle behandlingsgrunnlag og opplysningene må da slettes.

3.4.6 Vilkår 7 og 8 – Løpende og etterfølgende kontroll

3.4.6.1 Nærmere om EOS-utvalgets kontroll

Etter e-tjenesteloven § 2-6 første ledd er E-tjenesten underlagt kontroll etter lov om kontroll med etterretnings-, overvåknings- og sikkerhetstjeneste av 3. februar 1995 nr. 7 (EOS-kontrolloven).

Formålet med EOS-utvalgets kontroll er blant annet å kartlegge om og forebygge at noens rettigheter krenkes, påse at virksomheten ikke utilbørlig skader samfunnets interesse og påse at virksomheten holdes innenfor rammen av lov, administrative eller militære direktiver og ulovfestet rett, jf. lovens § 2.

EOS-utvalget kan gjennomføre kontroll av eget tiltak eller etter klage fra enkeltpersoner eller virksomheter, jf. § 5. Kontrollen skal omfatte tjenestens tekniske virksomhet, herunder overvåkning og innhenting av informasjon og behandling av personopplysninger, jf. § 6 annet ledd. Videre skal utvalget påse at samarbeid og informasjonsutvekslingen med innenlandske og utenlandske samarbeidsparter holdes innenfor rammene av tjenestlige behov og gjeldende regelverk. Av EOS-kontrolloven § 6 fjerde ledd nr. 2 fremgår det at EOS-utvalget skal «sikre at virksomheten holdes innenfor rammen av tjenestens fastlagte oppgaver».

Etter § 2 tredje ledd er formålet rent kontrollerende og utvalget skal følge prinsippet om etterfølgende kontroll. Utvalget kan ikke instruere de kontrollerte organer, men kan likevel kreve innsyn i og uttale seg om løpende saker. Kontrollen gjennomføres i praksis ved inspeksjoner, behandling av klagesaker og behandling av saker som tas opp av eget tiltak, jf. Prop. 80 L (2019-2020) punkt 6.2.2.

Etter EOS-kontrolloven § 14 har EOS-utvalget rett til å uttale sin mening om forholdet som omfattes av kontrollen, og kan påpeke feil eller forsømmelser i tjenestene. Kommer

utvalget til at en avgjørelse må anses som ugyldig eller klart urimelig, eller klart strider mot god forvaltningspraksis, kan det gi uttrykk for dette.

I forbindelse med vedtakelsen av reglene om tilrettelagt innhenting ble det innført en særregulering av EOS-utvalgets kontroll i e-tjenesteloven § 7-11 og 7-12:

> **§ 7-11.** ***Løpende kontroll***
> EOS-utvalget skal føre løpende kontroll med Etterretningstjenestens etterlevelse av bestemmelsene i dette kapittelet, blant annet med at søk bare gjennomføres i tråd med rettens kjennelser og at korttidslageret og testdata utelukkende brukes til teknisk understøttelse.
>
> EOS-utvalget skal ha uhindret tilgang til all informasjon, interne retningslinjer og prosedyrer, lokaler, utstyr, programvare, filteroppdateringer, aktivitetslogger og annet som benyttes ved virksomhet etter dette kapittelet.
>
> Etterretningstjenesten skal tilrettelegge for kontrollen gjennom tekniske løsninger.

EOS-utvalget har etter bestemmelsen en plikt til å gjennomføre løpende kontroll med E-tjenestens etterlevelse av bestemmelsene om tilrettelagt innhenting. Denne bestemmelsen innebærer en utvidelse av EOS-utvalget kontrolloppgaver sammenlignet med det som følger av EOS-kontrolloven. Den løpende kontrollen som fremgår av § 7-11, kommer i tillegg til den alminnelige kontrollen etter EOS-kontrolloven.

EOS-utvalget skal også løpende kontrollere at bestemmelsene i loven etterleves. Kontrollen omfatter blant annet at søk gjennomføres i tråd med rettens kjennelse og at korttidslageret og testdata utelukkende brukes til teknisk understøttelse. For å kunne gjennomføre slik kontroll skal EOS-utvalget ha uhindret tilgang til all informasjon og E-tjenesten skal tilrettelegge for kontrollen gjennom tekniske løsninger, jf. § 7-11, annet og tredje ledd.

Etter § 7-12 er EOS-utvalget også gitt kompetanse til å fremme begjæring om stans og sletting dersom virksomheten gjennomføres i strid med disse bestemmelsene. Bestemmelsen gir EOS-utvalget en særlig kompetanse for kontroll av TI i forhold til EOS-kontrolloven hvor utvalget kun kan påpeke uoverensstemmelse. Bestemmelsen lyder:

> **§ 7-12.** ***Begjæring om stansing og sletting***
> Hvis EOS-utvalget mener at virksomhet etter dette kapittelet gjennomføres i strid med loven, kan utvalget fremme begjæring for Oslo tingrett med krav om at ulovlig virksomhet opphører, og at ulovlig innhentet informasjon slettes. Før begjæringen fremmes, skal Etterretningstjenesten gjøres kjent med utvalgets syn og gis mulighet til å rette seg etter det.
>
> Reglene i kapittel 8 gjelder tilsvarende så langt de passer.

Dersom EOS-utvalget mener at virksomheten som gjennomføres er i strid med loven, følger det av § 7-12 at EOS-utvalget kan fremme begjæring for Oslo tingrett med krav om at den ulovlige virksomheten opphører og at ulovlig innhentet informasjon slettes. Før slik begjæring fremmes skal E-tjenesten gjøres kjent med utvalgets syn og gis mulighet for å rette forholdet. I forarbeidene er det lagt til grunn at E-tjenesten normalt vil rette seg etter EOS-utvalgets syn og at bestemmelsen er ment som en sikkerhetsventil. Utvalget har kun kompetanse til å fremme en begjæring for retten og har ikke møterett eller mulighet for å anke. I slike tilfeller vil det normal oppnevnes en særskilt advokat som skal målbære allmenne interesser i saken. Den særskilte advokaten har også rett til å anke.

I tillegg til den løpende kontrollen skal EOS-utvalget føre etterfølgende kontroll av at tilrettelagt innhenting er i samsvar med loven. Alle søk som foretas skal kunne kontrolleres i ettertid og etter e-tjenesteloven § 7-10 annet ledd skal det utarbeides aktivitetslogger. EOS-utvalget skal også varsles om utlevering av overskuddsinformasjon etter § 7-13 annet ledd.

Etter e-tjenestelovens § 11-7 kan enhver klage til EOS-utvalget etter EOS-kontrolloven. Ettersom verken offentligheten eller enkeltpersoner har innsyn i E-tjenestens virksomhet, er denne klageadgangen den eneste muligheten for personer som frykter at de er utsatt for krenkelser, til å få avkreftet eller bekreftet dette. EOS-utvalget behandler klaget etter EOS-kontrolloven § 5.

Klager får vite konklusjonen etter gjennomgangen til EOS-utvalget, jf. EOS-kontrolloven § 15 som lyder:

> Uttalelser til klagere bør være så fullstendige som mulig uten at det gis graderte opplysninger. Opplysning om at noen har vært gjenstand for overvåkings-virksomhet eller ikke, anses som gradert hvis annet ikke blir bestemt. Ved klager mot tjenestene om overvåkingsmessig virksomhet skal det bare uttales om klagen har gitt grunn til kritikk eller ikke. Mener utvalget at en klager bør gis en mer utfyllende begrunnelse, gir det forslag om det overfor den tjeneste det gjelder eller vedkommende departement.
>
> Hvis en klage gir grunn til kritikk eller meningsytringer for øvrig, skal begrunnet uttalelse om dette rettes til sjefen for den tjeneste det gjelder eller vedkommende departement. Også ellers skal uttalelser i klagesaker alltid meddeles sjefen for den tjeneste klagen er rettet mot.
>
> Uttalelser til forvaltningen graderes etter sitt innhold.

Retten nevner for fullstendighetens skyld også at Stortinget i vedtak om kontroll 11. juni 2020 i forbindelse med vedtakelsen av loven i 2020, har bedt regjeringen sørge for en uavhengig evaluering av e-tjenesteloven senest fire år etter at hele loven har trådt i kraft.

3.4.6.2 Løpende kontroll

Som nevnt ovenfor skal EOS-utvalget føre løpende kontroll med E-tjenestens etterlevelse av reglene om tilrettelagt innhenting «blant annet med at søk bare gjennomføres i tråd med rettens kjennelser og at korttidslageret og testdata utelukkende brukes til teknisk understøttelse», jf. e-tjenesteloven § 7-11 (1).

Stiftelsen mener at denne løpende kontrollen er mangelfull. Stiftelsen har tatt utgangspunkt i Centrum för Rättvisa avsnitt 270 hvor det oppstilles et krav til at kontrollen skal utføres av en uavhengig instans som er «sufficiently robust to keep the "interference" to what is "necessary in a democratic society» og at organet må være i stand til å vurdere om det aktuelle tiltaket er nødvendig og forholdsmessig. Stiftelsen mener at EOS-utvalget ikke har tilstrekkelig kapasitet til å kunne ivareta denne kontrollen.

EOS-utvalget består av sju medlemmer og har et fast sekretariat på 29 ansatte. Ifølge Stiftelsen er det en betydelig skjevfordeling av ressursene mellom overvåkningstjenestene og EOS-utvalget. Den manglende kapasiteten medfører at det ikke gjennomføres et kontinuerlig tilsyn, men at kontrollen er basert på stikkprøver, jf. egen beskrivelse i årsmeldingen 2020. Stiftelsen viser også til at EOS-utvalget i sin høringsuttalelse 12. februar 2019 selv har påpekt at en slik kontroll som lovforslaget la opp til ikke var mulig.

Under saksforberedelsen er det også anført at kontrollmekanismene med tilgang og søk er mangelfulle. Her ble det vist til at det fremgikk av EOS-utvalgets årsrapport for 2022 at E-tjenesten ikke hadde lagt til rette for utvalgets kontroll gjennom tekniske løsninger. Av EOS-utvalgets årsrapport for 2023 er det opplyst at E-tjenesten har fulgt opp dette og at EOS-utvalget er i dialog med E-tjenesten om videre tilrettelegging for kontroll. Slik retten oppfatter det er det i dag i hovedsak ressurssituasjonen hos EOS-utvalget som er grunnlaget for anførselen, nemlig at EOS-utvalget mangler ressurser/kapasitet til å føre tilstrekkelig kontroll.

Det er videre anført at det er en svakhet at EOS-utvalget kun kan gi uttrykk for sin mening, og at utvalget ikke har kompetanse til å fatte et formelt bindende vedtak, jf. EOS-kontrolloven § 14. EOS-utvalget kan ikke begjære stans i innhentingen eller sletting av innhentede opplysninger etter § 7-12, og kompetansen er begrenset til å fremme en begjæring for Oslo tingrett. EOS-utvalget har heller ikke møterett ved rettens behandling av saken eller mulighet for å anke rettens kjennelse.

Staten mener at reglene i e-tjenesteloven §§ 7-11 og 7-12 sikrer en tilstrekkelig løpende kontroll med TI og at kontrollen også må sees i sammenheng med krav om forhåndsgodkjenning av domstolen før innhentingen kan iverksettes. Det er videre vist til at EOS-utvalgets kontroll i Norge er minst like effektiv som SIUNs kontroll i Sverige, og at EMD kom til at SUINs kontroll tilfredsstilte kravet til løpende kontroll (Centrum för Rättvisa avsnitt 345-353).

Retten har kommet til at reguleringen av den løpende kontrollen med tilrettelagt innhenting gir en tilstrekkelig garanti mot misbruk.

Det er ingen tvil om at EOS-utvalget må anses som et uavhengig organ og loven sikrer at utvalget har uhindret tilgang til all informasjon, prosedyrer og utstyr som benyttes av E-tjenesten i forbindelse med tilrettelagt innhenting, jf. e-tjenesteloven § 7-11. E-tjenesten plikter også å tilrettelegge for kontrollen gjennom tekniske løsninger. Retten mener at loven på denne måten setter EOS-utvalget i stand til løpende å vurdere sakens materielle side og om et tiltak er nødvendig og forholdsmessig. Når det gjelder stiftelsens anførsel om manglende kapasitet, mener retten at det klart ligger innenfor statens skjønnsmargin å avgjøre hvilke ressurser som skal tilføres overvåkningsorganet. Vurderingstemaet i denne saken er hvilke rettslige rammer lovgivingen inneholder for at EOS-utvalget skal kunne utføre løpende kontroll med E-tjenesten. Slik saken er anlagt, er det derfor ikke nødvendig for retten å ta stilling til spørsmålet om ressurssituasjonen.

Retten viser videre til at EMD i Centrum för Rättvisa (avsnitt 345 til 353) vurderte at den svenske SIUN hadde kompetanse til å vurdere alle aspekter ved FRAs virksomhet, fra innhenting, analyse, bruk og sletting av materialet, og at SIUN får tilgang til all relevant informasjon fra FRA (avsnitt 347). EMD mente derfor at SIUN hadde kompetanse og de nødvendige verktøy for å vurdere om et tiltak var i samsvar med både de formelle kravene for innhentingen og forholdsmessigheten ved slik innhenting (avsnitt 348). SIUN hadde i enkelte tilfeller også myndighet til å treffe bindende avgjørelser, blant annet at ulovlig innhentet materiale må slettes. EMD kom til at den svenske ordningen var tilfredsstillende selv om ikke alle SIUNs anbefalinger («recommendations») kunne håndheves. Det ble her vist til at FRA hadde rutiner som sørget for at SIUNs uttalelser og anbefalinger ble behandlet seriøst og at disse hadde gitt grunnlag for endringer (avsnitt 350).

EOS-utvalget har selv ingen instruksjons- og vedtaksmyndighet overfor E-tjenesten. Retten legger etter bevisførselen til grunn at det er utviklet gode og effektive systemer i E-tjenesten for å følge opp rapporterte avvik. I tillegg har EOS-utvalget myndighet til å fremme begjæring om stans og sletting til Oslo tingrett, jf. e-tjenesteloven § 7-12. Selv om EOS-utvalget selv ikke har møterett i saken, mener retten at EMDs krav til en løpende uavhengig kontroll klart er tilfredsstilt.

Retten nevner at det i Centrum för Rättvisa (avsnitt 350) også ble lagt vekt på at SIUN avga årlige offentlige rapporter som var gjenstand for revisjon av den svenske riksrevisjonen. Tilsvarende gjelder for EOS-utvalget som årlig utgir en offentlig rapport, og E-tjenesten er også underlagt kontroll fra Riksrevisjonen.

Retten kan på denne bakgrunn ikke se at det er grunnlag for å fastslå at reguleringen av EOS-utvalgets løpende kontroll er i strid med de krav som oppstilles av EMD i Centrum för Rättvisa.

3.4.6.3 Etterfølgende kontroll

Stiftelsen har videre anført at den etterfølgende kontrollen er mangelfull. EMD oppstiller et krav om et effektivt rettsmiddel for den som mistenker at egen kommunikasjon er overvåket. Dette skal avgjøres av et uavhengig organ som med bindende virkning kan fastslå at overvåkningen er ulovlig og beslutte at ulovlig innhentet informasjon skal slettes. Det oppstilles også krav om at utfallet av den etterfølgende kontrollen må være en begrunnet og rettslig bindende avgjørelse, jf. Centrum för Rättvisa avsnitt 362. Etter EOS-kontrolloven § 15 første ledd har en klager ikke krav på en begrunnelse utover om klagen har ført til kritikk eller ikke. Adgangen til å be om ytterligere begrunnelse er betinget av E-tjenestens eller departementets samtykke. EMDs krav om en begrunnet avgjørelse er dermed ikke oppfylt.

Endelig har Stiftelsen anført at EMDs konklusjon om dobbeltrolle er overførbar til EOS-utvalgets rolle som både har fått ansvar for løpende og etterfølgende kontroll. En slik ordning kan lede til at tilsynsmyndigheten må vurdere sin egen tilsynsmyndighet, noe som kan lede til interessekonflikter. Dette innebærer at det ikke finnes reelle kontroll-mekanismer.

Staten mener at den etterfølgende kontrollen er tilstrekkelig. Det er vist til at EOS-utvalget etter EOS-kontrolloven § 15 første ledd kan informere en klager om at en undersøkelse har medført kritikk eller ikke. Dette i motsetning til Sverige, hvor SIUN kun kan informere en klager om at undersøkelsen er gjennomført. EOS-utvalget har også større adgang til å begrunne avgjørelsene sine. EOS-utvalget har videre muligheten til å fremme forslag til E-tjenesten eller departementet om at klager bør gis en mer utfyllende begrunnelse. Staten viser også til at EOS-utvalget, til forskjell fra SIUN, fører en løpende kontroll med TI i sanntid etter e-tjenesteloven § 7-11.

Til anførselen om dobbeltrolle viser staten til at EOS-utvalget ikke har noen myndighet til å gi tilgang til kommunikasjonsstrømmer, slik som var tilfellet for SIUN, og at argumentet om dobbeltrolle derfor ikke gjør seg gjeldende for Norges del.

Retten har ved vurderingen tatt utgangspunkt i at EMD oppstiller et krav om at enhver som mistenker at egen kommunikasjon har blitt innhentet av etterretningstjenesten skal ha et effektivt rettsmiddel tilgjengelig for å få prøvd om det aktuelle tiltaket er lovlig eller ikke.

EMD anerkjenner at det ikke kan oppstilles et krav om notifikasjon for bulkinnhentingssystemer (Centrum för Rättvisa avsnitt 271 og avsnitt 355). I samsvar med

dette plikter heller ikke E-tjenesten å gi underretning til den som har vært gjenstand for informasjonsinnhenting, jf. e-tjenesteloven § 11-7 annet punktum. EMD uttaler videre i avsnitt 355 at:

> (…) However, the absence of a functioning notification mechanism should be counterbalanced by the effectiveness of the remedies that must be available to individuals who suspect that their communications may have been intercepted and analysed.

For å sikre en effektiv etterfølgende kontroll er det ifølge EMD avgjørende at kontrollen gjennomføres av et uavhengig organ som sikrer en rettferdig prosess, og som så langt som mulig er kontradiktorisk. Kontrollen skal munne ut i en begrunnet og bindende avgjørelse om stans i innhentingen eller sletting av ulovlig innhentet materiale, jf. Centrum för Rättvisa avsnitt 273.

Etter den svenske loven hadde kontrollorganet SIUN en plikt til å undersøke om en klagers kommunikasjon hadde blitt innhentet, men klager fikk selv ingen informasjon om utfallet av klagen utover forholdet var undersøkt. Sammenholdt med at SIUN i tillegg til å være kontrollorgan, også kunne autorisere FRAs tilgang til kommunikasjonsstrømmer, mente EMD at det var en risiko for at SIUN kunne komme i en interessekonflikt ved behandlingen av klager som berører egne avgjørelser (avsnitt 359):

> 359. However, while it is true that the Inspectorate is an independent body, the Court observes that, having regard to that body's duty to supervise and monitor the FRA's activities, which includes taking or authorising operational decisions such as those concerning access to the signal carriers, use of selectors, analysis, use and destruction of intercept material (see paragraphs 50-53 above), the Inspectorate's additional role of *ex post facto* review on request from individuals may lead to situations where it will have to assess its own activities in supervising bulk interception by the FRA. In the conditions of secrecy, which legitimately characterise the relevant procedures, and failing a legal obligation for the Inspectorate to provide reasons to the individual concerned, there may be doubts as to whether the Inspectorate's examination of individual complaints in such situations affords adequate guarantees of objectivity and thoroughness. It cannot be excluded that the dual role of the Inspectorate may generate conflicts of interest and, therefore, the temptation to overlook an omission or misconduct in order to avoid criticism or other consequences.

Slik retten leser EMDs avgjørelse var det kombinasjonen av disse forholdene som var grunnen til at EMD mente at det svenske systemet hadde en svakhet knyttet til etterfølgende kontroll.

Stiftelsen har også anført at EOS-utvalget har tilsvarende dobbeltrolle ved at utvalget både foretar løpende og etterfølgende kontroll. Etter rettens syn kan denne anførselen åpenbart ikke føre frem. Etter rettens syn er det snarere en fordel for å føre en effektiv kontroll at det

er samme instans som kontrollerer E-tjenesten gjennom hele prosessen. Retten legger som nevnt til grunn at EOS-utvalget er en helt uavhengig instans, og at den norske ordningen her skiller seg fra ordningen som ble vurdert i Centrum för Rättvisa.

Etter rettens syn kan det imidlertid reises spørsmål om det også er en mangel ved den norske ordningen at klagebehandlingen i EOS-utvalget ikke munner ut i en begrunnet bindende avgjørelse.

Som redegjort for ovenfor, skal EOS-utvalget informere en klager om en undersøkelse har medført kritikk eller ikke, jf. EOS-kontrolloven § 15 (1). Til sammenligning kunne det svenske kontrollorganet SIUN kun informere en klager om at undersøkelsen er gjennomført uten opplysninger om klagen hadde ført til kritikk eller ikke.

Spørsmålet om loven oppfyller kravet til effektiv prøvingsrett ble drøftet i Prop. 80 L (2019-2020) punkt 4.4.4.2. Her ble det vist til at selv om det ved klagebehandlingen i EOS-utvalget ikke er en kontradiktorisk prosess eller munner ut i en bindende avgjørelse, er det mulig å bringe spørsmålet om det foreligger et brudd på menneskerettighetene inn for domstolen. Departementet la til grunn at bevisforbudsregelen i tvisteloven § 22-1 (opplysninger av betydning for rikets sikkerhet mm) ikke var absolutt, og at Kongen i statsråd kan gi tillatelse til å fremlegge sikkerhetsgraderte opplysninger. Det ble videre vist til at dette ble gjort i 2020 i sak 19-026476TVI-OTIR/07 (Ølen Betong). Departementet la til grunn at bevisforbudsregelen i tvisteloven § 22-1 ikke utgjør et hinder for reell prøving i domstolene av denne typen saker og at dette var tilstrekkelig for at det foreligger et effektivt rettsmiddel.

Retten er enig i at det er mulighet å bringe saken inn for de alminnelige domstoler og dermed sikre en kontradiktorisk prosess som munner ut i en begrunnet og bindende avgjørelse. Det må imidlertid legges til grunn at det skal en del til før bevisforbudet etter tvisteloven § 22-1 oppheves. Retten antar derfor at dette kun vil skje i et fåtall av de klagesakene som EOS-utvalget skal behandle.

Kravet om at en klager skal gis en begrunnet bindende avgjørelse oppveies i noen grad av at EOS-utvalget har en større adgang til å initiere at det blir gitt en begrunnelse enn det svenske SIUN. Hvis EOS-utvalget mener at en klager bør gis en mer utfyllende begrunnelse, har utvalget muligheten til å fremme forslag om dette til E-tjenesten eller departementet, jf. EOS-kontrolloven § 15 annet ledd. Etter rettens syn bør E-tjenesten så langt som mulig tilstrebe å gi en slik begrunnelse for å sikre tilstrekkelig etterfølgende kontroll med innhentingen. Retten antar imidlertid at dette i mange tilfeller ikke vil være mulig som følge av behovet for å skjerme informasjon om E-tjenestens virksomhet, jf. også e-tjenesteloven § 11-4.

I forlengelsen av dette skal EOS-utvalget, dersom utvalget mener at en klage gir grunn til kritikk, gi en begrunnet uttalelse om dette til sjefen for E-tjenesten eller departementet, jf. § 15 (3). Retten legger videre til grunn at dersom en aktivitet som EOS-utvalget mener er ulovlig ikke avsluttes, enten på tjenestens eget initiativ eller etter instruks fra departementet, kan Stortinget holde regjeringen eller statsråden ansvarlig. Denne muligheten har en disiplinerende effekt på forvaltningen og det antas at EOS-utvalgets kontroll i praksis vil bli fulgt opp, jf. Prop. 80 L (2019-2020) punkt 4.4.4.3. En tilsvarende mulighet ble også vurdert av EMD for den svenske loven. EMD mente at dette var relevante, men ikke tilstrekkelige klagemekanismer, og la særlig vekt på at disse ikke var uavhengige organer, jf. Centrum för Rättvisa avsnitt 362.

Selv om det i loven er åpnet for at en klager kan få en begrunnelse for inngrepet, og at det er en viss adgang til å få prøvd spørsmålet om det foreligger en krenkelse for domstolene, mener retten at dette isolert sett ikke er tilstrekkelig til å være et effektivt rettsmiddel i relasjon til EMDs krav. Dette utgjør etter rettens syn en svakhet ved den norske kontrollordningen. Det er imidlertid summen av de nasjonale rettsmidlene som vil være avgjørende for om det foreligger tilstrekkelige rettsikkerhetsgarantier, jf. helhetsvurderingen nedenfor.

3.4.7 Helhetsvurderingen

Retten har etter en samlet vurdering kommet til at den norske reguleringen av TI er i samsvar med EMK artikkel 8.

Reguleringen av TI er basert på tilgjengelige, detaljerte regler med et klart definert formål og det fremgår klart av loven i hvilke tilfeller innhenting av kommunikasjonen kan skje. Det er i saken ikke anført at prosedyrene for tillatelse til speiling, seleksjon, analyse og bruk av innhentede data er i strid med de krav som er oppstilt, og retten legger til grunn at disse også er i samsvar med kravene. Retten har videre kommet til at loven fastsetter klare regler om lagring og sletting av innhentet kommunikasjon.

EMD oppstiller også krav til rettssikkerhetsgarantier i alle ledd («end-to-end safeguards») for å hindre misbruk. Disse rettssikkerhetsgarantiene består dels av at det må gis tillatelse fra domstolen for å gjennomføre ulike tiltak og dels av løpende og etterfølgende kontroll av de tiltak som iverksettes. Det er summen av disse rettssikkerhetsgarantiene som er avgjørende for om det foreligger brudd på EMK artikkel 8.

Retten har ovenfor kommet til at det er en svakhet ved den etterfølgende kontrollen at en klager ikke har et tilstrekkelig effektivt rettsmiddel for å få fastslått om det har skjedd en krenkelse av menneskerettighetene. Retten mener imidlertid at kravet om tillatelser og kontrollregimet sett under ett gir en tilstrekkelig garanti mot misbruk.

EMD la i Centrum för Rättvisa avgjørende vekt på systemet for forhåndsgodkjenning av inngrepene:

> 368. Crucially, the judicial pre-authorisation procedure as it exists in Sweden and the supervision exercised by an independent body in Sweden serve in principle to ensure the application of the domestic legal requirements and the Convention standards in practice and to limit the risk of disproportionate consequences affecting Article 8 rights. Notably, regard must be had to the fact that in Sweden the limits to be observed in each bulk interception mission, as well as its lawfulness and proportionality in general, are the subject matter of judicial pre-authorisation proceedings before the Foreign Intelligence Court, which sits in the presence of a privacy protection representative defending the public interest.

Som nevnt under punkt 3.3.3 ovenfor, mente EMD at det svenske systemet inneholdt tre svakheter; manglende sletting av overskuddsmateriale, deling av etterretningsinformasjon med utenlandske tjenester uten å vurdere opplysningene samt mangler ved den etterfølgende kontrollen. Utover at deling av etterretningsopplysninger med utenlandske tjenester ble ansett som en alvorlig svakhet («significant shortcoming»), gir Domstolen ingen føringer på hvilken vekt de øvrige svakhetene tillegges ved vurderingen. Når det gjaldt den etterfølgende kontrollen, uttalte EMD:

> 372. Finally, the Inspectorate's dual role and the absence of a possibility for members of the public to obtain reasoned decisions in some form in response to inquiries or complaints regarding bulk interception of communications weakens the *ex post facto* control mechanism to an extent that generates risks for the observance of the affected individuals' fundamental rights. Moreover, the lack of an effective review at the final stage of interception cannot be reconciled with the Court's view that the degree of interference with individuals' Article 8 rights increases as the process advances (see paragraphs 239 and 245 above) and falls short of the requirement of "end-to-end" safeguards (see paragraph 264 above).

Retten har ved vurderingen av om den norske loven tilfredsstiller kravet til rettssikkerhetsgarantier i alle ledd («end-to-end safeguards») lagt vekt på at E-tjenesten må innhente forhåndsgodkjenning fra retten i to omganger for å kunne gjennomføre søk i og analyser av de lagrede dataene, jf. ovenfor punkt 1.1.1. Dette skiller seg fra den svenske ordningen hvor rettens forhåndsgodkjennelse ble gitt samlet for begge disse trinnene.

Retten skal i begge disse tilfellene foreta en fullstendig legalitetskontroll på bakgrunn av vilkårene fastsatt i loven, herunder at innhentingen ligger innenfor E-tjenestens oppgaver, er forholdsmessig og ikke strider mot noen av innhentingsforbudene. For rettens behandling skal det som hovedregel oppnevnes en særskilt advokat som skal ivareta den enkeltes rettigheter og samfunnets interesser, eksempelvis personvernhensyn. Retten kan ved behov beslutte muntlige forhandlinger og kjennelsen skal begrunnes og kan ankes.

Rettens forhåndsgodkjennelse må sees i sammenheng med den løpende kontrollen som ivaretas av EOS-utvalget. Utvalget kontrollerer at lovens bestemmelser etterleves og at søk gjennomføres i tråd med rettens kjennelse. For å kunne gjennomføre slik kontroll skal EOS-utvalget ha uhindret tilgang til all informasjon og E-tjenesten skal tilrettelegge for kontrollen gjennom tekniske løsninger, jf. § 7-11, annet og tredje ledd. EOS-utvalget er i loven § 7-12 også gitt kompetanse til å fremme begjæring for retten om stans og sletting dersom virksomheten gjennomføres i strid med disse bestemmelsene. Også i denne forbindelse blir det oppnevnt en særskilt advokat som skal ivareta de implisertes interesser.

Også den etterfølgende kontrollen ivaretas av EOS-utvalget som ikke har en tilsvarende dobbeltrolle som svenske SIUN. Retten mener også at den norske ordningen om at klager får opplyst om en klage har ført til kritikk eller ikke, innebærer en bedre sikkerhet mot misbruk enn under den svenske ordningen. I tillegg har EOS-utvalget mulighet til å oppfordre E-tjenesten eller departementet til å gi en utfyllende begrunnelse overfor klager. Dette var heller ikke mulig under den svenske ordningen. Endelig har retten vektlagt muligheten for å prøve spørsmålet for retten. Denne kontrollen suppleres av andre kontrollmekanismer slik som tjenestens interkontroll og departementets forvaltningskontroll. Samlet sett mener retten at det norske systemet inneholder tilstrekkelige garantier mot misbruk gjennom hele prosessen.

Retten har etter dette kommet til at det norske systemet er i samsvar med de krav som er oppstilt av EMD.

3.5 Kildevern – Forholdet til EMK artikkel 10 Grunnlovens § 100

Kildevernet er medienes, redaktørenes og journalistenes rett til ikke å oppgi sine kilder og er en sentral del av ytringsfriheten etter Grunnlovens § 100 og EMK artikkel 10.

3.5.1 Partenes anførsler

Stiftelsen har gjort gjeldende at TI er i strid med kildevernet etter EMK artikkel 10. Gjennom TI gis myndighetene tilgang til mer eller mindre all datatrafikk som krysser den norske grensen. Det er ikke tvilsomt at TI og det tilhørende metadatalageret vil inneholde kommunikasjon mellom journalister og deres kilder eller data som på annen måte kan avsløre hvem som er pressens kilder. En kilde som kommuniserer med journalister via elektroniske medier vil ikke kunne stole på at kommunikasjonen forblir fortrolig. Dette vil ha en nedkjølende effekt på det offentlige ordskiftet og borgernes vilje til å varsle om kritikkverdige forhold.

Kildevernet brytes alene ved at metadata viser at det har vært kommunikasjon mellom en kilde og en journalist, uten at E-tjenesten har fått innsyn i innholdet/informasjonen som er betrodd journalisten. Ingen av bestemmelsene i loven begrenser adgangen til bulkinnhenting og lagring av opplysninger som er omfattet av kildevernet.

E-tjenestelovens § 5-2 annet ledd og 9-6 gir heller ikke tilfredsstillende garantier mot slike brudd.

Den personelle og territorielle avgrensningen av bestemmelsene verner ikke grenseoverskridende journalistisk arbeid hvis kilden er utenlandsk og i utlandet. Det er vist til EMDs avgjørelse i Wieder og Guarnieri mot Storbritannia som ifølge Stiftelsen innebærer at EMK gjelder fullt ut, uavhengig av om personene, hvis kommunikasjon innsamles, lagres og behandles av E-tjenesten i Norge, befinner seg i Norge eller utenfor Norge.

Videre peker Stiftelsen på at kravet om «stor sannsynlighet for at innhentingen vil frembringe kildeidentifiserende opplysninger» innebærer at E-tjenesten selv må ha tilgang til opplysninger som i utgangspunktet er omfattet av kildevernet for å kunne vurdere dette, og uten at de påkrevde rettssikkerhetsgarantiene, herunder domstolskontrollen, blir overholdt.

Kildevernet er heller ikke unntatt hastekompetansen i lovens § 8-10, noe som innebærer at kildevernet er brutt før retten kan forhindre det.

Staten har gjort gjeldende at de norske TI-reglene er forenelige med EMK artikkel 10.

EMD skiller mellom tilgang til konfidensielt journalistisk materiale som er innhentet med vilje og materiale som er innhentet som et tilfeldig biprodukt av TI.

Målrettet innhenting mot journalister er regulert i lovens § 5-2 annet og tredje ledd og er i samsvar med de krav som EMD oppstiller. Bestemmelsen gjelder både for søk i lagrede metadata (§ 7-8) og målrettet innhenting og lagring av innholdsdata (§ 7-9).

Dersom slikt materiale dukker opp som et tilfeldig biprodukt, krever fortsatt lagring og bruk tillatelse fra domstolen, jf. lovens § 9-6 annet og tredje ledd. Dette er i samsvar med EMDs krav.

Når det gjelder den personelle og territorielle avgrensingen av bestemmelsene, peker staten på at TI kun gjelder grensekryssende kabler hos tilbydere av kommunikasjonstjenester i Norge og at kommunikasjon fra en utenlandsk journalist i utlandet ikke er berørt at TI. For øvrig er kommunikasjonen som nevnt av stiftelsen omfattet.

Staten har videre anført at også hastekompetansen i loven § 8-10 er forenelig med EMK artikkel 10. Dette er en meget snever unntaksregel som skal benyttes med stor varsomhet og som er innrammet i rettssikkerhetsgarantier, jf. § 8-10 annet ledd. Hastekompetansen har aldri blitt benyttet og eksistensen av en slik regel er ikke i strid med EMK artikkel 10.

3.5.2 Rettens vurdering

Retten har kommet til at reglene om TI i e-tjenesteloven er forenelige med EMK artikkel 10 og de krav som EMD oppstiller i Big Brother Watch m.fl.

3.5.2.1 Big Brother Watch m.fl. mot Storbritannia

EMD har i storkammeravgjørelsen Big Brother Watch m.fl. mot Storbritannia 25. mai 2021 behandlet spørsmålet om den britiske lovgivningen om bulkinnhenting innebar en krenkelse av blant annet kildevernet etter EMK artikkel 10. EMD identifiserte svakheter ved det britiske lovgrunnlaget som etter en helhetsvurdering innebar en krenkelse av kildevernet.

EMD tok i sin vurdering utgangspunkt i at kildevern er en hjørnestein i pressefriheten og dermed ytringsfriheten (avsnitt 442) og at inngrep i kildevernet bare kan tillates dersom det er «justified by an overriding requirement in the public interest» (avsnitt 444). Et slikt inngrep må videre være rammet inn av prosessuelle garantier. Den viktigste prosessuelle garantien er at en dommer eller annen uavhengig instans kan prøve om inngrepet kan rettferdiggjøres.

EMD skiller mellom tilgang til konfidensielt journalistisk materiale som er innhentet med vilje («intentionally») og tilgang til materiale som er et tilfeldig biprodukt av TI («unintentionally, as a «bycatch» of the bulk interception operation») (avsnitt 447). EMD slår fast at målrettet innhenting mot journalister er mer inngripende enn i tilfeller hvor etterretningstjenesten mer eller mindre tilfeldig får tilgang til informasjon som kan gripe inn i kildevernet.

Ved målrettet innhenting av journalistisk materiale, for eksempel ved bruk av selektorer eller søkebegreper knyttet til en journalist, følger det av EMDs avgjørelse at slik innhenting må ha forhåndsgodkjennelse av en dommer eller annen uavhengig instans. Domstolen stiller også krav om at dommeren/instansen må settes i stand til å ta stilling til om bruken av selektorer eller søkebegreper er rettferdiggjort av hensyn til et overordnet krav i allmennhetens interesse og at mindre inngripende tiltak vil være tilstrekkelige for å ivareta formålet (avsnitt 449).

I de tilfellene hvor etterretningstjenesten mer eller mindre tilfeldig får tilgang til informasjon som kan gripe inn i kildevernet, er videre lagring og analyse av informasjonen betinget av at en domstol eller annen uavhengig instans har tillatt det (avsnitt 450).

3.5.2.2 Bestemmelsene om kildevern i e-tjenesteloven

I e-tjenesteloven § 5-2 annet ledd er det gitt en egen bestemmelse om målrettet innhenting mot journalister mv. Bestemmelsen må sees i sammenheng med e-tjenesteloven § 9-6 som gjelder behandlingen av opplysninger som kan identifisere en kilde.

Målrettet innhenting

Etter e-tjenesteloven § 5-2 første ledd kan E-tjenesten iverksette målrettet innhenting når konkrete holdepunkter gir grunn til å undersøke om innhentingen kan frembringe informasjon som er relevant for etterretningsformål.

Etter bestemmelsens annet ledd kan målrettet innhenting mot journalister omfattet av § 9-6 første ledd, eller der det er stor sannsynlighet for at innhentingen vil frembringe kildeidentifiserende opplysninger, bare iverksettes dersom det er strengt nødvendig at de hensyn som begrunner kildevernet, viker for nasjonale sikkerhetsinteresser. Tillatelse til å iverksette målrettet innhenting etter annet ledd gis av retten ved kjennelse, jf. tredje ledd. Bestemmelsens andre og tredje ledd ble tilføyd ved endringslov 6. juni 2023 nettopp med sikte på å tilpasse den norske loven til EMDs krav i Big Brother Watch.

Målrettet innhenting er definert i e-tjenesteloven § 1-3 bokstav e) som «systematisk arbeid for å finne informasjon knyttet til identifiserte etterretningsmål». Målrettet innhenting vil normalt skje etter at et etterretningsmål er identifisert og pågår over tid for å samle mest mulig informasjon om etterretningsmålet, jf. høringsnotat 12. november 2018 punkt 9.3. For å avgrense informasjonsinnhentingen benyttes det ulike utvalgskriterier; selektorer. Disse kan være knyttet til person eller til modus, jf. ovenfor.

Innhentingen kan bare skje i tråd med de øvrige lovbestemte vilkårene, herunder at innhentingen må ha til formål å frembringe informasjon som er relevant for å ivareta E-tjenestens oppgaver etter lovens kapittel 3, kravet til forholdsmessighet, jf. § 5-4, diskrimineringsforbudet i § 9-4 og innhentingsforbudene i §§ 4-1 og 4-8.

Bestemmelsen i § 5-2 annet ledd gjelder for det første for «journalister som er omfattet av § 9-6 første ledd» eller «målrettet innhenting der det er stor sannsynlighet for at innhentingen vil frembringe kildeidentifiserende opplysninger som er omfattet av § 9-6 første ledd. Av spesialmerknadene til bestemmelsen fremgår det:

> Bestemmelsen oppstiller to alternative forutsetninger for at grunnvilkåret skal komme til anvendelse. For det første får grunnvilkåret anvendelse dersom Etterretningstjenesten har til hensikt å utføre systematisk arbeid for å finne informasjon knyttet til et identifisert etterretningsmål som er journalist. Begrepet «etterretningsmål» er legaldefinert som «objekt, person, virksomhet eller annet som informasjons-innhentingen retter seg mot», jf. § 1-3 bokstav d. Prøvingen er avgrenset til tilfeller hvor journalisten er bosatt i Norge, norsk statsborger eller arbeider på oppdrag for virksomhet i Norge som omfattes av medieansvarsloven § 2. Etter omstendighetene kan også andre enn journalister omfattes av personkretsen som vernes av bestemmelsen, forutsatt at vedkommende utfører arbeid som er i kjernen av journalistisk virksomhet. Hva som ligger i begrepet «journalistisk virke», er belyst i merknaden til § 9-6 i Prop. 80 L (2019–2020) side 225–226.

> For det andre får grunnvilkåret anvendelse dersom Etterretningstjenesten har til hensikt å utføre systematisk arbeid for å finne informasjon knyttet til et etterretningsmål uavhengig av om vedkommende er journalist eller ikke, dersom det er stor sannsynlighet for at innhentingen vil frembringe opplysninger som er betrodd noen i deres journalistiske virke og som kan avsløre hvem som er kilde for opplysningen, jf. § 9-6 første ledd. Med «stor sannsynlighet» menes at det må foreligge særskilte holdepunkter som tilsier at det er betydelig mer enn alminnelig sannsynlighetsovervekt for at innhentingen vil frembringe slike kildeidentifiserende opplysninger. Det er ikke tilstrekkelig at innhentingen i teorien vil kunne frembringe kildeidentifiserende opplysninger. Det er heller ikke tilstrekkelig at etterretningsmålet en eller annen gang har hatt kommunikasjon med en journalist eller har vært kilde til opplysninger i pressen. Det kreves kvalifisert sannsynlighets-overvekt. Samtidig settes ikke kravet så høyt at det er nødvendig med sikker kunnskap for at vilkåret skal være oppfylt.

Etter § 5-2 annet ledd kan målrettet innhenting bare iverksettes dersom «det er strengt nødvendig at de hensyn som begrunner kildevernet, viker for nasjonale sikkerhetsinteresser». Bestemmelsen skal forstås på samme måte som etter § 9-6, jf. nedenfor. Vurderingen foretas av domstolen.

Retten legger til grunn at målrettet innhenting etter § 5-2 annet ledd faller inn under kategorien konfidensiell informasjon som er innhentet med vilje («intentionally»), jf. Big Brother Watch avsnitt 447 følgende. EMD oppstiller et krav om at slik innhenting må forhåndsgodkjennes av en domstol. Dette er også ordningen etter § 5-2 tredje ledd. Retten viser også til de krav som er oppstilt til begjæringen om slik forhåndsgodkjenning i lovens § 8-2 og hva retten kan prøve, jf. § 8-4.

Behandling av opplysninger som kan identifisere en kilde

Lovens § 9-6 inneholder et forbud mot at E-tjenesten «behandler» opplysninger som kan identifisere en kilde. Det er her tale om behandling etter at innhenting av kommunikasjonen har skjedd.

Forbudet innebærer at E-tjenesten som hovedregel ikke skal behandle informasjon som er egnet å avsløre identiteten til en journalistisk kilde. Forbudet retter seg mot «opplysninger som er betrodd noen i deres journalistiske virke» dersom opplysningene kan avsløre hvem som har avgitt dem. Det følger av merknadene til § 9-6 i Prop. 80 L (2019-2020) side 225 at det er et vilkår at opplysningen er gitt under forutsetning av anonymitet, jf. begrepet «betrodd». I tillegg må den aktuelle opplysningen være egnet til å avsløre identiteten til den som har avgitt den.

Om uttrykket «journalistisk virke» fremgår det av spesialmerknadene til bestemmelsen:

> I kjernen av begrepet «journalistisk virke» er samfunnsrelatert journalistikk i en medievirksomhet ledet av en person med oppgaver tilvarende en ansvarlig redaktør

> og som er tilsluttet pressens selvbedømmeordning med tilhørende etiske retningslinjer. Også annen medievirksomhet kan regnes som «journalistisk virke», herunder virksomheten til frilansere, dokumentarfilmskapere, forfattere og journaliststudenter. I vurderingen må det sees hen til om virksomheten ivaretar en samfunnsfunksjon og har et journalistisk formål herunder om den har til formål å legge til rette for en åpen og opplyst offentlig debatt, avsløre kritikkverdige forhold eller lignende. Begrepet må for øvrig forstås i samsvar med utviklingen etter Grunnloven § 100 og EMK artikkel 10.

Det følger videre av første punktum at forbudet kun gjelder dersom personen som driver journalistisk virke, eller betror seg til denne, er bosatt i Norge, er norsk statsborger eller arbeider på oppdrag for en virksomhet i Norge som er omfattet av mediefridomslova § 2. Sistnevnte alternativ tar sikte på utenlandske journalister mv. som har en form for formalisert relasjon til den norske virksomheten, jf. spesialmerknadene.

Etter bestemmelsens annet ledd kan informasjonen likevel behandles dersom det er «strengt nødvendig» at de hensyn som begrunner kildevernet viker for nasjonale sikkerhetsinteresser. Det følger av Prop. 80 L (2019-2020) punkt 12.8.6 at unntaksbestemmelsen skal vurderes med utgangspunkt i Grunnlovens § 100 og EMK artikkel 10. Av spesialmerknadene fremgår det at de aktuelle opplysningene må være av vesentlig betydning for utførelsen av et konkret etterretningsformål, og at informasjonen må være tilnærmet umulig å tilveiebringe på en annen, mindre inngripende måte. For det andre vil kildevernet kun vike dersom formålet med behandlingen veier tyngre enn hensynet til kildevernet. Dette vil i hovedsak utelukkende være aktuelt der formålet med behandlingen er å løse oppgaver etter lovens § 3-1. Den nedkjølende effekten dette vil kunne ha står sentralt i forholdsmessighetsvurderingen.

Retten legger til grunn at behandlingen av opplysninger som kan identifisere en kilde etter § 9-6 faller inn under kategorien utilsiktet innhenting, jf. inndelingen gjort i Big Brother Watch avsnitt 449. EMD oppstiller her et krav om at videre behandling av opplysningene er betinget av en tillatelse gitt av retten. Dette er også ordningen etter lovens § 9-6 som krever at slik tillatelse skal gis av retten.

3.5.2.3 Rettens vurdering

Stiftelsen har for det første anført at lagringen av metadata i seg selv innebærer et inngrep i ytringsfriheten.

EMD har i Big Brother Watch (avsnitt 450) akseptert at selve innhentingen, uten at det innhentede materiale ble undersøkt, ikke innebærer et alvorlig inngrep i artikkel 10.

> (…) Therefore, it accepted that the initial interception, without examination of the intercepted material, did not constitute a serious interference with Article 10 of the Convention. (…)

Det er videre uttalt at det er vanskelig på innhentingsstadiet å vurdere i hvilken grad kommunikasjon med journalister og deres kilder blir omfattet, og at det derfor ikke er mulig på tidspunktet for forhåndsgodkjennelse av retten å vurdere om en slik innhenting vil være «justified by an overriding requirement in the public interest» og om mindre inngripende tiltak kan benyttes (avsnitt 449).

På denne bakgrunn mener retten at det ikke er i strid med konvensjonen at slikt materiale havner i metadatalageret. Dersom slikt materiale oppdages, må dette enten slettes umiddelbart eller så må E-tjenesten be om rettens tillatelse til å fortsette og lagre og behandle materialet.

Stiftelsen har videre anført at den personelle og territorielle avgrensningen ikke gir tilstrekkelig vern for grenseoverskridende journalistisk arbeid. Retten er ikke enig i dette.

Det følger av redegjørelsen ovenfor at reglene omfatter så vel journalister som andre som «utfører arbeid som er i kjernen av journalistisk virksomhet». Lovens § 9-6 bruker uttrykket «journalistisk virke» og retten legger til grunn at de to bestemmelsene skal avgrenses på samme måte. Uttrykkene innebærer at ikke bare journalister omfattes av bestemmelsene, men at disse etter omstendighetene også vil omfatte frilansere, forfattere, dokumentarfilmskapere og journaliststudenter. Forutsetningen er at de er bosatt i Norge, er norske statsborgere eller arbeider på oppdrag for en virksomhet i Norge som er omfattet av mediefridomslova § 2.

Stiftelsen har også vist til at bestemmelsene ikke verner utenlandske kilder i utlandet. Retten er enig i at denne kategorien faller utenfor vernet som er oppstilt i e-tjenesteloven §§ 5-2 annet ledd og 9-6. I slike situasjoner er det imidlertid ikke tale om grenseoverskridende kommunikasjon og reglene om tilrettelagt innhenting gjelder ikke i slike tilfeller.

Endelig har Stiftelsen anført at inngrep i kildevernet ikke er unntatt E-tjenestens hastekompetanse etter e-tjenesteloven § 8-10 og at kildevernet vil være brutt før retten får mulighet til å vurdere dette.

Etter denne bestemmelsen kan ordre fra sjefen for E-tjenesten, dersom det ved opphold er stor fare for at informasjon av vesentlig betydning går tapt, tre i stedet for rettens kjennelse. I slike tilfeller skal tjenesten straks og senest innen 24 timer etter at innhentingen ble påbegynt, forelegge saken for retten. Dersom retten mener at søket eller innhentingen var ulovlig, skal dette meddeles EOS-utvalget og retten kan pålegge sletting av informasjonen som har blitt innhentet.

Spørsmålet om kontroll av hastekompetanse for å autorisere innhenting av informasjon generelt ble behandlet i Centrum for Rättvisa (avsnitt 295). Domstolen kom her til at den svenske ordningen – som tilsvarer den norske – inneholdt tilstrekkelige garantier mot misbruk og ordningen ble ansett å være i samsvar med EMK artikkel 8.

Retten er ikke kjent med at EMD har tatt eksplisitt stilling til hvilke krav som skal stilles til prosedyrer i hastesaker for bulkinnhentingssystemer i relasjon til kildeidentifiserende opplysninger. I Big Brother Watch (avsnitt 445) uttaler imidlertid EMD følgende i sin gjennomgang av de generelle prinsippene som gjelder for kildevern:

> (…) In situations of urgency, a procedure should exist to identify and isolate, prior to the exploitation of the material by the authorities, information that could lead to the identification of sources from information that carries no such risk (see, *mutatis mutandis*, *Wieser and Bicos Beteiligungen GmbH v. Austria*, no. 74336/01, §§ 62-66, ECHR 2007-XI).

Spørsmålet om prosedyrene for å behandle innhentet material ble imidlertid ikke nærmere kommentert at EMD i relasjon til bulkinnhentingssystemene.

Etter rettens syn er det ikke åpenbart at den skisserte løsningen er overførbar til data innhentet i medhold av hastekompetansen etter e-tjenesteloven. Bestemmelsen i § 8-10 er ment som en meget snever unntaksregel, noe som også reflekteres i vilkårene om at det ved opphold er «stor fare» for at etterretningsinformasjon «av vesentlig betydning» for E-tjenestens oppgaver kan «gå tapt». I forarbeidene er det eksempelvis nevnt at dette kan være aktuelt ved alvorlige cyberangrep som skjer på en helligdag, jf. Prop. 80 L (2019-2020) punkt 11.9.9.3. Retten legger til grunn at det i slike tilfeller også vil være «strengt nødvendig at de hensyn som begrunner kildevernet, viker for nasjonale sikkerhetsinteresser», jf. § 9-6 (2).

Sjef for E-tjenesten, Nils-Andreas Stensønes, har bekreftet at det er en meget høy terskel for å bruke hastekompetansen i § 8-10, og at dette kun vil være aktuelt i de tilfellene hvor det oppstår akutt fare for menneskeliv e.l.

I mangel av klare retningslinjer fra EMD for bruk av hastekompetansen for slik virksomhet, mener retten at vilkårene for å benytte denne kompetansen sammenholdt med den etterfølgende kontrollen og plikten til å slette ulovlig innhentet informasjon, gir en tilstrekkelig garanti mot misbruk. Retten legger på bakgrunn av Stensønes' forklaring også til grunn at hastekompetansen ikke har blitt benyttet. Etter rettens syn er selve eksistensen av en slik mulighet ikke i strid med EMK.

Retten har på denne bakgrunn kommet til at e-tjenesteloven § 5-2 og § 9-6 er i samsvar med de krav EMD har oppstilt for å beskytte kildevernet.

3.6 Forholdet til EØS-retten

3.6.1 Innledning

Kommunikasjonsverndirektivet (direktiv 2002/58 EF) er en del av EØS-avtalen og er implementert i norsk rett ved lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekom-loven).

EU-domstolen avsa 6. oktober 2020 dom (prejudisiell avgjørelse) i flere saker om behandlingen av personopplysninger etter kommunikasjonsverndirektivet; Sak C-623/17 Privacy International og forente saker C511/18, C-512/18 og C-520/18 La Quadrature du Net m.fl.

La Quadrature du Net (LQN) gjaldt lovgivningen i henholdsvis Frankrike og Belgia om lagring av elektronisk kommunikasjon (metadata). I den franske lovgivningen var formålet med lagringen etterforskning, identifisering og forfølgelse av kriminalitet, mens den belgiske lovgivingen i tillegg skulle sikre nasjonal sikkerhet, forsvar og offentlig sikkerhet. Privacy International (PI) gjaldt spørsmålet om britisk etterretningstjeneste hadde lov til å skaffe og bruke opplysninger om elektronisk kommunikasjon. Felles for sakene var om lovgivningen som pålegger ekomtilbydere å lagre eller overføre data til sikkerhets- og etterretningstjenester av hensyn til nasjonal sikkerhet er i samsvar med kommunikasjonsverndirektivet artikkel 15.

3.6.2 Nærmere om EU-domstolens avgjørelse i La Quadrature du Net

LQN har flest likhetstrekk med tilrettelagt innhenting etter e-tjenesteloven og retten redegjør kort for innholdet i denne avgjørelsen.

EU-domstolen tar ved sin tolkning utgangspunkt i at formålet med kommunikasjonsvern-direktivet er å beskytte brukerne av elektroniske kommunikasjonstjenester mot risikoen knyttet til deres personvern som følge av ny teknologi, og da særlig økte muligheter for automatisert lagring og behandling av opplysninger. Direktivet skal også sikre full respekt for rettighetene som fremgår av EUs charter om grunnleggende rettigheter art. 7 og 8.

Prinsippet om konfidensialitet har kommet til uttrykk i direktivets artikkel 5. Bestemmelsen fastsetter at medlemsstatene skal sikre «fortrolighet om kommunikasjon som foregår via offentlige kommunikasjonsnett». Uten samtykke fra brukeren skal det å avlytte, fange opp eller lagre være forbudt, unntatt når slik virksomhet er i samsvar med artikkel 15 nr. 1.

Direktivet artikkel 15 nr. 1 oppstiller et unntak fra dette prinsippet når det er et nødvendig, egnet og forholdsmessig tiltak i et demokratisk samfunn for å sikre nasjonal sikkerhet, forsvar og offentlig sikkerhet, samt forebygging, etterforskning og strafforfølging av

kriminalitet. Lagring av opplysninger for slike formål kan bare gjøres for en begrenset periode og formålene som muliggjør slik lagring etter artikkel 15 nr. 1 er uttømmende regulert (LQN avsnitt 112).

Eventuelle unntak må videre være i tråd med EU-rettens generelle prinsipper, herunder forholdsmessighetsprinsippet og de grunnleggende rettighetene som fremgår av Charteret (LQN avsnitt 113). Domstolen slår videre fast at lagring av metadata utgjør et inngrep i retten til privatliv og personvern slik disse er sikret i Charteret artikkel 7 og 8, og at dette gjelder uavhengig av om opplysningene er av sensitiv karakter eller ei. Det er heller ikke av betydning om opplysningene faktisk brukes (LQN avsnitt 116 flg). Lagringen i seg selv utgjør en risiko for misbruk.

EU-domstolen uttaler videre at rettighetene i Charteret ikke er absolutte (LQN avsnitt 120) og at rettighetene skal vurderes i lys av sin funksjon i samfunnet. Charteret artikkel 52 (1) tillater begrensninger i disse rettighetene når de er fastsatt i lov, respekterer kjernen i rettigheten og overholder prinsippet om forholdsmessighet. Om forholdsmessighets-prinsippet uttaler EU-domstolen:

> 132. In order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subjected to automated processing, particularly where there is a significant risk of unlawful access to that data. Those considerations apply especially where the protection of the particular category of personal data that is sensitive data is at stake (…)
>
> 133 Thus, legislation requiring the retention of personal data must always meet objective criteria that establish a connection between the data to be retained and the objective pursued (…)

Når det gjelder direktivets virkeområde knyttet til preventive lagring av metadata for å beskytte den nasjonale sikkerhet, kom EU-domstolen til at pålegg om lagring av metadata av hensyn til nasjonal sikkerhet var omfattet av direktivet til tross for TEU artikkel 4 (2), jf. LQN avsnitt 99.

EU-domstolen redegjør deretter for hva unntaket for nasjonal sikkerhet omfatter:

> 135 In that regard, it should be noted, at the outset, that Article 4 (2) TEU provides that national security remains the sole responsibility of each Member State. That responsibility corresponds to the primary interest in protecting the essential

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

Domstolen fastslår deretter at hensynet til nasjonal sikkerhet kan begrunne mer inngripende tiltak enn de øvrige hensynene som er opplistet i direktivet artikkel 15 nr. 1:

> 136 The importance of the objective of safeguarding national security, read in the light of Article 4 (2) TEU, goes beyond that of the other objectives referred to in Article 15 (1) of Directive 2002/58, inter alia the objectives of combating crime in general, even serious crime, and of safeguarding public security. Threats such as those referred to in the preceding paragraph can be distinguished, by their nature and particular seriousness, from the general risk that tensions or disturbances, even of a serious nature, affecting public security will arise. Subject to meeting the other requirements laid down in Article 52 (1) of the Charter, the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives.

Basert på disse synspunktene konkluderer EU-domstolen med at direktivets bestemmelser ikke er til hinder for lovgivning som tillater myndighetene å pålegge tjenestetilbydere å lagre metadata fra alle brukere av kommunikasjonstjenester forutsatt at dette skjer

> 137 (…) for a **limited period of time**, as long as there are **sufficiently solid grounds** for considering that the Member State concerned is confronted with a **serious threat**, as referred to in paragraphs 135 and 136 of the present judgment, to national security which is shown to be **genuine and present or foreseeable**. Even if such a measure is applied indiscriminately to all users of electronic communications systems, without there being at first sight any connection, within the meaning of the case-law cited in paragraph 133 of the present judgment, with a threat to the national security of that Member State, it must nevertheless be considered that the existence of that threat is, in itself, capable of establishing that connection.
>
> 138 The instruction for the preventive retention of data of all users of electronic communications systems must, however, **be limited in time to what is strictly necessary.** Although it is conceivable that an instruction requiring providers of electronic communications services to retain data may, owing to the ongoing nature of such a threat, be renewed, the duration of each instruction cannot exceed a foreseeable period of time. Moreover, such data retention must be subject to limitations and must be circumscribed by strict safeguards making it possible to protect effectively the personal data of the persons concerned against the risk of abuse. Thus, that retention cannot **be systematic in nature**.

For å sikre at slik lagring av metadata begrenses til disse tilfellene oppstiller Domstolen er krav om at slike pålegg om lagring er undergitt kontroll av en domstol eller annen uavhengig instans, jf. LQN avsnitt 139.

Domstolen oppstiller her grunnvilkårene som må være oppfylt for at ekomtilbydere kan pålegges en plikt til å lagre data av hensyn til nasjonal sikkerhet. For det første må det foreligge tilstrekkelig konkrete omstendigheter («sufficiently solid grounds») som gjør det mulig å anta det er en alvorlig trussel mot nasjonal sikkerhet. Trusselen må videre være reell og aktuell eller mulig å forutse («genuine and present or foreseeable»). Domstolen presiserer i avsnitt 137 at selve eksistensen av en kvalifisert trussel i seg selv anses egnet til å etablere forbindelse mellom dataene som søkes lagret og formålet. Utover dette går Domstolen ikke nærmere inn på hva som ligger i disse begrepene.

Lagringen må være begrenset i tid til det som er strengt nødvendig («limited in time to what is strictly necessary"), og lagringen må rammes inn av strenge minstekrav som sikrer en effektiv beskyttelse mot misbruk. Lagringen kan ikke være systematisk («systematic in nature") og beslutninger om slike tiltak må undergis en effektiv kontroll av domstolene eller et uavhengig organ.

Disse vilkårene omtaler gjerne som LQN-kriteriene.

Det har under lovforarbeidet vært reist spørsmål om EU-domstolens tolkning kan legges til grunn ved tolkningen og anvendelsen av e-tjenestelovens bestemmelser om målrettet og tilrettelagt innhenting. Retten oppfatter at partene i saken ikke er uenige om at kravene som er oppstilt i LQN får betydning for tolkningen av den norske loven og retten er enig i dette.

Det ble videre under lovforarbeidet drøftet om LQN-kriteriene burde fremgå direkte av lovens § 7-3, jf. blant annet den interdepartementale arbeidsgruppens rettslige analyse. Stiftelsen har anført at kriteriene burde vært lovfestet.

Retten legger til grunn at kravene til prøving av disse vilkårene vil endre seg fra den innledende speilingen til mer konkrete målsøk og analyse. Etter rettens syn ville en lovfesting av LQN-kriteriene ikke i tilstrekkelig grad reflektere at prøvingsintensiteten blir sterkere jo lengere ut i innhentingen man kommer. Kriteriene kan synes noe strenge i den innledende fasen av informasjonsinnhentingen (speilingen), mens de er for lite stringente i de neste fasene om søk og behandling av informasjonen. Etter rettens syn vil LQN-kriteriene ha størst betydning i fasen med lagring og søk i materialet, og mindre betydning i forbindelse med speilingen. Retten mener derfor at det er fornuftig at kriteriene innfortolkes i lovens nødvendighetskriterium for å kunne hensynta denne glideskalaen i prøvingsintensitet. Etter rettens syn vil dette også i tilstrekkelig grad sikre anvendelsen av kriteriene.

3.6.3 Rettens vurdering

Stiftelsen har overordnet anført at formålene med masseovervåkingen er for vide og at vilkårene ikke er strenge og klare nok. Det er videre anført at masseovervåkningen kan skje i lengre tid enn det som er strengt nødvendig og at det er utilstrekkelige sikkerhetsmekanismer.

Staten har anført at e-tjenesteloven er i tråd med de krav som oppstilles av EU-domstolen i LQN.

3.6.3.1 Er formålene som kan begrunne TI for vide?

Stiftelsen har for det første anført at EU-domstolen krever at systemet utelukkende kan forsvares for formål som er essensielle for nasjonal sikkerhet. Norsk lovgivning åpner for at speiling etter omstendighetene kan begrunnes i løsere nasjonale sikkerhetshensyn, jf. det anførte under EMK, og at e-tjenesteloven § 3-2 ikke er i samsvar med de krav EU-domstolen oppstiller.

Retten har kommet til at denne anførselen ikke kan føre frem.

Som redegjørelsen over viser, kom EU-domstolen til at pålegg om lagring av metadata av hensyn til nasjonal sikkerhet var omfattet av direktivet til tross for TEU artikkel 4 (2), jf. LQN avsnitt 99. Domstolen har videre definert hva som omfattes av «nasjonal sikkerhet» jf. LQN avsnitt 135 referert ovenfor. Det fremgår her at formålet ikke bare omfatter direkte trusler og retten legger til grunn at også forhold omfattet av e-tjenesteloven § 3-2 er omfattet av denne passusen. Retten viser i den forbindelse til redegjørelsen som er gitt ovenfor i punkt 3.4.3 hvor retten har kommet til at e-tjenesteloven § 3-1 og 3-2 – lest i sammenheng – gir anvisning på et innbyrdes sammenhengende formål som skal frembringe informasjon om utenlandske forhold som utfordrer nasjonal sikkerhet. Etter rettens syn harmonerer dette godt med EU-domstolen krav.

3.6.3.2 Er terskelen for å iverksette TI for lav?

Stiftelsen har videre anført at EU-domstolen krever at det foreligger tilstrekkelige konkrete holdepunkter («sufficiently solid grounds») som gjør det mulig å anta at det er en alvorlig trussel mot nasjonal sikkerhet som er reell og aktuell eller mulig å forutse. Dette innebærer at det er oppstilt en høy terskel knyttet til alvorlighetsgraden av en konkret trussel som kan begrunne et pålegg til tjenestetilbydere om plikt til å lagre data. Ordlyden i § 7-3 om «nødvendig for å etablere et informasjonsgrunnlag for etterretningsformål» oppstiller en betydelig lavere terskel. Vilkåret er dessuten vagt formulert slik at det er vanskelig for domstolen å prøve dette.

Retten har kommet til at vilkåret i lovens § 7-3 harmonerer godt med kravet EU-domstolen oppstiller. Kravet er at det foreligger tilstrekkelig konkrete omstendigheter som gjør det

mulig å anta at staten står ovenfor en alvorlig trussel mot nasjonal sikkerhet som må anses å være reell og aktuell eller kan forutsees. Det er tilstrekkelig at det foreligger «omstendigheter» («circumstances») og disse må være tilstrekkelig konkrete, uten noen nærmere spesifisering. Det oppstilles altså ikke et krav til bevis i vanlig forstand. Det er ikke nødvendig at det foreligger mistanke om at bestemte personer skal foreta konkrete handlinger som kan skade rikets sikkerhet, jf. LQN avsnitt 137 referert ovenfor. At det ikke oppstilles krav til mistanke mot bestemte personer, fremgår også av LQN avsnitt 138. Dette er også bakgrunnen for at slik lagring av metadata kalles «preventiv».

Det er tale om å avverge fremtidige trusler og det er nok at omstendighetene gjør det «mulig å anta at en alvorlig trussel kan forutsees». Det er derfor tilstrekkelig at det foreligger en generell trusselsituasjon av en bestemt art. Dette underbygges videre av at en tillatelse til speiling kan gis over en lengre periode og om nødvendig fornyes. Det kan derfor ikke oppstilles et krav til at trusselen er reell og aktuell, men det er tilstrekkelig at den kan forutses.

I forarbeidene er det gitt uttrykk for samme terskel som LQN, jf. de generelle merknadene i Prop. 92 L (2022-2023) side 39 flg:

> Departementet understreker at et krav om konkrete bevis for at det foreligger en alvorlig trussel ikke er anvendelig for et bulkinnhentingssystem for utenlandsetterretningsformål. Departementet viser til EMDs uttalelse i *Centrum för rättvisa mot Sverige* om at straffeprosessuelle krav ikke egner seg for forebyggende lagring i bulk, se punkt 5.2.3 ovenfor. Departementet viser videre til at en sentral oppgave for Etterretningstjenesten er å avdekke hittil ukjente trusler mot Norge. Dersom Etterretningstjenesten utelukkende skal innhente informasjon om kjente trusler og kjent truende aktivitet, så vil den ikke evne å avdekke fremtidige trusler *rettidig*. Det vil gi utenlandske trusselaktører et langt friere spillerom og det vil frata norske myndigheter og beslutningstakere en avgjørende kilde til informasjon om utenlandske trusler og forhold av betydning for nasjonal sikkerhet. Man kan således ikke vente med å speile kommunikasjonsstrømmene til man har håndfaste bevis for at en konkret trussel foreligger. Tvert imot må speilingen skje forebyggende og i forkant når det kan påvises at det generelle trusselbildet i en digitalisert verden tilsier at speiling er nødvendig for å etablere et informasjonsgrunnlag som gjør at Etterretningstjenesten kan utføre sine oppgaver.

Tilsvarende fremgår av spesialmerknadene til bestemmelsen:

> Etterretningstjenesten må opplyse retten om hvilke omstendigheter og andre relevante forhold som begrunner speiling på begjæringstidspunktet. Hva som er å anse som *relevante forhold*, må ses i sammenheng med Etterretningstjenestens oppgaver, som blant annet er å *rettidig* avdekke trusler eller forhold som kan utvikle seg til å bli trusler – det vil si på et tidspunkt hvor det for andre fremdeles er ukjent at det er omstendigheter i utlandet som utgjør en trussel eller som har et trusselpotensiale som nevnt. Det kan dermed være begrenset hvor konkret beskrivelsen av trusselen eller trusselpotensialet kan bli. For eksempel må det

> aksepteres at Etterretningstjenesten begrunner en speilingsbegjæring med at det foreligger en generell trussel knyttet til cyberspionasje eller fremmede staters påvirkningsoperasjoner, uten at denne kan knyttes til et kjent mål. Det vil ikke være nødvendig å dokumentere at en trusselaktør utøver pågående trusselaktivitet mot Norge eller norske interesser på begjæringstidspunktet, dersom Etterretningstjenestens faglige vurderinger og analyser understøtter at omstendighetene kan utvikle seg i denne retningen.

Endelig viser retten til at Borgarting lagmannsrett i avgradert avgjørelse som er fremlagt i saken, fant at de norske bestemmelsene oppfyller kriteriene som EU-domstolen har oppstilt:

> (…) Det er etter lagmannsrettens vurdering uansett forsvarlig å legge til grunn at de norske bestemmelsene om bulkinnsamling av rådata ved speiling, med tilhørende lagring av metadata, oppfyller det alvorlighetskriteriet som EU-domstolen har trukket opp. De generelle truslene mot norske sikkerhetsinteresser som er beskrevet i begjæringen i saken her, må betegnes som alvorlige og med risiko for at de kan bli realisert.

Stiftelsen har videre anført at EU-domstolen oppstiller krav om at lovgivingen inneholder «clear and precise rules». Retten nøyer seg her med å vise til det som er sagt ovenfor under drøftelsen om forholdet til EMK, jf. punkt 3.4.3.2 ovenfor.

3.6.3.3 Skjer lagringen for lengere tid enn nødvendig?

Stiftelsen har vist til at EU-domstolen har oppstilt krav om at lagringen må være tidsbegrenset («forseeable period of time») og begrenset til det som er strengt nødvendig («limited in time to what is strictly necessary»). Lagringen må heller ikke være «systematic in nature». På denne bakgrunn mener Stiftelsen av e-tjenesteloven § 8-6 som setter en lengstefrist på to år ikke er i samsvar med EU-domstolens krav.

Retten er ikke enig i dette. Uttrykket «forseeable period of time» gir ingen anvisning om en konkret lengde utover at tidsperioden tiltaket varer, må være forutsigbar. Dette gir den enkelte stat en viss skjønnsmargin til å fastsette tidsrammene for tiltaket.

Retten har ovenfor redegjort for lovens § 8-6 hvor det er gitt lengstefrister for de ulike tiltak. Lengstefristen for speiling etter § 7-3 første ledd er satt til to år og retten mener at dette ligger innenfor uttrykket «forseeable period of time». Det fremgår imidlertid av bestemmelsen at rettens tillatelse ikke skal gis for lengere tid enn nødvendig. Retten skal dermed innenfor rammene av lengstefristen avgjøre tillatelsens varighet i den enkelte sak utfra det som er nødvendig.

Retten viser også her til avgradert kjennelse fra Borgarting lagmannsrett (side 13-14) hvor vilkåret ble vurdert:

Det styrende for tidsbegrensningen av speilingstillatelsen må være de etterretningsmessige behovene som begrunner tillatelsen. Hvis det er grunn til å tro at disse behovene vil kunne variere vesentlig over tid, kan det tilsi at speilingstillatelsen revurderes etter relativt kort tid.

3.6.3.4 Er sikkerhetsmekanismene tilstrekkelige?

Stiftelsen har også reist spørsmål om EU-domstolens krav om sikkerhetsmekanismer og uavhengig kontroll i LQN avsnitt 132, jf. ovenfor, er tilstrekkelig regulert i den norske loven.

Etter rettens syn vil kravet om å innhente tillatelse fra retten om speiling i den konkrete sak, sammenholdt med løpende og etterfølgende kontroll, klart oppfylle kravet om sikkerhetsmekanismer for å forhindre misbruk. Retten nøyer seg her med å vise til det som er sagt ovenfor i punkt 3.4.6.

3.7 Oppsummering

Retten har ovenfor kommet til at de norske reglene for tilrettelagt innhenting i e-tjenesteloven er i samsvar med de krav som oppstilles av EMD etter EMK artikkel 8.

Reguleringen av TI er basert på tilgjengelige, detaljerte regler med et klart definert formål og det fremgår klart av loven i hvilke tilfeller innhenting av kommunikasjonen kan skje. Det er i saken ikke anført at prosedyrene for tillatelse til speiling, seleksjon, analyse og bruk av innhentede data er i strid med de krav som er oppstilt og retten legger til grunn at disse også er i samsvar med kravene. Retten har videre kommet til at loven fastsetter klare regler om lagring og sletting av innhentet kommunikasjon.

EMD oppstiller også krav til rettssikkerhetsgarantier i alle ledd («end-to-end safeguards») for å hindre misbruk. Disse rettssikkerhetsgarantiene består dels av at det må gis tillatelse fra domstolen for å gjennomføre ulike tiltak og dels av løpende og etterfølgende kontroll av de tiltak som iverksettes. Retten mener at det er en svakhet ved den etterfølgende kontroll av et tiltak ved at en klager har begrensede muligheter til å få fastslått om det har skjedd en rettighetskrenkelse. Det kan derfor reises spørsmål ved om det foreligger et tilstrekkelig effektiv rettsmiddel. Retten har imidlertid etter en samlet vurdering kommet til at rettssikkerhetsgarantiene er tilstrekkelige og at det derfor ikke foreligger brudd på EMK artikkel 8.

Retten har videre kommet til at reglene om tilrettelagt innhenting er i samsvar med de krav EMD har oppstilt etter EMK artikkel 10 om kildevernet og EU-domstolens krav etter kommunikasjonsverndirektivet.

Retten har endelig kommet til at saksøkerne ikke har rettslig interesse i å få fastsettelsesdom for at staten er uberettiget til å innhente, lagre og behandle elektronisk

kommunikasjon innhentet i bulk ved midtpunktinnhenting og endepunktinnhenting etter e-tjenesteloven §§ 6-9 og 6-10 (krav 2). Dette kravet skal følgelig avvises.

4. Sakskostnader

Staten v/ Forsvarsdepartementet har vunnet saken og har krav på erstatning for sine sakskostnader, jf. tvisteloven § 20-2 (1) og (2). Etter rettens syn foreligger det ikke slike tungtveiende grunner som gjør det rimelig å frita saksøkerne for kostnadsansvaret, jf. tvisteloven § 20-2 (3).

Statens prosessfullmektig har fremlagt en salæroppgave på til sammen 407 000 kroner. Det har ikke kommet innsigelser til beløpets størrelse. Til sammenligning har saksøkerne fremlagt en kostnadsoppgave på 3 843 100 kroner. Retten finner at kostnadene er rimelige og nødvendige, jf. tvisteloven § 20-5, og retten legger kravet til grunn.

DOMSSLUTNING

1. Kravet i saksøkernes påstand pkt. 2 avvises.
2. For øvrig frifinnes staten ved Forsvarsdepartementet.
3. Stiftelsen Tinius og Tom Erik Thorsen dømmes til i fellesskap å betale 407 000 – firehundreogsjutusen – kroner til staten ved Forsvarsdepartementet.
   Oppfyllelsesfristen er på 2 – to – uker.

Retten hevet

Yngvild Thue

Veiledning om anke i sivile saker vedlegges.

Veiledning om anke i sivile saker

I sivile saker er det reglene i tvisteloven kapitler 29 og 30 som gjelder for anke. Reglene for anke over dommer, anke over kjennelser og anke over beslutninger er litt ulike. Nedenfor finner du mer informasjon og veiledning om reglene.

Ankefrist og gebyr
Fristen for å anke er én måned fra den dagen avgjørelsen ble gjort kjent for deg, hvis ikke retten har fastsatt en annen frist. Disse periodene tas ikke med når fristen beregnes (rettsferie):

- fra og med siste lørdag før palmesøndag til og med annen påskedag
- fra og med 1. juli til og med 15. august
- fra og med 24. desember til og med 3. januar

Den som anker, må betale behandlingsgebyr. Du kan få mer informasjon om gebyret fra den domstolen som har behandlet saken.

Hva må ankeerklæringen inneholde?
I ankeerklæringen må du nevne

- hvilken avgjørelse du anker
- hvilken domstol du anker til
- navn og adresse på parter, stedfortredere og prosessfullmektiger
- hva du mener er feil med den avgjørelsen som er tatt
- den faktiske og rettslige begrunnelsen for at det foreligger feil
- hvilke nye fakta, bevis eller rettslige begrunnelser du vil legge fram
- om anken gjelder hele avgjørelsen eller bare deler av den
- det kravet ankesaken gjelder, og hvilket resultat du krever
- grunnlaget for at retten kan behandle anken, dersom det har vært tvil om det
- hvordan du mener at anken skal behandles videre f.eks. om det bør være muntlig behandling i rettsmøte, skriftlig behandling og/eller rettsmekling.

Hvis du vil anke en tingrettsdom til lagmannsretten
Dommer fra tingretten kan ankes til lagmannsretten. Du kan anke en dom hvis du mener det er

- feil i de faktiske forholdene som retten har beskrevet i dommen
- feil i rettsanvendelsen (at loven er tolket feil)
- feil i saksbehandlingen

Hvis du ønsker å anke, må du sende en skriftlig ankeerklæring til den tingretten som har behandlet saken. Hvis du fører saken selv uten advokat, kan du møte opp i tingretten og anke muntlig. Retten kan tillate at også prosessfullmektiger som ikke er advokater, anker muntlig.

Det er vanligvis en muntlig forhandling i lagmannsretten som avgjør en anke over en dom. I ankebehandlingen skal lagmannsretten konsentrere seg om de delene av tingrettens avgjørelse som er omtvistet, og som det er knyttet tvil til.

Lagmannsretten kan nekte å behandle en anke hvis den kommer til at det er klar overvekt av sannsynlighet for at dommen fra tingretten ikke vil bli endret. I tillegg kan retten nekte å behandle noen krav eller ankegrunner, selv om resten av anken blir behandlet.

<u>Retten til å anke er begrenset i saker som gjelder formuesverdi under 250 000 kroner</u>
Hvis anken gjelder en formuesverdi under 250 000 kroner, kreves det samtykke fra lagmannsretten for at anken skal kunne bli behandlet.

Når lagmannsretten vurderer om den skal gi samtykke, legger den vekt på

- sakens karakter
- partenes behov for å få saken prøvd på nytt
- om det ser ut til å være svakheter ved den avgjørelsen som er anket, eller ved behandlingen av saken

Hvis du vil anke en tingretts kjennelse eller beslutning til lagmannsretten
En *kjennelse* kan du som hovedregel anke på grunn av

- feil i de faktiske forholdene som retten har beskrevet i kjennelsen
- feil i rettsanvendelsen (at loven er tolket feil)
- feil i saksbehandlingen

Kjennelser som gjelder saksbehandlingen, og som er tatt på bakgrunn av skjønn, kan bare ankes dersom du mener at skjønnsutøvelsen er uforsvarlig eller klart urimelig.

En *beslutning* kan du bare anke hvis du mener
- at retten ikke hadde rett til å ta denne typen avgjørelse på det lovgrunnlaget, eller
- at avgjørelsen åpenbart er uforsvarlig eller urimelig

Hvis tingretten har avsagt dom i saken, kan tingrettens avgjørelser om saksbehandlingen ikke ankes særskilt. Da kan dommen isteden ankes på grunnlag av feil i saksbehandlingen.

Kjennelser og beslutninger anker du til den tingretten som har avsagt avgjørelsen. Anken avgjøres normalt ved kjennelse etter skriftlig behandling i lagmannsretten.

Hvis du vil anke lagmannsrettens avgjørelse til Høyesterett
Høyesterett er ankeinstans for lagmannsrettens avgjørelser.

Anke til Høyesterett over *dommer* krever alltid samtykke fra Høyesteretts ankeutvalg. Samtykke gis bare når anken gjelder spørsmål som har betydning utover den aktuelle saken, eller det av andre grunner er særlig viktig å få saken behandlet av Høyesterett. Anke over dommer avgjøres normalt etter muntlig forhandling.

Høyesteretts ankeutvalg kan nekte å ta anker over *kjennelser* og *beslutninger* til behandling dersom anken ikke reiser spørsmål av betydning utover den aktuelle saken, og heller ikke andre hensyn taler for at anken bør prøves. Anken kan også nektes fremmet dersom den reiser omfattende bevisspørsmål.

Når en anke over kjennelser og beslutninger i tingretten er avgjort ved kjennelse i lagmannsretten, kan avgjørelsen som hovedregel ikke ankes videre til Høyesterett.

Anke over lagmannsrettens kjennelser og beslutninger avgjøres normalt etter skriftlig behandling i Høyesteretts ankeutvalg.