GLITTERTIND

Oslo tingrett
Via Aktørportalen

Oslo, 6. mars 2024
Sak nr.: 10589-507
Dok.nr.: 6DZNQ6CFDSAV-1000408783-127
Ansvarlig advokat: Jon Wessel-Aas

STEVNING
TIL
OSLO TINGRETT

Sak nr.:	[sak nr.]
Saksøker 1:	Stiftelsen Tinius v/styrets leder, org.nr. 976 472 667 Olav Vs gate 5, 0161 Oslo
Saksøker 2:	Tom Erik Thorsen Dalsbottenlia 8, 3726 Skien
Partshjelpere:	1. Norsk Redaktørforening 2. Norsk Presseforbund 3. Norsk Journalistlag 4. Mediebedriftenes Landsforening 5. Den norske Forleggerforening 6. Norsk Pen 7. Norsk Faglitterær Forfatter- og oversetterforening
Prosessfullmektiger for alle:	Advokat Jon Wessel-Aas og advokat Emanuel Feinberg Advokatfirmaet Glittertind AS
Rettslig medhjelper:	Advokatfullmektig Elmira Oshnavie Advokatfirmaet Glittertind AS
Saksøkt:	Staten v/Forsvarsdepartementet Postboks 8005 Dep. 0030 Oslo
Prosessfullmektig:	Foreløpig ingen

Saken gjelder: Vilkårlig og ulovlig digital masseovervåkning og bulkinnsamling av elektronisk kommunikasjon, etter etterretningstjenesteloven.

INNHOLD

1 INNLEDNING

1.1 Kort om søksmålet

1.1.1 Generelt

Stiftelsen Tinius og Tom Erik Thorsen anlegger søksmål mot staten ved Forsvarsdepartementet, med Oslo tingrett som rett verneting.

Søksmålet gjelder omfattende og vilkårlig digital masseovervåkning av personer i Norge med hjemmel i nye bestemmelser i etterretningstjenesteloven. Denne overvåkning skjer gjennom bulkinnsamling, lagring og innsyn i informasjon om borgernes, herunder saksøkernes, elektroniske kommunikasjon. Det anføres at disse overvåkningstiltakene krenker saksøkernes personvern og ytringsfrihet etter Grunnloven, Den europeiske menneskerettskonvensjonen (EMK) og EØS-retten.

Det kreves dom for at staten v/Forsvarets etterretningstjeneste (E-tjenesten) er uberettiget til å innhente, lagre og behandle informasjon etter de aktuelle hjemlene. I tillegg kreves det dom for at det som hittil er innhentet og lagring av opplysninger ved bruk av de samme hjemlene må slettes.

1.1.2 Tilrettelagt innhenting

For det første gjelder søksmålet de nye reglene i etterretningstjenesteloven kapittel 7 om tilrettelagt innhenting (TI), som gir Etterretningstjenesten (E-tjenesten) mulighet til å samle inn, lagre og lese all datatrafikk som krysser den norske grensen.[1] Det omfatter også kommunikasjon mellom personer som befinner seg i Norge, ettersom det aller meste av elektronisk kommunikasjon i Norge går via utenlandske servere. Dette innebærer at informasjon om store deler av privat kommunikasjon mellom personer som befinner seg i Norge og det meste som personer i Norge foretar seg på internett kan innsamles, lagres og leses av norske myndigheter. Forsvarsdepartementet er ansvarlig myndighet for E-tjenesten og er i tillegg det departementet som har ansvaret for etterretningstjenesteloven. E-tjenesten har et årlig budsjett på 3 milliarder kroner og minst 2 000 ansatte.

Konsekvensen av E-tjenestens nye overvåkningshjemmel, er at store deler av norske borgeres digitale liv kunne bli hentet inn og lagret av norske myndigheter. Det vil ikke lenger være mulig å opprettholde et privatliv overfor myndighetene. Denne krenkelsen av retten til privatliv og personvern henger nært sammen med pressens kildevern, ettersom hvem som helst av oss kan være pressens kilder, og fordi den omfattende digitale overvåkningen fører til at det ikke lengre vil være mulig å ha tillit til at digital kommunikasjon med journalister er fortrolig.

Illustrerende for hvor inngripende tiltaket er, er at Lysne II-utvalget som på oppdrag fra Forsvarsdepartementet, med E-tjenesten selv som utvalgets sekretariat, i sin tid utredet det systemet – den gang benevnt Digitalt grenseforsvar (DGF) - som nå er realisert i E-tjenesteloven, i de

[1] Lov om Etterretningstjenesten (LOV-2020-06-19-77).

avsluttende deler av utredningen fant grunn til å peke på behovet for en form for dødmannsknapp, dersom et slikt system ble realisert:[2]

> *«En særskilt problemstilling er knyttet til en potensiell fremtidig ikke-demokratisk maktovertakelse. Det bør utvikles mekanismer og rutiner for både sletting av all informasjon lagret i DGF, og for ødeleggelse av DGF-utstyret. Disse mekanismene og rutinene bør innrettes slik at det kan iverksettes ved ikke-demokratisk maktovertakelse.»*

Lignende lovgivning i andre europeiske land har blitt underkjent av Den europeiske menneskerettsdomstolen (EMD) og EU-domstolen. EMD kom i storkammerdommene henholdsvis Centrum för rättvisa mot Sverige[3] og Big Brother Watch m.fl. mot Storbritannia[4] til at henholdsvis den svenske og britiske etterretningstjenestes overvåkningsregime med bulkinnsamling av kommunikasjonsdata var i strid med Den europeiske menneskerettskonvensjon (EMK) artikkel 8 og artikkel 8 og 10.

EU-domstolen har blant annet i dommene La Quadrature du Net[5] og Privacy International[6] kommet til at britisk, fransk og belgisk lovgivning som pålegger ekomtilbydere å lagre eller overføre data til sikkerhets- og etterretningstjenester av hensyn til nasjonal sikkerhet er i strid med EUs kommunikasjonsverndirektiv (2002/58/EC)[7] – et direktiv også Norge er bundet av, og som er gjennomført i ekomloven[8] med forskrifter.

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

1.1.3 Midpunktinnhenting og endepunktinnhenting

Søksmålet omfatter videre deler av E-tjenesteloven kapittel 6; nærmere bestemt paragrafene 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 hvilken som helst annet overføringsmedium og uavhengig av teknologi, mens kommunikasjonen er i transitt mellom avsender og mottaker. Slik innhenting vil også omfatte bulkinnhenting av kommunikasjonsdata.

---

[2] Lysne II-utvalget, Digitalt grenseforsvar, rapport levert til Forsvarsdepartementet 26. august 2016, punkt 9.5.5.
[3] Centrum för rättvisa mot Sverige, no. 35252/08, i storkammer, [2021].
[4] Big Brother Watch mot Storbritannia, no. 58170/13, 62322/14, 24960/15, I storkammer[2021].
[5] Dom av 6. oktober 2020, *La Quadrature du Net,* C-511/18, C-512/18 og C-520/18, ECLI:EU:C:2020:791.
[6] Storkammerom av 6. oktober 2020, *Privacy International,* C-623/17, ECLI:EU:C:2020:790.
[7] Europaparlaments- og rådsdirektiv 2002/58/EF av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon.
[8] Lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon

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. Det er presisert i forarbeidene at bestemmelsen ikke inneholder avgrensninger med hensyn til teknologi, slik at den gjelder uavhengig både av hvilke «endepunkter» (der informasjon ligger lagret) den gjelder og av på hvilken måte E-tjenesten får tilgang til avlesning og innhenting (bortsett fra at eventuelle pålegg om tilrettelegging fra tjenestetilbydere av kommunikasjonstjenester må følge reglene i kapittel 7). Bestemmelsen hjemler også innhenting av rådata i bulk.

Heller ikke disse tiltakene tilfredsstiller Grunnlovens og EMKs krav til lovlige inngrep i ytringsfriheten og personvernet – og en grunnleggende mangel i den sammenheng, er at metodene kan brukes uten noen som helst forhåndsgodkjennelse eller prøving av retten eller tilsvarende uavhengig judisiell kontroll.

1.1.4 Kjøp av metadata i bulk

Som omtalt nærmere nedenfor, ble det gjennom EOS-utvalgets årsmelding for 2022[9] kjent at E-tjenesten, i påvente av at reglene om TI skulle vedtas/settes i kraft, kjøpt metadata i bulk fra kommersielle aktører. Det kreves dom for at E-tjenestens behandling og lagring av kommunikasjonsdata etter *kjøp* av metadata i bulk må opphøre, da denne virksomheten, som også påpekt av EOS-utvalget, fullstendig mangler grunnforutsetningen for inngrep i ytringsfriheten og personvernet: lovhjemmel.

1.2 Videre opplegg

I punkt 2 er saksøker 1, Stiftelsen Tinius og dens formål og virksomhet nærmere omtalt. I samme punkt presenteres også saksøker 2, Tom Erik Thorsen, nærmere.

I punkt 3 kommenteres søksmålsvilkårene i tvisteloven.

I punkt 4 gis en kort omtale av sakens bakgrunn, herunder en omtale av etterretnings- og overvåkningstjenestene i Norge og det overordnede regelverket for tjenestene.

I punkt 5 gis en overordnet oversikt over statens menneskerettslige forpliktelser etter Grunnloven og EMK, inkludert en kort gjennomgang av de mest relevantene dommene fra EMD av betydning for saken. I punkt 6 gis på tilsvarende måte en overordnet oversikt over Norges forpliktelser etter EØS-retten og en kort gjennomgang av de mest relevante dommene fra EU-domstolen. Dette for å gi en overordnet rettslig ramme, før vi begrunner nærmere hvorfor Grunnloven, EMK og EØS-retten er krenket.

[9] EOS-utvalgets årsmelding til Stortinget - Dokument 7:1 (2022–2023).

I punkt 7 redegjøres det kort for saksøkers anførsler knyttet til hvorfor etterretningstjenesteloven kapittel 7 er i strid med de overnevnte reglene. I punktene henholdsvis 8 og 9 gjøres tilsvarende med hensyn til henholdsvis midtpunktinnhenting/endepunktinnhenting og kjøp av metadata i bulk.

2 KORT OM SAKSØKERNE

2.1 Stiftelsen Tinius

Stiftelsen Tinius ble etablert i 1996 for å videreføre Schibsted som mediekonsern. Stiftelsen kontrollerer den største aksjeposten i Schibsted (gjennom det heleide selskapet Blommenholm Industrier AS), som gir stiftelsen negativ kontroll med Schibsted.[10] Schibsted omfatter blant annet store medier som Aftenposten, Verdens Gang og Bergens Tidende i Norge og Aftonbladet og Svenska Dagbladet i Sverige. Opprettelsen av stiftelsen Tinius utgjør en særskilt garanti for frihet og uavhengighet for Schibsteds aviser og massemedier. Et hovedelement i retningslinjene fastlagt i Stiftelsen Tinius vedtekter er at Schibstedkonsernet skal videreføres som mediekonsern, og drives etter de redaksjonelle og forretningsmessige hovedlinjer som ble lagt til grunn ved opprettelsen av konsernet.

Av stiftelsens formål i vedtektene § 3, fremgår det at å sikre frie og uavhengige redaksjoner og rammebetingelser for frie og uavhengige medier er sentralt i stiftelsens virke:

> *«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.»*

Bilag 1: Stiftelsen Tinius' vedtekter

Pressens kildevern er en grunnleggende forutsetning for frie og uavhengige medier, og blant de viktigste rammebetingelsene mediere opererer under. Stiftelsen mener at den nye overvåkningslovgivningen uthuler ytringsfriheten og undergraver kildevernet, og derfor skader pressens arbeid. Et trygt kildevern er avgjørende for journalistisk virksomhet og kvalitet. Stiftelsen mener at lovene vil ha en nedkjølende effekt på norske borgeres ønske om å ytre seg og vil ha store konsekvenser for samfunnet og demokratiet. Kilder vil ikke lenger kunne ha mulighet og tillit til at

[10] Stiftelsen er p.t. i sluttforhandlinger om en avtale om å overta som 100 prosent eier av hele Schibsteds medievirksomhet, og vil derfor – formodentlig – være eneeier av Schibsted Media i løpet av 2024, jf. pressemelding av 11. desember 2023: https://www.tinius.com/no/nyheter/stiftelsen-tinius-vil-kjope-schibsteds-nyhetsmedier.

de kan ha fortrolig kommunikasjon med journalister, noe som er svært skadelig for pressens virksomhet.

Stiftelsen er opptatt av å tydelig definere Schibsteds samfunnsansvar og -påvirkning, og støtter selskapets nåværende visjon om å bidra til et samfunn basert på åpenhet og tillit. Stiftelsens aktive eierskap i Schibsted er som nevnt blant annet styrt av formålet om å sikre «kvalitet og troverdighet i alle Schibsteds tjenester og produkter, og garantere for fri og uavhengig journalistikk» og «påvirke de rammebetingelser som er vesentlig for å sikre frie og uavhengige redaksjoner».

Som nyere eksempel fra Stiftelsen Tinius' arbeid nevnes at det var stiftelsen som i 2022 klaget TikTok inn til Datatilsynet. Stiftelsen har videre engasjert seg i arbeidet mot produksjon og spredning av falske nyheter, blant annet ved å bidra økonomisk til opprettelsen av faktisk.no. Det var videre stiftelsen som sammen med Amedia-stiftelsen tok initiativet til og ledet kampanjen #ettminnutt om ytringsfrihet, pressefrihet og troverdige medier. Stiftelsen kommuniserer med, samarbeider med og støtter dessuten en rekke organisasjoner/institusjoner/personer både innenlands og utenlands, som jobber for frie medier og pressefrihet.

I tillegg til at lovgivningen som åpner for masseovervåkning av norske borgere, kommer i konflikt med kjernen i de verdier stiftelsen har til formål å sikre, blir Stiftelsen Tinius' egen virksomhet rammet av tiltakene. Stiftelsen kommuniserer for eksempel med medier i stater der pressefriheten er under sterkt press, og rammes hardt av at E-tjenesten nå får tilgang til denne kommunikasjonen. Videre rammes stiftelsens virksomhet ved at E-tjenesten kan få tilgang til det meste av «innenlandskommunikasjonen» internt i stiftelsen, med stiftelsens virksomheter og eksternt til andre, ettersom det meste av digital kommunikasjon i Norge går via utenlandske servere.

2.2 Tom Erik Thorsen

Tom Erik Thorsen er i tillegg til å være en norsk borger bosatt i Norge, ansvarlig redaktør for avisen/mediet Varden, utgitt av Varden AS.

Thorsen berøres direkte av det angrepne overvåkningstiltaket, ved at det gjøres samme inngrep i hans personvern og ytringsfrihet som det gjøres overfor enhver borger. Videre berøres han direkte i sin funksjon som redaktør, ved at det de delene av det angrepne overvåkningstiltaket som gjør inngrep i pressens kildevern, dermed gjør et inngrep i pressefriheten som han utøver og er avhengig av i sitt virke som redaktør.

3 KRAVET FRA SAKSØKERNE OPPFYLLER TVISTELOVEN § 1-3, JF. § 1-4

3.1 Oversikt

Saksøkerne og deres krav oppfyller vilkårene i tvisteloven §§ 1-3, jf. § 1-4 etter intern norsk rett og etter folkerettslige regler, jf. tvisteloven § 1-2.

Først vil vi påvise at søksmålet skal fremmes etter internrettslige regler om søksmålsadgang. Deretter vil vi påvise at folkeretten gir selvstendig grunnlag for å fremme søksmålet, jf. tvisteloven § 1-2.

3.2 Søksmålet skal fremmes etter internrettslige regler om søksmålsadgang

De relevante vilkårene for å vurdere om saken skal fremmes er oppstilt i tvisteloven §§ 1-3 og 1-4. Søksmålet må gjelde et «rettskrav», og rettskravet må ha tilstrekkelig «aktualitet», I tillegg må partene ha tilstrekkelig «tilknytning» til søksmålsgjenstanden, jf. HR-2021-417-P (Acer), avsnitt 121.

Tilknytningskravet inviterer ikke til nærmere drøftelse: Staten har utvilsomt *passiv søksmålskompetanse* som overvåkende myndighet. Stiftelsen Tinius har *aktiv søksmålskompetanse* ved å være direkte berørt som følge av at stiftelsens egen kommunikasjon omfattes av tiltakene saken gjelder, jf. tvisteloven § 1-3. I tillegg ligger søksmålet «innen [stiftelsens] formål og naturlige virkeområde å ivareta», jf. tvisteloven § 1-4. Tiltakene som angripes har vesentlige negative virkninger for ytringsfriheten generelt og redaksjoners adgang til å virke fritt, som stiftelsen skal arbeide for å ivareta. Thorsen berøres både ved at tiltakene treffer ham som alminnelige samfunnsborger og særskilt som følge av hans virke som redaktør og journalist.

Kravene til *aktualitet* og *rettskrav* vil i en sak som dette glid over i hverandre, sml. HR-2021-417-P (Acer) avsnitt 125. Høyesteretts konkluderte der med at det er adgang til å fremme søksmål av mer generell karakter dersom forholdene ligger til rette for det. I tråd med avsnitt 173 i kjennelsen må det foreligge «særlig behov for rettslig avklaring» og «rettsspørsmålet [må] egne seg til å bli prøvd i en generell form». Denne vurderingen beror på en helhetsvurdering, der Høyesterett har fremhevet følgende som særlige relevante momenter (avsnitt 174):

- Reiser søksmålet uavklarte rettsspørsmål av prinsipiell rekkevidde?
- Er det vanskelig eller klart uhensiktsmessig å få spørsmålet prøvd på en mer konkret måte?
- Vil spørsmålet bli godt nok opplyst ved å tillate søksmålet nå og i denne formen, eller vil domstolene få et bedre grunnlag for å avgjøre saken dersom den fremmes i en mindre generell form?
- Hvor generelt er kravet som gjøres gjeldende – knytter det seg til et konkret og avgrenset faktum?

Det er ingen tvil om at søksmålet reiser uavklarte rettsspørsmål av stor prinsipiell rekkevidde. De muligheter dagens informasjonsteknologi gir for overvåkning, og de personverns- og ytringsfrihetsspørsmål bruken av disse mulighetene reiser, er viktige samfunnsspørsmål. De tiltakene søksmålet gjelder var gjenstand for omfattende debatt ved lovens innføring og det ble rettet betydelig kritikk mot innføringen.

Videre gjør tiltakenes karakter at søksmålet ikke kan fremmes på en mer konkret måte. Overvåkningen skjer i det skjulte uten mulighet for offentlig innsyn og kontroll. Det vil dermed ikke være mulig å fremme søksmålet knyttet til konkret utøvelse av regelverket.

Spørsmålet i saken er godt opplyst ved den overvåkningen loven tillater og rammene for denne, og det er uansett ikke mulig å fremme saken på en annen måte som gjøre saken blir bedre opplyst. Søksmålet er knyttet til konkretisert og avgrenset atferd (konkretisert innhenting av informasjon etc.) og spørsmålet om denne er lovlig.

3.3 Søksmålet må fremmes etter folkerettslige regler

3.3.1 EMK

Saksøkerne gjør gjeldene at overvåkningen loven gir grunnlag for krenker deres rettigheter etter EMK.

For EMD er det normalt ikke adgang til å fremme representative søksmål med abstrakt prøving av lovgivning. For prøving av lovgivning som gir grunnlag for generell overvåkning uten annen reell mulighet for overprøving har imidlertid EMD gjort unntak. Centrum för rättvisa mot Sverige er et eksempel på dette. EMD drøftet der klagerens status som «victim» i dommens avsnitt 166 – 177, og EMD oppsummerte slik i avsnitt 175 – 177:

> *"175. In the context of the issue of victim status, without prejudice to the conclusions to be drawn in respect of the substantive requirements of Article 8 § 2 and Article 13 in the present case, the Court notes that the domestic remedies available in Sweden to persons who suspect that they are affected by bulk interception measures are subject to a number of limitations. In the Court's view, even if these limitations are to be considered inevitable or justified, the practical result is that the availability of remedies cannot sufficiently dispel the public's fears related to the threat of secret surveillance.*
>
> *176. It follows that it is not necessary to examine whether the applicant, due to its personal situation, is potentially at risk of seeing its communications or related data intercepted and analysed.*
>
> *177. On the basis of the above considerations the Court finds that an examination of the relevant legislation in abstracto is justified. The Government's objection that the applicant may not claim to be the victim of a violation of his or her Convention rights allegedly occasioned by the mere existence of Swedish bulk interception legislation and activities is therefore rejected."*

Begge saksøkerne vil på denne bakgrunn være aksepterte rettighetssubjekter under EMK og ha krav på få ivaretatt sine rettigheter for EMD. Subsidiaritetsprinsippet, jf EMK artikkel 13, innebærer at rettighetshavere etter EMK må få prøve sine krav for nasjonale domstoler først. Dette innebærer at norske domstoler må fremme saken til behandling, jf tvisteloven § 1-4.

3.3.2 EØS-avtalen

Saksøkerne gjør også gjeldende at tiltakene er i strid med Norges forpliktelser etter EØS-avtalen. Det følger av det EØS-rettslige effektivitetsprinsippet at borgere har krav på få håndhevet anførte krenkelser av EØS-retten for domstolene. I motsatt fall vil det ikke finnes noen effektive virkemidler for å sikre at borgernes rettigheter blir ivaretatt.

Ettersom det ikke er noen annen måte saksøkerne kan få rettslig prøving av om overvåkningen krenker deres rettigheter etter EØS-avtalen enn et søksmål som dette, krever også det EØS-rettslige effektivitetsprinsippet at søksmålet må fremmes, jf. tvisteloven § 1-2.

4 SAKENS BAKGRUNN

4.1 EOS-tjenestene i Norge

E-tjenesten, PST og Nasjonal sikkerhetsmyndighet (NSM) utgjør de såkalte etterretnings-, overvåkings og sikkerhetstjenestene (EOS-tjenestene) i Norge. De tre tjenestene har flere samarbeidsarenaer som Felles cyberkoordineringssenter (FCKS) og Felles etterretnings- og kontraterrorsenter (FEKTS), hvor tjenestene sammenstiller kunnskap og koordinerer bruk av ressurser.[11]

E-tjenesten er Norges nasjonale utenlandsetterretningstjeneste, og er underlagt Forsvaret. Om E-tjenestens virksomhet vises det til E-tjenestens trusselvurdering, Fokus fra 2023[12] og 2024[13].

NSM er Norges direktorat for forebyggende nasjonal sikkerhet. Direktoratet gir råd om sikring av informasjon, systemer, objekter og infrastruktur av nasjonal betydning, og gjennomfører tilsyn og andre kontrollaktiviteter på sivil og militær side. NSM har også et nasjonalt ansvar for å avdekke, varsle og koordinere håndtering av alvorlige IKT-angrep.

4.2 Etterretningstjenestelovens regler om tilrettelagt innhenting

Lov 19. juni 2020 nr. 77 om Etterretningstjenesten (etterretningstjenesteloven) avløste den tidligere etterretningstjenesteloven av 1998. I den nye etterretningstjenesteloven ble blant annet en ny form for innhenting av informasjon gjort tilgjengelig for E-tjenesten, såkalt «tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon» (TI), regulert i lovens nye kapittel 7.

Lovteksten beskriver kommunikasjonen som omfattes av tilrettelagt innhenting som «elektronisk kommunikasjon som transporteres over den norske grensen». Dette er under dagens forutsetninger ment å omfatte kommunikasjon som transporteres gjennom fiberoptiske kabler over den norske landegrensen, det vil si via internett, se Prop. 80 L (2019–2020) s. 213 og Forsvarsdepartements høringsnotat s. 208.[14] Ettersom lovteksten er gitt en teknologinøytral utforming, omfattes også andre teknologier som bidrar til at elektronisk kommunikasjon transporteres over den norske grensen, der det er nødvendig at ekomtilbydere legger til rette for innhentingen.

Lovendringene som ble innført innebærer at E-tjenesten er gitt adgang til bulkinnsamling av, lagring av og søk i både metadata og innholdet i *all elektronisk kommunikasjon* som krysser Norges

[11] «Om Etterretnings-tjenesten» hentet fra E-tjenestens hjemmeside.
[12] Fokus 2023 (etterretningstjenesten.no).
[13] Fokus 2024 - Etterretningstjenesten.
[14] Forsvarsdepartements høringsnotat av 12. november 2018.

geografiske grenser. Dette omfatter det meste av elektronisk kommunikasjon mellom personer som oppholder seg i Norge, ettersom det aller meste av kommunikasjonsdata fra Norge går via utenlandske servere.

Den nye etterretningstjenesteloven trådte i kraft 1. januar 2021, med unntak av kapittel 7 og 8 om tilrettelagt innhenting. Den 1. januar 2022 trådte kapittel 7 og 8 i kraft, med unntak av § 7-3 om beslutning om tilrettelegging for innhenting av grenseoverskridende elektronisk kommunikasjon, som trådte i kraft 2. september 2022.

I høringsnotatet av 27. juni 2022 sendte Forsvarsdepartementet en rekke forslag til endringer i etterretningstjenesteloven på høring.[15] Bakgrunnen for forslagene var rettsutviklingen i EMD og EU-domstolen. Nærmere bestemt avsigelsen av EMD-dommene Big Brother Watch m.fl. mot Storbritannia og Centrum för Rättvisa mot Sverige og EU-domstolens dom La Quadrature du Net m.fl., som viste at etterretningstjenestelovens regler ikke var i samsvar med EMK og EØS-retten.

En rekke tungtveiende høringsinstanser pekte på at heller ikke det nye lovforslaget var i samsvar EMK og/eller EØS-retten. Det vises til blant annet følgende instansers høringsuttalelser:

- Datatilsynet[16]
- Dommerforeningens menneskerettighetsutvalgs[17]
- Norges institusjon for menneskerettigheter (NIM)[18]
- Norsk Journalistlag[19]
- Norsk Presseforbund[20]
- Norsk rikskringkasting (NRK)[21]
- Teknisk naturvitenskaplig forening[22]

Også EOS-utvalget pekte på flere mangler og uklarheter ved lovforslaget i sin høringsuttalelse.[23]

Høringsnotatet ble likevel, med enkelte endringer, fulgt opp i Prop. 92 L (2022–2023). Lovforslaget ble behandlet i Stortinget 6. og 12. juni 2023, der regjeringens forslag til endringer ble vedtatt av Stortingets flertall.

---

[15] Forsvarsdepartementets høringsnotat av 27. juni 2022.
[16] Datatilsynets høringsuttalelse 26. september 2022.
[17] Dommerforeningens menneskerettighetsutvalgs høringsuttalelse 27. september 2022.
[18] Norges institusjon for menneskerettigheter (NIM) sin høringsuttalelse 27. september 2022.
[19] Norsk Journalistlags høringsuttalelse 27. september 2022.
[20] Norsk Presseforbunds høringsuttalelse 27. september 2022.
[21] NRKs høringsuttalelse 27. september 2022.
[22] Teknas høringsuttalelse 27. september 2022.
[23] EOS-utvalgets høringsuttalelse 26. september 2022.

4.3 EOS-utvalgets stikkprøvekontroll av EOS-tjenestene

EOS-utvalget er et stortingsoppnevnt organ som skal kontrollere norske virksomheter som utøver etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-tjenestene). Utvalget kan ytre sin mening om forhold som ligger innenfor kontrollområdet, men kan ikke fatte bindende vedtak eller lignende. Kontrollen med enkeltsaker og operasjoner er etterfølgende og i hovedsak stikkprøvebasert. Det vises til EOS-utvalgets egen beskrivelse av sin kontrollvirksomhet i årsmeldingen for 2022.[24]

Budsjettene til E-tjenesten, PST og Nasjonal sikkerhetsmyndighet har doblet seg de siste fem årene, og ligger nå på til sammen 4,8 milliarder kroner årlig.[25] Over 3 300 personer jobber i de tre tjenestene. Dette er også forhold som er omtalt i pressen, blant annet i Morgenbladet.[26]

Til sammenligning har EOS-utvalgets syv medlemmer hjelp fra 22 ansatte, mens EOS-utvalget utgifter ifølge årsmeldingen for 2022 var på 35 millioner kroner i 2022. Av årsmeldingen fremgår at av dagens sju medlemmer har fem partipolitisk bakgrunn, mens de to øvrige har juridisk og teknologisk faglig bakgrunn. Også de foregående årene har utvalgets medlemmer bestått av fem med partipolitisk bakgrunn.

I 2022 gjennomførte utvalget totalt 22 inspeksjoner for alle de tre EOS-tjenestene, herunder tre inspeksjoner av E-tjenesten sentralt. Samme år tok utvalget opp 8 saker av eget tiltak med tjenestene. I 2022 tok utvalget 40 klager på EOS-tjenestene til behandling, mot 25 klager i 2021.

I EOS-utvalgets årsmelding for 2022 fremgår det at utvalget i en inspeksjon i desember 2021 ble gjort oppmerksom på at E-tjenesten var i dialog med en ekomtilbyder om overføring av reelle data etter 1. januar 2022, med formål om å teste og utvikle systemet for tilrettelagt innhenting. Etterretningstjenestelovens § 7-3 var på dette tidspunktet ikke trådt i kraft. EOS-utvalget skriver i årsmeldingen:

> *«Under henvisning til at e-loven § 7-3 ikke var trådt i kraft, stilte utvalget spørsmål til tjenesten om det rettslige grunnlaget for overføring av reelle data for test- og utviklingsformål. E-tjenesten anførte at e-loven § 7-2 utgjorde et selvstendig rettsgrunnlag for tjenesten til å pålegge ekomtilbyder å utlevere reelle data for testformål. Subsidiært anførte tjenesten at personopplysningsloven ga ekomtilbyder en rett til å utlevere reelle data til E-tjenesten. Utvalget delte ikke tjenestens syn. Siden e-loven § 7-3 om beslutningsmyndighet ikke hadde trådt i kraft, mente utvalget at E-tjenesten ikke hadde hjemmel til å pålegge ekomtilbyder å utlevere reelle data etter § 7-2. Utvalget mente videre at det ikke utgjorde et tilstrekkelig hjemmelsgrunnlag for*

[24] EOS-utvalgets årsmelding til Stortinget - Dokument 7:1 (2022–2023).
[25] Statsbudsjett for 2023 Prop. 1 S (2022–2023) punkt 6 Utgifter under programkategori 04.10 fordelt på kapitler
[26] Morgenbladets artikkel 9. juni 2023.

E-tjenesten at ekomtilbyderen eventuelt hadde hjemmel i annet regelverk for utlevering av reelle data.»[27]

Det bes opplyst om E-tjenesten fastholder sitt syn om at etterretningstjenesteloven § 7-2 utgjør selvstendig rettsgrunnlag for tjenesten til å pålegge ekomtilbydere å utlevere data.

Videre fremgår det av årsmeldingen at E-tjenesten ikke har lagt til rette for utvalgets kontroll gjennom tekniske løsninger. Det bes opplyst hva som er status for dette arbeidet og bes fremlagt dokumentasjon for dette, dersom E-tjenesten mener at dette nå er på plass.

Av årsmeldingen fremgår det også at E-tjenesten mangler «logging av søk i rådata i bulk» og at EOS-utvalget derfor mener at E-tjenesten bryter EMK. I årsmeldingen heter det:

«I takt med økte datamengder og økt kompleksitet i tjenestenes datasystemer, blir teknisk tilrettelegging for utvalgets kontroll stadig viktigere. Kontrollmekanismer er en forutsetning for at E-tjenestens innsamling i bulk[10] skal være i samsvar med Den europeiske menneskerettskonvensjonen (EMK). I e-loven er E-tjenesten pålagt å logge søk i rådata i bulk som tar utgangspunkt i et søkebegrep tilknyttet en person i Norge.[11] Hensikten med loggen er å forhindre misbruk og legge til rette for effektiv kontroll.[12]

På denne bakgrunn ba utvalget om å få fremlagt en oversikt over de siste søkene i denne kategorien.[13]

Tjenesten opplyste at alle søk i rådata i bulk logges, men at det ikke er laget funksjonalitet for å markere om et søk tar utgangspunkt i en person som oppholder seg i Norge. Ifølge tjenesten ville det være en manuell og svært tidkrevende jobb å lage en slik oversikt. E-tjenesten ga videre uttrykk for at e-lovens krav til logging er oppfylt, fordi det er mulig å knytte enkeltsøk opp mot vurderinger og godkjenninger som lå til grunn for søket. Tjenesten viste til at loven ikke stiller konkrete krav til hvordan loggingen skal skje.

Utvalget delte ikke tjenestens oppfatning. Den store informasjonsmengden i loggen, samt utfordringene med å navigere i den, fører til at utvalget ikke kan føre en effektiv kontroll. At tjenesten ikke kunne presentere en oversikt over de siste søkene som er gjort i en kategori som krever særlig begrunnelse, viser at lovens krav om logging for kontrollformål ikke er oppfylt.

For at en logg skal være kontrollerbar, må den i seg selv kunne benyttes til å avdekke feil. Det er ikke godt nok at loggen kan benyttes til å undersøke et avvik som det

---

[27] EOS-utvalgets årsmelding til Stortinget - Dokument 7:1 (2022–2023). punkt 4.2.1.

allerede er mistanke om. Utvalget kritiserte E-tjenesten for mangelfull oppfyllelse av kravet til logging av søk i bulkdata for kontrollformål. Utvalget oppfordret tjenesten til å videreutvikle loggfunksjonaliteten slik at utvalget kan føre en effektiv kontroll.»[28]

Det bes opplyst hva som er status for oppfyllelsen av kravet til logging av søk i bulkdata for å tilrettelegge for EOS-utvalgets kontroll gjennom logger som er egnet til å avdekke feil.

EOS-utvalget har i flere av de senere års årsmeldinger tatt opp mangler og kritikkverdige forhold hos E-tjenesten, også når det gjelder tilrettelegging for EOS-utvalgets tilsynsfunksjon.[29]

Bakgrunnen for opprettelsen av EOS-utvalget er Lund-kommisjonens rapport (Lund-rapporten), som dokumenterte ulovlig overvåkning av nordmenn i etterkrigstiden og frem til slutten av 1980-tallet.[30] Kommisjonens rapport er omfattende, og det vises særlig til følgende sider i Lund-rapporten: s. 3–30, 955–988 og 993–1089.

4.4 Virkningen av masseovervåkning

Omfattende overvåkning har alvorlig konsekvenser for demokratiets funksjon. I Datatilsynets personvernundersøkelse fra 2019/2020 svarte 16 prosent at de har unnlatt å delta i kommentarfeltet i en nettavis eller i en Facebook-debatt fordi de er usikre på om myndighetene har tilgang til informasjonen de legger igjen. 13 prosent svarte at de har unnlatt å foreta et søk på nett på grunn av usikkerhet knyttet til om myndighetene har tilgang til informasjonen. Nesten én av ti har av samme årsak unnlatt å søke hjelp eller søke etter informasjon om problemer knyttet til psykisk helse, misbruk, avhengighet eller andre sensitive problemer.[31]

En rekke vitenskapelige studier dokumenterer en nedkjølingseffekt som resultat av masseovervåkningstiltak. Harvard-studien «Chilling Effects: Online Surveillance and Wikipedia Use» (2016) viser at søk rundt kontroversielle temaer på Wikipedia falt umiddelbart etter at amerikanske myndigheters masseovervåkning ble kjent etter Snowden-avsløringene i 2013.

Bilag 2: Penney, «Chilling Effects: Online Surveillance and Wikipedia Use» (2016)

Videre viser en rapport fra Internet Policy Review (2017, vol. 6 issue. 2) at statlig overvåking har en nedkjølende effekt på individenes vilje til å delta i demokratiske aktiviteter, og gir utslag i manglende samfunnsdeltakelse, endret oppførsel, selvsensur og konformitet.

---

[28] EOS-utvalgets årsmelding til Stortinget - Dokument 7:1 (2022–2023) punkt 4.4.

[29] EOS-utvalgets årsmeldinger kan leses via EOS-utvalgets nettsider, her: https://eos-utvalget.no/hjem/publikasjoner/arsmeldinger/

[30] Dokument nr. 15. (1995—96) Rapport til Stortinget fra kommisjon som ble nedsatt av Stortinget for å granske påstander om ulovlig overvåkning av norske borgere (Lund-rapporten). (Avgitt til Stortingets presidentskap 28. mars 1996) - https://www.stortinget.no/no/Saker-og-publikasjoner/Stortingsforhandlinger/Lesevisning/?p=1995-96&paid=5&wid=b&psid=DIVL882&pgid=b_0511

[31] Personvernundersøkelsen 2019/2020, Datatilsynet.

Bilag 3: Penney, «Internet surveillance, regulation, and chilling effects online: a comparative case study», Internet Policy Review (2017)

Human Rights Watchs rapport «With Liberty to Monitor All» dokumenterer hvordan overvåking berører journalister og deres kilder, og følgelig også demokratiet.[32]

Det er derimot vanskelig å finne etterprøvbar dokumentasjon for at sammenlignbare tiltak har avverget angrep og trusler av den alvorlighetsgrad og karakter som Forsvarsdepartementet har lagt til grunn at systemet for tilrettelagt innhenting kan gjøre.

5 STATENS MENNESKERETTSLIGE FORPLIKTELSER ETTER GRUNNLOVEN OG EMK

5.1 Grunnloven § 102 og EMK artikkel 8

Grunnloven § 102 omhandler blant annet retten til privatliv og til personvern. I første ledd første setning heter det at:

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

Menneskerettighetsutvalget fremholdt i sin utredning til Stortinget Dok. 16 (2011–2012) på s. 176, personvernets betydning for demokratiet: Overvåking og kontroll kan ha en nedkjølende effekt på den frie meningsutvekslingen. På utredningen s. 175 uttaler utvalget at bestemmelsen skal «forstås i lys av og suppleres med det internasjonale konvensjonsvernet og med tidligere ulovfestet rett». I Rt. 2015 s. 93 avsnitt 57 har Høyesterett lagt dette til grunn:

> *Jeg legger til grunn at § 102 skal tolkes i lys av de folkerettslige forbildene, men likevel slik at fremtidig praksis fra de internasjonale håndhevingsorganene ikke har samme prejudikatsvirkning ved grunnlovstolkningen som ved tolkningen av de parallelle konvensjonsbestemmelsene: Det er etter vår forfatning Høyesterett – ikke de internasjonale håndhevingsorganene – som har ansvaret for å tolke, avklare og utvikle Grunnlovens menneskerettsbestemmelser.*

Dette er lagt til grunn i senere rettspraksis, og innebærer at EMDs rettspraksis i tilknytning til EMK artikkel 8 er sentral for tolkningen av Grunnloven § 102.

Grunnloven § 102 omfatter all kommunikasjon, uavhengig av medium. Arnfinn Bårdsen beskriver dette som grunnleggende, ettersom Grunnloven med dette gir enhver rett til respekt for all sin kommunikasjon, også når den foregår via moderne informasjonsteknologi.[33] Etter Bårdsens syn er det for eksempel ingen tvil om at tilrettelagt innhenting vil rammes av Grunnloven § 102.

---

[32] Human Rights Watchs rapport «With Liberty to Monitor All» (2014)

[33] Arnfinn Bårdsen, "Grunnloven og overvåkning», i Magnus Matningsdal og Asbjørn Strandbakken (red.), *Integritet og ære: festskrift til Henry John Mæland*, Gyldendal (2019).

Inngrep i retten til privatliv og personvern kan etter EMK artikkel 8 kun rettferdiggjøres dersom det er i samsvar med lov, forfølger ett av de angitte legitime formålene i artikkel 8 nr. 2 og er nødvendig i et demokratisk samfunn:

> *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

5.2 Grunnloven § 100 og EMK artikkel 10

Grunnloven § 100 stadfester retten til ytringsfrihet. I § 100 første til tredje ledd heter det:

> *Ytringsfrihet bør finne sted.*
>
> *Ingen kan holdes rettslig ansvarlig for å ha meddelt eller mottatt opplysninger, ideer og budskap med mindre det lar seg forsvare holdt opp imot ytringsfrihetens begrunnelse i sannhetssøken, demokrati og individets frie meningsdannelse. Det rettslige ansvar bør være foreskrevet i lov.*
>
> *Frimodige ytringer om statsstyret og hvilken som helst annen gjenstand er tillatt for enhver. Det kan bare settes klart definerte grenser for denne rett der særlig tungtveiende hensyn gjør det forsvarlig holdt opp imot ytringsfrihetens begrunnelser.*

Etter Grunnloven § 100 sjette ledd er staten forpliktet til å «legge forholdene til rette for en åpen og opplyst offentlig samtale.» Også Grunnloven § 100 må tolkes i lys av EMK, slik at EMDs praksis etter EMK artikkel 10 er sentral for tolkningen av ytringsfrihetsvernet i Grunnloven § 100.

Pressens kildevern skal sikre at personer som besitter informasjon om forhold som er av allmenn interesse, kan formidle dette til/via pressen i fortrolighet. Uten et solid kildevern kan ikke pressen ivareta sine viktige samfunnsroller som offentlig vaktbikkje, informasjonskanal og tilrettelegger for den offentlige samtale.

Etter EMDs praksis er kildevernet som følger av EMK artikkel 10, og som blant annet beskytter pressens ytringsfrihet, ikke begrenset til et vern mot å identifisere kilden ved navn, bilde eller annen personidentifikasjon. Så lenge journalistens kilder kan bli avslørt, omfatter vernet etter EMK artikkel 10 også uredigert og upublisert materiale. At innhentingen ikke har til formål å avsløre pressens kilder er i henhold til rettspraksis ikke avgjørende.

5.3 Sentral praksis fra Den europeiske menneskerettsdomstolen (EMD)

5.3.1 Roman Zakharov mot Russland

I storkammerbehandlingen av Roman Zakharov-saken var spørsmålet om det foregikk skjult overvåkning av telekommunikasjon i Russland som innebar en krenkelse av EMK artikkel 8. Klageren hadde gått til sak mot tre mobiloperatører med påstand om at det var gjort inngrep i hans rett til respekt for sin korrespondanse. Dette med bakgrunn i en lovbestemmelse som tillot at mobiloperatører installerte utstyr han mente muliggjorde overvåkning av telekommunikasjon fra den nasjonale sikkerhetstjenesten.[34] EMD kom til at artikkel 8 var krenket.

EMD viser i dommen til seks minimumskrav til hva lovverk som hjemler skjulte innhentingsmetoder må regulere for å hindre maktmisbruk – de såkalte *Weber-kriteriene*:

1. The nature of offenses which may give rise to an interception order.
2. A definition of the categories of people liable to have their communications intercepted.
3. A limit on the duration of interception.
4. The procedure to be followed for examining, using and storing the data obtained.
5. The precautions to be taken when communicating the data to other parties.
6. The circumstances in which intercepted data may or must be erased or destroyed.

I Roman Zakharov-dommen slo EMD i avsnitt 231 fast at disse kriteriene også kommer til anvendelse i saker som gjelder overvåkning av hensyn til nasjonal sikkerhet, se også Centrum för rättvisa mot Sweden avsnitt 249.

EMD kom i den konkrete saken til at den russiske lovgivningen ikke ga tilstrekkelige og effektive garantier mot vilkårlighet og risiko for misbruk, som er særlig høy i et system der sikkerhetstjenesten og politiet med tekniske midler har direkte tilgang til all mobiltelefonkommunikasjon.

5.3.2 Centrum för rättvisa mot Sweden (35252/08)

I storkammerdommen Centrum för rättvisa mot Sverige var spørsmålet om svensk etterretningstjenestes masseovervåkningsregime med bulkinnsamling av kommunikasjonsdata var i strid med EMK artikkel 8. EMD kom til at EMK artikkel 8 var krenket.

Norge var blant statene som intervenerte. Den norske regjeringen argumenterte for at EMDs vurdering i en sak som denne burde være en helhetsvurdering av om rettsikkerhetsgarantiene var «sufficient and adequate», uten at det ble oppregnet og stilt absolutte krav. I tillegg oppfordret den norske regjeringen EMD til å avstå fra å importere EU-domstolens tilnærming og kriterier.[35]

---

[34] Roman Zakharov mot Russia, no. 47143/06, i Storkammer, [2015], avsnitt 10.

[35] Centrum för rättvisa mot Sverige, avsnitt 234–235 og tilsvarende i Big brother watch and others mot Storbritannia avsnitt 308–310.

EMD betraktet bulkovervåkning som en gradvis prosess der graden av inngrep i individers rettigheter etter EMK artikkel 8 øker etter hvert som prosessen skrider frem. Selv enkel lagring av data om privatlivet til en person utgjør et inngrep i artikkel 8, jf. dommens avsnitt 239–245.

Storkammeret videreutvikler i dommen Weber-kriteriene, og tilpasser kriteriene til overvåkning i form av bulkinnsamling. Som følge av hvordan den teknologiske utviklingen har endret måten folk kommuniserer på, det økte omfanget av overvåkningsvirksomhet og forskjellene mellom målrettet overvåkning og bulkovervåkning, oppstilte Storkammeret åtte kriterier domstolen måtte vurdere om nasjonal lovgivning klart definerte:

1. The grounds on which bulk interception may be authorised.
2. The circumstances in which an individual's communications may be intercepted.
3. The procedure to be followed for granting authorisation.
4. The procedures to be followed for selecting, examining and using intercept material.
5. The precautions to be taken when communicating the material to other parties.
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.
7. The procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance.
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.[36]

EMD foretok på denne bakgrunn en «global assessment» – helhetlig vurdering – av hvordan overvåkningssystemet virker, med fokus på garantier mot misbruk og om prosessen er gjenstand for «end to-end safeguards».[37]

EMD trakk særlig frem tre sentrale mangler ved det svenske regimet for bulkinnsamling av kommunikasjonsdata:

1. Mangelen på en klar regel om ødeleggelse av innhentet materiale som ikke inneholder personlig data.
2. Fraværet av et krav om at personverninteresser må vektlegges ved utveksling av etterretningsmateriale med utenlandske partnere.
3. Fraværet av effektiv etterfølgende kontroll.[38]

Når det gjaldt den etterfølgende kontrollen mente EMD denne var svekket som følge av Statens inspektion för försvarsunderrättelseverksamheten (SIUN) sin dobbeltrolle, ved atSIUN både utførte kontroll og behandlet klager, og på grunn av fraværet av muligheten til å få en begrunnet avgjørelse etter en henvendelse eller klage knyttet til bulkovervåkning.

---

[36] Centrum för rättvisa mot Serige avsnitt 275.
[37] Centrum för rättvisa mot Sverige avsnitt 274.
[38] Centrum för rättvisa mot Sverige avsnitt 369.

Det svenske systemet inneholdt derfor etter EMDs syn ikke tilstrekkelige «end-to-end safeguards» for å gi «adekvate og effektive» garantier mot vilkårlighet og misbruk, slik at artikkel 8 var krenket.[39]

5.3.3 Big Brother Watch m.fl. mot Storbritannia

I storkammmerdommen Big Brother Watch m.fl. mot Storbritannia var spørsmålet om britisk etterretningstjenestes bulkinnsamling av kommunikasjonsdata utgjorde en krenkelse av EMK artikkel 8 og 10. Dommen ble avsagt samme dag som Centrum för rättvisa mot Sverige, og EMD legger de samme rettslige utgangpunktene til grunn i de to dommene.

EMDs storkammer mente at heller ikke det britiske regimet for skjult overvåkning (The Regulation of Investigatory Powers Act 2000 – «RIPA», artikkel 8 (4)), hadde tilstrekkelige «end-to-end safeguards» som ga «adekvate og effektive» garantier mot vilkårlighet og misbruk. EMK artikkel 8 var derfor krenket. Storkammeret pekte ut tre grunnleggende mangler ved overvåkningsregimet:

1. Fraværet av uavhengig autorisasjon av bulkinnsamling.
2. At kategoriene av velgerne (selektorene) ikke var inkludert i begjæringen om godkjenning.
3. At sterke velgere knyttet til identifiserbare enkeltpersoner ikke var underlagt forhåndsgodkjenning.

EMD kom til at regimet for bulkovervåkning også krenket EMK artikkel 10. Storkammeret slo fast at inngrep i beskyttelsen av journalistiske kilder ikke er forenelig med EMK artikkel 10, med mindre «it is justified by an overriding requirement in the public interest». Slike inngrep må underlegges prosessuelle garantier, særlig kontroll foretatt av en dommer eller et annet uavhengig og upartisk beslutningsorgan, med makt til å avgjøre om hensynet til offentlig interesse veier tyngre enn kildevernet, *før* slikt materiale utleveres. Avgjørelsen bør styres av klare kriterier, og dommeren må kunne nekte eller begrense utlevering av materialet. I hastetilfeller bør det eksistere en prosedyre for identifisering og isolering av informasjon som kan føre til identifisering av kilder.[40]

Under det britiske artikkel 8 (4)-regimet kunne etterretningstjenesten få tilgang til konfidensielt journalistisk materiale med (1) intensjon om dette, (2) gjennom bevisst bruk av velgere eller søkeord knyttet til en journalist eller nyhetsorganisasjon eller (3) utilsiktet, som er biprodukt av andre overvåkningsoperasjoner. EMD sammenliknet inngrepet i de to første tilfellene med ransaking av en journalists hjem eller arbeidsplass, og stilte følgende krav:

> *"[…] before the intelligence services use selectors or search terms known to be connected to a journalist, or which would make the selection of confidential journalistic material for examination highly probable, the selectors or search terms must have been authorised by a judge or other independent and impartial decision-making body invested with the power to determine whether they were "justified by*

[39] Centrum för rättvisa mot Sverige avsnitt 373–374.

[40] Big Brother Watch m.fl. mot Storbritannia avsnitt 444–445.

an overriding requirement in the public interest" and, in particular, whether a less intrusive measure might have sufficed to serve the overriding public interest."

Denne samme forhåndsvurderingen kunne ikke foretas ved *utilsiktet* tilgang konfidensielt journalistisk materiale, men EMD anså det som avgjørende at nasjonal lovgivning inneholder

> *"[…] robust safeguards regarding the storage, examination, use, onward transmission and destruction of such confidential material. Moreover, even if a journalistic communication or related communications data have not been selected for examination through the deliberate use of a selector or search term known to be connected to a journalist, if and when it becomes apparent that the communication or related communications data contain confidential journalistic material, their continued storage and examination by an analyst should only be possible if authorised by a judge or other independent and impartial decision-making body invested with the power to determine whether continued storage and examination is "justified by an overriding requirement in the public interest"."*

Under vurderingen av det britiske regimet opp mot kravene etter EMK artikkel 10, pekte EMD på de manglene rettsikkerhetsgarantiene som ble identifisert under vurderingen etter EMK artikkel 8, og viste i tillegg til ytterligere to svakheter:

1. Det var ikke noe krav om at velgere eller søkeord som er knyttet til en journalist skal autoriseres av en dommer eller et annet uavhengig beslutningsorgan i tråd med kravene beskrevet over – det eneste som krevdes ifølge lovningen var at begrunnelsen og dennes nødvendighet og proporsjonalitet var klart dokumentert.
2. Også sikkerhetstiltakene ved utilsiktet innhenting av slik informasjon var utilstrekkelige, ettersom alt som krevdes for videre lagring og analyse av materialet var at det ble tatt «spesielt hensyn» til overvåkning som kan ha involvert konfidensielt journalistisk materiale.

Når det gjaldt adgangen til innhenting av kommunikasjonsdata fra kommunikasjonstjeneste-leverandører (det britiske «Kapittel II-regimet»), sluttet Storkammeret seg til kammerets vurderinger av at EMK artikkel 8 og 10 var krenket.

5.3.4 Wieder and Guarnieri mot Storbritannia[41] (64371/16 og 64407/16)

I en nylig avgjørelse av 12. september 2023 – med andre ord etter vedtakelse av også de siste delene av E-tjenesteloven – avsa EMD dom i saken Wieder and Guarnieri mot Storbritannia.

Klagerne var henholdsvis en amerikansk statsborger, bosatt i USA, og en italiensk statsborger, bosatt i Tyskland. Et hovedspørsmål i saken var hvorvidt Storbritannias ansvar etter EMK artikkel 8 –

[41] Wieder and Guarnieri mot Storbritannia, no. 64371/16 og 64407/16 [2023].

under henvisning til EMDs storkammerdom i Big Brother Watch-saken (jf ovenfor) – også omfattet klagerne og bulkinnsamling av deres elektroniske kommunikasjon, selv om klagerne verken var bosatt i eller hadde brukt elektronisk kommunikasjon i Storbritannia.

Storbritannia anførte at konvensjonsstatenes ansvar (jurisdiksjon) etter EMK artikkel 1 ikke kunne gjelde der avsender eller mottaker av elektronisk kommunikasjon befant seg utenfor konvensjonsstatens (her Storbritannias) territorium. Dette var EMD uenig i. EMDs behandling av dette spørsmålet fines i dommens avsnitt 74 – 95.

EMD pekte på at "the interception of communications and the subsequent searching, examination and use of those communications interferes both with the privacy of the sender and/or recipient, and with the privacy of the communications themselves". Når innhentingen mv. (forutsetningsvis også) av klagernes elektroniske kommunikasjon skjedde i Storbritannia, skjedde også inngrepet i klagernes rettigheter etter EMK artikkel 8 i Storbritannia, slik at det falt innunder Storbritannias ansvar/jurisdiksjon etter EMK artikkel 1 – uavhengig av hvor klagerne selv befant seg (dommens avsnitt 94 og 95).

Ettersom det ikke var omstridt at det britiske systemet for bulkinnsamling på flere punkter var i strid med EMK artikkel 8 (jf storkammerdommen i Big Brother-saken), ble konklusjonen i saken at Storbritannia hadde krenket EMK artikkel 8 også overfor klagerne.

Dommen har stor betydning, fordi E-tjenestelovens overvåkningshjemler bygger på en forutsetning om at statens menneskerettslige forpliktelser (i alle fall i hovedsak) kun gjelder når inngrep gjøres i kommunikasjon der både avsender og mottaker befinner seg i Norge. Den forutsetningen er ikke gyldig.

6 STATENS EØS-RETTSLIGE FORPLIKTELSER

6.1 Relevante EØS-regler

I EU reguleres elektroniske kommunikasjonsnett og -tjenester i hovedsak av den såkalte «ekompakken» – en samling rettsakter som ble vedtatt i 2002. I Norge er disse forpliktelsene gjennomført i lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven). Særlig viktig i denne forbindelse er kommunikasjonsverndirektivet (2002/58/EC). Direktivet er EØS-relevant og gjennomført i norsk rett i ekomloven med forskrifter.

Det følger av kommunikasjonsverndirektivet artikkel 5 nr. 1 at medlemsstatene gjennom nasjonal lovgivning plikter å sikre fortrolighet for kommunikasjon som foregår via offentlige kommunikasjonsnett og offentlig tilgjengelige elektroniske kommunikasjonstjenester, samt fortrolighet for trafikkdata knyttet til slik kommunikasjon. Videre følger det av artikkel 5 nr. 1 at medlemsstatene særlig skal forby enhver annen person enn brukerne å avlytte, registrere, lagre eller på andre måter fange opp eller overvåke kommunikasjonen og tilhørende trafikkdata uten samtykke fra brukeren, med unntak av tilfeller der dette er tillatt i henhold til lov i samsvar med artikkel 15 nr. 1.

Av direktivet artikkel 15 nr. 1 følger det at medlemsstatene ved lov kan treffe tiltak som griper inn i rettighetene etter artikkel 5, av hensyn til blant annet «forebygging, etterforskning, avsløring og

rettslig forfølgning av straffbare handlinger». Et slik tiltak må være «nødvendig, egnet og rimelig i et demokratisk samfunn».

Det er videre angitt i artikkel 15 at medlemsstatene kan vedta «lovgivningstiltak om lagring av opplysninger i et begrenset tidsrom» dersom dette er berettiget ut fra en av grunnene oppgitt i bestemmelsen. Slik direktivet lyder i EU, er det videre angitt at tiltakene skal være i samsvar med «de allmenne prinsippene i fellesskapsretten, herunder prinsippene i artikkel 6 nr. 1 og 2 i traktaten om den Europeiske union», som blant annet refererer til EUs pakt om grunnleggende rettigheter (Charteret), herunder artikkel 7 (retten til privat- og familieliv) og artikkel 8 (rett til beskyttelse av personlige data). Slik direktivet er inntatt i EØS-avtalen, er denne passusen erstattet med «de allmenne prinsippene i EØS-retten».

6.2 Sentral praksis fra EU-domstolen

6.2.1 Digital Rights Ireland og Kärntner Landesregierung[42]

I storkammerdommen Digital Rights Ireland og Kärntner Landesregierung (Digital Rights) konkluderte EU-domstolen med at EUs datalagringsdirektiv var ugyldig. Datalagringsdirektivet krevde generell lagring av kommunikasjonsdetaljer (trafikkdata) fra bruk av fasttelefon og mobiltelefon, opplysninger om internettbruk, e-post og bredbåndsbruk mv.

EU-domstolen bemerket at kampen mot alvorlig kriminalitet, og særlig organisert kriminalitet og terror, er av største betydning for å verne om offentlig sikkerhet, og at kampens effektivitet i stor grad kan avhenge av muligheten til å bruke utradisjonelle etterforskningsmetoder. Domstolen uttalte likevel at et slikt formål ikke i seg selv kunne rettferdiggjøre lagringen av opplysningene. Det krevdes med andre ord noe mer for å anse inngrepet proporsjonalt, nærmere bestemt måtte lagringen være begrenset til det som var «strictly necessary». I vurderingen av om direktivet var begrenset til det som var strengt nødvendig påpekte EU-domstolen tre viktige mangler ved direktivet:

For det første mente domstolen at direktivet favnet for vidt ved at det på generelt vis krevde lagring av alle typer elektronisk kommunikasjon og omfattet alle brukere og abonnenter, uten at det ble foretatt unntak, begrensninger eller sondringer tilpasset det angitte formålet om bekjempelse av kriminalitet. Direktivet krevde ikke at de registrerte var mistenkt for alvorlig kriminelle handlinger, eller at de hadde noen form for befatning med slike handlinger, til tross for at formålet med direktivet var begrensning av alvorlig kriminalitet. På denne måten utgjorde direktivet et inngrep i de fundamentale rettighetene til praktisk talt hele den europeiske befolkning.

For det andre bemerket domstolen at direktivet ikke krevde at de kompetente nasjonale myndigheters tilgang og etterfølgende bruk av personopplysningene ble begrenset til formålet om bekjempelse av kriminalitet. I stedet påla direktivet medlemsstatene selv ansvaret for å definere

[42] Storkammerdom av 8. april 2014, *Digital Rights Ireland og Kärntner Landesregierung,* C-293/12 og C-594/12, ECLI:EU:C:2014:238.

hvilke prosedyrer som skulle følges, med krav om at nødvendighets- og proporsjonalitetsprinsippet skulle følges.

For det tredje slo domstolen ned på varigheten av lagringen. Direktivet krevde en minste lagringstid på seks måneder, uten å sondre mellom de ulike kategoriene av opplysninger og den mulige nytten opplysningene kunne utgjøre med tanke på direktivets formål. Direktivet åpnet for lagring i opptil to år, og det var ikke oppgitt kriterier for vurdering av om tidsperioden var begrenset til det som var strengt nødvendig. EU-domstolen mente derfor at reguleringen av lagringsperioden ikke var begrenset til det som var «strictly necessary».

På bakgrunn av disse tre manglene, kom EU-domstolen til at direktivet materielt sett overskred grensen for det som kunne aksepteres i henhold til det overordnede personopplysningsvernet etter Charterets artikkel 7 og 8.

6.2.2 Tele2 Sverige AB og Watson og andre[43]

I denne storkammersaken hadde EU-domstolen forent to saker til felles behandling: Tele2 Sverige AB og Watson og andre. Selv om datalagringsdirektivet var blitt kjent ugyldig, hadde man i de aktuelle statenes nasjonale lovgivning pålegg om tilsvarende lagring. EUs kommunikasjonsverndirektiv gjaldt fortsatt for teleoperatørenes virksomhet, herunder med hensyn til begrensninger i adgangen til lagring av data. EU-domstolen ble derfor i Tele2 og Watson stilt spørsmål om hvilke grenser kommunikasjonsverndirektivet setter for slik generell datalagring. EU-domstolen kom også her til at lagringen var i strid med EU-retten.

6.2.3 La Quadrature du Net[44] og Privacy International[45]

I EU-domstolens prejudisielle avgjørelser (tolkningsavgjørelser) i Privacy International (heretter forkortet «PI») og La Quadrature du Net (heretter forkortet «LQN») kom EU-domstolen til at britisk, fransk og belgisk lovgivning som påla ekomtilbydere å lagre eller overføre data til sikkerhets- og etterretningstjenester av hensyn til nasjonal sikkerhet, var i strid med kommunikasjonsverndirektivet artikkel 15.

EU-domstolen konkluderte i dommene med at artikkel 15 nr. 1 ikke forbyr lovgivning som åpner for at kompetente myndigheter kan pålegge tjenestetilbydere å lagre metadata fra alle brukerne av elektroniske kommunikasjonssystemer for en begrenset periode, men at det blant annet forutsetter at det foreligger

> *"[…] 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*

[43] Storkammerdom av 21. desember 2016, *Tele2 Sverige AB og Watson og andre,* C-203/15 og C-698/15, ECLI:EU:C:2016:970.
[44] Note 5.
[45] Note 6.

judgment, to national security which is shown to be genuine and present or foreseeable."

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

7 NÆRMERE OM ETTERRETNINGSTJENESTELOVEN KAPITTEL 7 OG REGELVERKETS FORHOLD TIL GRUNNLOVEN, EMK OG EØS-RETTEN

7.1 Om regelverket i etterretningstjenesteloven kapittel 7

7.1.1 Hjemmelen for tilrettelagt innhentning, utvalg og filtrering – §§ 7-1 og 7-6

Rettsgrunnlaget for tilrettelagt innhenting fremgår av etterretningstjenesteloven § 7-1:

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.

Hjemmelen i § 7-1 gir noen overordnede rammer for adgangen til tilrettelagt innhenting, men oppstiller i beskjeden grad reelle skranker for når tilrettelagt innhenting er tillat, utover å stille krav til at tilrettelagt innhenting følger lovens system. Når vilkårene er oppfylt, kan E-tjenesten gis adgang til å «innhente elektronisk kommunikasjon som transporteres over den norske grensen».

Det er ikke tvilsomt at norsk innenlandsk kommunikasjon normalt krysser grensen, slik departementet legger til grunn i Prop. 80 L på s. 104. Tilrettelagt innhenting rammer i praksis svært store deler av all kommunikasjon som foregår digitalt, uavhengig av hvor endebrukerne befinner seg. Dette innebærer at også kommunikasjon mellom personer i Norge omfattes, i strid med E-tjenestens oppgaver, som i utgangspunktet begrenser seg til å drive utenlandetterretning, jf. lovens kapittel 3.. Samtidig omfattes også enveiskommunikasjon, dvs. personers aktivitet på internett, uten at det skjer i direkte kommunikasjon med andre personer, slik som f.eks. et google-søk.

E-tjenesten skal etter lovens § 7-6 gjennom utvalg og filtrering forsøke å hindre lagring av metadata om kommunikasjon mellom en avsender og mottaker som begge befinner seg i Norge:

Etterretningstjenesten skal gjennom utvalg og filtrering søke å hindre lagring etter § 7-7 av metadata om kommunikasjon mellom avsender og mottaker som begge befinner seg i Norge, hvis ikke en av dem omfattes av § 4-2 første ledd.

Plikten til utvalg og filtrering gjelder kun så langt det er mulig. Hva som er mulig avhenger av hvilke tekniske løsninger som er tilgjengelige, samtidig som det er E-tjenesten som i utstrakt grad vil ha kunnskap og definisjonsmakt over hvilke avhjelpende tiltak som er mulig å iverksette. At det dreier seg om en begrenset plikt, som i begrenset grad kan avhjelpe inngrep borgerens privatliv og personvern, erkjennes av departementet i forarbeidene:

> *At tjenesten skal «søke å» hindre lagring, synliggjør at det ikke alltid vil være mulig å filtrere bort irrelevant data. Det vil ofte måtte lagres store mengder irrelevante data fra enkelte kommunikasjonsstrømmer, fordi det ikke er mulig å filtrere bort informasjonen som er uten interesse. I den utstrekning det er mulig å filtrere bort irrelevante data, for eksempel ved hjelp av geografiske kjennetegn, skal dette like fullt gjøres.*[46]

7.1.2 Ekomtilbyderes tilretteleggingsplikt – § 7-2

Hjemmelen for tilrettelagt innhenting er ledsaget av en tilretteleggingsplikt i § 7-2, hvoretter bestemte tjenesteytere er pålagt å «speile og gjøre tilgjengelig for Etterretningstjenesten utvalgte kommunikasjonsstrømmer» og «på annen måte tilrettelegge for utvalg, filtrering, testing, innhenting, lagring og søk». Videre er det i § 7-2 angitt en ikke-uttømmende liste over tilbydernes plikter:

> *a. gi informasjon om signalmiljø, dataformater, tekniske innretninger og fremgangsmåter*
> *b. tillate at tjenesten installerer utstyr og etablerer midlertidig eller permanent tilstedeværelse for å drifte utstyr på steder som kontrolleres av tilbyder*
> *c. medvirke til teknisk drift og vedlikehold av etablerte løsninger*
> *d. bidra til at tjenesten kan gjennomføre testinnhenting og testanalyser av trafikk i nett og tjenester*
> *e. sørge for tilgang til kommunikasjon uten hinder av linkkryptering eller tilsvarende kryptering som tilbyder kontrollerer*
> *f. medvirke til sikkerhetsmessig forsvarlige løsninger.*

Plikten gjelder tilbydere som omfattes av ekomloven § 1-5, dvs. «enhver fysisk eller juridisk person som tilbyr andre tilgang til elektronisk kommunikasjonsnett eller -tjeneste»,[47] og tilbydere av internettbaserte kommunikasjons- eller meldingstjenester) som er tilgjengelige for allmennheten.

7.1.3 Beslutning om tilrettelegging – § 7-3

Beslutningsmyndigheten knyttet til tilrettelagt innhenting er regulert i etterretningstjenestelovens § 7-3. Bestemmelsen ble foreslått endret i Prop. 92 L (2022–2023), og skiller nå mellom:

---

[46] Prop.80 L (2019–2020) s. 215.
[47] Ekomloven § 1-5 nr. 16.

1. Tillatelse knyttet til *speiling som grunnlag for* søk i lagrede metadata etter § 7-8 og målrettet innhenting og lagring av innholdsdata etter § 7-9 (første ledd).
2. Beslutning om speiling for å gjennomføre tekniske analyser (annet ledd).
3. Andre beslutninger om å pålegge tilretteleggingsplikt enn de som omfattes av første og andre ledd (tredje ledd).

Første ledd bestemmer at rettens kjennelse om tillatelse etter lovens kapittel 8 kreves for at sjefen for E-tjenesten skal ha adgang til å gi pålegg om speiling av elektronisk kommunikasjon som transporteres over den norske grensen, som grunnlag for søk i lagrede metadata etter § 7-8 og målrettet innhenting og lagring av innholdsdata etter § 7-9.

I *andre ledd* er sjefen for E-tjenesten gitt kompetanse til å pålegge speiling av elektronisk kommunikasjon som transporteres over den norske grensen for å gjennomføre «tekniske analyser med det formål å avklare om det foreligger grunnlag for å fremme begjæring om rettens tillatelse til speiling etter første ledd». I Prop. 92 L (2022–2023) heter det på s. 33 at teknisk analyse betyr

> *«[…] informasjon som bidrar til å besvare spørsmål om hva slags trafikk som går i kommunikasjonsstrømmene og hvorvidt trafikken er grenseoverskridende (kommunikasjonsstrømmenes art og karakter) hvor speiling og tilgjengeliggjøring bør finne sted samt hvilken kommunikasjon som skal prioriteres når det ikke er datakraft og overføringskapasitet til å behandle alt. Informasjon som fremskaffes gjennom teknisk analyse skal være på et aggregert nivå.»*

«Tekniske analyser» gjelder tilsynelatende andre handlinger enn dem som er omfattet av reglene om testinnhenting og testanalyse i lovens § 7-5. Det er uklart hvor grensen mellom handlingene som omfattes av de to bestemmelsene går, etter at bestemmelsen om teknisk analyse kom inn i § 7-3 annet ledd ved lovendringen i 2023. I § 7-5 første og andre ledd heter det:

> *Etterretningstjenesten kan gjennomføre testinnhenting og testanalyser av trafikk og nett som omfattes av dette kapittelet. Testinnhenting og testanalyser skal utelukkende brukes for å muliggjøre utvalg, filtrering, lagring, søk, reprosessering, forståelse av signalmiljø og gjenkjenning av tjenester og dataformater, samt annen teknisk understøttelse.*
>
> *Testinnhenting gjennomføres ved uttrekk av ufiltrert kommunikasjon fra én eller flere kommunikasjonsstrømmer. Ett uttrekk skal ikke overstige 30 sekunder. Det kan ikke gjøres mer enn ett uttrekk hver time.*

Etter *tredje ledd* er sjefen for E-tjenesten gitt kompetanse til å treffe andre beslutninger om å pålegge tilretteleggingsplikt enn de som omfattes av første og andre ledd, for inntil to år av gangen. Etter ordlyden omfatter dette testinnhenting og testanalyse etter lovens § 7-5 og innhenting av lagring av metadata etter § 7-7, ettersom disse handlingene ikke omfattes av verken etterretningstjenesteloven § 7-3 første og andre ledd eller § 8-1 første ledd.

Bestemmelsen som ble vedtatt i Stortinget i juni 2023 er betydelig endret sammenliknet med forslaget som var på høring. I departementets høringsnotat fra 27. juni 2022 var en formulering av EU-domstolens såkalte *La Quadrature-kriterier* tatt inn i bestemmelsen § 7-3 tredje ledd bokstav c, der det het at det måtte foreligge «en alvorlig trussel mot nasjonal sikkerhet som er reell og aktuell eller forutsebar og som ikke kan avdekkes i tilstrekkelig grad ved mindre inngripende tiltak». Kriteriene er nå erstattet med et krav om at krav om at speiling må være «nødvendig for å etablere et informasjonsgrunnlag for etterretningsformål», slik at terskelen for inngrep er senket betydelig sammenliknet med hva EU-domstolen krever. Dette er nærmere behandlet i stevningens punkt 7.2.2.

7.1.4 Innhenting og lagring av metadata i bulk og søk lagrede metadata – §§ 7-7 og 7-8

E-tjenestens behandling av *metadata* er regulert i etterretningstjenesteloven §§ 7-7 og 7-8. Metadata er ifølge § 7-7 «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». E-tjenestens tilgang til metadata er svært inngripende, fordi slik data gir detaljert innsikt i kommunikasjonsmønstre.

Etter § 7-7 første ledd første punktum kan E-tjenesten innhente og lagre metadata i bulk:

> *Etter utvalg og filtrering i samsvar med § 7-6 kan Etterretningstjenesten innhente og lagre metadata i bulk om elektronisk kommunikasjon som transporteres over den norske grensen.*

Bestemmelsen åpner sammen med § 7-3 for svært omfattende innhenting av data om store deler av befolkningen og deres elektroniske kommunikasjon og aktivitet.

I § 7-7 tredje og fjerde ledd er det bestemt av E-tjenesten skal opprette og vedlikeholde en liste over hvilke typer metadata som kan lagres, for å hindre lagring av innholdsdata, og at lagrede metadata skal slettes senest etter 18 måneder. I femte ledd heter det at for «teknisk analyse, feilsøking og oppdatering av lagrede metadata i den hensikt å muliggjøre søk gjelder § 7-5 femte ledd første punktum tilsvarende.»

Søk i metadata er regulert i lovens § 7-8 første ledd:

> *Etterretningstjenesten kan innenfor rammen av rettens kjennelse etter kapittel 8 foreta søk i metadata lagret i samsvar med § 7-7. Søkene skal baseres på søkebegreper.*

I bestemmelsens annet ledd er det bestemt at slike søk kun kan utføres av personell i Etterretningstjenesten som er vurdert som skikket til det, som utpekes av sjefen for tjenesten og som har fått særskilt opplæring. Den enkelte skal bare kunne utføre søk i henhold til søkeprivilegier som er tilpasset vedkommendes oppdragsportefølje.

7.1.5 Innhenting og lagring av innholdsdata – § 7-9

Innhenting og lagring av innholdsdata er regulert i etterretningstjenesteloven § 7-9:

Etterretningstjenesten kan innenfor rammen av rettens kjennelse etter kapittel 8 målrettet innhente og lagre innholdsdata med tilhørende metadata fra elektronisk kommunikasjon som transporteres over den norske grensen. Innholdsdata er data som ikke er metadata.

Innholdsdata defineres som «data som ikke er metadata», dvs. alle data som ikke er «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.», jf. etterretningstjenesteloven § § 7-7.

7.1.6 Kontroll med tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon

Det er gitt regler om kontroll med tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon i etterretningstjenestelovens kapittel 7 og 8.

Etter § 7-10 skal E-tjenesten iverksette systematiske tiltak for å sikre at virksomhet etter lovens kapittel 7 gjennomføres i samsvar med loven. Alle søk skal ifølge bestemmelsen kunne kontrolleres i ettertid gjennom aktivitetslogger som skal være tilgjengelige for EOS-utvalgets kontroll. Det er på det rene at det *ikke* har vært tilfellet, jf. EOS-utvalgets årsmelding for 2022.

EOS-utvalget skal etter § 7-11 føre løpende kontroll med E-tjenesten etterlevelse av bestemmelsene, blant annet med at søk bare gjennomføres i tråd med rettens kjennelser og at korttidslageret og testdata utelukkende brukes til teknisk understøttelse. 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, jf. lovens § 7-12.

I etterretningstjenesteloven § 7-13 er det inntatt er forbud mot utlevering av overskuddsinformasjon fra tilrettelagt innhenting til andre norske eller utenlandske myndigheter. Informasjon som ikke er å regne som overskuddsinformasjon kan på den annen side utleveres til norske eller utenlandske myndigheter dersom vilkårene i lovens kapittel 10 er oppfylt. Informasjon som har fremkommet gjennom tilrettelagt innhenting kan ikke brukes som grunnlag for ileggelse av straff i *norsk* rett, jf. § 7-14, men det er få grenser mot at utlevering av informasjon som kan lede til straffeforfølgning i andre stater.

Etter § 8-1 kan retten ved kjennelse gi E-tjenesten tillatelse til å:

a. gi pålegg om å speile elektronisk kommunikasjon som transporteres over den norske grensen etter § 7-3 første ledd

b. iverksette søk i lagrede metadata etter § 7-8

c. iverksette målrettet innhenting og lagring av innholdsdata etter § 7-9

d. iverksette målrettet innhenting etter § 5-2 andre ledd

e. behandle opplysninger som omfattes av § 9-6 første ledd.

Rettens tillatelse kan ikke gis for lengre tid enn nødvendig, jf. lovens § 8-6. 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.

Retten skal oppnevne en særskilt advokat, med mindre retten finner det ubetenkelig, jf. § 8-5. Retten kan beslutte muntlig forhandling, jf. § 8-3.

7.2 Forholdet til Grunnloven, EMK og EØS-retten

7.2.1 Systemet for TI er i strid med pressens kildevern etter EMK artikkel 10 og Grunnloven § 100

Kildevernet skal sikre at personer som besitter informasjon om forhold som er av allmenn interesse kan formidle dette via pressen, uten frykt for straff eller represalier. Formålet med kildevernet er ikke å verne kilden som sådan, men snarere å verne om pressens evne til å formidle informasjon om kritikkverdige forhold, og på den måten sette befolkningen i stand til å kunne stille makthavere eller andre til ansvar. Bakgrunnen for vernet er særlig hensynet til at potensielle kilder ikke skal demotiveres fra å komme med opplysninger. Uten et solid kildevern kan ikke pressen ivareta sine viktige samfunnsroller som offentlig vaktbikkje, informasjonskanal og tilrettelegger for den offentlige samtale.

Etter EMDs praksis er kildevernet som følger av EMK artikkel 10 – som blant annet beskytter pressens ytringsfrihet – ikke begrenset til et vern mot å identifisere kilden ved navn, bilde eller annen personidentifikasjon. Så lenge journalistens kilder kan bli avslørt, omfatter vernet etter EMK artikkel 10 også upublisert materiale. At innhentingen ikke har til formål å avsløre pressens kilder er etter EMDs og Høyesteretts praksis ikke avgjørende.

Systemet for tilrettelagt innhenting innebærer at myndighetene gis tilgang til mer eller mindre all datatrafikk som krysser den norske grensen, inkludert private meldinger mellom personer som befinner seg i Norge. Tilrettelagt innhenting griper derfor inn i kildevernet ved at myndighetene kan få innsyn i hvem som har kommunisert med journalister og innholdet i kommunikasjonen. 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.

Departementet skriver i Prop. 92 L (2022–2023) punkt 4.1 at det ikke uten videre kan legges til grunn at reglene om kildevern på straffeprosessens område og rettspraksis knyttet til disse reglene har direkte overføringsverdi til reglene i etterretningstjenesteloven. Det trekkes her feilaktige slutninger om kildevernets rekkevidde og uavhengig kontroll av vernet om anonyme kilder.

Departementet hadde også selv et annet syn i høringsnotatet av 27. juni 2022 på s. 7, der de om EMDs dom Big Brother Watch mot Storbritannia skriver at «[a]vgjørelsen tydeliggjør også de menneskerettslige prinsippene som gjelder generelt for etterretningstjenesters innhenting og bruk av kildeidentifiserende materiale.» I Big Brother Watch-dommen ble Storbritannia ansett for å ha

opptrådt i strid med EMK artikkel 10, fordi det britiske bulkinnsamlingsregimet ikke i tilstrekkelig grad vernet om konfidensielt journalistisk materiale.

I høringsrunden påpekte en rekke høringsinstanser at departementets forståelse av kildevernets rekkevidde var for snever. Det gjaldt blant annet Dommerforeningen, Nasjonal institusjon for menneskerettigheter (NIM), Norsk Journalistlag, Norsk Presseforbund og NRK.

7.2.2 Formålene som kan begrunne tilrettelagt innhenting er for vide

E-tjenesten kan ifølge etterretningstjenesteloven § 7-1 innhente elektronisk kommunikasjon som transporteres over den norske grensen «for etterretningsformål», dvs. formål om å ivareta en eller flere av E-tjenestens oppgaver etter lovens kapittel 3, jf. § 1-3 bokstav c. Formålene som kan begrunne tilrettelagt innhenting gjelder dermed alle E-tjenestens oppgaver slik de beskrives i lovens kapittel 3. Dette innebærer at E-tjenesten er gitt *svært vide fullmakter* til å benytte seg av denne metoden for informasjonsinnhenting.

Etterretningsformålene i etterretningsloven §§ 3-1 og 3-2 omfatter blant annet sikring av Norges «politiske og økonomiske handlefrihet», «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», «episode- og krisehåndtering» og eksportkontroll etter eksportkontrolloven eller i sanksjonsforskrifter i medhold av annen lovgivning.

Norges institusjon for menneskerettigheter (NIM) tok i høringsrunden opp at det i stor grad er overlatt til E-tjenesten å definere virkeområdet for innhentingen:

> *«Innenfor rammen av hva som kan karakteriseres som «utenlandske militære og sivile forhold» synes det å være få klare avgrensninger. Blant annet fremgår det i forslaget §3-2, første ledd, bokstav a, at E-tjenesten skal innhente og analysere informasjon for «ivaretakelse av prioriterte utenriks-, forsvars- eller sikkerhetspolitiske interesser knyttet til forhold og utviklingstrekk i andre stater og regioner,». Umiddelbart fremstår det som at dette går videre enn å kun dreie seg om nasjonal sikkerhet.*
>
> *Ettersom oppgavebeskrivelsen i kapittel 3 danner yttergrensen for adgangen til bulkinnsamling er det også helt sentralt at disse oppgavene fastsettes på en måte som ikke i altfor stor grad overlater til E-tjenesten å definere innholdet.*
>
> *NIM mener derfor at det innenfor rammen av oppgavebeskrivelsene i kapittel 3, bør fastsettes ytterligere innskrenkninger eller presiseringer av hvilke formål som kan berettige tilrettelagt innhenting. Det på ingen måte gitt at det er nødvendig at virkeområdet korresponderer med E-tjenestens generelle oppgavebeskrivelse.»*

I EU-domstolens praksis er det stilt krav til at det må foreligge tilstrekkelig konkrete omstendigheter som gjør det mulig å anta at det er en alvorlig trussel mot *den nasjonale sikkerhet*, noe som utgjør en skranke for hvilke formål som kan begrunne tilrettelagt innhenting. Slik NIM påpeker i sin

høringsuttalelse, er formålene i lovens kapittel 3 vidt formulert og dreier seg om langt mer enn nasjonal sikkerhet. Dette innebærer at tilrettelagt innhenting er tillatt i langt flere tilfeller enn hva EU-domstolen tillater.

På bakgrunn av den svært vide formålsangivelsen, som går langt utover nasjonal sikkerhet, er det etter saksøkernes syn også klart at det første av EMDs kriterier, som dreier seg om «the grounds on which bulk interception may be authorised», ikke er oppfylt. EMD har i Big Brother Watch m.fl. mot Storbritannia uttalt at jo videre formålene er formulert, jo større er potensialet for misbruk.[48]

7.2.3 Terskelen for inngrep ved tilrettelagt innhenting er for lav

EU-domstolen krever at det må foreligge tilstrekkelig konkrete omstendigheter som gjør det mulig å anta at det er en alvorlig trussel mot den nasjonale sikkerhet, som er reell og aktuell eller mulig å forutse. Dette kravet innebærer at det er oppstilt en høy terskel knyttet til alvorlighetsgraden av en konkret trussel som kan begrunne pålegg til tjenestetilbydere om plikt til å lagre data.

EU-domstolen har utdypet hva den sikter til med nasjonal sikkerhet under det første kriteriet i La Quadrature du Net-dommens avsnitt 135:

> *"[…] the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilizing 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."*

Terskelen for speiling som grunnlag for søk i lagrede metadata etter § 7-8 og innhenting og lagring av innholdsdata etter § 7-9, ble i Prop. 92 L (2022–2023) foreslått endret sammenliknet med forslaget i høringsnotat, med den virkning at EU-domstolens La Quadrature-kriterier er fjernet fra lovteksten. Dette til tross for at det blant høringsinstansene var bred støtte for å inkludere kriteriene. Også statens egne, interdepartementale arbeidsgruppe som fikk ansvar for å vurdere lovgivningen opp mot EMD og EU-domstolens nye dommer, konkluderte med at:

> *«Loven anses også forenlig med avgjørelsene fra EU-domstolen, med forbehold for at LQN-kriteriene trolig bør komme klarere til uttrykk i § 7-3.»*[49]

I den nå vedtatte lovteksten er kriteriene erstattet med ordlyden «nødvendig for å etablere et informasjonsgrunnlag for etterretningsformål», som oppstiller en betydelig lavere terskel enn hva EU-domstolen krever. Vilkåret er svært vagt formulert, slik at det vil være vanskelig for domstolen å overprøve, noe som gir E-tjenesten et vidt spillerom. Videre inneholder vilkåret kun en nødvendighetsvurdering der søkelyset er rettet mot *E- tjenestens behov* for informasjonsgrunnlag for etterretningsformål. Verken EU-domstolens krav om at det er (1) tilstrekkelig konkrete

[48] Big Brother Watch and others mot Storbritannia avsnitt 370.

[49] Sitert fra gjengivelse i Prop. 92 L (2022–2023) punkt 2.2

omstendigheter som gjør det mulig å anta at det er en alvorlig trussel mot den nasjonale sikkerhet, eller kravet om at (2) trusselen anses må reell og aktuell eller mulig å forutse, er ivaretatt som en del av terskelen for å tillate speiling.

La Quadrature-kriteriene og hensynene bak dem er heller ikke ivaretatt i loven for øvrig, slik departementet uriktig legger til grunn i Prop.92 L (2022–2023). Departementet legger i forarbeidene stor vekt på at terskelens betydning for systemets etterretningsmessige verdi. Argumentasjonen fremstår slik at terskelen for speiling bevisst er senket på bekostning av individers rett til personvern. Dette er forsøkt rettferdiggjort med en påstand som at dataene som lagres er effektivt beskyttet mot misbruk. EU-domstolen kriterier knytter seg imidlertid ikke bare til rettsikkerhetsgarantiene omkring innhenting av data, men også til i hvilke tilfeller innhenting i det hele tatt kan tillates.

Etterretningstjenesteloven legger i det hele tatt ikke opp til at det kan gjøres noen reell vurdering av hvilke trusler som foreligger mot den nasjonale sikkerhet på speilingsstadiet. Dette er ikke en del av kriteriene domstolen skal prøve, og heller ikke blant informasjonen E-tjenesten må gi domstolen i sin begjæring, jf. lovens § 8-2 (1) og (2).

Terkelsen for inngrep i form av speiling er betydelig senket sammenliknet med den tidligere formuleringen av La Quadrature-kriteriene. Dette innebærer at inngrepet i individers privatliv og personvern vil kunne tillates i et betydelig større antall tilfeller i lovteksten som nå er vedtatt i Stortinget, i strid med EU-domstolens krav.

Det norske systemet legger opp til omfattende innhenting av data uten noen tilstrekkelig og konkret prøving av trusselnivået, med et mer eller mindre permanent system for lagring av rådata - og dermed reelt sett også metadata (som kan gjenskapes fra rådataene), uten at dette i tilstrekkelig grad kan knyttes direkte til bestemte alvorlige trusler mot nasjonal sikkerhet.

7.2.4 Beviskravene er ikke konkrete

Bevisene for at EU-domstolens kriterier er oppfylt må ifølge domstolen være konkrete («sufficiently solid grounds for considering»).[50] Kravene til en alvorlig trussel mot nasjonal sikkerhet som kan begrunne innhenting, er som nevnt at den er *reell og aktuell* eller *mulig å forutse*.

I Forsvarsdepartementets høringsnotatet av 27. juni 2022 er det på s. 24 uttalt at:

> *«Det er likevel grunn til å understreke at verdien av en slik overprøving ved retten ikke må overdrives. De forhold som tingretten skal prøve, faller utenfor hva en dommer normalt er forutsatt å vurdere og gjelder en vurdering som forutsetter omfattende innsikt i alle deler av trusselbildet mot Norge og norske interesser. Det vil derfor være naturlig å anta at domstolen vil se hen til de regelmessige vurderinger av trusselbildet*

[50] La Quadrature du Net, avsnitt 137.

som blant annet fremkommer av Etterretningstjenestens og PSTs graderte vurderinger. Disse fremlegges også for offentligheten i ugraderte versjoner.»

Disse trusselvurderingene, som skal utgjøre hovedelementet i vurderingen av om speiling skal tillates etter § 7-3, tilhører etterretningsmyndighetene. Etter loven vil det derfor være E-tjenestens *egne* vurderinger som er det bærende for om det skal samles inn personopplysninger etterretningsmyndighetene ønsker å få samlet inn. Dette er i strid med de kravene som er oppstilt i EU-domstolens rettspraksis.

Det stilles i etterretningstjenesteloven ikke krav til at det må foreligge *tilstrekkelig konkrete* omstendigheter som gjør det mulig å anta at det er en alvorlig trussel mot den nasjonale sikkerhet. Domstolen vil i sin prøving ikke motta informasjon om gjør en slik vurdering mulig, jf. lovens § 8-2. Dette innebærer at det vil kunne bli innført et mer eller mindre permanent system for lagring av rådata, og dermed også metadata, uten at dette i tilstrekkelig grad kan knyttes direkte til bestemte alvorlige trusler mot nasjonal sikkerhet.

7.2.5 Plikten til filtrering mangler realitet

Plikten til utvalg og filtrering i etterretningstjenesteloven § 7-6 er «svake plikter». E-tjenesten er kun forpliktet til å gjøre utvalg og implementere filtre som *så langt det er mulig* søker å hindre innhenting av kommunikasjon om ikke krysser grensen eller intern kommunikasjon.

En rekke høringsinstanser har pekt på at avgrensningen til grenseoverskridende kommunikasjon har liten eller ingen betydning. Trafikken vil normalt passere grensen, selv om det er tale om kommunikasjon mellom en avsender og en mottaker som begge befinner seg i Norge. Hvilken digital kommunikasjon som krysser grensen, er ganske vilkårlig. Blant høringsinstansene som gir uttrykk for synspunkter i denne retningen, er Advokatforeningen, Datatilsynet, Den norske dataforening – IT-politisk råd, Elektronisk Forpost Norge og SINTEF. Telenor skriver i sin høringsuttalelse:

«En stadig større del av norske borgeres og virksomheters innbyrdes kommunikasjon passerer over Norges grenser. Dette er en konsekvens av at kommunikasjonen i økende grad foregår over utenlandske tjenester, samt at ekom-tilbydernes egne tjenester i økende grad baserer seg på fasiliteter utenfor Norges grenser jf. ekomforskriften § 7-5.»[51]

Hvor stor andel av kommunikasjonen som kan regnes som grensekryssende avhenger av hvilke forutsetninger som legges til grunn. NRK viser i en artikkel at egne tester gjort av NRK Beta og estimater fra Telenor viser at en betydelig andel av helt ordinær norsk trafikk vil kunne lagres av norske myndigheter.[52]

[51] https://www.regjeringen.no/contentassets/121962acfa35479baa3ecc29874fcaec/horingssvar-telenor.pdf?uid=Høringssvar_Telenor

[52] Slik kan den nye etterretningsloven påvirke deg (nrkbeta.no)

Forutsetningen om kommunikasjon mellom personer i Norge skal filtreres ut, gir ikke mening for mange av kommunikasjonsmåtene, ettersom det er svært vanskelig å se for seg treffsikker filtrering, uten å kjenne identiteten til personen bak f.eks. et brukernavn eller en IP-adresse på forhånd. Dette med mindre man samler inn store mengder identifiserende informasjon og gjør en sammenkobling, noe som i seg selv ville være ekstremt inngripende, og som E-tjenesten mangler hjemmel til å gjøre. Departementet selv erkjenner i Prop.80 L (2019–2020) s. 215 følgende:

> *«At tjenesten skal «søke å» hindre lagring, synliggjør at det ikke alltid vil være mulig å filtrere bort irrelevant data. Det vil ofte måtte lagres store mengder irrelevante data fra enkelte kommunikasjonsstrømmer, fordi det ikke er mulig å filtrere bort informasjonen som er uten interesse.»*

Tekna anser i sitt høringssvar at det er urealistisk å få til en effektiv og treffende filtrering. I samme retning uttaler Datatilsynet seg:

> *«At det er vanskelig å filtrere bort overskuddsinformasjon er åpenbart. Det vises til høringsnotatets pkt. 8.6.3, hvor det argumenteres med at det ikke finnes «realistiske alternativer for å filtrere ut ikke-relevant informasjon fra datasettene.» fra informasjon som er innhentet gjennom tilrettelagt innhenting. Metodene for filtrering beskrives ved å vise til et eksempel om å filtrere bort samtaler fra + 47 til + 47. Dette vil trolig få begrenset betydning, sett hen til hvordan kommunikasjon foregår på ulike plattformer i dag. Lovforslagets bestemmelse om filtrering er uklart formulert, og kan gi et uriktig inntrykk av filtrenes effektivitet. Dette gjør det vanskelig å overskue hvem som i praksis vil kunne bli gjenstand for søk.»*

I lys av dette er det i beste fall uklart om filtrering i noen betydelig grad vil kunne avhjelpe inngrep i privatlivet og personvernet til personer i Norge som kommuniserer med hverandre eller selv er aktive på internett. Samtidig utgjør innhenting og filtrering av personopplysninger i seg selv alvorlige inngrep i personvernet.

Etter EMDs ovenfor refererte dom i saken Wieder and Guarnieri mot Storbritannia, er det uansett slik 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. De kriteriene som EMD ellers har oppstilt for at slik overvåkning skal være forenlig med EMK, gjelder fullt ut også overfor kommunikasjon der avsender og/eller mottaker befinner seg utenfor Norge. Dette innebærer at E-tjenestelovens forsøk på å skille mellom innenlands og utenlandskommunikasjon egentlig er irrelevant for dette søksmålets tema.

7.2.6 Domstolskontrollen er mangelfull

Som del av kravet til «end-to-end safeguards» stiller EMD klare krav til at bulkovervåkning skal være underlagt «independent authorisation at the outset, when the object and scope of the bulk operation are being defined», dvs. *før* innsamlingen begynner.[53]

Det er på det rene at dette kravet ikke er oppfylt for testanalyse etter etterretningstjenesteloven § 7-3. Om saksøkte skulle være av en annen oppfatning, bes det opplyst. Videre er heller ikke teknisk analyse etter etterretningstjenestelovens § 7-3 (2) underlagt domstolskontroll eller annen avhengig kontroll. Om saksøkte skulle være av en annen oppfatning, bes det opplyst.

I strid med EMDs praksis er det heller ingen domstolskontroll ved selve lagringen av metadata. Om saksøkte skulle være av en annen oppfatning, bes det opplyst, herunder med henvisning hvor i lovverket dette eventuelt fremgår.

Dette innebærer at det skjer lagring av kommunikasjonsdata før det skjer noen domstolskontroll.

Den domstolskontrollen deler av systemet for tilrettelagt innhenting er underlagt innebærer heller ingen «effective safeguard against abuse», slik EMD har stilt krav om. Dette er departementet selv inne på i høringsnotatet av 27. juni 2022:

> *«Det er likevel grunn til å understreke at verdien av en slik overprøving ved retten ikke må overdrives. De forhold som tingretten skal prøve, faller utenfor hva en dommer normalt er forutsatt å vurdere og gjelder en vurdering som forutsetter omfattende innsikt i alle deler av trusselbildet mot Norge og norske interesser.»*

Departementets oppsummerer høringsuttalelsene til det opprinnelige forslaget til ny etterretningstjenestelov slik i Prop. 80 L (2019–2020) s. 117:

> *«Advokatforeningen støtter forslaget om domstolskontroll, men stiller spørsmål ved hvilken reell mulighet domstolen har til å utøve effektiv kontroll. Foreningen mener at domstolens faktiske mulighet til å utøve forhåndskontroll bør styrkes. Datatilsynet, Den internasjonale juristkommisjon norsk avdeling (ICJ-Norge) og NRK gir uttrykk for synspunkter i samme retning.»*

Flere av høringsinstansene var kritiske til at domstolen skal være avhengig av E-tjenesten for sakens opplysning, spesielt med hensyn til tekniske forhold. NIM uttalte følgende i høringsrunden, men henvisning til EMDs krav:

> *«Behovet for særskilt kompetanse er fremhevet av EMD. Ettersom det er lagt opp til at avgjørelsene skal treffes av ordinære dommere, er det nærliggende at retten gis*

[53] Centrum för Rättvisa mot Sverige avsnitt 264.

fagkyndig bistand. Av hensyn til domstolens uavhengighet er NIM i utgangspunktet lite positive til forslaget om at dette alene ivaretas ved at E-tjenesten selv medbringer fagkyndig. Etter NIMs oppfatning bør det legges opp til et spor hvor domstolen kan innhente uavhengig faglig bistand, og på den måten også sikre at domstolens kontroll oppleves som reell, effektiv og uavhengig.»

I den helhetsvurdering som EMDs praksis også legger opp til, vil også denne svakheten spille inn.

Innholdet i rettens kjennelser etter E-tjenesteloven kapittel 8, er graderte, jf § 8-7, men det fremgår så vidt kan ses ikke at opplysning om at det *er* avsagt kjennelser, er gradert. Det bes derfor opplyst om følgende:

- Hvor mange kjennelser etter E-tjenesteloven kapittel 8 har Oslo tingrett avsagt siden lovens ikrafttredelse?
- I hvor mange av sakene har det vært gjennomført muntlige forhandlinger?
- I hvor mange saker har E-tjenestens begjæringer blitt tatt til følge?
- I hvor mange saker har henholdsvis E-tjenesten og/eller den særskilte advokaten anket tingrettens kjennelse til lagmannsretten og/eller videre til Høyesterett?

7.2.7 Systemet for TI åpner for retrospektive søk

I forarbeidene og høringsnotatene til etterretningstjenesteloven legges det stor vekt på at systemet for tilrettelagt innhenting må legge til rette for «retrospektiv analyse»/«retrospektive søk». I høringsnotatet av 12. november 2018 er det uttalt:

«Utvalget foreslår at metadata skal lagres i så lang tid som anses nødvendig for å løse etterretningsoppdrag, og maksimalt 18 måneder. Dette antallet måneder vurderes som nødvendig og tilstrekkelig for å kunne gjennomføre en tilfredsstillende retrospektiv analyse av trafikkdata.»

Videre er retrospektive søk behandlet i høringsnotatet av 27. juni 2022:

«For det tredje er det behov for å gjøre retrospektive søk tilbake i tid, hvilket forutsetter at beslutning om speiling av kommunikasjonsstrømmer for lagring av metadata i tid kommer forut for rettens tillatelse til å gjøre søk i lagrede data.
[…]
Når Etterretningstjenesten får rettens tillatelse til å gjøre søk, er det derfor av stor betydning at det finnes et historisk søkegrunnlag. Behovet for å gjøre retrospektive søk tilbake i tid underbygger således ytterligere at det ikke er mulig å foreta en samlet vurdering av hvilke kommunikasjonsstrømmer som bør speiles sett opp mot de søkene som man begjærer om rettens samtykke til å gjennomføre.»

Her fremkommer det at E-tjenesten vil gjøre «tilbakevirkende» søk i data som ble samlet inn *før* retten har gitt godkjenning til å gjøre søk.

Datatilsynet har vært kritiske til adgang til å gjøre retrospektive søk, også når det er blitt innført domstolskontroll på speilingsstadiet. I høringen til høringsnotatet av 27. juni 2022 uttalte Datatilsynet følgende:

> *«Forslaget åpner for retrospektivt søk i allerede innsamlede kommunikasjonsstrømmer og fortsatt innsamling etter domstolskontroll. Datatilsynet mener dette ikke innebærer en reell utvelgelse av kommunikasjonsstrømmer da opplysningene allerede er innsamlet og domstolskontrollen blir illusorisk siden det allerede har blitt foretatt søk etter etterretningsrelevante opplysninger før tidspunktet for domstolskontroll.*
> *[…]*
> *Datatilsynet vil bemerke at formuleringen «utelukkende skal benyttes for testing og analyse» ikke beskriver formålene med metadatalageret i tilstrekkelig grad. Slik bestemmelsen i § 7-7 om metadatalageret er utformet i dag så vil metadatalageret inneholde alle relevante kommunikasjonsstrømmer og brukes til testing og analyse, men også som grunnlag for retrospektive søk – altså søk tilbake i tid før domstolens beslutning og innhenting av kommunikasjonsstrømmer.*
> *[…]*
> *Hovedproblemet med forslaget er at metadatalageret beholdes for å danne grunnlag for retrospektive søk og ikke bare som et utgangspunkt for test og analyse for å finne kommunikasjonsstrømmer med etterretningsrelevant informasjon.*
>
> *Dette er en ordning det er vanskelig å finne støtte for i EMD-praksis, og den er heller ikke drøftet i høringsnotatet.»*

Slik Datatilsynet skriver i sin høringsuttalelse til Stortinget 20. mars 2023 er dette en ordning som er i strid med EMDs og EU-domstolens praksis:

> *«Forslaget gir også mulighet for retrospektive søk. Dette åpner for at Etterretningstjenesten kan gjøre søk i materiale innhentet før det foreligger en avgjørelse fra domstolen som åpner for søk. Dette er ikke en ordning som det er åpnet for i EMD og Europadomstolen.»*

7.2.8 Den løpende kontrollen er mangelfull

Hele prosessen med bulkinnsamlig må ifølge EMD underlegges tilsyn av en uavhengig myndighet som er

> *«[s]ufficiently robust to keep the "interference" to what is "necessary in a democratic society".»*[54]

[54] Centrum för rättvisa mot Sverige avsnitt 270.

Kontrollen skal vurderes i henhold til EMDs syvende krav til klart definerte regler i nasjonal lovgivning:

> *«The procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance».*[55]

Av etterretningstjenesteloven § 7-11 første ledd fremgår det at EOS-utvalget skal 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.» I andre og tredje ledd er det gitt regler om EOS-tjenestens tilgang til informasjon og E-tjenestens plikt til å tilrettelegge for kontroll gjennom tekniske løsninger.

EOS-utvalget selv mente i sin høringsuttalelse til forslaget til ny etterretningstjenestelov i 2018, at en slik kontroll lovforslaget la opp til ikke var mulig:

> *«EOS-utvalgets kontroll med EOS-tjenestene, inkludert E-tjenesten, er ikke innrettet slik at den innebærer en full kontroll av alle sider av tjenestenes EOS-virksomhet. En fullstendig kontroll ville være for omfattende for utvalget, og det er et spørsmål om en slik kontroll overhodet er mulig eller ønskelig. Utvalget velger hvilke av tjenestens aktiviteter som skal undersøkes nærmere, blant annet basert på kriterier i EOS-kontrolloven og utvalgets vurderinger av hvor risikoen for rettighetskrenkelser og regelbrudd med alvorlige konsekvenser er størst. Selv om utvalget har full innsynsrett i E-tjenesten, med unntak for særlig sensitiv informasjon, vil ikke alle tjenestens aktiviteter bli kontrollert.*
>
> *Evalueringen av EOS-utvalget i 2016 viste at utvalgets kapasitet allerede da var presset. Utvalgsmodellen begrenser utvalgets kapasitet og dermed omfanget av kontrollvirksomheten. En utvidelse av kontrolloppgaven til å omfatte en styrket kontroll med tilrettelagt innhenting vil føre til flere oppgaver for utvalget. Det vil redusere utvalgets kapasitet til å kontrollere de andre EOS-tjenestene og andre sider ved E-tjenestens virksomhet.»*

Kontrollmekanismene med tilgang og søk er mangelfulle. Videre er det er en betydelig forholdsmessig skjevfordeling av ressurser mellom overvåkningstjenestene og EOS-utvalget. Som vist ovenfor, har budsjettene til PST, E-tjenesten og Nasjonal sikkerhetsmyndighet har doblet seg de siste fem årene, til 4,8 milliarder kroner årlig pr. 2023. Anslagsvis 3300 personer jobber i disse tre tjenestene. Til sammenligning har EOS-utvalgets syv medlemmer hjelp fra 22 ansatte, og et budsjett på 41 millioner kroner i året.. EOS-utvalgets leder har i forbindelse med innføring av den nye

[55] Centrum för rättvisa mot Sverige avsnitt 275.

etterretningstjenesteloven uttalt at «selve kontrollmodellen begynner å utfordres», se Morgenbladets artikkel fremlagt ovenfor.

7.2.9 Den etterfølgende kontrollen er mangelfull

EMD stiller i sitt åttende kriterium krav til den etterfølgende kontrollen med bulkinnsamlig av kommunikasjonsdata:

> *«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.»*

På dette kontrollstadiet legger EMD særlig vekt på hvilken mulighet den enkelte har til å få prøvd lovmessigheten av et mulig eller faktisk inngrep. EMD stiller derfor krav til at et effektivt rettsmiddel skal være tilgjengelig for den som mistenker at sin kommunikasjon er overvåket, for å kunne utfordre overvåkningens lovlighet og overholdelse av EMK.[57]

Dette behovet kan ivaretas ved notifikasjon til den enkelte etter at inngrepet er avsluttet. I fravær av et krav om notifikasjon, krever EMD at det må være tilgjengelig et rettsmiddel gjennom et organ uavhengig av utøvende myndigheter, som sikrer en rettferdig og kontradiktorisk prosess. Organet må ha myndighet til å beslutte at overvåkning er ulovlig og beslutte ødeleggelse av ulovlig innhentet data.[58] EMD stiller i Centrum för Rättvisa mot Sverige avsnitt 362 krav til at utfallet av den etterfølgende kontrollen skal være er begrunnet og rettslig bindende avgjørelse:

> *"[A] legal procedure before an independent body, which in so far as possible offers an adversarial process resulting in reasoned and legally binding decisions, is an essential element of an effective ex post facto review."*

Utfallet av EOS-utvalgets klagebehandling er nærmere regulert i EOS-kontrolloven § 15 (1):

> *Uttalelser til klagere bør være så fullstendige som mulig uten at det gis graderte opplysninger. Opplysning om at noen har vært gjenstand for overvåkingsvirksomhet 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.*

Av bestemmelsen fremgår at den som klager til EOS-utvalget ikke har krav på noen begrunnelse, utover en uttalelse om hvorvidt klagen har gitt grunn til kritikk eller ikke, når klagen gjelder overvåkingsmessig virksomhet, jf. bestemmelsens tredje ledd. Opplysning om at noen har vært gjenstand for overvåkingsvirksomhet eller ikke, anses ifølge annet ledd som gradert, hvis annet ikke

[56] Centrum för rättvisa mot Sverige avsnitt 275.
[57] Centrum för rättvisa mot Sverige, avsnitt 271.
[58] Centrum för rättvisa mot Sverige, avsnitt 271–273.

blir bestemt. Adgangen til å gi en ytterligere begrunnelse er betinget av E-tjenestens eller departementets samtykke. I Prop.80 L (2019–2020) på s. 232 uttaler departementet:

> *«Det understrekes at bestemmelsen ikke innebærer noe forbud mot å gi slik underretning. Dette innebærer at Etterretningstjenesten eller overordnet myndighet etter forholdene kan gi underretning dersom lovbestemt taushetsplikt eller andre regler ikke er til hinder for det, og det for øvrig regnes som sikkerhetsmessig forsvarlig. På grunn av behovet for å skjerme informasjon om Etterretningstjenestens virksomhet, vil underretning likevel sjelden være aktuelt.»*

Dette innebærer at EMDs krav til en begrunnet avgjørelse ikke er oppfylt. Den norske lovgivningen er på dette punktet sammenliknbar med den svenske lovgivningen. I Centrum för Rättvisa mot Sverige trakk EMD fram fraværet av en effektiv etterfølgende kontroll som en av tre grunnleggende mangler ved det svenske systemet, blant annet på grunn av fraværet av muligheten til å få en begrunnet avgjørelse etter en henvendelse eller klage knyttet til bulkovervåkning.

Samtidig fremgår det av EOS-kontrolloven § 15 (1) at den sanksjon EOS-tjenesten har tilgang til overfor E-tjenesten er «kritikk». Utvalget har ikke myndighet til å beslutte at overvåkning er ulovlig og beslutte ødeleggelse av ulovlig innhentet data, jf. etterretningstjenesteloven § 7-12. Dette innebærer at EOS-utvalgets etterfølgende kontroll ikke oppfyller EMDs krav til at det skal kunne avgis en rettslig bindende avgjørelse, med beslutning om at overvåkningen er ulovlig og avgjørelse om ødeleggelse av ulovlig innhentet data.

Ifølge EMD var den etterfølgende kontrollen i det svenske systemet også mangelfull fordi tilsynsmyndigheten har en dobbeltrolle, ved at den både førte tilsyn med etterretningstjenestens aktiviteter og gjennomførte etterfølgende kontroll på forespørsel fra enkeltpersoner. Også denne konklusjonen er overførbar til EOS-utvalgets rolle, som er gitt ansvar for både den løpende og den etterfølgende kontrollen. En slik ordning kan ifølge EMDs Storkammer lede til at tilsynsmyndigheten måtte vurdere sin egen tilsynsvirksomhet, noe som kan lede til interessekonflikter. Dette innebærer at det ikke finnes reelle kontrollmekanismer.

Felles for mekanismene i systemet for tilrettelagt innhenting som angivelig skal ivareta borgernes rettigheter, er at de baserer seg på manuelle og menneskelige prosesser som ikke vil gi noe realistisk vern av rettighetene det gjøres inngrep i, slik at systemet ikke gir noen beskyttelse eller kontroll av individets interesser.

7.2.10 Kravene til overvåkningens varighet, lagringstid og sletting er mangelfulle

Den unødvendig og uforholdsmessig lange lagringstiden av kommunikasjonsdata er i strid med EMDs krav til nødvendighet og forholdsmessighet. EMDs kriterier inneholder krav til klare regler om «[t]he limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed».[59]

[59] Centrum för rättvisa mot Sverige, avsnitt 275.

Det bes opplyst om innhentet data slettes fra alle systemer i virksomheten når lagringstiden er utløpt og/eller om det finnes innhentede data (eksempelvis rådata) som ikke slettes.

I lovens § 9-8 er det gitt generelle regler om 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 av gangen. 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.*
>
> *Sletting av personopplysninger i operative systemer og registre som er tilgjengelige for etterretningsproduksjon, er ikke til hinder for lagring av opplysningene etter annen lov.*

Denne sletteplikten oppfyller ikke EMDs krav. Når rådata kan beholdes i inntil 15 år, og noen ganger lengre, innebærer det at data reelt sett ikke blir slettet i denne perioden. Som eksempel nevnes at metadata kan gjenskapes med utgangpunkt i rådataene. Det kan heller ikke forventes av data delt med andre aktører blir slettet.

Videre stilles det ikke krav om sletting av data som ikke inneholder personopplysninger eller kildeidentifiserende opplysninger. I § 9-8 andre ledd fremgår det likevel at metadata som er innhentet og lagret i bulk i samsvar med § 7-7, skal slettes senest etter 18 måneder, jf. § 7-7 tredje ledd. Dette gjelder imidlertid ikke innholdsdata, som dermed kan lagres i 15 år og noen ganger lengre, jf. § 9-8 andre ledd første punktum. Lagring av slike data kan være svært inngripende overfor virksomheter, og kan som eksempel gripe inn i hensynet til å bevare forretningshemmeligheter.

7.2.11 Reglene om deling av overvåkningsmateriale oppfyller ikke EMDs krav

EMD stiller i Centrum för Rättvisa mot Sverige avnsitt 276 krav til utlevering av overvåkningsmateriale innhentet ved bulkinnsamling til andre stater og internasjonale organisasjoner:

> *"[…] the Court considers that the transmission by a Contracting State to foreign States or international organisations of material obtained by bulk interception should be limited to such material as has been collected and stored in a Convention compliant manner and should be subject to certain additional specific safeguards pertaining to the transfer itself. First of all, the circumstances in which such a transfer may take place must be set out clearly in domestic law. Secondly, the transferring State must ensure*

that the receiving State, in handling the data, has in place safeguards capable of preventing abuse and disproportionate interference. In particular, the receiving State must guarantee the secure storage of the material and restrict its onward disclosure. This does not necessarily mean that the receiving State must have comparable protection to that of the transferring State; nor does it necessarily require that an assurance is given prior to every transfer. Thirdly, heightened safeguards will be necessary when it is clear that material requiring special confidentiality – such as confidential journalistic material – is being transferred. Finally, the Court considers that the transfer of material to foreign intelligence partners should also be subject to independent control."

De norske reglene om deling av overvåkningsmateriale med andre oppfyller ikke EMDs krav, verken når det gjelder deling med andre nasjonale myndigheter, andre staters myndigheter eller internasjonale organisasjoner.

8 NÆRMERE OM MIDTPUNKTINNHENTING OG ENDEPUNKTINNHENTING

I E-tjenesteloven § 6-9 er det gitt følgende bestemmelse:

> *Etterretningstjenesten kan innhente elektronisk kommunikasjon i transitt og kartlegge kommunikasjonsinfrastruktur. Bestemmelser om tilrettelagt innhenting av elektronisk kommunikasjon som transporteres over den norske grensen, er gitt i kapittel 7 og 8.*

Bestemmelsen gir E-tjenesten blant annet 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 hvilken som helst annet overføringsmedium og uavhengig av teknologi, mens kommunikasjonen er i transitt mellom avsender og mottaker. Slik innhenting vil også omfatte bulkinnhenting av kommunikasjonsdata, jf. forarbeidene (høringsnotat av 12. november 2018 punkt 8.3.2).

I E-tjenesteloven § 6-10 er det gitt følgende bestemmelse:

> *Etterretningstjenesten kan observere og innhente ikke åpent tilgjengelig elektronisk informasjon i datasystemer eller lignende systemer eller tjenester som etterretningsmål besitter eller antas å ville benytte.*
>
> *Dersom det er grunn til å tro at innhentingen vil omfatte informasjon som ikke er ment for kommunikasjon, skal den ikke gjennomføres med mindre det er strengt nødvendig.*

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. Det er presisert i forarbeidene at bestemmelsen ikke inneholder avgrensninger med hensyn til teknologi, slik at den gjelder uavhengig både av hvilke «endepunkter» (der informasjon ligger lagret) det gjelder og av på hvilken måte E-tjenesten får tilgang til avlesning og innhenting (bortsett fra at eventuelle pålegg

om tilrettelegging fra tjenestetilbydere av kommunikasjonstjenester må følge reglene i kapittel 7). Et slikt «endepunkt» kan for eksempel være en server hos en tjenesteleverandør som lagrer elektronisk informasjon for/om et stort antall personer. Også denne bestemmelsen hjemler innhenting av rådata i bulk.

Heller ikke disse tiltakene tilfredsstiller Grunnlovens og EMKs krav til lovlige inngrep i ytringsfriheten og personvernet – og en grunnleggende mangel i den sammenheng, er at metodene kan brukes uten noen som helst forhåndsgodkjennelse av retten eller tilsvarende uavhengig judisiell kontroll.

9 NÆRMERE OM E-TJENESTENS KJØP AV METADATA I BULK

EOS-utvalget har avdekket at E-tjenesten, før etterretningstjenesteloven kapittel 7 trådte i kraft, har kjøpt metadata i bulk fra kommersielle aktører uten hjemmel i etterretningstjenesteloven. Saksøkerne mener at dette er et inngrep som mangler hjemmel i lov, og dermed utgjør et ulovlig inngrep i retten privatliv, personvern og ytringsfrihet. Saksøkerne krever derfor at E-tjenestens behandling og lagring av kommunikasjonsdata etter kjøp av metadata fra kommersielle aktører opphører.

EOS-utvalget pekte i sin årsmelding til Stortinget for 2022 på at E-tjenestens kjøp av metadata i bulk er et inngrep i retten til privatliv, som skjer uten at etterretningstjenestelovens regler følges:

> *«Utvalget har stilt spørsmål til E-tjenesten om tjenestens hjemmelsgrunnlag for kjøp av metadata fra kommersielle aktører. E-tjenesten mente at enkelte anskaffelser av data fra kommersielle tilbydere ikke innebærer bruk av en inngripende metode etter e-loven kapittel 6.*
>
> *Tjenesten anså derfor at forbudet mot innhenting i Norge etter e-loven § 4-1 ikke kom til anvendelse for den type anskaffelse av metadata som saken gjaldt. E-tjenesten mente at det er måten tjenesten kommer i besittelse av dataene på som er avgjørende for om anskaffelsen faller inn under e-loven kapittel 6 eller ikke.*
>
> *Det sentrale spørsmålet for utvalget var om kjøp av metadata i bulk som inneholder personopplysninger utgjør et inngrep i enkeltpersoners privatliv. Rettspraksis fra Den europeiske menneskerettighetsdomstolen (EMD) viser at metoder som utgjør et slikt inngrep, krever klar forankring i lov.*
>
> *I forarbeidene[7] til e-loven skrev Forsvarsdepartementet (FD) at «hensikten med forslaget er å gi klarere rettslige rammer for Etterretningstjenestens bruk av inngripende metoder, av hensyn til det menneskerettslige lovkravet».*
>
> *Selv om FD mente at innhenting fra åpne kilder i utgangspunktet «faller inn under den alminnelige handlefrihet»[8], foreslo departementet likevel å regulere metoden særskilt. Dette ble i høringsnotatet til ny e-lov begrunnet med at «innhentingen ikke skjer med*

samtykke fra den eller de personer som berøres av innhentingen, og fordi summen av informasjon som innhentes om en og samme person, og sammenstillingen av slik informasjon over tid, etter omstendighetene kan utgjøre et inngrep overfor den enkelte, selv om den enkelte selv har valgt å dele informasjonen åpent».[9]

Utvalget uttalte at de samme hensynene gjør seg gjeldende ved kjøp av metadata i bulk som inneholder personopplysninger som personer etterlater seg på nett. Sammenstilling av slike metadata kan generere innholdsdata, og gjennom sammenstillingen av data fra flere kilder er det risiko for at personer kan identifiseres fra datasett som i utgangspunktet er anonyme.

Utvalget mente at denne typen kjøp måtte anses som innhenting av informasjon som kan medføre inngrep overfor den enkelte. Slik innhenting kan bare skje i den utstrekning det er hjemmel for det i e-loven kapittel 6. Utvalget var uenig med E-tjenesten i lovlighetsvurderingen.

E-tjenesten ble av utvalget oppfordret til å foreta en ny vurdering av om metodebruken må forankres i kapittel 6 i e-loven for å være lovlig. E-tjenesten har opplyst at den vurderer å ta problemstillingen opp med Forsvarsdepartementet.»[60]

Det bes opplyst i hvilket omfang E-tjenesten har kjøpt metadata fra hvilke kommersielle aktører.

Det anføres uansett at den innsamling, lagring og behandling som er gjort eller gjøres gjennom slike kjøp som beskrevet, er i strid med både EMK artikkel 8 og 10 og Grunnloven §§ 100 og 102, prinsipalt og alene av den grunn av at aktiviteten (inngrepet) mangler lovhjemmel.

10 PROSESSUELT

Stiftelsen Tinius varslet offentlig 24. mars 2023, med bred dekning i de fleste riksdekkende aviser, at stiftelsen vil fremme dette søksmålet mot staten, jf. tvisteloven § 5-2.

Flere av de offentlige dokumenter som det er vist til i stevningen, med referanser og eventuelt lenker oppgitt i fotnoter, vil bli aktuelle som del av utdraget for retten. For å rasjonalisere, og unngå at dokumentomfanget blir unødvendig stort, har vi foreløpig ikke fremlagt alt som bilag. Et relevant utvalg vil bli gjort senere i saksforberedelsen, slik at det utvalget blir fremlagt som bilag som kan inntas i utdraget for retten.

Saksøker vil komme nærmere tilbake til hvor mange dager som bør settes av til saken når statens tilsvar foreligger. Foruten dokumentbevis vil det føres vitner, blant annet til å opplyse de tekniske og teknologiske forholdene forbundet med de angrepne tiltakene.

---

[60] EOS-utvalgets årsmelding til Stortinget - Dokument 7:1 (2022–2023) punkt 4.3

11 PÅSTAND

Med forbehold om ytterligere anførsler og bevis, nedlegges slik påstand:

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.

* * *

Stevningen lastet opp i Aktørportalen.

Advokatfirmaet Glittertind AS

Jon Wessel-Aas
advokat (H)

Emanuel Feinberg
advokat (H)

BILAGSLISTE