GLITTERTIND

Borgarting lagmannsrett
via Aktørportalen

Oslo, 5. mai 2025
Sak nr.: 10589-507
Dok.nr.: 6DZNQ6CFDSAV-1000408783-1293
Ansvarlig advokat: Jon Wessel-Aas

ANKE

TIL

BORGARTING LAGMANNSRETT

Sak nr.:	24-038001TVI-TOSL/04
Ankende parter:	1. Stiftelsen Tinius 2. Tom Erik Thorsen
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
Ankemotpart:	Staten v/Forsvarsdepartementet
Prosessfullmektig:	Advokat Ida Thue Regjeringsadvokaten
Rettslig medhjelper:	Advokat Kaija Bjelland Regjeringsadvokaten

INNHOLD

***

1 INNLEDNING

1.1 Innledende merknader

De ankende parter anla søkmål mot staten v/Forsvarsdepartementet, der påstanden for Oslo tingrett lød slik:

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

Oslo tingrett avsa 26. mars 2025 dom i saken, med slik slutning:

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

Stiftelsen Tinius og Tom Erik Thorsen (heretter også benevnt i fellesskap som «Stiftelsen») anker dommen i sin helhet, idet de mener at den bygger feilaktig rettsanvendelse. Stiftelsen og Thorsen vil i ankesaken nedlegge samme påstand som for tingretten.

Tingrettens dom ble forkynt for de ankende parter 26. mars 2025. Ettersom det har vært rettsferie fra og med 12. april og til og med 21. april 2025, jf. domstolloven § 140, er ankefristen 6. mai 2025. Anken er følgelig rettidig.

1.2 Kort om sakens bakgrunn

Ved den nye etterretningstjenesteloven kapittel 7 (om tilrettelagt innhenting – i det videre også benevnt som «TI») lovfestet staten for første gang omfattende vilkårlig masseovervåkning – innhenting, lagring og behandling i bulk – av data om store deler av befolkningens daglige digitale kommunikasjon / aktivitet.

Innsamlingen gjennom TI skjer ved pålegg til tilbydere av elektroniske kommunikasjonstjenester om å tilrettelegge for at Etterretningstjenesten (E-tjenesten) får tilgang til og kan speile og hente ut data fra kommunikasjonsstrømmene inn og ut av Norge, via tilbydernes systemer. De innsamlede og lagrede dataene vil per definisjon i vesentlig grad bestå av kommunikasjonsdata og dermed også informasjon om personer, som i seg selv overhodet ikke har relevans for legitime etterretningsformål.

Betegnende for alvoret er at det utvalget som på oppdrag fra Forsvarsdepartementet utredet hvordan et system (den gang kalt «Digitalt grenseforsvar» - DGF) som kunne gi e-tjenesten tilgang til slike data, Lysne II-utvalget, selv understreket viktigheten av at et slikt system og slike datalagre ikke måtte komme i «feil hender»:

> *«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.»*

Som uttrykt av EMD allerede i 1978, i den grunnleggende avgjørelsen om hemmelig overvåkning (som det konsekvent er vist til i alle senere avgjørelser om hemmelig overvåkning), storkammerdommen i *Klass m.fl. mot Tyskland* avsnitt 42 (med våre uthevninger):

> *«Powers of secret surveilance of citizens,* ***characterizing as they do the police state****, are* ***tolerable*** *under the Convention* ***only in so far as strictly necessary*** *for safegouarding the democratic institutions.»*

Når det gjelder slik vilkårlig masseovervåkning som i vår sak – det vil si innsamling og lagring i bulk av kommunikasjonsdata fra befolkningens bruk av elektroniske kommunikasjonstjenester – er utgangspunktet at det er ulovlig etter EØS-retten, etter EMK og etter Grunnloven.

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

På denne bakgrunn har europeiske staters forsøk på å innføre masseovervåkning i form av preaktiv innsamling og lagring av kommunikasjonsdata i bulk, til bruk i *kriminalitetsbekjempelse,* flere ganger blitt underkjent av blant annet EU-domstolen.

Til tross for dette innførte flere stater tilsvarende masseovervåkningssystemer til bruk for å ivareta *nasjonale sikkerhetsinteresser.*

Også slike systemer har blitt underkjent både av EU-domstolen og EMD. Begge domstolene har likevel åpnet for at denne typen masseovervåkning i form av bulkinnsamling unntaksvis kan aksepteres for å ivareta nasjonal sikkerhet, forutsatt at formålet er tilstrekkelig konkret og tungtveiende (reelle nasjonale sikkerhetsinteresser) og at innrammingen og rettssikkerhetsgarantiene er gode nok. Som uttrykt av EMD i storkammer i *Big Brother Watch mot Storbritannia* avsnitt 339:

> *"In view of the risk that a system of secret surveillance set up to protect national security (and other essential national interests) may undermine or even destroy the*

proper functioning of democratic processes under the cloak of defending them, the Court must be satisfied that there are adequate and effective guarantees against abuse."

De ankende parter mener at det norske systemet for masseovervåkning ikke tilfredsstiller de EØS- og EMK-rettslige krav som er oppstilt av henholdsvis EU-domstolen og EMD. De ankende parter er enig i et system for digitalt grenseforsvar både er viktig og at det kan forsvares innenfor rammene av borgernes grunnleggende rettigheter. Det er samtidig et helt usedvanlig potent system som utfordrer maktforholdet mellom staten og borgerne og demokratiets rammer på en måte som få, om noen, andre statlige tiltak gjør. Det skiller seg også fra andre inngrep i grunnleggende rettigheter ved at det skjer i det skjulte. Det er derfor essensielt at systemet begrenses til det som er strengt nødvendig og rammes inn med strenge rettssikkerhetsgarantier som borgerne kan ha tillit til at er reelle.

Også lovfesting i etterretningstjenesteloven §§ 6-9 og 6-10 av henholdsvis midtpunktinnhenting og endepunktinnhenting, anføres å krenke EMK og Grunnloven, da bestemmelsene hjemler blant annet bulkinnsamling av kommunikasjonsdata i statens egenregi (det vil si at det gjøres uten tilrettelegging fra tilbydere av elektroniske kommunikasjonstjenester), blant annet uten noen form for domstolskontroll. Begge bestemmelsene – hver for seg og samlet sett – åpner også for bulkinnsamling av kommunikasjon som omfatter kommunikasjon til og fra saksøkerne og enhver annen person som befinner seg i Norge. jf. blant annet etterretningstjenesteloven § 4-7.

1.3 Kort om de ankende parter - oppdatering

Når det gjelder de ankende parter, er tingrettens beskrivelse i hovedsak dekkende, men den må korrigeres for så vidt gjelder stiftelsen Tinius:

Gjennom større transaksjoner som ble gjennomført i 2024 – er stiftelsen Tinius (gjennom sitt heleide selskap Blommenholm Industrier AS) i dag *eneeier* av Schibsted Media AS.

Schibsted Media-konsernet omfatter en rekke store medier i Norge, herunder Aftenposten. Verdens Gang og Bergens Tidende. I tillegg omfatter det Aftonbladet og Svenska Dagbladet i Sverige. Schibsted Media AS har også nylig inngått avtale om kjøp av henholdsvis TV4 i Sverige og MTV i Finland (som begge tilsvarer TV 2 i Norge), der gjennomføringen av kjøpet vil skje i løpet av høsten 2025.

Stiftelsen Tinius er derfor eneeier av et mediekonsern som omfatter flere store medier i Norge, Sverige og (i løpet av 2025) Finland.

Som det fremgår av tingrettens dom, har stiftelsen Tinius i henhold til vedtektene et ideelt formål som er formulert slik:

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.

Med tanke på denne sakens tema, skal stiftelsen Tinius i dag sikre og forsvare disse verdiene i et mediekonsern der redaksjonene daglig skal kommunisere seg imellom på tvers av de nordiske landegrensene. Det dreier seg også om kommunikasjon på tvers an landegrensene om og med redaksjonenes kilder.

1.4 Praktiske konsekvenser av søksmålets karakter

Som det også fremgår av tingrettens dom, dreier saken seg om abstrakt prøving av deler av etterretningstjenesteloven, opp mot de skranker som henholdsvis EMK / Grunnloven og EØS-retten oppstiller til de aktuelle overvåkningstiltakene.

I et slikt søksmål, der «faktum» er etterretningstjenesteloven, blir det det noe kunstig å operere med det normalt skarpe skillet mellom «faktum» og juss og mellom bevisvurdering og rettsanvendelse.

Når det i innledningen i anken er sagt at anken gjelder rettsanvendelsen, omfatter det dels også tingrettens tolkning / fremstilling av de relevante bestemmelsene i etterretningstjenesteloven, selv om anken hovedsakelig gjelder tingrettens tolkning og anvendelse av EMK og EØS-retten på etterretningstjenesteloven.

I den videre gjennomgangen av de nærmere ankegrunnene, har vi ansett det som mest hensiktsmessig å i hovedsak behandle angrepene på tingrettens tolkning / fremstilling av etterretningstjenesteloven og tingrettens anvendelse av henholdsvis EMK og EØS-retten på etterretningstjenesteloven i sammenheng.

Vi har nedenfor foretatt en hovedinndeling av behandling av ankegrunnene slik at dem som gjelder påstandens krav 1 (om tilrettelagt innhenting – TI) behandles i punkt 2, mens dem som gjelder krav 2 (om ende- og midtpunktinnhenting) behandles i punkt 3. I punkt 4 behandles de ankegrunner som gjelder kildevernet særskilt, da de har en side til både krav 1 og krav 2.

Saken er omfattende og komplisert, og det er mye med tingrettens dom de ankende parter er uenige i. Vi vil begrense oss til det vi mener står mest sentralt, uten at anken kan forstås som en uttømmende beskrivelse av ankende parters innvendinger mot dommen.

2 ANKEGRUNNENE KRAV 1: TILRETTELAGT INNHENTING (TI)

2.1 TI vurdert etter EMK artikkel 8 (og Grunnloven § 102)

2.1.1 Innledende bemerkninger om premisser som preger tingrettens dom

Før vi går nærmere inn på ankegrunnene under dette punktet, vil vi knytte noen overordnede kommentarer til enkelte av tingrettens innfallsvinkler / utgangspunkter og vurderinger – som også synes å ha preget flere av de feil som de ankende partene mener at tingrettens dom lider av. (Flere

av punktene vil ha relevans også for ankegrunner som behandles under punktene henholdsvis 3 og 4 nedenfor.)

2.1.2 Hva metadatalageret som genereres av TI består av

For det første peker vi på at det metadatalageret som E-tjenesten etter etterretningstjenesteloven kapittel 7 har adgang til å etablere fra bulkinnsamlingen og (for hver bulkinnsamling) beholde i opptil 18 måneder for å kunne gjøre retrospektive søk i, kun avgrenses mot data fra kommunikasjon mellom avsender og mottaker som begge befinner seg i Norge (når kommunikasjonen finner sted), jf. etterretningstjenesteloven § 7-6.

Som lovgiver har erkjent – og tingretten også er innom – er det imidlertid teknologisk umulig å skille ut all slik «innenrikskommunikasjon». Bruker man for eksempel nettbaserte meldingstjenester (som for eksempel iMessage på iPhone) går kommunikasjonen per definisjon via disse tjenestenes servere utenfor Norge, selv om de to personene som kommuniserer med hverandre befinner seg i Norge.

Minst like viktig er det – som det sakkyndige vitnet, professor Gjøsteen, også forklarte utførlig for tingretten – å forstå at det aller meste av befolkningens bruk av digitale tjenester i Norge innebærer at man (gjennom bruk av smarttelefoner og pc-er, og også gjennom bruk av alle de andre stadig økende antall ting som er koblet til nettet, herunder moderne biler og mange andre «duppeditter» vi omgir oss med) «kommuniserer» med og via servere i utlandet. Også EMD Alt dette fanges opp av TI. Og det meste av dette regnes altså heller ikke som innenrikskommunikasjon som i prinsippet skal filtreres bort etter TI-reglene; det inngår i det som det *er meningen* å samle inn data om.

Det skillet mellom på den ene side «norsk»- og på den annen side utenlandskommunikasjon som både lovgiver og dels også tingretten er opptatt av, er derfor irrelevant i dagens digitale virkelighet, et poeng som også EMD har fremhevet i sine nyere avgjørelser (eksempelvis i *Big Brother Watch* avsnitt 322). Som vi skal se i punkt 2.1.3 nedenfor, er dette skillet heller ikke så rettslig relevant som lovgiver har forutsatt, og som tingretten også synes å ha lagt til grunn i mange av sine vurderinger.

2.1.3 Statens ansvar etter EMK for personer som befinner seg utenfor Norge

Både lovgiver (og tingretten i vår sak) har operert med den (viser det seg, feilaktige) oppfatning at statens forpliktelser etter EMK *ikke* gjelder overfor personer som befinner seg utenfor Norge og kommuniserer derfra, selv om E-tjenestens innhenting av og behandling av informasjon om deres kommunikasjon skjer fra og i Norge (slik TI foregår og slik også midtpunkt- og endepunkthenting etter etterretningstjenesteloven §§ 6-9 og 6-10 kan foregå).

I forarbeidene drøfter departementet dette inngående, men konkluderer med at EMD på det tidspunktet ikke hadde tatt uttrykkelig stilling til dette (jurisdiksjons)spørsmålet.[1] Det ble i den sammenheng også vist til at Høyesterett i Rt-2005-833 uttalte at norske domstoler måtte være

[1] Høringsnotat av12. november 2018, Forslag til ny lov om Etterretningstjenesten, punkt 4.1.3

varsomme med å anlegge samme dynamiske tolkning av EMK som EMD selv, og departementet mente at heller ikke lovgiver burde legge større bånd på seg enn EMK krever.

Denne forutsetningen preger flere valg i etterretningstjenesteloven av relevans i vår sak, ved at man fokuserer på det menneskerettslige vernet av personer i Norge og av deres innenrikskommunikasjon. Det gjelder både TI, avgrensningen av bestemmelsene som søker å ivareta pressens kildevern, samt (de manglende) rettssikkerhetsgarantiene ved midtpunkt- og endepunktinnhenting etter etterretningstjenesteloven §§ 6-9 og 6-10.

Denne forutsetningen svikter imidlertid etter EMDs dom i *Wieder og Guarnieri mot Storbritannia,* som ble avsagt 12. september 2023, etter at etterretningstjenesteloven var vedtatt og satt i kraft. Der ble det aktuelle jurisdiksjonsspørsmålet for første gang avklart av EMD.

Avgjørelsen i *Wieder og Guarnieri* har tingretten behandlet under punktet om rettslig interesse, på dommens s. 10-11. Tingretten har imidlertid misforstått dommen, og også dermed på feilaktig grunnlag «parkert» den som ikke relevant i vår sak.

Saken gjaldt den samme britiske overvåkningen av grensekryssende elektronisk kommunikasjon som var del av de systemene som ble vurdert av EMD i 2020 i storkammerdommen i *Big Brother Watch* – og var slik sett avledet av den.

I *Wieder og Guarnieri*-saken var klagerne to utenlandske borgere som verken bodde i Storbritannia eller anførte at de hadde oppholdt seg der. De brukte imidlertid elektronisk kommunikasjon som regelmessig passerte Storbritannias grenser. Under henvisning til dette og til at når EMD i *Big Brother Watch* allerede hadde slått fast at det aktuelle britiske overvåkningstiltaket var i strid med EMK, hevdet de at også deres rettigheter etter EMK var krenket. Den britiske staten hevdet at dens jurisdiksjon etter EMK artikkel 1 og dermed ansvar etter EMK artikkel 8 med hensyn til slik overvåkning, ikke kunne strekke seg til personer som befant seg utenfor Storbritannia da kommunikasjonen som eventuelt ble omfattet av overvåkningen fant sted.

EMD tok utgangspunkt i at dette spørsmålet hittil ikke hadde noen avklaring i EMDs praksis, men konkluderte etter en lengre drøftelse med at det avgjørende er hvor innhentingen, lagringen og eventuelt behandlingen av kommunikasjonsdataene skjer fra. Når dette skjedde fra Storbritannia, var Storbritannia ansvarlig etter EMK for inngrepet som skjer overfor både sender og mottaker av kommunikasjonen og i selve kommunikasjonsfortroligheten, uavhengig av om klagerne selv befant seg utenfor landets grenser. Jf. følgende uttalelse i dommens avsnitt 95 og 95:

> *94. Turning to the facts of the case at hand, 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. Under the section 8(4) regime the interference with the privacy of communications clearly takes place where those communications are intercepted, searched, examined and used and the resulting injury to the privacy rights of the sender and/or recipient will also take place there.*

> *95. Accordingly, the Court considers that the interference with the applicants' rights under Article 8 of the Convention took place within the United Kingdom and therefore fell within the territorial jurisdiction of the respondent State.*

Drøftelsen som ledet frem til denne avklaringen var tydelig inspirert av en dom fra Tysklands forfatningsdomstol (Bundesverfassungsgericht) av 19. mai 2020, om den tyske stats ansvar for personer utenfor Tysklands grenser etter tysk grunnlov, ved tysk etterretnings bruk av tilsvarende overvåkning av grenseoverskridende elektronisk kommunikasjon. EMD gjennomgikk og siterte utførlig fra denne dommen i sin dom avsnitt 35 flg. (under punktet «Relevant comparative law and practice»). Tysklands forfatningsdomstol konkluderte med at den tyske stat hadde ansvar, og uttalte blant annet følgende, gjengitt i EMDs dom avsnitt 38, i engelsk oversettelse:

> *The developments in information technology have led to a situation where data is shared through global channels, where it is randomly routed via satellite or cable according to technical criteria that have no regard to national borders (...). This makes it possible to intercept a considerable number of foreign communications from within Germany. Moreover, communication in society has become increasingly international. In view of cross-border services, exchanges – both within states and across national borders – between citizens as fundamental rights holders mainly rely on telecommunications services that do not differentiate between domestic and foreign communications (...). Given that, under the current realities of information technology, actions and communication relations of all kinds have become increasingly digital, and given the constant increase in data processing capacities, the possibilities for conducting telecommunications surveillance extend to broad areas of all of civil society, even outside a state's own jurisdiction – just as domestic communications are also subject to surveillance by other states (...).*
>
> *In light of such developments, an understanding of fundamental rights according to which their protection ended at national borders would deprive holders of fundamental rights of all protection and would result in fundamental rights protection lagging behind the realities of internationalisation ([...]). It could undermine fundamental rights protection in an increasingly important area that is characterised by intrusive state action and where – in the field of security law – fundamental rights are especially significant in general. By contrast, in binding the state as the relevant actor, Art. 1(3) [of the Basic Law] accounts for such novel risks and helps bring them into the general framework of the rule of law that is created by the Basic Law.*

Alt dette har tingretten i vår sak sett bort fra, og istedenfor fokusert på en helt annen del av *Wieder og Guarnieri*, der EMD uttaler seg om klagernes status som offer etter EMK artikkel 34 – og i tillegg konkludert feilaktig om det punktet.

På det punktet hadde nasjonale myndigheter i Storbritannia – under henvisning til EMDs egen praksis – erkjent at (under forutsetning av at Storbritannia overhodet hadde jurisdiksjon, hvilket de

nasjonale myndighetene jo mente at de ikke hadde) klagerne oppfylte vilkårene for offerstatus. Dette bestred Storbritannia heller ikke i saken for EMD. Men som EMD korrekt påpeker i innledningen til det punktet i dommen, i avsnitt 96, er dette et *ex officio*-spørsmål for EMD, da det er en forutsetning for *EMDs* formelle kompetanse til å prøve klagen.

Det er derfor feil, når tingretten på s. 20 (etter bare å ha sitert deler av EMDs generelle utlegninger om kravene til offerstatus i slike overvåkningssaker) uttaler at «EMD tok ikke eksplisitt stilling til om de aktuelle klagerne hadde offerstatus da dette ikke var bestridt av britiske myndigheter. EMD la dette til grunn.»

Som sagt, kan ikke EMD la være å ta stilling til om kravene etter EMK artikkel 34 er oppfylt. Det er et *ex officio*-spørsmål som er avgjørende for EMDs kompetanse til å behandle en klage. EMD lot heller ikke være å ta stilling, som tingretten skriver. EMD viste til at nasjonale myndigheter selv hadde vist til relevant EMD-praksis og akseptert at klagerne hadde offerstatus i saken – noe EMD også aksepterte. Det EMD sa i konklusjonen under dette punktet, i dommens avsnitt 100, var følgende:

> *100. In the present case, it is not necessary for the Court to give detailed consideration to this question since the IPT, referring to the Court's case-law, expressly accepted that the applicants had victim status in respect of their Article 8 complaint concerning the section 8(4) regime (see paragraph 21 above). The Government did not challenge that finding and Court would therefore accept that the applicants in the present case can claim to be victims of the alleged violation for the purposes of Article 34 of the Convention.*

2.1.4 Grunnleggende forskjeller mellom det svenske systemet som EMD vurderte i *Centrum för Rättvisa* og det norske TI-systemet

Både partene og tingretten har vært enige om at av de systemene som har vært vurdert i de to sentrale EMD-dommene om bulkinnsamlingsregimer, storkammerdommene i henholdsvis *Big Brother Watch* og *Centrum för Rättvisa*, er det det svenske som er mest sammenlignbart med norske TI.

Som de ankende parter fremhevet i tingretten, er det da imidlertid svært viktig å ha klart for seg at det er noen grunnleggende forskjeller på TI og det svenske systemet som ble vurdert i *Centrum för Rättvisa.* Disse forskjellene har avgjørende betydning når retten på bakgrunn av EMDs vurdering av det svenske systemet, skal anvende EMDs såkalte «global assessment» på TI.

<u>Det norske TI-systemets hovedtrekk:</u>
Som det fremgår både av etterretningstjenesteloven selv og av tingrettens (i hovedsak dekkende) beskrivelse av TI-systemet, er de vesentlige trekkene ved systemet slik:

Når de nærmere vilkårene for det er oppfylt, får E-tjenesten tillatelse av retten til å pålegge tilbydere av elektroniske kommunikasjonstjenester å tilrettelegge for at E-tjenesten kan speile uvalgte kommunikasjonsstrømmer i transitt som går inn og ut av Norge, på E-tjenestens egne servere. Disse

strømmene inneholder i utgangspunktet «alt» i den aktuelle kommunikasjonsstrømmen, ubearbeidet rådata (både metadata og innhold).

Bortsett fra at selve innholdet i kommunikasjonen filtreres bort, og man forsøksvis (men erkjent i stor grad utjenlig) filtrerer bort ren innenrikskommunikasjon, ekstraheres alle metadata i bulk til det såkalte metadatalageret hos E-tjenesten, der dataene kan bli liggende i opptil 18 måneder.

Det vises til det som er sagt i punkt 2.1.2 ovenfor, om innholdet i metadatalageret. Metadatalageret inneholder per definisjon i det vesentligste informasjon som i seg selv er uten interesse for etterretningsformål. (Det etableres uten bruk av nærmere, målrettet filtrering basert på selektorer / søkekriterier.) Formålet med metadatalageret er at det skal være tilgjengelig for senere (domstolsgodkjente) retrospektive søk basert på bruk av relevante selektorer / søkekriterier.

Så lenge en speilingstillatelse varer (opptil 2 år av gangen), kan E-tjenesten gjenta ovennevnte øvelse, og dermed løpende etterfylle metadatalageret med nye metadata (der hvert nye påfyll kan beholdes i opptil 18 måneder).

Etter tillatelse fra retten i det enkelte tilfellet kan E-tjenesten foreta målrettede retrospektive søk i metadatalageret, basert på relevante selektorer / søkekriterier.

Det svenske systemet som ble vurdert i *Centrum för Rättvisa:*

Det svenske systemet som ble vurdert i *Centrum för Rättvisa,* er ganske annerledes innrettet, slik det er beskrevet i EMDs dom. Det fremgår særlig av dommens avsnitt 18 og avsnittene 25-29.

I dette systemet er utgangspunktet at FRA (Försvarets Radioanstalt) mottar en konkret, detaljert oppdragsbeskrivelse om et presist etterretningsbehov fra den aktuelle etterretningstjenesten. Oppdragsbeskrivelsen skal inneholde «information about (i) the issuing authority, (ii) the part of the Government's annual tasking directive it concerns, (iii) the phenomenon or situation intended to be covered, and (iv) the need for intelligence on that phenomenon or situation" (*Centrum för Rättvisa* avsnitt 21).

På bakgrunn av en slik konkret bestilling må FRA inngi en begjæring til domstolen (Försvarsunderrättelsedomstolen) om tillatelse til å foreta den nødvendige innhentingen av data fra grensekryssende kommunikasjonsstrømmer. Begjæringen må inneholde informasjon om

- Oppdraget datainnhentingen knytter seg til og behovet for dataen
- Kommunikasjonsbærere som FRA trenger tilgang til
- Hvilke selektorer / søkekriterier som vil bli brukt for å begrense innhentingen til det som er relevant for det konkrete oppdraget, herunder gi en særlig begrunnelse for nødvendigheten av å eventuelt bruke såkalte personselektorer
- Ønsket varighet av tillatelsen (maksimalt seks måneder)

Dersom domstolen finner at vilkårene for å gi tillatelse, skal tillatelsen spesifisere

- Oppdraget innhentingen kan utføres for

- Kommunikasjonsbærerne som FRA vil ha tilgang til
- Varigheten av tillatelsen – kan ikke overstige 6 måneder av gangen
- Selektorer og søkekriterier som kan brukes
- Andre vilkår som er nødvendig for å begrense inngrepet ved innsamlingen

Basert på en slik tillatelse får FRA tilgang på kommunikasjonsstrømmene i de aktuelle kommunikasjonsbærerne, via bestemte samlingspunkter der de relevante strømmene speiles mens der er i transitt. Fordi FRA må bruke de ovennevnte selektorene / søkekriteriene i sin innhenting, får FRA bare samlet inn kommunikasjonsdata som «treffes» av denne målrettede avgrensningen knyttet til det enkelte oppdraget som begrunnet innhentingen.

FRA sitter derfor kun igjen med det som forutsetningsvis har etterretningsmessig interesse knyttet til det aktuelle oppdraget. Basert på disse dataene foretas det en nærmere prosessering og analyse som danner grunnlag for en rapport til den tjenesten oppdraget kom fra.

Det svenske systemet kan derfor grovt beskrives slik at man der slår sammen både speiling og målrettet søk ved bruk av selektorer / søkekriterier i én sammenhengende prosess, slik at FRA / etterretningstjenestene, selv om utgangspunktet er bulkaksess til kommunikasjonsstrømmer, raskt innsnevrer hva som trekkes ut, og aldri sitter igjen med mer data enn den som forutsetningsvis er av etterretningsmessig relevans for det konkrete oppdraget som begrunnet innhentingen.

Derfor verken opparbeider eller sitter svensk etterretning igjen med et slikt metadatalager som man gjør i det norske TI-systemet.

Når tingretten på s. 25 i sin dom ser bort fra dette, ved å vise til at det utover det som er beskrevet (utførlig) og lagt til grunn i EMDs dom, ikke har vært «nærmere bevisførsel» om det svenske systemets utforming – og tilføyer at det heller ikke er nødvendig for å vurdere det norske systemet etter EMDs kriterier, gjør tingretten en etter de ankende parters syn vesentlig feil.

For det første er det ikke nødvendig eller relevant med ytterligere «bevisføring». Når man skal forstå EMDs rettsanvendelse i *Centrum för Rättvisa* er det det faktum, den beskrivelse av det svenske systemet som EMD har lagt til grunn som er avgjørende. Og skal man på en meningsfull måte anvende EMDs dom i den saken til å analysere hvordan tilsvarende vurdering vil slå ut på det norske systemet, må man selvsagt forstå hva de mest sentrale forskjellene på de respektive systemene er.

Særlig vil fraværet av i det svenske systemet av et tilsvarende metadatalager som det norske, være sentralt å ha for øyet når EMDs vurderingstemaer skal brukes på norske TI. En vurdering av det norske systemet åpenbart fokuseres særlig på om det er nødvendig og forholdsmissig i et demokratisk samfunn å innrette systemet slik at man, basert på tillatelser med opptil to års varighet, innhenter enorme mengder data om borgeres digitale liv, for så å lagre dem i opptil 18 måneder (selv om man vet at det vesentligste av informasjonen ikke har interesse for noe etterretningsmål).

2.1.5 Tingrettens anvendelse av EMK

2.1.5.1 Vurderingstemaet etter EMK- herunder EMDs «global assessment»

De ankende parter har ikke avgjørende innvendinger til tingrettens redegjørelse for de *generelle* rettslige utgangspunktene og vurderingstemaene etter EMK artikkel 8 som finnes i dommens punkter 3.3.1 og 3.3.2.

Det samme gjelder i hovedsak også for tingrettens redegjørelse i dommens punkt 3.3.3 for de nærmere generelle vurderingskriteriene som kan utledes av EMDs dom i *Centrum för Rättvisa* (jf. tilsvarende i *Big Brother Watch*) når det gjelder anvendelse av EMK artikkel 8 på bulkovervåkningssystemer.

Når det derimot gjelder tingrettens konkrete anvendelse av vurderingskriteriene, mener de ankende parter at retten dels visert at den ikke har forstått hvordan vurderingen skal foretas.

Det fremstår blant annet som om retten betrakter de åtte momentene som inngår i EMDs global assessment mer som enkeltvilkår (og benevner dem også løpende som «vilkår 1», vilkår 2» osv.), enn som hva de skal være; momenter som skal vurderes og samlet spille inn i en overordnet helhetsvurdering, slik at svakheter ved enkelte momenter kan veies opp av kvaliteten i systemet under andre momenter, men da også slik at sterke svakheter ved ett moment vil innebære at det også stilles desto høyere krav til systemet under de øvrige momentene (jf. *Centrum för Rättvisa* avsnitt 364). Dette vil utdypes i behandlingen nedenfor av vurderingen av momentene i vår sak.

Det er i tillegg, som nevnt ovenfor i punkt 2.1.4 om noen vesentlige forskjeller på det svenske systemets innretning og norske TI, en gjennomgripende svakhet at tingretten ikke har forstått og / eller villet legge vekt på disse forskjellene, når den har foretatt sin vurdering av TI, basert på tolkning og anvendelse av EMDs dom i *Centrum för Rättvisa.*

Det er ellers korrekt når tingretten i dommens punkt 3.4.1 oppfatter at det er under momentene 1, 2, 6, 7 og 8 av global assessment-momentene at de ankende partene mener at svakhetene i TI ligger. Her skal det under henvisning til hva som allerede er nevnt ovenfor, bemerkes at tingretten benevner momentene som «vilkår» eller «krav» som enten er eller ikke er «oppfylt».

Nedenfor gjennomgås de ankende parters syn på feil i tingrettens konkrete vurdering, under de nevnte momentene og deretter i helhetsvurderingen.

2.1.5.2 Formålene som kan begrunne TI – global assessment moment 1

Formålene som kan begrunne TI er et sentralt moment i den vurderingen lagmannsretten skal gjøre. Er formålet som kan begrunne masseovervåkningen vidt kan overvåkningen brukes oftere og bredere, og den vil derfor også være mer inngripende.

Det norske systemet gir unektelig E-tjenesten vide rammer. Loven skiller mellom to forskjellige sett med formålsangivelser i §§ 3-1 og 3-2. Formålene i § 3-1 er typiske kjerneoppgaver for å ivareta nasjonal sikkerhet, mens formålene i § 3-2 er mer perifere i relasjon til nasjonale sikkerhetsoppgaver, jf. nærmere i punkt 2.2.3 under, der dette behandles under EØS-retten.

Tingretten legger korrekt til grunn at formålene som kan begrunne TI etter den norske loven gir vide fullmakter. Dette skal veie tungt inn i den helhetsvurderingen lagmannsretten skal gjøre etter EMK.

Tingretten ser ut til å gjøre en isolert vurdering av om formålet kan forsvares innenfor de EMK-rettslige rammer. Dette samsvarer i så fall ikke med den vurderingen EMD anviser. Som nevnt ovenfor: De forskjellige momentene skal vurderes og samlet spille inn i en overordnet helhetsvurdering. Selv om det er andre forhold som kan veie opp, kan det være liten tvil om at den norske lovens vide formålsangivelse må veie tungt og skjerpe kravene til de øvrige momentene og til de rettssikkerhetsgarantiene som må kreves.

2.1.5.3 Omstendigheter som kan medføre innhenting av enkeltpersoners kommunikasjon – global assessment moment 2

På dette punktet (dommens punkt 3.4.4) synes tingretten å oppfatte at Stiftelsens anførsel går ut på at svakheten i TI utelukkende går ut på en ikke nærmere konkretisert anførsel om at TI- systemet her er «problematisk, og at dette innebærer en «masseovervåkning»».

Deretter går tingretten over i en lengre gjennomgang av lovreguleringen av prosessen med innhenting av kommunikasjonsdata under TI-systemet, for så å konkludere med at «de omstendigheter som kan føre til at enkeltpersoners kommunikasjon innhentes ved tilrettelagt innhenting tilfredsstiller kravene til en tilstrekkelig klar og forutberegnelig lovgiving.»

Med dette har tingretten misforstått Stiftelsens anførsler og – etter de ankende parters syn – også anvendt EMK og EMDs praksis feil.

Stiftelsens poeng under dette momentet er at det ikke bare dreier seg om kvaliteten på lovgivningen. Det dreier seg minst like mye om at selve systemet også er innrettet slik at den enkelte borger kan ha tillit til at selv om deres kommunikasjon kan inngå blant de dataene som omfattes av den innledende fasen av bulkinnsamlingen (jf. *Centrum för Rättvisa* avsnitt 239 og EMDs utrykk «initial retention»), fordi den nødvendigvis baserer seg på stor grad av vilkårlighet, er systemet innrettet slik at borgernes data i minst mulig grad forblir lagret eller analysert, med mindre de har interesse for etterretningsformål (jf. også moment 1).

Da er stiftelsens poeng når det gjelder TI-systemet, at en av dets vesentlige svakheter nettopp er at det (i motsetning til det svenske systemet) *ikke* er innrettet slik at man så snart som mulig sorterer bort andre metadata enn dem som antas å ha interesse for etterretningsformål. Tvert imot; TI-systemet forutsetter at man bygger opp et enormt metadatalager, som inneholder metadata om store deler av befolkningens daglige, digitale aktivitet – og der det meste per definisjon ikke har interesse for etterretningsformål.

En korrekt rettsanvendelse på dette punkt leder derfor til at TI-systemet lider av en avgjørende svakhet når det gjelder dette momentet i helhetsvurderingen, sett særlig i sammenheng med moment 6 (jf. Punkt 2.1.5.4 nedenfor).

2.1.5.4 Varighet, lagring og sletting - global assessment moment 6

Stiftelsens hovedanførsel under dette punktet var – og er – at TI-systemet, som både åpner for at

- selve speilings- / innhentingstillatelsene kan gis for så lange perioder av gangen som opptil to år, og
- at man – som gjentatt flere ganger ovenfor – bygger opp et enormt metadatalager der for det meste ikke etterretningsrelevante data om store deler av befolkningens daglige digitale aktivitet kan bli liggende i opptil 18 måneder,

i seg selv innebærer at inngrepet i både de ankende parters og alle andres rettigheter etter artikkel 8 går mye lenger enn det som er «strictly necessary» og forholdsmessig – og derfor alene utgjør en *avgjørende svakhet.*

Også på dette punktet begår tingretten hva de ankende parter mener er alvorlige rettsanvendelsesfeil, på flere punkter.

For det første misforstår tingretten også her vurderingen etter EMK, når den tilsynelatende mener at det også under dette momentet først og fremst bare er spørsmål om varighet / lagring /sletting er klart nok regulert i loven.

Da overser retten at det overordnende vurderingstemaet etter EMK artikkel 8 (2) er om et inngrep er (i saker om hemmelig overvåkning *strengt*) nødvendig og forholdsmessig.

For det andre synes tingretten å oppfatte EMD slik at når EMD i *Centrum för Rättvisa* avsnitt 331 uttaler at «(t)he duration of bulk interception operations is, of course, a matter for the domestic authorities to decide», betyr det at spørsmål om blant annet hvor lenge speilings- / innhentingstillatelser kan gis for, hvor mye data om hva som kan lagres hvor lenge osv. er unntatt domstolenes prøving og ikke kan inngå i nødvendighets- og forholdsmessighetsvurderingen etter EMK.

Det er selvsagt ikke korrekt. I så fall skulle Norge for eksempel kunne bestemme at metadata om alles kommunikasjon kunne samles inn løpende og lagres inn i evigheten, så lenge det var tydelig lovregulert.

Den aktuelle uttalelsen skal ikke forstås som annet enn at vurderingen av varigheten på konkrete bulkinnsamlingsoperasjoner i utgangspunktet er noe som de respektive nasjonale myndighetene må vurdere – forstått slik at det ikke er EMD som skal gi en generell fasit på hvilke frister som skal gjelde. Som EMD selv presiserer andre steder i både *Centrum för rättvisa* og *Big Brother Watch*, vil de enkelte staters etterretningssystemer kunne variere i både utforming og innretning – og at det ikke finnes noe fasit i den sammenheng, heller.

Poenget er – igjen – at man må lese dette på bakgrunn av at det overordnede vurderingstemaet er om de inngrep det er tale om, er strengt nødvendige og forholdsmessige. Alle momentene i EMDs global assessment sorterer under den overordnede vurderingen av om lovreguleringen er klar og inngrepet er strengt nødvendig og forholdsmessig.

Dette går også tydelig frem tidligere i premissene i *Centrum för rättvisa* avsnittene 252-253, der EMD uttaler følgende om den overordnede vurderingen (med våre uthevninger av enkelte, for sammenhengen sentrale presiseringer:

> *252.As to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the Court has recognised that the national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security (see Weber and Saravia, cited above, § 106).*
>
> *253.However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security (and other essential national interests) may undermine or even destroy the proper functioning of democratic processes under the cloak of defending them, the Court must be satisfied that there are adequate and effective guarantees against abuse.* ***The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures****, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law.* ***The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the"interference" to what is "necessary in a democratic society".***

Det er med andre ord klart at retten verken skal eller kan nøye seg med å vurdere om reglene om varighet, lagring, sletting m.m. er klart nok lovregulert – også «*the nature, scope and duration of the possible measures»* skal inngå i og undergis en nødvendighets- og forholdsmessighetsvurdering.

At EMD i saker om hemmelig overvåkning – og i særdeleshet den som involverer bulkinnsamling – også er særlig opptatt av at systemene er tydelig lovregulert, er nettopp fordi selve overvåkningen, inngrepene, skjer i det skjulte, slik at borgerne ikke har innsyn i hvordan overvåkningen konkret praktiseres, heller ikke når den rammer dem og deres kommunikasjon.

2.1.5.5 Manglende løpende- og etterfølgende kontroll - global assessment moment 7 og 8

Det er, slik tingretten har beskrevet på dommens s. 40-50, EOS-utvalget som fører kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-tjenestene). EOS-utvalgets virksomhet er beskrevet på dommens s. 40-42.

Tingretten har i sin vurdering selv pekt på en rekke svakheter med kontrollsystemet, men likevel konkludert med at den kontrollen som føres av tilrettelagt innhenting gir en tilstrekkelig garanti mot misbruk. De ankende parter fastholder at de svakhetene som hefter ved EOS-utvalgets kontroll av etterretningstjenestene ikke i tilstrekkelig grad oppfyller de EMK-rettslige kravene som er stilt til løpende- og etterfølgende kontroll, men den konsekvens at det ikke foreligger tilstrekkelige «end-to-end safeguards».

Løpende kontroll

Når det gjelder den løpende kontrollen er det særlig to punkter som de ankende parter mener er mangelfull. For det første er ikke EOS-utvalget utstyrt med tilstrekkelig med ressurser for å ivareta de forpliktelsene som følger av EMD. For det andre er det en mangel at EOS-utvalget ikke har noen instruksjons- og vedtaksmyndighet overfor E-tjenesten.

Den løpende kontrollen som føres av tilrettelagt innhenting fremgår av etterretningstjenesteloven § 7-11 og angir at utvalget skal sikre at E-tjenesten etterlever reglene om TI *«blant annet med at søk bare gjennomføres i tråd med rettens kjennelser og at korttidslageret og testdata utelukkende brukes til teknisk understøttelse».*

EMD har vurdert hva som ligger i kravet om tilstrekkelig løpende kontroll og uttalt at en uavhengig myndighet må *være «[s]ufficiently robust to keep the "interference" to what is "necessary in a democratic society».*[2] Det innebærer blant annet at det uavhengige kontrollorganet må ha tilstrekkelig ressurser for å ha muligheten til å sikre at innsamlingen, lagringen og behandlingen holdes på et nivå som er nødvendig og forholdsmessig.

Retten har i sin vurdering vist til, og tilsynelatende erkjent, at EOS-utvalgets ressurser er begrenset til kun å gjennomføre en stikkprøvebasert kontroll. I den sammenhengen konstaterer retten at:

> *«Når det gjelder stiftelsens anførsel om manglende kapasitet, mener retten at det klart ligger innenfor statens skjønnsmargin å avgjøre hvilke ressurser som skal tilføres overvåkningsorganet. Vurderingstemaet i denne saken er hvilke rettslige rammer lovgivingen inneholder for at EOS-utvalget skal kunne utføre løpende kontroll med E-tjenesten.»*

Retten ser med andre ord til å legge til grunn at det «klart» ligger innenfor statens skjønnsmargin at staten selv skal avgjøre hvilke ressurser som skal tildeles organisasjonen som fører kontroll av statens egen myndighetsutøvelse. Det er ikke riktig. Selv om staten har en viss skjønnsmargin når det gjelder egen ressursallokering, må likevel de krav som knyttet til tilstrekkelig rettssikkerhetsgarantier være oppfylt.

Slik tingretten også beskriver, mangler EOS-utvalget kompetanse til å instruere E-tjenesten gjennom bindende vedtak. Utvalget kan kun inngi begjæring til retten om at retten beslutter stans i innhentingen og sletting, men utvalget har ikke selv møterett eller ankeadgang i rettslige prosesser etter § 7-12 (begjæring om stans og sletting). Dette innebærer at kontrollmekanismen i praksis er mindre effektiv – med tilsvarende større risiko for at krenkelser kan foregå over tid før det reageres med bindende virkning. Å kunne «gi uttrykk for sin mening» uten formell beslutningsmyndighet kan ikke anses som effektiv kontroll i EMK-rettslig forstand.

[2] (*Centrum för rättvisa* avsnitt 270).

Retten foretar en vurdering av om EOS-utvalgets tilsyn er i tråd med de krav EMD stiller i *Centrum f*or *Rättvisa*, og sammenligner i den sammenheng det svenske kontrollorganet SIUN (Statens inspektion för försvarsunderrättelsesverksamheten) med EOS-utvalget. Etter en sammenligning av de ulike tilsynsorganene konkluderer retten med at det ikke er grunnlag for å fastslå at reguleringen av EOS-utvalgets løpende kontroll er i strid med de krav som oppstilles av EMD i *Centrum för Rättvisa*. De ankende parter er ikke enig i denne vurderingen.

SIUN er et uavhengig forvaltningsorgan, ledet av en person som er eller har vært dommer, og det har både tilsyns- og håndhevingsmyndighet. SIUN har i motsetning til EOS-utvalget både rett og plikt til å gripe inn direkte ved uregelmessigheter i den svenske signaletterretningstjenestens virksomhet. SIUN har adgang til alle relevante dokumenter og databaser, og kan fatte vedtak som medfører umiddelbar stans i overvåkning. EOS-utvalget har ingen slik beslutningsmyndighet. Det kan som nevnt kun uttrykke sitt syn overfor E-tjenesten og eventuelt fremme begjæringer til domstolen, uten adgang til selv å møte i retten, uten partsstatus og uten mulighet for å anke rettens avgjørelse. Utvalgets rolle er derfor håndhevingsmessig mer begrenset, og står slik sett i kontrast til SIUNs.

Også her er de øvrige forskjellene i innretningen på det svenske systemet og det norske TI-systemet (jf. ovenfor i punktene 2.1.1 og 2.1.2.3) relevante. Med den begrensede mengden data svensk etterretning sitter igjen med etter hver innsamling, kombinert med at de enkelte speilings-/innsamlingstillatelsene kan vare i maksimalt seks måneder, før de opphører og eventuelt må fornyes av domstolen, blir SIUNs kontrolloppgave tilsvarende mer oversiktlig og mindre krevende enn den EOS-utvalget har etter etterretningstjenesteloven.

SIUN er dessuten et spesialistorgan, opprettet utelukkende for å føre kontroll med den bestemte metoden for overvåkning, mens EOS-utvalget jo skal føre tilsyn både med E-tjenestens øvrige virksomhet og med virksomheten i samtlige av de øvrige EOS-tjenestene (PST, NSM med flere).

Den manglende kompetansen til selv å fatte bindende avgjørelser overfor E-tjenesten medfører at kontrollmekanismen i praksis blir svekket, og at muligheten for effektiv uavhengig kontroll reduseres betydelig. Sammenholdt med utvalgets manglende ressurser, fører dette til at den ikke er er *«[s]ufficiently robust»* til å sikre at E-tjenesten overholder sine forpliktelser.

Etterfølgende kontroll

Tingretten har i sin vurdering lagt til grunn at den norske kontrollordningen, til tross for visse svakheter, samlet sett tilfredsstiller kravene etter EMK artikkel 8. De ankende parter mener at retten undervurderer betydningen av manglende rettslig bindende og begrunnede avgjørelser etter klage, og at retten basert på feil forståelse av EMD, mener at EOS-utvalgets dobbeltrolle ikke kan sammenlignes med SIUNs dobbeltrolle. Disse forholdene innebærer at det ikke foreligger noe effektivt rettsmiddel i EMKs forstand når det gjelden den etterfølgende kontrollen.

Det følger av *Centrum för Rättvisa*[3] at enhver som mistenker at sin kommunikasjon er blitt overvåket, som hovedregel må ha adgang til et rettsmiddel som kan lede til en rettslig bindende og begrunnet avgjørelse. EOS-kontrolloven § 15 gir imidlertid ikke en klager rett til en slik avgjørelse – bare en konklusjon om klagen har «ført til kritikk eller ikke»..

Tingretten erkjenner riktignok denne svakheten, men viser til at saken i teorien kan bringes inn for de alminnelige domstoler. Dette er imidlertid ikke et reelt rettsmiddel slik EMK krever. Muligheten til å gå til domstol er begrenset av tvisteloven § 22-1 om bevisforbud. Som tingretten selv påpeker, vil dette gjøre at flertallet av dem som ønsker å få prøvd om deres rettigheter er krenket, i praksis står uten tilgang til reell rettslig prøving.

Dermed foreligger det ikke en «praktisk og effektiv» rett til klagebehandling med et rettslig resultat, slik EMD krever. En slik ordning oppfyller ikke kravene etter EMK artikkel 8 og artikkel 13.

Videre fastholder de ankende parter at EOS-utvalgets dobbeltrolle er en alvorlig svakhet.

I likhet med SIUN i Sverige, hvis dobbeltrolle EMD kritiserte i *Centrum för Rettvis* [4], fører EOS-utvalget både den løpende kontrollen og den etterfølgende kontrollen ved behandling av eventuelle klager fra enkeltborgere.

Dermed stilles EOS-utvalget i en rolle der det i en klagebehandling kan måtte evaluere lovligheten av praksis og tiltak som det selv i den løpende kontrollen har vurdert og akseptert, eventuelt observert, men unnlatt å reagere på.

På dette – viktige – punktet har tingretten (jf. dommens s. 46-47) tilsynelatende misforstått hvilken dobbeltrolle EMD reagerte på i *Centrum för Rättvisa.*

Tingretten siterer på s. 46 det relevante avsnittet (359) i *Centrum för Rättvisa*. Der er det er jo nettopp det faktum at SIUN både har rollen med å føre løpende kontroll med at FRAs gjennomføring av de tillatelsene domstolen (Försvarsunderrättelsedomstolen) har gitt, skjer i samsvar med tillatelsene og innenfor loven, *og i tillegg* har rollen med i ettertid å behandle eventuelle klager fra enkeltindivider, som EMD kritiserer.

Dette er forholdet med EOS-utvalget òg, og tingretten har selv i dommens punkt 3.4.6.2 (om løpende kontroll) vurdert EOS-utvalget rolle som sammenlignbart med SIUNs, til tross for enkelte forskjeller.

Det er derfor svært vanskelig å forstå hvordan tingretten kan konkludere med at EMDs kritikk av SIUNs dobbeltrolle ikke også rammer EOS-utvalgets dobbeltrolle.

---

[3] avsnitt 362.

[4] avsnitt 359

2.1.5.6 Helhetsvurderingen

De ankende parter mener at det – ikke minst når man i motsetning til tingretten, på korrekt vis sammenligner norske TI med det svenske systemet som ble vurdert i *Centrum för Rättvisa* – er åpenbart at TI må anses å krenke EMK artikkel 8, basert på den helhetsvurderingen som skal foretas.

De feilene i tingrettens rettsanvendelse som er påpekt løpende i punktene ovenfor, har – naturligvis – fulgt med over i tingrettens helhetsvurdering.

Grovt oppsummert har tingretten i realiteten nøyd seg med å peke på at TI er regulert av tilgjengelige lovbestemmelser som inneholder hva retten mener er klare regler om alle prosedyrer, for deretter å slå fast at det avgjørende da er om summen av uavhengig løpende og etterfølgende kontroll i alle ledd («ende-to-end-safeguards») er tilfredsstillende.

Med unntak for at tingretten er kommet til at det er en svakhet ved den etterfølgende kontrollen klager ikke har et tilstrekkelig effektivt rettsmiddel for å få fastslått om det har skjedd en krenkelse av menneskerettighetene, konkluderer den med at kravet om tillatelser fra retten og kontrollregimet sett under ett er godt nok.

Som det allerede vil ha fremgått, mener de ankende parter at tingretten med sin feilaktige tilnærming, i realiteten har hoppet over det som er den grunnleggende og overordnede vurderingen etter EMK artikkel: Om det inngrepet TI utgjør, er begrenset til det som er strengt nødvendig og forholdsmessig.

Foretas en korrekt vurdering vil særlig det som er sagt ovenfor i punktene 2.1.5.3 (moment 2), 2.1.5.4 (moment 6) og 2.1.5.5 (moment 7 og 8), lede til en konklusjon om at TI går svært mye lenger enn hva som strengt nødvendig og forholdsmessig.

2.2 TI vurdert opp mot EØS-retten – LQN-kriteriene

2.2.1 Overordnet

Kommunikasjonsverndirektivet (direktiv 2002/58 EF) stiller strenge krav til vern av innholdet i og data om borgernes elektroniske kommunikasjon. Direktivet er en del av EØS-avtalen og er gjennomført i norsk rett gjennom ekomloven.

EU-domstolen har i tidligere prinsippavgjørelser avgjort at vilkårlig masseovervåkning (bulkinnsamling og -lagring av metadata) av borgernes elektroniske kommunikasjon er i strid med direktivet, jf. EUs Charter om grunnleggende friheter artiklene 7, 8 og 11 vern av henholdsvis privatliv, personopplysninger og ytringsfrihet.[5]

[5] Jf. dommene i sakene *Digital Rights Ireland (*C-293/12)*, Kärntner Landesregierung* (C-594/12), *Tele2 Sverige AB* (C-203/15) og *Watson og andre* (C-698/15).

I storkammersaken La Quadrature du Net (LQN) fikk EU-domstolen opp spørsmålet om det likevel kan være lov med vilkårlig massovervåkning, dersom formålet med overvåkningen er å ivareta nasjonal sikkerhet.

EU-domstolen kom til slik masseovervåkning i utgangspunktet er forbudt, men at det unntaksvis, og på særlig strenge vilkår, likevel kan være tillatt.

Tingretten har feilaktig lagt til grunn at norsk lovgivning holder seg innenfor de stenge rammene i EU-domstolen har satt.

2.2.2 EU-domstolens krav til presis lovgivning

Det er vanlig at unntak fra EU-rettslige regler må forankres i lov. LQN stiller imidlertid et særskilt strengt lovkrav. Dette strenge lovkravet må sees i sammenheng med at den vilkårlige masseovervåkningen – i motsetning til annen myndighetsutøvelse – skjer i det skjulte uten ordinær mulighet for kontroll og overprøving, herunder uten partsrettigheter for de berørte. For å begrense den nedkjølende effekten vilkårlig masseovervåkning vil lede til, er det derfor særlig viktig at rammene for overvåkningen er særlig klare og presise.[6]

På den bakgrunn fastslo EU-domstolen i LQN at loven som skal legge til rette for bulkinnhenting «must lay down clear and precise rules governing the scope and application».[7] Det kreves altså ikke bare at det eksisterer en lovhjemmel i formell forstand, men det kreves at det eksisterer en hjemmel som i seg selv inneholder klare og presise regler om når, hvordan og i hvilket omfang myndighetene kan gripe inn i borgeres grunnleggende rettigheter ved masseovervåkning. Den normale fleksibilitet lovgiver kan tillate seg ved bruk av rettslige standarder og skjønnsmessige bestemmelser er følgelig vesentlig innsnevret.

Til tross for dette, har tingretten tilsynelatende lagt avgjørende vekt på at loven må være tilstrekkelig fleksibel til å kunne håndtere ulike krav på ulike stadier – fra innledende speiling til senere konkrete søk.

LQN etablerer imidlertid at det ikke er adgang til å ha slike fleksible lovregler som tingretten legger til grunn. Følgelig er tingrettens tilnærming feil og loven oppfyller ikke LQNs krav til presis lovgivning.

Kravet til presis lovgivning må for øvrig vurderes i sammenheng med hva LQN-kriteriene krever at loven skal være presis om, jf. manglene under. Dette kravet får derfor også betydning for de øvrige innvendingene på EØS-rettslig grunnlag.

[6] La Quadrature du Net (C-511/18) avsnitt 132.
[7] La Quadrature du Net (C-511/18) avsnitt 132.

2.2.3 Formålene som kan begrunne masseovervåkningen er for vide

I henhold til EU-domstolens praksis må det foreligge en trussel som er «genuine and present or foreseeable» mot nasjonal sikkerhet.[8] Dette innebærer at det må eksistere en umiddelbar eller forutsigbar trussel mot nasjonal sikkerhet som rettferdiggjør tiltakene som settes i verk. Utgangspunktet, som nevnt over, er at masseovervåkning til andre formål enn nasjonal sikkerhet alltid er forbudt.

Til tross for dette åpner etterretningstjenesteloven § 3-2 for vilkårlig masseovervåkning basert på mer generelle sikkerhetsvurderinger og bredere hensyn. Dette er hensyn som ikke i seg selv oppfyller EU-domstolens krav om at slik overvåking kun kan rettferdiggjøres for å ivareta grunnleggende nasjonal sikkerhet.

Loven oppstiller følgende formål i § 3-2:

a. *ivaretakelse av prioriterte utenriks-, forsvars- eller sikkerhetspolitiske interesser knyttet til forhold og utviklingstrekk i andre stater og regioner*
b. *nasjonal beredskapsplanlegging*
c. *episode- og krisehåndtering*
d. *planlegging og gjennomføring av nasjonale eller internasjonale militære operasjoner*

Loven åpner følgelig for masseovervåkning også for formål som ikke er sterke nok i henhold til kriteriene i LQN.

Tingretten erkjenner at lovens formålsangivelser gir E-tjenesten «forholdsvis vide fullmakter» når det gjelder innhenting og behandling av metadata, men mener at en samlet tolkning av formålsbestemmelsene likevel gir tilstrekkelig avgrensning av myndighetenes handlingsrom.

Dette resonnementet harmonerer dårlig med EU-domstolens ovennevnte krav til «precise rules governing the scope and application».[9] EU-domstolen har som nevnt understreket at lovgivning som tillater og definerer selve inngangsvilkårene for bulkinnsamling må være spesifikke – det er ikke adgang til videre skjønnsmessige vurderingskriterier. EØS-retten tillater derfor ikke at rammene for bruk av vilkårlig masseovervåkning settes av en samlet tolkning av formålsbestemmelsene, slik tingretten legger til grunn.

Ankende parter fastholder følgelig at formålene som kan begrunne masseovervåkningen er for vide.

[8] La Quadrature du Net (C-511/18) avsnitt 137.
[9] La Quadrature du Net (C-511/18) avsnitt 132.

2.2.4 Vilkårene for masseovervåkningen er ikke strenge nok

EU-domstolen krever at det foreligger tilstrekkelige konkrete holdepunkter («sufficiently solid grounds») som gjør det mulig å anta at det er en alvorlig trussel mot nasjonal sikkerhet som er reell og aktuell eller mulig å forutse.[10]

EU-domstolen stiller med dette klare inngangsvilkår som må være oppfylt for at masseovervåkning kan være tillatt (i tillegg må det være nødvendig og forholdsmessig). Det er ikke tilstrekkelig at overvåkningen generelt er nyttig for å ivareta nasjonale sikkerhetsinteresser – EU-domstolens oppstilte vilkår må være oppfylt.

Den norske loven oppstiller ikke noe slikt inngangsvilkår. Tvert om tok lovgiver uttrykkelig avstand fra en lovtekst der dette vilkåret ble oppstilt som et klarere krav enn i gjeldende lov:

I det siste lovutkastet som var ute på bred høring etter at EU-domstolens storkammer hadde avsagt LQN, lød forslaget til lovtekst slik (vår utheving):[11]

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

Selv om loven her oppstilte klarere kriterier enn i dagens lov, var flere høringsinnspill svært tydelige på at vilkårene ikke var formulert på en måte som innfridde EU-domstolens krav. Til illustrasjon ga Dommerforeningens menneskerettighetsutvalg, ved Thom Arne Hellerslia, uttrykk for følgende[12]:

> *I høringsnotatet fremgår det at begrunnelsen bak bestemmelsen i bokstav c er de rettslige kriteriene som ble fastsatt i EU-domstolens avgjørelser fra oktober 2020, de såkalte La Quadrature du Net-kriteriene. For det første kreves det at det er tilstrekkelig konkrete omstendigheter («sufficiently solid grounds») som gjør det mulig å anta at det er en alvorlig trussel mot den nasjonale sikkerhet. For det andre må trusselen anses reell og aktuell eller*

[10] La Quadrature du Net (C-511/18) avsnitt 137.

[11] Høringsnotat – Forslag til endringer i etterretningstjenesteloven av 27. juni 2022 s. 30-3.

[12] Høringssvar fra Dommerforeningens menneskerettighetsutvalg av 27. september 2022.

mulig å forutse. Slik vi ser det, kan det spørres om den foreslåtte formuleringen i bokstav c i tilstrekkelig grad er dekkende for den første delen av kriteriet. (…)

Beviskravene synes å være strengere enn det departementet legger opp til, og vi vil foreslå at de såkalte La Quadrature du Net-kriteriene – den første delen av disse – uttrykkes tydeligere i lovteksten.

Vi er også skeptiske til at La Quadrature du Net-kriteriene gjøres til en del av forholdsmessighetsvurderingen. Det er i stedet naturlig at disse kriteriene utgjør inngangsvilkår, hvoretter det dersom disse vilkårene er oppfylt, skal foretas en nødvendighets og forholdsmessighetsvurdering etter §§ 5-3 og 5-4.

Begrunnelsen for å svekke loven på denne måten var blant annet at departementet mente det var viktig å unngå for streng praktisering av reglene.[13] Lovgiver ønsket med andre ord helt uttrykkelig å gjøre kriteriene mindre strenge. Det ble videre presisert at trusselbildet fortsatt skulle vektlegges («tillegges betydning»), men kun som ledd i en helhetsvurdering. De ankende parter har svært vanskelig for å se hvordan denne endringen og forarbeidenes klare retningslinjer for tolkningen er forenlig med EU-domstolens krav om at loven må inneholde absolutte inngangsvilkår som må være oppfylt for at vilkårlig masseovervåkning kan være lovlig.

Kritikken i høringsrunden ledet til at departementet endret ordlyden til det som ble gjeldende lov – altså mindre konkrete krav, enn det som først var foreslått for å oppfylle EU-domstolens krav. Deretter – etter å ha svekket lovens sikkerhetsgarantier – ble det invitert til høringsrunde i Stortinget med kun 3 (!) dagers varsel.

Slik ankende parter ser det oppfyller ikke loven EU-domstolens krav, særlig fordi loven legger opp til en bred helhetsvurdering istedenfor å kreve at gitt klare vilkår er oppfylt.

Tingrettens drøftelse bærer preg av at retten kan ha misforstått de ankende parters anførsler. Drøftelsen knytter seg utelukkende til en vurdering av hvor strenge inngangskriteriene er, og særlig om det må foreligge bevis for en konkret trussel.

Tingretten berører ikke spenningsforholdet mellom EU-domstolen krav til klare lovfestede inngangskriterier, og det at lovgiver har tatt uttrykkelig avstand fra slike inngangskriterier. Tingretten har heller ingen kommentarer eller vurdering av innvendingene som ble fremmet i høringsinstansene knyttet til denne problematikken.

Tingretten har for øvrig uttrykt seg på en måte som sår tvil om tingretten har forstått hvilket alvorlig inngrep vilkårlig masseovervåkning er, ved å gi uttrykk for at LQN-kriteriene «kan synes noe strenge i den innledende fasen av informasjonsinnhentingen (speilingen)».

[13] Prop. 92 L 2022–2023 - Endringer i etterretningstjenesteloven (domstolskontroll i saker om kildevern og ved speiling av kommunikasjonsstrømmer mv.) s. 38.

Tingretten ser ved dette ut til å ha misforstått hva EU-domstolens krever, og hvor stort inngrep den innledende informasjonsinnhentingen representerer.

Speilingen er en prosess som er uløselig tilknyttet lagring. Speiling innebærer at datastrømmer overføres til E-tjenesten og etter speilingen skjer det en filtrering før materialet lagres. Det er imidlertid åpent erkjent i forarbeidene at filtreringen som gjøres før lagring er ineffektiv. Speilingen og den påfølgende lagringen utgjør slik sett et samlet inngrep der det lagres enorme mengder informasjon om alle i samfunnet (vilkårlig masseovervåkning).

EU-domstolen har vært tydelig på at kriteriene gjelder hele systemet, også det innledende stadiet hvor data samles uten særskilte søkekriterier og lagres til fremtidig behov. Realiteten er at det er ved speiling og påfølgende umiddelbare lagring til senere bruk at det mest alvorlige inngrepet i borgernes rettigheter skjer; det er denne overvåkningen som foretas uten at det er noen konkrete holdepunkter for at informasjonen er relevant eller kan tilknytes noe eller noen som rettferdiggjør lagring. Det er denne vilkårlige masseovervåkningen som kan ha en avkjølende effekt på den frie meningsutvekslingen i samfunnet m.v.

De ankende parter fastholder følgelig at EU-domstolens krav til tilstrekkelig presise og klare inngangskriterier som omtalt i LQN avsnitt 136 ikke er oppfylt ved den norske loven.

2.2.5 Masseovervåkningen kan skje i lengre tid enn det som er strengt nødvendig

Ettersom EU-domstolen kun har tillatt masseovervåkning der nasjonale sikkerhetsinteresser unntaksvis kan berettige det, krever EU-domstolen at overvåkningen kun må skje for en «forseeable period of time» og at den ikke kan være «systematic in nature».[14]

Det er et selvstendig poeng at regelverket krever en relativt hyppig fornyet vurdering av om nasjonal sikkerhet gjør det strengt nødvendig med overvåkning. Dette sikrer at masseovervåkningen ikke skjer lengre enn det de nasjonale sikkerhetsinteressene reelt sett kan legitimere. Ordet «forseeable» må derfor forstås som en tidsperiode som ikke er lengre enn den sikkerhetsmyndighetene i tilstrekkelig grad kan forutse et noenlunde realistisk fremtidig trusselnivå.

Til tross for dette, åpner den norske loven for at tillatelsen kan gis for hele to år. De ankende parter mener dette er for langt sett hen til de krav EU-domstolen har oppstilt. Trusselbildet endrer seg gjerne både vesentlig og raskt, og trusselvurderingen på et gitt tidspunkt har veldig lite relevans for hvordan situasjonen vil være to år frem i tid. Ved å åpne for tillatelser i hele to år, åpner loven for at det kan skje unødvendig masseovervåkning i lengre tidsperioder.

Til sammenligning åpnet det svenske systemet som ble vurdert i *Centrum för rättvisa* kun for beslutninger som gjaldt i 6 måneder (i tillegg til å ha en langt mindre inngripende innretning enn TI for øvrig, jf. ovenfor i punkt 2.1)

[14] La Quadrature du Net (C-511/18) avsnitt 138.

Det franske systemet, som var ett av de som ble vurdert i LQN, måtte begrenses til ett år for å oppfylle EU-rettens krav.[15]

Uten nærmere drøftelse, og uten å kommentere spenningsforholdet til de langt strammere rammene i andre lands systemer, legger tingretten uten videre til grunn at «to år … ligger innen uttrykket forseeable period of time».

Som det følger av resonnementene over, mener de ankende parter at denne vurderingen er gal.

Tingretten viser for øvrig til at domstolen ved konkrete tillatelser kan begrense retten til speiling og lagring til et kortere tidsforløp. Dette har imidlertid liten betydning i saken her. Retten her skal prøve om rammene loven setter, gir tilstrekkelige garantier for at tillatelsene kun gis for en «forseeable period of time». Det gjør ikke etterretningstjenesteloven, som overlater begrensninger til domstolens skjønn.

3 ANKEGRUNNENE KRAV 2: ENDE- OG MIDTPUNKTINNHENTING

3.1 Innledning

Tingretten har avvist ankende parters krav nr. 2, jf. dommens punkt 3.2.

Tingretten mener at de ankende parter ikke har tilstrekkelig tilknytning til kravet som fremmes. Stiftelsen mener kravet skal fremmes og gjør gjeldende at ankende parter både har tilstrekkelig tilknytning etter interne norske regler, jf. tvisteloven §§ 1-3 og 1-4 og etter særlige regler om adgang til søksmål etter både EMK og EØS-retten, jf. tvisteloven § 1-2.

3.2 Overordnet om kravet

Påstanden for krav nr. 2 ser slik ut:

> *Staten v/Forsvarsdepartementet er uberettiget til å innhente, lagre og behandle elektrisk kommunikasjon innhentet i bulk ved midtpunktinnhenting og endepunktinnhenting etter paragrafene henholdsvis 6-9 og 6-10 i Lov om Etterretningstjenesten*

Kravet må leses i sammenheng med lovens system:

Loven gjør et tydelig skille mellom etterretningsmetoder som E-tjenesten kan gjøre i egenregi og metoder som krever tilrettelegging fra tredjepart.

Metoder som krever tilrettelegging fra tredjepart er innrammet av særskilte rettsikkerhetsgarantier (forutgående domstolskontroll mv.), innført som følge av dommer fra EMD og EU-domstolen, jf. § 7-1 («det er nødvendig at tilbydere … legger til rette for innhentingen»).

[15] Conseil d'état 21. april 2021, avsnitt 45.

Metoder E-tjenesten kan gjøre i egenregi er i etterretningstjenesteloven ikke innrammet av de samme særskilte rettsikkerhetsgarantiene.

Lovens metoder i §§ 6-9 og 6-10 (henholdsvis midt- og endepunktinnhenting) gir E-tjenesten mulighet til å gjennomføre tilsvarende inngripende overvåkning som den som reguleres av kapittel 7, så lenge det skjer i egenregi uten tilrettelegging. Dette skjer blant annet uten *noen form for domstolskontroll overhodet*, og rådata innehentet gjennom disse metodene kan dessuten lagres av E-tjenesten i opptil 15 år (med mulighet for forlengelse), jf. etterretningstjenesteloven § 9-8 annet ledd.

Avgjørelsene fra EMD som oppstiller særskilte rettsikkerhetsgarantier for masseovervåkning / bulkinnhenting gjør imidlertid ikke noe skille mellom etterretning i egenregi og etterretning som skjer gjennom ekstern tilrettelegging.

Det finnes ingen god begrunnelse i forarbeidene for hvorfor lovgiver har valgt å forbeholde rettsikkerhetsgarantiene til TI, og ikke innført dem for tilsvarende overvåkning i egenregi, utover at departementet postulerer at disse metodene (i motsetning til TI) «berører ikke norsk innenlandsk kommunikasjon på en måte som begrunner slike særregler».[16]

Vår forståelse er at staten er *materielt* uenig i at staten kan gjennomføre tilsvarende informasjonsinnhenting som etter kapittel 7, særlig fordi staten mener overvåkning etter §§ 6-9 og 6-10 ikke gir hjemmel til etterretning mot personer i Norge, jf. §§ 1-4 og 4-1. De ankende parter mener dette forsvaret tilslører realitetene:

For det første gjelder forbudet i etterretningstjenesteloven § 4-1 «innhentingsmetoder etter kapittel 6 overfor personer i Norge». Forbudet gjelder verken norske borgere eller andre som befinner seg utenfor Norge, for eksempel på den svenske siden av Svinesund.

For det andre må etterretningstjenesteloven § 4-1 sees i sammenheng § 4-7, som nettopp klargjør at E-tjenesten også har adgang til å gjennomføre masseovervåkning (innhenting av rådata i bulk) selv om informasjon om personer i Norge følger med. Presisjonen i § 4-7 er avgjørende for at tilrettelagt innhenting etter kapittel 7 er lovlig til tross for § 4-1 (fordi TI i utgangspunktet regnes som en form for midtpunktinnhenting, jf. § 6-9, selv om den må skje etter de særlige reglene i kapittel 7). Paragraf 4-7 gjelder tilsvarende dersom E-tjenesten gjennomfører bulkinnhenting i egenregi, slik loven gir hjemmel til etter både paragraf 6-9 og paragraf 6-10. Vi kan derfor ikke se at statens materielle innsigelse kan føre frem.

Det er i tillegg et sentralt poeng at EMDs avgjørelse i *Wieder og Guarnieri* gjør skillet mellom borgeres rettigheter innenlands og utenlands mindre viktig, jf. punkt 2.1.3 over.

[16] Prop. 80 L 105, 2019-2020, Lov om Etterretningstjenesten (etterretningstjenesteloven), s. 105.

For spørsmål om rettslig interesse er denne materielle uenigheten uansett ikke av betydning. De ankende parters pretensjoner skal legges til grunn.

3.3 Tingrettens vurdering

Tvisteloven § 1-3 (2) krever at den som reiser sak må påvise et «reelt behov» for å få kravet avgjort, blant annet ut fra en vurdering av partens «tilknytning» til kravet.

Etter tvisteloven § 1-4 er stiftelser gitt rett til å fremme krav i eget navn om forhold som ligger innenfor organisasjonens formål og naturlige virkeområde å ivareta, når § 1-3 ellers er oppfylt. Dette er en særregulering av kravet til aktiv søksmålstilknytning for blant annet stiftelser. Stiftelser er ved dette gitt særskilt adgang til å fremme søksmål som ikke angår stiftelsens egne krav, men som gjelder allmenne interesser eller en større krets personer.

Slik vi forstår tingretten legger den avgjørende vekt på det nevnte tilknytningskriteriet når retten konkluderer med at «en dom i saksøkernes favør ikke vil ha noe faktiske eller rettslige virkninger for dem». Konklusjonen understøttes av at en virkning for mennesker som befinner seg i utlandet, og som saksøkerne kommuniserer med, etter tingrettens vurdering ikke kan «etablere en tilstrekkelig tilknytning til kravet.

Hverken etter intern norsk rett, eller etter EMK- og EØS-retten, er denne tilnærmingen tilfredsstillende.

Etter norske regler følger det som nevnt uttrykkelig av tvisteloven § 1-4 at tilknytningskravet er oppfylt dersom kravet som bringes inn for retten ligger innenfor stiftelsens naturlige virkeområde å ivareta. Tingretten skriver ingenting om dette og etter ankende parters syn løses tilknytningskravet for Stiftelsen Tinius relativt klart av denne bestemmelsen.

Det følger av det som er beskrevet i punkt 3.2 over at etterretningstjenesteloven §§ 6-9 og 6-10 gir E-tjenesten hjemmel til overvåkningsmetoder med svært stor virkning også for den norske befolkningens kommunikasjon. Eksempelvis kan E-tjenesten med hjemmel i §§ 6-9 og 6-10 gjennomfør de samme tiltakene som reguleres av kapittel 7 så lenge det gjøres i egenregi, og det er neppe tvil om at tiltakene som reguleres av kapittel 7 gir E-tjenesten rett til å gjennomføre bulkinnhenting av informasjon om svært mye av det nordmenn gjør på og via internett og internettbaserte tjenester. Det samme åpner derfor §§ 6-9 og 6-10 for.

Videre etablerer EMK særskilt adgang til domstolsprøving i overvåkningssaker, der alle kan være omfattet av overvåkningen, men ingen kan påvise konkret at de er omfattet. Den såkalt Zakharov-testen stiller to alternative kriterier for slik rett til domstolsprøving.[17] Ett av disse alternativene er at overvåkningen etablerer et system der hvilken som helst person kan få sin kommunikasjon overvåket. Slik ankende parter ser det gir §§ 6-9 og 6-10 E-tjenesten hjemmel til å foreta

17

masseovervåkning som gjør at hvilken som helst person kan få sin kommunikasjon overvåket. De ankende parter kan derfor også fremme krav på dette grunnlaget.

Også effektivitetsprinsippet etter EØS-retten gir grunnlag for å fremme kravet.[18] Konsekvensen av tingrettens avvisning er at lovhjemler som gir staten rett til omfattende masseovervåkning av norske borgere og EU-borgere – tiltak som EU-domstolen har vært svært opptatt av at skal kunne være gjenstand for domstolskontroll –, er unntatt domstolskontroll. Dette er neppe i samsvar med EØS-rettens effektivitetsprinsippet.

4 ANKEGRUNNENE – SÆRSKILT OM KILDEVERNET (EMK ARTIKKEL 10)

Innledningsvis er det under dette punkt viktig ha klart for seg at TI og ikke minst det metadatalageret som E-tjenesten blir sittende med gjennom TI, som følge av statens *forsettlige* valg om å innrette TI, *helt sikkert* også inneholder metadata om kommunikasjon mellom journalister og deres kilder og / eller metadata som kan avsløre hvem som er presens kilder. Dette gjelder i alle fall metadata om:

- Mellom medier i Norge og kilder i utlandet
- Mellom kilder i Norge og medier i utlandet
- Mellom redaksjoner i Norge og redaksjoner i utlandet
    - Som også seg imellom utveksler sensitiv kildeinformasjon

All denne kommunikasjonen har staten EMK-rettslig ansvar for, jf. *Wieder og Guarnieri.* Som vi også vet, vil metadatalageret uvegerlig inneholde metadata om kommunikasjon mellom personer som begge befinner seg i Norge når de kommuniserer – herunder journalister og deres kilder.

Den ankende parter anførte på den bakgrunn for tingretten at kildevernet etter EMK artikkel 10 krenkes *allerede gjennom lagringen i metadatalageret hos E-tjenesten i opptil 18 måneder*.

På dette punkt har tingretten anvendt EMK feil, når den tilsynelatende legger til grunn at selve lagringen ikke kan utgjøre en krenkelse.

Feil skyldes tilsynelatende at tingrettens forståelse av EMDs generelle uttalelser i *Big Brother Watch*. Det vises blant annet til følgende observasjon i tingrettens dom på s. 54:

> *EMD skiller mellom tilgang til konfidensielt journalistisk materiale som er innhentet med vilje («intentionally») og tilgang til materiale som er et tilfeldig biprodukt av TI («unintentionally, as a «bycatch» of the bulk interception operation»)*

Som beskrevet ovenfor, har staten innrettet TI slik at metadatalageret med «vilje» («intentionally») *helt sikkert* vil inneholde også kildeavslørende informasjon. Det er som på pekt også under behandlingen av EMK artikkel 8, det grunnleggende problemet med innretningen av TI – på dette

[18]

punktet i motsetning til det svenske systemet. Fordi man i TI- systemet *ikke* bruker selektorer / søkekriterier for å skille ut de metadata som kan ha interesse for konkrete etterretningsformål, men velger å lagre alle metadata i et stort metadatalager i inntil 18 måneder, som man senere kan søke i, har man bevisst valgt å lagre kildeavslørende informasjon i inntil 18 måneder.

En «unintenional» «bycatch», som EMD snakker om, ville for eksempel være at man i det svenske systemet gjennom bruk av selektorer / søkekriterier på de rådataene som speiles i bulk, for å kun trekke ut og sitte igjen med data som «treffes» av de etterretningsrelevante selektorene / søkekriteriene, utilsiktet ble sittende med kildeavslørende data. Ettersom slike «bycatches», selv om de utgjør *inngrep* i kildevernet etter artikkel 10, etter EMDs praksis ikke i seg selv nødvendigvis utgjør en *krenkelse* i seg selv, blir det avgjørende i slike tilfeller at man har rettsikkerhetsgarantier for å unngå at slik informasjon blir misbrukt. Jf. også *Big Brother Watch* avsnitt 450 (sitert, men misforstått av tingretten på s. 57 i dommen), der EMD snakker om «the **initial interception**» (vår utheving). Her siktes det til det som i TIs tilfelle vil være den innledende speilingen / innhentingen av kommunikasjonsstrømmer i bulk. Tingretten synes også å blande «interception» med «storage» (som EMD bruker om lagring), når den under henvisning til EMDs uttalelse konkluderer med at «at det ikke er i strid med konvensjonen at slikt materiale havner i metadatalageret»

Det norske TI- systemet legger som sagt bevisst opp til at – blant alle andre vilkårlige metadata om befolkningens daglige, digitale aktivitet – E-tjenesten i metadatalageret vil sitte på store mengder kildeavslørende informasjon i opptil 18 måneder. Det er *ingenting* i TI-systemet som legger opp til å begrense forekomsten av slik informasjon i metadatalageret – snarere tvert imot: Det legges opp til at det skal havne der. Det kan på mange måter sammenlignes med et beslag (der innholdet «forsegles» for innsyn, inntil retten eventuelt godkjenner at myndighetene kan se på det). Det vil i seg selv en åpenbar nedkjølende effekt på potensielle kilders tillit til at de kan kommunisere fortrolig med journalister. I den sammenheng kan det blant annet vises til Høyesteretts kjennelse i Rt-2015-1286 avsnitt 70, der peker på at allerede det forhold at PST hadde tatt beslag i en filmskapers upubliserte materiale, gjorde at flere av filmskaperens kilder hadde trukket seg (selv om beslaget var forseglet i påvente av kjennelse fra retten på om kildevernet og selv om beslaget ikke hadde som formål å avsløre filmskaperens kilder).

Stiftelsen anførte også at de bestemmelsene som forsøksvis skal ivareta kildevernet – etterretningstjenestelovens § 5-2, jf. § 9-6 – uansett ikke tilfredsstiller EMK artikkel 10.

Tingretten ser på dette punktet ut til å ha oversett at Stiftelsens anførsler ikke kun gjelder med hensyn til informasjon samlet inn og lagret i metadatalageret etter TI-systemet. På dette punktet dreier det seg også om informasjon som E-tjenesten kan innhente (også i bulk) gjennom endepunkt- og midtpunktinnhenting, jf. vår behandling ovenfor i punkt 3 – uten noen domstolskontroll.

De territorielle og personelle avgrensingene i paragraf 5-2 jf. paragraf 9-6, medfører blant annet at kommunikasjon mellom utenlandsk kilde og en utenlandsk redaksjon (for eksempel i en av Schibsteds svenske aviser, som samarbeider redaksjonelt med en av Schibsteds norske redaksjoner) *overhodet ikke omfattes av bestemmelsene.* Når E-tjenesten også *fra Norge,* med hjemmel i paragrafene henholdsvis 6-9 og 6-10 fritt kan drive midtpunktinnhenting og / eller endepunktinnhenting (via «hacking» / dataavlesning av telefoner, pc-er, servere mv.) i utlandet, kan

de hjemlene også brukes til å innhente slike kildeavslørende opplysninger – uten domstolskontroll generelt og uten at kildevernbestemmelsene i etterretningstjenesteloven kommer til anvendelse.

Det i seg selv innebærer at etterretningstjenesteloven på dette punktet krenker kildevernet etter EMK artikkel 10. Men fordi tingretten ikke har vurdert bestemmelsene i kombinasjon med midtpunkt- og endepunktinnhenting, har den oversett dette.

Stiftelsen anførte at det under enhver omstendighet utgjør en krenkelse av kildevernet etter artikkel 10, at E-tjenenesten er gitt hastekompetanse etter etterretningstjenesteloven § 8-10, som også omfatter også til å sette til side kildevernet uten å få rettens forhåndsgodkjennelse. Det vil, som påpekt for tingretten, innebære at kildevernet er «blåst» før retten får tatt stilling til det – alene basert på E-tjenestens egen vurdering.

Tingretten mener at heller ikke dette er i strid med EMK artikkel 10. Det er de ankende parter uenige i.

Når tingretten blant annet viser til at EMD i *Centrum for Rättvisa* i den sammenhengen, er det feilslått. Kildevernet overhodet ikke et tema i den saken. At EMD i den saken – i sin helhetsvurdering av det svenske systemet – ikke reagerte på den generelle hastekompetansebestemmelsen (som utelukkende dreide seg om iverkesttelse av den initiale speilingen, i henhold til det særlige svenske systemet) gir ingen føringer til spørsmålet i vår sak.

Heller ikke *Big Brother Watch* kan tas til inntekt for at slik hastekompetanse som vi diskuterer i vår sak er akseptabelt. I den saken var problemet at det britiske systemet fullstendig manglet en bestemmelse som var egnet til å ivareta kildevernet. Men når man ser på hva EMD uttalte om de generelle prinsippene – ikke minst i den delen som tingretten selv siterer på dommens s. 59, ser man at EMD nettopp sier noe om hva som kreves i hastesaker. Tingretten har imidlertid utelatt resten av det aktuelle avsnittet, som er avgjørende for å forstå den siste delen (som tingretten har gjengitt). Det kommer i forlengelse av at EMD i avsnitt 444 viser til sin tidligere praksis om at myndigheters innsyn i materiale som kan krenke kildevernet, forutsetter forutgående prøving i domstolene. Deretter kommer avsnitte som tingretten kun har sitert siste del av. Vi gjengir derfor avsnittet I sin helhet (*Big Brother Watch* avsnitt 445):

> *445. Given the preventive nature of such review the judge or other independent and impartial body must be in a position to carry out this weighing of the potential risks and respective interests prior to any disclosure and with reference to the material that it is sought to have disclosed so that the arguments of the authorities seeking the disclosure can be assessed properly. The decision to be taken should be governed by clear criteria, including whether a less intrusive measure can suffice to serve the overriding public interests established. It should be open to the judge or other authority to refuse to make a disclosure order or to make a limited or qualified order so as to protect sources from being revealed, whether or not they are specifically named in the withheld material, on the grounds that the communication of such material creates a serious risk of compromising the identity of journalist's sources (see Sanoma Uitgevers B.V., cited above, § 92 and Nordisk Film & TV A/S v. Denmark (dec.), no.*

40485/02, ECHR 2005-XIII). In situations of urgency, a procedure should exist to identify and isolate, prior to the exploitation of the material by the authorities, information that could lead to the identification of sources from information that carries no such risk (see, mutatis mutandis, Wieser and Bicos Beteiligungen GmbH v. Austria, no. 74336/01, §§ 62-66, ECHR 2007-XI).

Som det fremgår, er det som EMD sier her at utgangspunktet er at myndigheter ikke kan foreta innsyn i materiale som kan inneholde kildeavslørende informasjon, uten at en domstol eller et tilsvarende judisielt organ har gjort en forutgående prøving av om (de svært strenge) vilkårene for inngrep i kildevernet er oppfylt. Den siste delen, som tingretten siterer fra, sier at selv i hastesaker, skal de delene av materialet som kan inneholde kildeavslørende informasjon *identifiseres og isoleres* – nettopp for å unngå at kilder avsløres før en domstol har vurdert saken. Det betyr at slik informasjon må forsegles inntil en domstol har vurdert spørsmålet.

Et minstekrav for at en slik bestemmelse om hastekompetanse som etterretningstjenesteloven åpner for, må derfor være at lovgiver innfører krav om at den delen av informasjonen som kan inneholde kildeavslørende opplysninger *forsegles*, slik at retten kan prøve spørsmålet før E-tjenesten kan se på det. Slik regelen står i dag, innebærer den i seg selv en krenkelse av EMK artikkel 10

5 VIDERE BEHANDLING

De ankende parter mener at fem rettsdager er nødvendig og tilstrekkelig for ankeforhandling. Fra denne side vil det i hovedsak føres de samme bevis som for tingretten.

6 PÅSTAND

På vegne av de ankende parter nedlegges slik

påstand:

1. Staten v/Forsvarsdepartementet er uberettiget til å innhente, lagre og behandle elektronisk kommunikasjon ved tilrettelagt innhenting etter kapittel 7 i lov om Etterretningstjenesten.

2. Staten v/Forsvarsdepartementet er uberettiget til å innhente, lagre og behandle elektronisk kommunikasjon innhentet i bulk ved midtpunktinnhenting og endepunktinnhenting etter paragrafene henholdsvis 6-9 og 6-10 i lov om Etterretningstjenesten.

3. Staten v/Forsvarsdepartementet pålegges å erstatte Stiftelsen Tinius' og Tom Erik Thorsens sakskostnader for tingretten og lagmannsretten.

* * *

Dette dokument lastes opp i Aktørportalen.

Advokatfirmaet Glittertind AS

Jon Wessel-Aas
advokat (H)

Emanuel Feinberg
advokat (H)