Rettslig analyse

Etterretningstjenesteloven kapittel 7 og 8 i lys av dommer fra Den europeiske menneskerettsdomstolen og EU-domstolen

Innholdsfortegnelse

1. Innledning og bakgrunn

1.1. De internasjonale rettsavgjørelsene som skal vurderes

Den 25. mai 2021 avsa Den europeiske menneskerettsdomstolen (EMD) to storkammerdommer om bulkinnhentingsregimer i Case of *Centrum för Rättvisa v. Sweden* (application no. 35252/08), her forkortet «CfR», og i *Case of Big Brother Watch and Others v. the United Kingdom* (application no. 58170/13, 62322/14 og 24690/15), her forkortet «BBW».

EU-domstolen (ECJ) hadde i forkant av dette, den 6. oktober 2020, avsagt dom i forente saker C-511/18, C-512/18 og C-520 (La Quadrature du Net), heretter «LQN», og sak C-623/17 (Privacy International), heretter «PI», om tolkning av direktiv 2002/58 EF (kommunikasjonsvernsdirektivet). Direktivet er innlemmet i EØS-avtalen og dermed bindende for Norge. EU-domstolen slo i tolkingsavgjørelsene fast at kommunikasjonsverndirektivet etter omstendighetene får anvendelse også når formålet med innsamlingen av data er ivaretagelsen av nasjonal sikkerhet.

Ingen av dommene forbyr bulkinnhenting av data for nasjonale sikkerhetsformål, men systemer for bulkinnhenting og bruk av bulkinnhentede data må oppfylle en rekke kriterier.

1.2. Lov om Etterretningstjenesten – utsatt ikrafttredelse av kapittel 7 og 8

Ny lov om Etterretningstjenesten (etterretningstjenesteloven) trådte i kraft 1. januar 2021. Regjeringen bestemte i oktober 2020, i etterkant av EU-domstolens tolkingsavgjørelser, og i påvente av storkammeravgjørelsene fra EMD, å utsette ikrafttredelsen av kapittel 7 og 8 om tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon («tilrettelagt innhenting») i etterretningstjenesteloven. Utsettelsen ble begrunnet i behovet for å avklare etterlevelsen av våre folkerettslige forpliktelser før ikrafttredelse.

Etterretningstjenesteloven erstatter den gamle loven om Etterretningstjenesten fra 1998. Loven kodifiserer i hovedsak gjeldende regelverk og praksis og gir Etterretningstjenestens virksomhet en sikker rettslig forankring, særlig med hensyn til den menneskerettslige utviklingen de siste tiårene. Bakgrunnen for den nye loven var Stortingets anmodningsvedtak nr. 466 av 21. februar 2017, hvor regjeringen ble bedt om å legge frem forslag til revidert lov. Anmodningsvedtaket kom som en følge av EOS-utvalgets særskilte melding til Stortinget 17. juni 2016, hvor utvalget bl.a. reiste spørsmål om gjeldende lov tilfredsstilte lovskravet som følger av menneskerettighetene.

Etterretningstjenesteloven inneholder også enkelte nyvinninger, hvorav reglene om tilrettelagt innhenting i lovens kapittel 7 og 8 står i en særstilling. Reglene har blitt utformet på bakgrunn av flere utredninger. Her nevnes særlig Lysne II-utvalgets rapport om digitalt grenseforsvar av 26. august 2016, som resulterte i en anbefaling om å etablere et digitalt grenseforsvar som gir Etterretningstjenesten tilgang til digitale datastrømmer som krysser landegrensen i fiberoptiske kabler. Forutsetningen for anbefalingen var et strengt kontrollregime i flere ledd, i tillegg til strenge begrensninger på bruken av informasjonen fra tilgangen. Lysne II-rapporten ble sendt på offentlig høring 5. oktober 2016. Rapporten og høringssvarene dannet deretter utgangspunkt for Forsvarsdepartementets høringsnotat av 12. november 2018, som dernest dannet grunnlaget for Prop. 80 L (2019-2020) om ny lov om Etterretningstjenesten, som inkluderte særregler om tilrettelagt innhenting. Lovforslaget ble behandlet av utenriks-

og forsvarskomiteen i Stortinget som avga sin innstilling 8. juni, Innst. 357 L (2019-2020). Loven ble vedtatt 19. juni 2020.

1.3. Arbeidet med den rettslige analysen

En arbeidsgruppe ble satt ned kort tid etter nyttår 2021. Gruppen er ledet av Forsvarsdepartementet (FD) og har med deltagere fra Justis- og beredskapsdepartementet (JD), Utenriksdepartementet (UD), Kommunal- og moderniseringsdepartementet (KMD) og Etterretningstjenesten (E-tjenesten).

Arbeidsgruppen har hatt i oppgave å foreta en helhetlig rettslig analyse av de overnasjonale dommene, med hensikt å vurdere hvilken betydning avgjørelsene har for den norske etterretningstjenesteloven, og om det er behov for å justere lovgrunnlaget.

1.4. Struktur og avgrensning

Formålet med analysen er å vurdere om etterretningstjenesteloven kapittel 7 og 8 oppfyller de kriterier som kan utledes av Norges internasjonale forpliktelser eller om det er behov for revisjon av enkelte bestemmelser. Herunder sees det nærmere på den EØS-rettslige relevansen av EU-domstolens avgjørelser.

Analysen avgrenses i utgangspunktet mot spørsmål om revisjon av bestemmelser i andre kapitler enn etterretningstjenesteloven kapittel 7 og 8. Analysen kommer likevel på enkelte områder inn på slike revisjonsbehov der dette fremstår som naturlig.

Dommene fra Den europeiske menneskerettsdomstol (EMD) behandles først (pkt. 2). De to storkammeravgjørelsene behandles samlet, da de i det vesentlige har sammenfallende vurderingstemaer og for øvrig må forstås i sammenheng. Dommene fra EU-domstolen behandles i pkt. 3. Avgjørelsene behandles i hovedsak samlet, da de i betydelig grad har sammenfallende vurderingstemaer og for øvrig må forstås i sammenheng. I pkt. 4 trekkes konklusjoner av de foregående analyser.

2. Dommene fra Den europeiske menneskerettsdomstolen (EMD)

2.1. Generelt

Dommene gjelder spørsmålet om hhv. svensk og britisk lovgivning som tillater innhenting av elektronisk kommunikasjon i bulk er i samsvar med Den europeiske menneskerettskonvensjonen (EMK) artikkel 8 og 10.

I CfR konstaterte EMD at det svenske bulkinnsamlingsregimet var basert på klare og detaljerte regler, at bruksområdet var klart avgrenset og at det inneholdt rettssikkerhetsmekanismer. Domstolen understreket at det svenske systemet inneholdt prosedyrer for uavhengig forutgående kontroll som sikret at lovgrunnlaget ble anvendt i praksis, og som reduserte risikoen for uforholdsmessige konsekvenser for den enkeltes rett til respekt for privatlivet. Det ble særlig vist til at det svenske systemet legger opp til at den uavhengige *Försvarsunderrättelsedomstolen* må forhåndsgodkjenne og prøve lovligheten og forholdsmessigheten av hver enkelt bulkinnsamlingsoperasjon, og at de allmenne interessene i den enkelte sak som forelegges domstolen ivaretas av et personvernombud. EMD fant tre mangler i det svenske systemet som *samlet* sett medførte at Sverige ble domfelt for krenkelse av EMK artikkel 8 om retten til respekt for privatlivet. Det var særlig manglene knyttet til et tynt lovgrunnlag for utlevering av informasjon til andre, og svakheter knyttet til etterhåndskontrollen, som medførte domfellelse.

I BBW konstaterte EMD krenkelse av EMK artikkel 8 om retten til respekt for privatliv og artikkel 10 om retten til ytringsfrihet. Domstolen fant at systemet, etter en helhetsvurdering, ikke inneholdt tilstrekkelige «*end-to-end safeguards*» som sikret adekvate og effektive garantier mot vilkårlighet og misbruk. Særlig pekte domstolen på fraværet av uavhengig forhåndsgodkjenning, at begjæringer om søk ikke inneholdt kategorier av søkebegreper og at det var mangler knyttet til internkontroll av personselektorer. Domstolen viser til at det britiske systemet inneholdt andre sterke sikkerhetsmekanismer, men at disse ikke veide opp for manglene. Lovgivningen møtte ikke lovskravet, og var dermed ikke i stand til å begrense inngrepet i EMK-rettighetene til hva som kan anses som «nødvendig i et demokratisk samfunn».

Avgjørelsene fra EMD gir viktige avklaringer på menneskerettsområdet vedrørende etterretnings- og sikkerhetstjenesters innhenting, lagring og videre bruk av elektronisk kommunikasjon ved hjelp av bulkinnhenting for nasjonale sikkerhetsformål.

Det er verdt å merke seg at EMD viser til tredjepartsinnlegg, inkludert Norges, i omtalen av bulkinnhenting som primært en utenlandsetterretningskapasitet, ikke en politikapasitet.[1]

Dommene bygger på, og bekrefter langt på vei, vurderingene i kammeravgjørelsene, som tilrettelagt innhenting ble vurdert opp mot i fjorårets proposisjon om etterretningstjenesteloven.[2] Dommene etablerer likevel noe omformulerte kriterier, og introduserer noen tilleggskriterier sammenlignet med kammeravgjørelsene og tidligere rettspraksis i EMD.[3]

Dommene avviser at bulkinnhenting av elektronisk kommunikasjon i seg selv er kategorisk uforholdsmessig, samtidig som de etablerer klare krav om garantier som må oppfylles for å motvirke misbruk – i særdeleshet krav til lovens kvalitet, rettssikkerhetskrav og krav til kontrollmekanismer før, under og etter innsamlingen av kommunikasjonsstrømmer og seleksjonen av relevante data har funnet sted.

Avgjørelsene bekrefter at innhenting av rådata i bulk i seg selv ikke er ulovlig etter EMK artikkel 8 og 10. Domstolen legger til grunn at bulkinnhentingsregimene er generelt rettet mot grensekryssende kommunikasjon for utenlandsetterretningsformål, herunder «*for the purposes of foreign intelligence gathering, the early detection and investigation of cyberattacks, counter-espionage and counter-terrorism.*»[4] Domstolen anerkjenner de spesielle omstendigheter som gjør seg gjeldende for bulkinnhenting for disse formålene, og som gjør at vilkårene for målrettet innhenting slik de følger av domstolens rettspraksis knyttet til straffeområdet, ikke kan anvendes tilsvarende. Dette inkluderer krav om «*reasonable suspicion*», som EMD uttaler «*is less germane in the bulk context, the purposes of which is in principle preventive, rather than for the investigation of a specific target and/or an identifiable criminal offence*».[5]

[1] BBW avsnitt 345.
[2] Prop. 80 L (2019-2020) punkt 11.5.
[3] Strategisk etterretning er bl.a. behandlet i *Weber and Saravia*, som trakk opp de såkalte Weber-kriteriene, samt i *Liberty and Others*.
[4] CfR avsnitt 259.
[5] CfR avsnitt 262.

EMD anerkjenner statenes behov for bulkinnhenting, sett opp mot trusselbildet og den teknologiske utviklingen, og erkjenner at det ikke finnes gode alternativer til en slik kapasitet. Domstolen uttaler bl.a. at bulkinnhenting er «*a valuable technological capacity to identify new threats in the digital domain*»,[6] og videre: [7]

> "*The Court is in no doubt that bulk interception is of vital importance to Contracting States in identifying threats to their national security (..) It appears that, in present-day conditions, no alternative or combination of alternatives would be sufficient to substitute for the bulk interception power*."

Domstolen ser bulkinnhenting som en gradvis prosess, hvoretter inngrep i rettighetene etter EMK artikkel 8 øker i styrke jo lenger ut i prosessen man kommer: [8]

> "*The Court considers that Article 8 applies at each of the above stages. While the initial interception followed by the immediate discarding of parts of the communication does not constitute a particularly significant interference, the degree of interference with individuals' Article 8 rights will increase as the bulk interception process progresses."*

Avgjørelsene bekrefter at statene har en vid skjønnsmargin («*a wide margin of appreciation*») hva angår beslutningen om å innføre et bulkinnhentingssystem:[9]

> "*In view of the proliferation of threats that States currently face from networks of international actors, using the Internet both for communication and as a tool, and the existence of sophisticated technology which would enable these actors to avoid detection, the Court considers that the decision to operate a bulk interception regime in order to identify threats to national security or against essential national interests is one which continues to fall within this margin."*

Det understrekes samtidig at skjønnsmarginen knyttet til *operasjonaliseringen* av et slikt system på grunn av potensialet for misbruk, er snevrere.[10] Det er en indre og nær sammenheng mellom statenes skjønnsmargin, lovskravet og nødvendighetskravet. Når domstolen vurderer lovligheten av et menneskerettslig inngrep som følge av en stats etterretningsvirksomhet, tar den utgangspunkt i om lovgivningen som åpner for fordekt etterretningsvirksomhet oppfyller lovkravets kvalitative side, herunder om loven er tilgjengelig og forutberegnelig, samt at inngrep bare gjøres når det er nødvendig og forholdsmessig. Det er særlig viktig at loven fastsetter adekvate og effektive rettssikkerhetsmekanismer og garantier mot misbruk.[11]

Denne tilnærmingen følger av tidligere rettspraksis fra EMD, og utgjorde en del av det menneskerettslige rammeverket som gjaldt da etterretningstjenesteloven ble utformet og vedtatt. Storkammeravgjørelsene av 25. mai 2021 skiller seg fra tidligere rettspraksis i den forstand at de går noe lenger i å beskrive hvilke rettssikkerhetsgarantier mot misbruk som må implementeres i systemet, med særlig vekt på viktigheten av uavhengig kontroll og

[6] CfR avsnitt 237.
[7] CfR avsnitt 365.
[8] CfR avsnitt 244.
[9] CfR avsnitt 252 og 254.
[10] CfR avsnitt 261.
[11] CfR avsnitt 248.

autorisasjon. Samtidig viderefører domstolen tidligere rettspraksis om å se hele systemet under ett («*by conducting a global assessment of the operation of the regime*»[12]), hvilket kan innebære at svakere rettssikkerhetsmekanismer på ett område kan oppveies av sterkere rettssikkerhetsmekanismer for andre deler av bulkinnhentingsregimet. Utgangspunktet er likevel at systemet må ha «*end-to-end safeguards*» på alle stadier: Når det besluttes å gjennomføre innhenting, når innhentingen gjennomføres og etter at innhentingen er gjennomført.[13] For å hindre misbruk, må det foretas nødvendighets- og forholdsmessighetsvurderinger på alle stadier av prosessen, basert på uavhengig autorisasjon forut for innhenting, kontroll underveis og uavhengig etterhåndskontroll. Domstolen uttaler at dette utgjør «*the cornerstone of any Article 8 compliant bulk interception regime*».[14]

2.2. Kriteriene for bulkinnsamling

I dommene listes det opp åtte forhold som – med nærmere kvalifisert innhold – må fremgå klart av den nasjonale lovgivningen for at lovskravet – sett i sammenheng med kravet om at tiltaket må være «nødvendig i et demokratisk samfunn» – skal være oppfylt:[15]

- På hvilket grunnlag og for hvilke formål innhenting av rådata i bulk kan autoriseres
- Hvilke omstendigheter som kan medføre innhenting av enkeltpersoners kommunikasjon
- Hvilke prosedyrer som gjelder for å gi autorisasjon
- Hvilke prosedyrer som gjelder for seleksjon, analyse og bruk av innhentede data
- Hvilke forholdsregler som må tas dersom innhentede data skal overføres til andre
- Tidsbegrensninger for innhentingen, lagring av innhentede data og omstendighetene som gjør at innhentede data må slettes
- Hvilke prosedyrer som gjelder for uavhengig tilsyn og kontroll, og deres kompetanse til å adressere manglende etterlevelse
- Hvilke prosedyrer som gjelder for uavhengig etterhåndskontroll, og hvilken kompetanse kontrollorganet har til å adressere manglende etterlevelse

2.3. Vurdering av tilrettelagt innhenting opp mot kriteriene

2.3.1. På hvilket grunnlag og for hvilke formål innhenting av rådata i bulk kan autoriseres

Dette vilkåret skal bidra til å sikre at kravet om forutberegnelighet ivaretas. EMD presiserer at forutberegnelighet i denne sammenheng ikke skal bety at den enkelte skal kunne forutse myndighetenes bruk av de aktuelle tiltakene og således settes i stand til å omgå dem ved å tilpasse sin adferd.[16]

Domstolen går gjennom signalspaningsloven i Sverige og opplistingen av hvilke formål bulkinnhenting kan benyttes for. Lovreguleringen, sammenholdt med ytterligere veiledning i forarbeidene til signalspaningsloven, gjør at domstolen konkluderer med at oppregningen er tilstrekkelig klar. Det må tas hensyn til at bulkinnhentingsregimer «*aims at uncovering unknown foreign threats whose nature may vary and evolve over time*».[17]

[12] CfR avsnitt 274. Se også nærmere under pkt. 3 i analysen her.
[13] CfR avsnitt 250.
[14] CfR avsnitt 264.
[15] CfR avsnitt 275.
[16] CfR avsnitt 247.
[17] CfR avsnitt 285.

Etterretningstjenesteloven kapittel 3 er vel så presis som signalspaningsloven. På samme måte som i Sverige, skal E-tjenesten ikke innhente informasjon for politiformål.[18] Försvarets Radioanstalt (FRA) kan imidlertid innhente informasjon om «*serious cross-border crime*». Det kan ikke E-tjenesten. Selv om flere av formålene i etterretningstjenesteloven § 3-1 også vil være aktiviteter som er straffbare etter norsk lov (slik som grenseoverskridende terrorisme i første ledd bokstav f og internasjonal våpenhandel i første ledd bokstav i) vil formålet for Etterretningstjenestens informasjonsinnhenting aldri være kriminalitetsbekjempelse, kun ivaretagelsen av nasjonal sikkerhet. Etterretningstjenestelovens oppgavesett er derfor enda mer avgrenset enn i Sverige.

Vilkåret om grunner og formål anses følgelig oppfylt for tilrettelagt innhentings vedkommende. Vilkåret innebærer intet nytt sett i forhold til vurderingene av om tilrettelagt innhenting var i samsvar med Norges menneskerettslige forpliktelser da etterretningstjenesteloven ble fremmet og vedtatt.[19]

2.3.2. Hvilke omstendigheter som kan medføre innhenting av enkeltpersoners kommunikasjon

EMD vurderer det svenske systemet i lys av at bulkinnhenting per definisjon vil innebære en bred innhenting, fordi hele kommunikasjonsstrømmer innhentes fremfor målrettet innhenting av kommunikasjon mellom en sender og mottaker. Omstendighetene som tilsier at enkeltstående kommunikasjon kan bli gjenstand for undersøkelse på et senere stadium i prosessen, er snevrere, men fortsatt relativt vide fordi seleksjon kan gjøres basert på andre kriterier enn personselektorer.[20] Det samme gjelder for tilrettelagt innhenting.

Domstolen legger vekt på at innhenting av rådata i bulk kun gjelder grensekryssende kommunikasjon, og at det ikke er tillatt å innhente kommunikasjon mellom en sender og mottaker i Sverige, selv om det erkjennes at det ikke alltid er lett å separere utenlandstrafikk fra innenlandstrafikk. Det samme gjelder for tilrettelagt innhenting.[21]

FRA kan innhente kommunikasjonsdata for utviklingsformål. Disse kan ikke benyttes for etterretningsformål, kun for tekniske analyseformål. Domstolen aksepterer begrunnelsen for dette. Tilsvarende gjelder for tilrettelagt innhenting.[22]

Domstolen vurderer at den svenske lovgivningen er tilstrekkelig klar når det gjelder vilkårene for innhenting av enkeltpersoners kommunikasjon.[23] Vilkåret anses også oppfylt for tilrettelagt innhenting.[24]

Etterretningstjenesteloven oppstiller i tillegg grunnvilkår for innhenting, se kapittel 5. En tilsvarende skranke finnes ikke i den svenske lovgivningen. Dette underbygger ytterligere at tilrettelagt innhenting tilfredsstiller kravet om tilstrekkelig klar og forutberegnelig lovgivning om når enkeltpersoners kommunikasjon kan innhentes. Vilkåret innebærer intet nytt sett i

[18] Etterretningstjenesteloven § 4-8.
[19] Se drøftelsene i Prop. 80 L (2019-2020) pkt. 11.5.3.2.
[20] CfR avsnitt 289.
[21] Etterretningstjenesteloven § 7-6.
[22] Etterretningstjenesteloven § 7-5.
[23] CfR avsnitt 294.
[24] Se etterretningstjenesteloven §§ 7-1, 7-5 og 7-6, jf. § 8-2.

forhold til vurderingene av om tilrettelagt innhenting var i samsvar med Norges menneskerettslige forpliktelser da etterretningstjenesteloven ble fremmet og vedtatt.[25]

2.3.3. Hvilke prosedyrer som gjelder for å gi autorisasjon

I dommene uttaler EMD at bulkinnhenting må være gjenstand for uavhengig autorisering fra starten av, når formålet og rekkevidden av operasjonen defineres:[26]

> *«[…] in order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined […]»*

Dette beskrives, sammen med kravene til løpende og etterfølgende kontroll, som et sentralt krav:[27]

> «*In the Court's view, these are fundamental safeguards which will be the cornerstone of any Article 8 compliant bulk interception regime."*

Domstolen presiserer at innhentingen må autoriseres av en instans som er uavhengig fra den utøvende:[28]

> *«[…] bulk interception should be authorised by an independent body; that is, a body which is independent of the executive.»*

At det er tale om en uavhengig instans som skal autorisere på tidspunktet for innhenting fra kommunikasjonsbærerne, fremkommer også gjennom domstolens uttalelse om hva denne instansen skal informeres om for å kunne foreta nødvendighets- og forholdsmessighetsvurderingen:[29]

> *«Furthermore, in order to provide an effective safeguard against abuse, the independent authorising body should be informed of both the purpose of the interception and the bearers or communication routes likely to be intercepted. This would enable the independent authorising body to assess the necessity and proportionality of the bulk interception operation and also to assess whether the selection of bearers is necessary and proportionate to the purposes for which the interception is being conducted.»*

EMD forklarer ikke nærmere hva som ligger i kravet om at instansen skal være «independent of the executive». Det er, som nevnt over, klart at det ikke er ensbetydende med en domstol: Det fremgår av første setning i CfR avsnitt 265 («judicial authorisation […] is not a "necessary requirement»). Innholdet i kravet om uavhengig instans må også forstås på

[25] Se drøftelsene i Prop. 80 L (2019-2020) pkt. 11.5.3.
[26] CfR avsnitt 264.
[27] CfR avsnitt 264
[28] CfR avsnitt 265.
[29] CfR avsnitt 266.

bakgrunn av domstolens uttalelser om at lovligheten og forholdsmessigheten undergis en helhetlig vurdering («global assessment)».[30]

Det er også et spørsmål om den instansen som avgjør om bulkinnhenting skal tillates, må ha tilgang til de søkebegreper det er snakk om å bruke.[31] Domstolen uttaler at praktiske hensyn tilsier at instansen ikke kan få forelagt seg alle kombinasjoner av søkebegreper, men at det som et minstekrav må oppgis hvilke typer eller kategorier av søkebegreper det er snakk om å bruke:[32]

> *"Taking into account the characteristics of bulk interception (see paragraphs 258 and 259 above), the large number of selectors employed and the inherent need for flexibility in the choice of selectors, which in practice may be expressed as technical combinations of numbers or letters, the Court would accept that the inclusion of all selectors in the authorisation may not be feasible in practice. Nevertheless, given that the choice of selectors and query terms determines which communications will be eligible for examination by an analyst, the authorisation should at the very least identify the types or categories of selectors to be used."*

Bruk av såkalt sterke søkebegreper (som kan knyttes til bestemte personer) krever at det i hvert enkelt tilfelle begrunnes hvorfor tiltaket kan rettferdiggjøres ut fra prinsippene om nødvendighet og forholdsmessighet. Begrunnelsen må nedtegnes og undergis en prosess med intern tillatelse, hvor det skjer objektiv og selvstendig kontroll med at bruken er i samsvar med disse prinsippene.[33]

Hver enkelt «signals intelligence mission» – et relativt vidt begrep som dekker omfattende innhentingsvirksomhet – krever autorisasjon fra særdomstolen i Sverige.[34] I tidskritiske tilfeller kan FRA selv treffe beslutning, men denne skal snarest mulig forelegges for domstolen. EMD vektlegger i vurderingen av det svenske systemet at selv om domstolsbehandlingen i Sverige er hemmelig, skal det normalt oppnevnes en spesialrepresentant for å ivareta personvernhensyn og andre allmenne hensyn. EMD finner dette systemet tilfredsstillende. EMD vektlegger også at når FRA fremmer begjæringer til domstolen, så vil domstolen bli informert om både formålet med innhentingen og hvilke kommunikasjonsbærere som det vil søkes i. At domstolen også vurderer forholdsmessigheten av innhentingen, og at domstolens avgjørelser er bindende, utgjør «*an important safeguard built into the Swedish bulk interception system*».[35]

For tilrettelagt innhenting legges det opp til forhåndsautorisasjoner fra de ordinære domstoler (Oslo tingrett) dersom E-tjenesten ønsker å gjennomføre søk i lagrede metadata, eller for innhenting og lagring av innholdsdata. Avgjørelsene er bindende. Loven etablerer en ordning med særskilt advokat som skal ivareta rettssikkerheten til enkeltindivider og samfunnets interesser.[36] Domstolen og den særskilte advokaten vil få seg forelagt både formålet med innhentingen og det faktiske og rettslige grunnlaget for innhentingen. Som ledd i angivelsen av det faktiske grunnlaget, vil domstolen få opplysninger om hvilke

[30] CfR avsnitt 366
[31] CfR avsnitt 268
[32] CfR avsnitt 268
[33] Cfr avsnitt 269
[34] Försvarsunderrättelsesdomstolen.
[35] CfR avsnitt 299.
[36] Etterretningstjenesteloven § 8-5.

kommunikasjonsstrømmer som søkene vil bli gjort i. Oslo tingrett vil videre få seg forelagt hvilke søkebegreper eller kategorier av søkebegreper som skal benyttes.[37]

Etterretningstjenesteloven § 7-3 første ledd første punktum legger imidlertid selve *beslutningsmyndigheten* om tilretteleggingsplikt overfor ekomtilbydere i det enkelte tilfellet – som inkluderer speiling av datastrømmer – til sjefen for Etterretningstjenesten. Tilbydere som pålegges å tilrettelegge for speiling av kommunikasjonsstrømmene skal så langt mulig gis anledning til å uttale seg, jf. § 7-3 første ledd annet punktum. Beslutningen kan påklages til departementet (Forsvarsdepartementet), som kan gi klagen oppsettende virkning. Departementets beslutning kan angripes for de ordinære domstoler. Videre skal beslutning om tilrettelegging, herunder speiling av kommunikasjonsstrømmer, meddeles EOS-utvalget og Nasjonal kommunikasjonsmyndighet, jf. § 7-3 tredje ledd første punktum. Hvis EOS-utvalget mener at pålegget om speiling er 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. § 7-12. Domstolens beslutning i slike saker vil være bindende.

Samlet sett er det grunn til å reise spørsmål ved om den norske ordningen tilfredsstiller kriteriet om uavhengig autorisasjon gitt at beslutningsmyndigheten knyttet til speilingen av datastrømmene er lagt til sjefen for Etterretningstjenesten. EMD beskriver dessuten kravet om uavhengig autorisasjon som et sentralt krav. Det er dermed uklart hvorvidt mindre strenge løsninger i denne delen av systemet i en helhetsvurdering vil kunne veies opp av styrker i kontrollmekanismene i andre deler av systemet. På den annen side vil det kunne tillegges vekt at etterretningstjenesteloven ikke åpner for tilgang til eller bruk av dataene før domstolen har gitt tillatelse til å gjennomføre søk i metadata eller innhente og lagre innholdsdata. Ettersom E-tjenesten ikke har aksess til de innhentede data før domstolen har tatt stilling til om vilkårene er oppfylt, herunder om tilgangen er nødvendig og forholdsmessig, kan det ikke utelukkes at beslutningsprosedyren i § 7-3 sett i lys av EOS-utvalgets løpende kontroll og anledning til å fremme begjæring om stans til Oslo tingrett, er forholdsmessig og tilfredsstiller EMDs krav.

Det fremstår som noe uklart hvorvidt EMD mener at den autoriserende instansen skal treffe selve beslutningen om hvilke kommunikasjonsstrømmer som skal være tilgjengelige for søk, eller hvorvidt instansen skal være informert («*should be informed*») om dette, slik at den er i stand til å vurdere proporsjonalitet og nødvendighet opp mot hvilke kommunikasjonsstrømmer det er tale om.

Arbeidsgruppen mener problemstillingene må utredes nærmere, særskilt med tanke på hvilke krav som kan utledes av EMK-retten. Utredningen bør etter arbeidsgruppens syn inkludere forslag til alternative løsninger og sendes på alminnelig høring.

Når det gjelder kravene EMD oppstiller til bruk av sterke selektorer/søkebegreper er dette relevant både ved målrettet innhenting og ved målsøk, jf. grunnvilkårene i etterretningstjenesteloven kapittel 5. Det følger av § 8-2 første ledd bokstav c og d at E-tjenesten må angi søkebegrepene den ønsker å benytte i begjæringen som fremmes for domstolen. Retten skal prøve at lovens vilkår er oppfylt jf. § 8-4. Det føres løpende og etterfølgende kontroll med at E-tjenestens etterlever domstolens kjennelser jf. etterretningstjenesteloven § 7-11 og EOS-kontrolloven. Det gjelder dessuten et særskilt krav til internkontrollsystem for tilrettelagt innhenting og en intern godkjenningsordning som

[37] Etterretningstjenesteloven § 8-2.

bygger på prinsippene i etterretningstjenesteloven §§ 6-12 og 6-13. I sum vurderes dette å oppfylle kravene som EMD oppstiller til bruken av slike søkebegreper.

Oppsummert mener arbeidsgruppen at det er behov for å foreta en nærmere utredning av beslutningsprosessen i § 7-3. Denne bestemmelsen bør derfor etter arbeidsgruppens syn ikke settes i kraft nå.

2.3.4. Hvilke prosedyrer som gjelder for seleksjon, analyse og bruk av innhentede data

EMD uttaler at utelukkelse av innenrikskommunikasjon fra bulkinnhentingsregimet er en viktig begrensning for myndighetenes handlefrihet og en garanti mot misbruk.[38] Etterretningstjenesteloven § 7-6 inneholder en tilsvarende regel i form av en plikt til å søke å hindre lagring av metadata om kommunikasjon mellom avsender og mottaker som begge befinner seg i Norge (med mindre en av dem opptrer på vegne av fremmed stat eller en statslignende aktør jf. § 4-2). I dagens teknologiske situasjon vil det imidlertid ikke være mulig å hindre lagring av ikke ubetydelige mengder metadata om intern kommunikasjon, fordi også norsk til norsk kommunikasjon krysser landegrensen, uten geografiske kjennetegn som gjør det mulig å filtrere den ut.[39]

EMD mener det er betydningsfullt at FRA er underlagt en lovbestemt plikt til å slette innenrikskommunikasjon så snart slik kommunikasjon er identifisert. En tilsvarende klar sletteplikt følger ikke uttrykkelig av etterretningstjenesteloven, men må utledes av dens system sett i lys av uttalelser i forarbeidene. Her presiseres at man må forstå plikten til å «søke å» hindre lagring av kommunikasjon mellom personer som befinner seg i Norge slik at irrelevante data ikke alltid vil være mulig å filtrere bort, og at filtreringsplikten ikke vil være brutt selv om det lagres irrelevante data.[40] Sett i lys av at § 7-6 gjelder kommunikasjon mellom personer i Norge, må slik kommunikasjon anses som «irrelevante data», altså data som er irrelevante for etterretningsformål, og dermed er å anse som overskuddsinformasjon jf. etterretningstjenesteloven § 1-3 bokstav g. Personopplysninger som ikke kan behandles for etterretningsformål skal slettes, jf. § 9-2 sammenholdt med § 9-8 første ledd. Overskuddsinformasjon innhentet gjennom tilrettelagt innhenting kan som den store hovedregel ikke utleveres jf. § 7-13, og vil dermed måtte slettes uten at den kan benyttes til etterretningsproduksjon eller utleveres til andre nasjonale myndigheter eller som ledd i internasjonalt samarbeid. Det kan følgelig utledes en sletteplikt etter etterretningstjenesteloven som tilsvarer den svenske. Arbeidsgruppen peker imidlertid på at man ved en senere revisjon av etterretningstjenesteloven kan vurdere å lovfeste denne sletteplikten, slik at den kommer tydeligere frem.

EMD vektlegger videre at FRA logger alle søk og beslutninger i prosessen. EMD uttaler at det ikke utgjør en avgjørende mangel at kravet fremgår av interne instrukser, men understreker at loggekravet bør fremgå av lov. Etterretningstjenesteloven § 7-10 fastsetter et krav om at alle søk skal kunne kontrolleres i ettertid gjennom aktivitetslogger som oppbevares i 10 år og er tilgjengelige for EOS-utvalget til enhver tid. I tillegg vil utvalget ha tilgang til alle interne beslutninger – som i E-tjenestens virksomhet for øvrig – knyttet til søk i og bruk av data fra tilrettelagt innhenting.

[38] CfR 308

[39] Dette påpekes særskilt i Prop 80 L (2019-2020) pkt. 11.8.2.3

[40] Prop. 80 L (2019-2020) punkt 17 merknad til § 7-6 s. 215

I BBW vurderer EMD at det er gjort et ulovlig inngrep i kildevernet etter EMK artikkel 10.[41] Målrettet innhenting mot journalister vurderes som mer inngripende enn tilfeller av innhenting hvor det er mer eller mindre tilfeldig at etterretningstjenestene får tilgang til konfidensielt journalistisk materiale. Domstolen uttaler at bruk av selektorer eller søkebegreper tilknyttet en journalist med stor sannsynlighet vil resultere i besittelse av betydelige mengder konfidensielt journalistisk materiale som kan undergrave kildevernet i større grad enn et pålegg om å avsløre en kilde. Følgelig vurderer EMD at en domstol eller en annen uavhengig og upartisk instans med beslutningsmyndighet må godkjenne etterretningstjenestenes bruk av selektorer eller søkebegreper som man vet er tilknyttet en journalist eller som svært sannsynlig vil medføre tilgang til konfidensielt journalistisk materiale. Denne instansen må ha kompetanse til å avgjøre om bruk av selektorene/søkebegrepene er rettferdiggjort av hensyn til et overordnet krav i allmennhetens interesse («*justified by an overriding requirement in the public interest*»), og om mindre inngripende tiltak ville vært tilstrekkelig for å ivareta dette formålet.

Etterretningstjenesteloven § 9-6 fastsetter et generelt forbud mot å behandle kildeidentifiserende materiale. Forbudet innebærer at Etterretningstjenesten som hovedregel ikke skal behandle informasjon som er egnet til å avsløre identiteten til en journalistisk kilde. Etter bestemmelsens annet ledd kan informasjonen likevel behandles dersom det er strengt nødvendig at de hensyn som begrunner kildevernet viker for nasjonale sikkerhetsinteresser, som etter forarbeidene skal forstås likt med EMDs forståelse av «*justified by an overriding requirement in the public interest*». Beslutningen om å fravike hovedregelen tilligger Forsvarsdepartementet. Beslutningen skal være skriftlig, redegjøre for det faktiske og rettslige grunnlaget og meddeles EOS-utvalget.

Etterretningstjenesteloven § 9-6 gjelder kun behandling etter innhenting, jf. § 9-3. Selv om bestemmelsen ikke får direkte anvendelse på innhentingsstadiet, er den ikke uten betydning i denne sammenheng. Det fremgår av lovens forarbeider at for tilrettelagt innhenting skal domstolen prøve saker som innebærer innhenting overfor journalister eller som med sannsynlighet vil frembringe konfidensielt journalistisk materiale: [42]

> «Den høye terskelen for inngrep i kildevernet vil likevel være gjenstand for prøving av domstolen som et ledd i forholdsmessighetsvurderingen etter § 5-4. Dette innebærer for eksempel et tilnærmet absolutt forbud mot målrettet innhenting etter lovforslaget § 7-9 av kommunikasjon mellom en journalist mv. som er vernet av lovforslaget § 9-6 og en kilde, og dette vil prøves av retten.»

For målrettet innhenting ved bruk av selektorer som tilhører personer som er vernet etter etterretningstjenesteloven § 9-6, vurderes at slik forhåndsprøving av domstolen er tilstrekkelig for å oppfylle kravene som EMD oppstiller.

Et annet spørsmål er om etterretningstjenesteloven er tilfredsstillende når det gjelder unntaksvis bruk av kildeidentifiserende materiale som E-tjenesten har kommet i besittelse av som et biprodukt av annen innhenting, ettersom det er departementet – ikke domstolen eller et annet uavhengig organ – som bestemmer om informasjonen kan behandles i et slikt tilfelle. EMD uttaler at det er imperativt at den nasjonale lovgivningen inneholder robuste rettssikkerhetsmekanismer knyttet til lagring, bruk, videreformidling og sletting av

[41] BBW avsnitt 448 flg.
[42] Prop. 80 L (2019-2020) pkt. 11.9.3.3.

kildeidentifiserende materiale.[43] Dersom E-tjenesten på et senere tidspunkt får kunnskap om at dataene inneholder konfidensielt journalistisk materiale, forutsetter fortsatt lagring og bruk at vurderingen av om vilkårene for dette er oppfylt foretas av en domstol eller et annet uavhengig og upartisk organ med beslutningsmyndighet.

Etter etterretningstjenesteloven er det som nevnt departementet som treffer beslutning om videre bruk etter unntaksregelen i § 9-6 annet ledd. EOS-utvalget skal meddeles beslutningen. Beslutningen skal være utformet på en måte som er egnet for overprøving, og EOS-utvalget vil derfor være i stand til å gjennomføre uavhengig legalitetskontroll av om terskelen er nådd i hvert enkelt tilfelle. Denne ordningen vil formodentlig ha en betydelig disiplinerende effekt, og i realiteten vil det derfor kunne argumenteres for at EOS-utvalget vil fungere som en uavhengig prøvingsmyndighet i disse sakene. EOS-utvalget vil for tilrettelagt innhentings vedkommende også kunne benytte seg av myndigheten i etterretningstjenesteloven § 7-12 til å fremme begjæring overfor domstolen om stans i pågående innhenting og sletting av innhentede data.

Det er likevel usikkert om denne reguleringen tilfredsstiller EMDs krav til *hvem* som skal treffe beslutningen. Det tilføyes at det i forbindelse med komitebehandlingen av lovforslaget våren 2020 ble vurdert, etter innspill fra pressens organer, å justere lovteksten slik at beslutningsmyndigheten ble tillagt domstolen og ikke departementet, men endringsforslaget ble ikke vedtatt av Stortinget. Arbeidsgruppen peker på at den rettslige usikkerheten som er oppstått etter avsigelsen av storkammeravgjørelsene knyttet til om gjeldende regulering er i overensstemmelse med våre konvensjonsforpliktelser, taler for at det så raskt som mulig foretas en nærmere utredning av spørsmålet, som sendes på offentlig høring. Utredningsarbeidet bør igangsettes umiddelbart, men det er ikke et selvstendig krav at en eventuell justering av etterretningstjenesteloven på dette punktet må være vedtatt av Stortinget før kapittel 7 og 8 i loven kan tre i kraft. Kapittel 5 og kapittel 9 hvor de relevante bestemmelsene om kildevern er nedfelt er allerede satt i kraft, og en justering av bestemmelser i disse kapitlene vil utgjøre en alminnelig lovrevisjon. Det bør tilstrebes at eventuelle lovendringer trer i kraft før tilrettelagt innhenting settes i *operativ drift*, men begrunnelsen for å fremme eventuelle lovendringsforslag er ikke primært av hensyn til tilrettelagt innhenting, men snarere av hensyn til at de deler av etterretningstjenesteloven som allerede er ikraftsatt, skal være fullt ut i samsvar med Norges menneskerettslige forpliktelser.

2.3.5. Hvilke forholdsregler som må tas dersom innhentede data skal overføres til andre

EMD mener utviklingen har vist at det bør oppstilles mer detaljerte retningslinjer for hvilke forholdsregler som må tas dersom innhentede data skal overføres til andre:[44]

> *«[..] it is now clear that some States are regularly sharing material with their intelligence partners and even, in some instances, allowing those intelligence partners direct access to their systems. Consequently, 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."*

[43] BBW avsnitt 450.
[44] CfR avsnitt 276.

Selv om dette kriteriet fremgår av tidligere rettspraksis, er det altså nytt at EMD gir spesifikk veiledning om hvilke forholdsregler som må tas i forbindelse med utlevering av innhentet informasjon til tredjeparter. EMD uttaler at utlevering av informasjon som stammer fra bulkinnhenting bare kan skje når innhenting og lagring har skjedd i samsvar med menneskerettslige kriterier. Ytterligere rettssikkerhetsmekanismer må gjelde selve utleveringen. For det første må kriteriene for utlevering fremgå av loven. For det andre må utleverende part forsikre seg om at mottaker har tilstrekkelig evne og system til å hindre misbruk og uforholdsmessige inngrep. Særlig må mottaker kunne garantere at mottatte opplysninger blir lagret sikkert og at opplysningene i begrenset grad blir utlevert videre. Særlige garantitiltak er nødvendig dersom det utleveres kildeidentifiserende materiale. Dette betyr ikke at mottaker nødvendigvis må ha de samme rettssikkerhetsgarantier på plass som utleverende part, ei heller at utleverende part må kreve slike forsikringer fra mottakeren i hvert enkelt tilfelle.[45]

I vurderingen av den svenske lovgivningen legger EMD først til grunn at hele formålet med etterretningsvirksomhet er å innhente informasjon som er relevant for andre myndigheter, og at internasjonalt etterretningssamarbeid er avgjørende («*crucial*») for å avdekke og motvirke potensielle trusler.[46]

EMD påpeker at det ikke foreligger en bestemmelse i det svenske lovverket som pålegger FRA å vurdere om utlevering er nødvendig og forholdsmessig ut fra hensynet til de berørtes personverninteresser. EMD kritiserer dette og betegner det som en vesentlig mangel («*substantial shortcoming*»).[47] Domstolen påpeker at selv om FRA mister kontrollen over opplysningene når de er utlevert, foreligger ingen plikt til å vurdere om mottakeren har adekvate ordninger for akseptabel behandling av de utleverte opplysningene.

Den norske etterretningstjenesteloven oppstiller til sammenligning slike lovfastsatte krav som EMD etterlyser, se § 10-3 første ledd bokstav a, jf. § 10-2 første ledd bokstav d, e og f.

2.3.6. Tidsbegrensninger for innhentingen, lagring av innhentede data og omstendighetene som gjør at innhentede data må slettes

EMD slår fast at det tilligger nasjonale myndigheter å beslutte varigheten av bulkinnhentingsoperasjoner, men at det må foreligge klare krav til hvor lenge en forhåndsautorisasjon gjelder og når innhentede data må slettes.[48]

Domstolen mener svensk lovgivning gir tilstrekkelig klare indikasjoner om dette, men anser at det er en mangel at det i loven ikke fremgår en regel om at FRA må kansellere en pågående innhentingsoperasjon dersom forutsetningene for denne ikke lenger er til stede eller innhentingen for øvrig ikke lenger er nødvendig. Domstolen uttaler at betydningen av denne mangelen ikke må overvurderes,[49] og at mangelen i seg selv ikke krenker EMK artikkel 8.

Norge har til sammenligning en slik regel i etterretningstjenesteloven § 8-6 annet ledd, hvor det fremgår at E-tjenesten skal avslutte pågående søk i metadata og innhenting og lagring av innholdsdata dersom lovens vilkår ikke lenger er til stede. At innhenting skal opphøre dersom den ikke (lenger) er nødvendig, følger dessuten forutsetningsvis av § 5-4 som krever at

[45] CfR avsnitt 276.
[46] CfR avsnitt 321.
[47] CfR avsnitt 326.
[48] CfR avsnitt 331.
[49] CfR avsnitt 335.

innhentingen må være forholdsmessig, ettersom nødvendighetskravet er en delkomponent i forholdsmessighetsvurderingen.

EMD påpeker at det er et viktig rettssikkerhetstiltak at et uavhengig organ kontrollerer om bestemmelser om sletting av informasjon etterleves.

Svensk lovgivning kritiseres for at det ikke er noen regel som pålegger sletting av irrelevant materiale som ikke inneholder personopplysninger. Slike opplysninger kan berøre juridiske personers kommunikasjonsfrihet etter EMK artikkel 8, selv om innhentet kommunikasjon i de fleste tilfeller også vil inneholde personopplysninger. I sum anser imidlertid EMD at slettereglene i Sverige er tilstrekkelig klare.

Norge har en regel om at lagrede metadata fra tilrettelagt innhenting skal slettes «senest etter 18 måneder» jf. § 7-7 tredje ledd. I ordet «senest» ligger et krav om at dersom det fremstår som klart at lagrede data ikke er relevante for oppdraget, skal de straks slettes. EOS-utvalget skal føre kontroll med at sletteplikten etterleves. Dette følger både av etterretningstjenesteloven § 7-11 om utvalgets løpende kontroll, og utvalgets ordinære kontrollmandat etter EOS-kontrolloven.

2.3.7. Hvilke prosedyrer som gjelder for uavhengig tilsyn og kontroll, og kontrollorganets myndighet til å adressere manglende etterlevelse

EMD vektlegger at kontrollen er uavhengig, og at kontrollmyndigheten har formell og reell myndighet til ikke bare å kontrollere at de formelle lovkrav er fulgt, men også kontrollere at inngrepene er forholdsmessige.[50] Statens inspektion för försvarsunderrättelseverksamheten (SIUN) er en uavhengig myndighet som kontrollerer FRAs signalspaningsvirksomhet fra begynnelse til slutt, herunder kontroll med at inngrep er forholdsmessige.

Det kan anføres at § 7-11 om EOS-utvalgets løpende kontroll med tilrettelagt innhenting går lengre enn i Sverige mht. effektiv kontroll, blant annet som følge av at SIUN ikke er pålagt «løpende kontroll» i tilnærmet sanntid, slik den norske bestemmelsen gir pålegg om. Videre vil EOS-utvalget ha fullstendig innsyn i alle deler av tilrettelagt innhenting på alle stadier av prosessen, og E-tjenesten har plikt til å tilrettelegge for kontroll, bl.a. gjennom utviklingen av tekniske løsninger.[51] EOS-utvalget vurderes å ha sterke fullmakter til å både kunne vurdere E-tjenestens etterlevelse av lovgivningen og rettens kjennelser og tjenestens vurderinger i de ulike fasene av tilrettelagt innhenting.

EMD vurderer at SIUN er en tilstrekkelig uavhengig kontrollinstans. EOS-utvalget i Norge tilfredsstiller de samme uavhengighetskrav.[52]

SIUN har i enkelte tilfeller myndighet til å treffe avgjørelser med bindende virkning, herunder at ulovlig innhentet materiale må slettes. EOS-utvalget har ingen instruksjons- eller vedtaksmyndighet overfor E-tjenesten, men det følger av særregelen i etterretningstjenesteloven § 7-12 at EOS-utvalget har myndighet til å fremme begjæring om stansing av pågående innhenting og sletting av innhentede data til Oslo tingrett. I praksis vil denne ordningen ha samme effekt som den svenske. Forholdet mellom fraværet av beslutningsmyndighet for EOS-utvalget og kravene etter EMK til effektiv kontroll ble for

[50] CfR avsnitt 348.
[51] Etterretningstjenesteloven § 7-11 annet og tredje ledd.
[52] Utvalgets uavhengighet er nedfelt i EOS-kontrolloven § 1

øvrig vurdert grundig i forbindelse med behandlingen av etterretningstjenesteloven.[53] Det ble vektlagt at EOS-utvalgets uttalelser i all hovedsak følges i praksis av tjenestene, og at det foreligger gode og effektive systemer for å følge opp rapporterte avvik og mekanismer for å sørge for etterlevelse av EOS-utvalgets uttalelser.

2.3.8. Hvilke prosedyrer som gjelder for uavhengig etterhåndskontroll, og hvilken myndighet kontrollorganet har til å adressere manglende etterlevelse

EMD vurderer at kontrolltiltak og adgang for den enkelte til å få prøvd om det er begått urett mot vedkommende, ikke er avhengig av et system for notifikasjon av den enkelte om at innhentingstiltak er benyttet overfor vedkommende.[54] Etterretningstjenesteloven § 11-7 andre punktum står seg godt i forhold til dette. EMDs resonnering er på linje med begrunnelsen i lovproposisjonen om at «(d)et ville være misvisende å lovfeste underretning som hovedregel når dette av legitime grunner i praksis ikke lar seg gjennomføre».[55]

Både i Sverige og Norge har enkeltpersoner klagerett til kontrollorganet, som kan behandle sakene uten at klagerne må sannsynliggjøre at de har blitt berørt av innhenting. Hvilken informasjon som kan gis til en klager etter at kontrollmyndigheten har behandlet saken, er også relativt lik i Sverige og Norge. EMD vurderer at klagebehandlingen bør munne ut i en viss form for begrunnelse overfor klager, eller alternativt overfor sikkerhetsklarerte personer som kan ivareta klagerens interesser. En kontradiktorisk prosess er å foretrekke. EMD viser til ordningen i UK med klager til *Investigatory Powers Tribunal (IPT)* som eksempel på en ordning som klarer å forene legitime sikkerhetshensyn med kontradiktoriske hensyn.[56] EMD konkluderer med at dette utgjør en mangel i det svenske systemet. Tilsvarende må kanskje legges til grunn for EOS-kontrolloven i Norge. Dette er imidlertid en generell utfordring med EOS-utvalgets klagebehandling, som også gjelder kontrollvirksomheten overfor PST og NSM, og ikke en spesifikk problemstilling for tilrettelagt innhenting.[57]

Det ble i lovproposisjonen vist til at selv om det ikke er en kontradiktorisk prosess ved klage til EOS-utvalget fra enkeltpersoner, vil det være mulig å bringe saker inn for de ordinære domstoler, og at dette vil gi en kontradiktorisk prosess selv om tvisteloven § 22-1 i enkelte tilfeller vil kunne hindre fremleggelse av sikkerhetsgraderte opplysninger.[58] Det ble pekt på at Kongen i statsråd kan gi tillatelse til fremleggelse av sikkerhetsgraderte opplysninger, og at dette nylig ble gjort for Oslo tingrett i den såkalte Ølen Betong-saken. Videre er det en viss nyanseforskjell mellom det svenske og norske systemet som muligens vil ha betydning. Der SIUN kun kan informere en klager over at det er gjennomført en undersøkelse, vil EOS-utvalget etter EOS-kontrolloven § 15 første ledd kunne informere en klager om at undersøkelsen har medført kritikk eller ikke. I det ligger en viss indikasjon av verdi for klageren. Videre ligger det i kontrolloven § 15 første ledd en mulighet til å gi ytterligere begrunnelse. Dersom EOS-utvalget mener at en klager bør gis en mer utfyllende begrunnelse, fremmer utvalget forslag om dette til vedkommende tjeneste eller departement. Hittil har denne muligheten i svært liten grad blitt benyttet, men lovgivningen åpner altså for en mer nyansert praksis enn i Sverige. Det vises også til at denne mangelen i svensk lovgivning ikke var begrunnelsen til at Sverige ble felt for brudd på EMK artikkel 8. Da problemstillingen

[53] Se Prop. 80 L (2019-2020) pkt. 4.4.
[54] CfR avsnitt 354 og 355.
[55] Prop. 80 L (2019-2020) pkt. 14.6.4.
[56] CfR avsnitt 363
[57] Se også drøftelser knyttet til EOS-utvalget av relevans for kontrollvirksomheten i Prop. 80 L (2019-2020) pkt. 4.4.
[58] Se Prop. 80 L (2019-2020) pkt. 4.4.4

ikke er direkte relevant for spørsmålet om ikrafttredelse av kapittel 7 og 8 i etterretningstjenesteloven, gås det ikke nærmere inn på dette i analysen her, jf. avgrensningen i punkt 1.4.

EMD vurderer videre at SIUN – i hvert fall i teorien – kan komme i en interessekonflikt som følge av at organet behandler en klage som kan berøre organets egne avgjørelser, bl.a. avgjørelse om å autorisere FRAs aksess til kommunikasjonsstrømmer.[59] Det kan ikke utelukkes at EMD har hatt hovedfokus på dette aspektet i den svenske kontrollmodellen når domstolen uttaler at det forelå en mangel på dette punktet. En tilsvarende interessekonflikt er ikke aktuell for EOS-utvalget.

2.4. Helhetsvurdering («global assessment»)

EMD uttaler at det ikke er domstolens rolle å beskrive en detaljert idealmodell som alle bulkinnhentingsregimer skal ligge innenfor, men at man i stedet må vurdere hvert enkelt systems helhet opp mot de generelle kriterier som domstolen oppstiller.[60] EMD konkluderer med at «*the main features*» ved det svenske bulkinnhentingsregimet er i samsvar med EMK, herunder «*in most aspects*» nødvendig i et demokratisk samfunn.[61] Domstolen har funnet tre mangler ved svensk lovgivning, som angitt ovenfor. I helhetsvurderingen som fører til domstolens konklusjon om brudd på EMK artikkel 8, legges det imidlertid størst vekt på de lovmessige manglene ved utlevering av informasjon til partnere. Tilsvarende mangel finner man ikke i etterretningstjenesteloven.

Foruten de kontrollmekanismer og rettssikkerhetsgarantier knyttet til tilrettelagt innhenting som er beskrevet over, må det i en helhetsvurdering av systemet også tas i betraktning øvrige mekanismer og regler som kommer til anvendelse. Bestemmelsene om grunnvilkår for innhenting i etterretningstjenesteloven kapittel 5 er viktige bestemmelser som skal hindre misbruk gjennom vilkårlig og ubegrunnet innhenting. Tilrettelagt innhenting må videre sees i sammenheng med lovens øvrige bestemmelser, herunder koblingen til prioriterte nasjonale etterretningsbehov (§ 2-2), territorialforbudet (§ 4-1), forbudet mot å innhente informasjon for politiformål (§ 4-8), forbudet mot industrispionasje (§ 4-9), den strenge formålsavgrensningen knyttet til innhenting av testdata (§ 7-5), forbudet mot utlevering av overskuddsinformasjon fra innhenting etter kapittel 7 (§ 7-13), forbudet mot å bruke informasjon fremkommet gjennom tilrettelagt innhenting som grunnlag for straff eller andre strafferettslige reaksjoner (§ 7-14), diskrimineringsforbudet (§ 9-4) og forbudet mot å gi bistand til politiet i form av søk eller innhenting etter kapittel 7 (§ 10-7).

Når en tar de aktuelle bestemmelsene i betraktning, herunder de positive og negative avgrensningene av hva, hvem og for hvilke formål E-tjenesten kan eller ikke kan innhente informasjon, kombinert med lovens øvrige kontrolltiltak og rettssikkerhetsgarantier, vurderes at tilrettelagt innhenting etter en slik helhetsvurdering oppfyller EMKs krav. Som nevnt over i punkt 2.3.3 reiser imidlertid arbeidsgruppen spørsmål om prosedyrene for beslutning om tilrettelegging etter etterretningstjenesteloven § 7-3 er innenfor de rammer som EMD oppstiller i dommene. Dette spørsmålet bør derfor utredes nærmere, og arbeidsgruppen anbefaler at denne bestemmelsen ikke settes i kraft nå.

[59] CfR avsnitt 359
[60] CfR avsnitt 366.
[61] CfR avsnitt 373.

3. EU-domstolens avgjørelser

3.1. Generelt

EU-domstolens prejudisielle avgjørelser (tolkningsavgjørelser) i *Privacy International* (heretter forkortet PI) og *La Quadrature du Net* (heretter forkortet LQN) gjelder spørsmålet om britisk, fransk og belgisk lovgivning som pålegger ekomtilbydere å lagre eller overføre data til sikkerhets- og etterretningstjenester av hensyn til nasjonal sikkerhet er i samsvar med kommunikasjonsverndirektivet artikkel 15, som slår fast hvilke unntak som kan gjøres fra pliktene etter bl.a. artikkel 5(1) om kommunikasjonsvern. Domstolen fortolker direktivet i lys av EU-traktaten artikkel 4(2) og bestemmelsene om retten til privatliv og personopplysningsvern i EUs pakt om grunnleggende rettigheter (heretter «Charteret»).

LQN gjaldt franske og belgiske regler som ga kompetanse til å pålegge tilbydere av elektroniske kommunikasjonstjenester å lagre trafikkdata og lokaliseringsdata for å beskytte den nasjonale sikkerhet og bekjempe alvorlig kriminalitet.

PI gjaldt britisk lovgivning som ga britiske myndigheter vide fullmakter til å pålegge tilbydere av elektroniske kommunikasjonstjenester plikt til generell og udifferensiert overføring av kommunikasjonsdata til britiske etterretnings- og sikkerhetstjenester av hensyn til nasjonal sikkerhet. Opplysningene ble deretter lagret av disse myndighetene og brukt av dem på linje med andre databaser, for eksempel til automatisk massebehandling og analyse, kryssjekk mot andre databaser med andre typer massepersonopplysninger, eller utlevering til andre. Det var ikke krav om forutgående tillatelse fra domstol eller uavhengig forvaltningsorgan, og heller ikke om underretning til de berørte.[62]

I PI konkluderer EU-domstolen med at den britiske lovgivningen tillater generell og udifferensiert overføring av metadata, og at overføringen her tilsvarer *generell tilgang* for britiske etterretnings- og sikkerhetstjenester. Domstolen slår fast at slik overføring («*general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national* security"[63]) ikke er i tråd med EU-retten. I LQN konkluderer domstolen tilsvarende med at EU-retten forbyr lovgivning som tillater generell og udifferensiert lagring av trafikk- og lokasjonsdata som et preventivt tiltak for formålene i direktivet artikkel 15(1). På visse vilkår er det imidlertid adgang til å ha regler om slik lagring ved en alvorlig trussel mot den nasjonale sikkerheten som må anses for å være reell og aktuell eller forutsebar,[64] når dette tidsmessig er begrenset til det strengt nødvendige (som kan forlenges) og det foreligger tiltak som beskytter de berørtes kommunikasjonsopplysninger mot misbruk.[65]

EU-domstolens avgjørelser gjaldt henholdsvis britisk, fransk og belgisk rett og er ikke direkte bindende for Norge. Norge er imidlertid bundet av direktivet som domstolen tolker fordi dette er innlemmet i EØS-avtalen. Særlige forhold knyttet til Norge som EØS-nasjon drøftes under.

Etter det arbeidsgruppen kjenner til har avgjørelsene ikke ført til at EU-land som har lovgivning som pålegger ekomtilbydere å overføre/lagre data av hensyn til nasjonal sikkerhet,

[62] PI avsnitt 50-52.
[63] PI domsslutning nr. 2.
[64] LQN avsnitt 137.
[65] LQN avsnitt 138.

har suspendert eller stanset sine bulkinnsamlingsregimer.[66] Det pågår dessuten forhandlinger om et nytt kommunikasjonsvernregelverk i EU (en ny kommunikasjonsvernforordning som skal erstatte direktivet). Det er foreløpig uklart når en ny forordning vil vedtas og tre i kraft.

3.2. EU-domstolens tolkning av kommunikasjonsverndirektivet

Arbeidsgruppen har i arbeidet med analysen primært tatt utgangspunkt i kriteriene som oppstilles i LQN, da denne dommen har flest likhetstrekk med tilrettelagt innhenting. Ved tolkningen av artikkel 15 i kommunikasjonsverndirektivet tar EU-domstolen i denne saken utgangspunkt i bestemmelsens ordlyd, kontekst og formål, samt lovgivningshistorien.[67]

EU-domstolen viser til at direktivets formål ifølge fortalen avsnitt 6 og 7 er å beskytte brukerne av elektroniske kommunikasjonstjenester mot farene for deres personopplysninger og privatliv som følger av bruken av ny teknologi, og da særlig de økte mulighetene for automatisert lagring og behandling av opplysninger. Direktivet skal sikre at rettighetene i Charteret artikkel 7 og 8 blir respektert. EU-domstolen viser også til Kommisjonens lovforslag, hvor det ble uttalt at man ønsket å sikre et høyt beskyttelsesnivå for personopplysninger og privatliv og legitime interesser for juridiske personer for alle elektroniske kommunikasjonstjenester, uavhengig av hvilken teknologi som blir brukt.[68]

Domstolen fremhever at direktivets regler om kommunikasjonsvern (artikkel 5) og begrensninger i adgangen til å behandle og lagre metadata (artikkel 6 og 9), gir konkret uttrykk til rettighetene som er sikret gjennom Charteret artikkel 7 og 8, slik at brukerne av elektroniske kommunikasjonstjenester kan forvente at kommunikasjon og tilknyttede opplysninger vil forbli anonyme, og ikke vil bli tatt opp med mindre de har samtykket til det.[69]

EU-domstolen går så over til å behandle unntaket i artikkel 15. En grunnleggende forutsetning her er at unntaket ikke kan være av en slik art at det i praksis blir til hovedregelen.[70] I tillegg til Charteret artikkel 7 og 8, er også artikkel 11 om ytringsfriheten relevant ved tolkningen av unntaket i direktivets artikkel 15.[71]

Når det konkret gjelder en plikt for tilbyderne til å lagre metadata, uttaler EU-domstolen at dette i seg selv utgjør et unntak fra plikten til kommunikasjonsfortrolighet i artikkel 5, og et inngrep i rettighetene etter artikkel 7 og 8 i Charteret, uavhengig av om informasjonen er sensitiv eller om de personene som det gjelder, har blitt påført ulemper.[72] Det er heller ikke relevant om lagrede opplysninger senere har blitt brukt, da tilgang til slike opplysninger må anses som et selvstendig inngrep, uavhengig av senere bruk.[73]

EU-domstolen viser til at metadata kan gi betydelig informasjon om privatlivet til de det gjelder. Når slike data ses i sammenheng, er det mulig å trekke svært presise slutninger som gjør det mulig å lage en profil av de aktuelle personene. Slike opplysninger kan være like

[66] Med mulig unntak av Belgia. Det er imidlertid uklart på det nåværende tidspunkt om ordningen i Belgia vil bli videreført etter noen lovjusteringer.
[67] LQN avsnitt 105.
[68] LQN avsnitt 106.
[69] LQN avsnitt 109.
[70] LQN avsnitt 111.
[71] LQN avsnitt 113-114.
[72] LQN avsnitt 115.
[73] LQN avsnitt 116.

sensitive som selve innholdet i kommunikasjonen.[74] Lagring av metadata kan derfor være i strid med retten til respekt for kommunikasjon i Charteret artikkel 7 og ha en avskrekkende effekt når det gjelder bruken av ytringsfrihet etter artikkel 11.[75] En generell og udifferensiert plikt til å lagre metadata i bulk, sett i sammenheng med den sensitive arten av opplysningene, må i seg selv anses for å innebære en fare for misbruk og urettmessig adgang.[76]

Unntaksbestemmelsen i direktivet artikkel 15 gjenspeiler imidlertid at rettighetene i Charteret ikke er absolutte. Det følger av Charteret artikkel 52(1) at det kan gjøres begrensninger i rettighetene hvis det følger av lovgivning, hvis essensen av rettighetene respekteres, og hvis det er i samsvar med proporsjonalitetsprinsippet.[77] De korresponderende rettighetene etter EMK vil, i samsvar med artikkel 52(3) i Charteret, utgjøre et minimumsnivå for beskyttelse.[78]

Hva gjelder proporsjonalitetsprinsippet, viser EU-domstolen til avsnitt 11 i fortalen til direktivet, om at unntak etter artikkel 15 fra prinsippet om kommunikasjonsfortrolighet må være strengt forholdsmessige, og til egen rettspraksis om at slike begrensninger bare kan legges til grunn i den utstrekning de er strengt nødvendige.[79] Det må foretas en avveining, hvor inngrepet vurderes opp mot de samfunnsinteressene som begrunner det.[80]

Kravet om proporsjonalitet innebærer at nasjonal lovgivning må ha klare og presise regler om virkeområdet og anvendelsen av det aktuelle tiltaket, i tillegg til minstekrav slik at opplysningene er tilstrekkelig sikret mot risikoen for misbruk. Slike regler må være bindende, og de må gjøre det klart i hvilke situasjoner og på hvilke vilkår tiltak om behandling av slike opplysninger kan vedtas. Dette skal sikre at inngrepet er begrenset til det som er strengt nødvendig. Behovet for slike minstekrav er enda større hvor personopplysninger undergis automatisk prosessering, spesielt der hvor det er en betydelig risiko for ulovlig tilgang til slike opplysninger. Dette gjelder særlig for opplysninger av sensitiv art.[81]

Lovgivning som krever lagring av personopplysninger må derfor alltid oppfylle objektive vilkår som etablerer en forbindelse mellom opplysningene og det aktuelle formålet.[82]

3.3. Vurdering av om dommene gjelder for tilrettelagt innhenting

3.3.1. Kommunikasjonsverndirektivets virkeområde

EU-domstolen tolker kommunikasjonsverndirektivet i både PI og LQN. Direktivet er en del av EØS-avtalen. Domstolen legger til grunn at tiltak som er begrunnet i hensynet til nasjonal sikkerhet omfattes av direktivet dersom tiltaket innebærer at tilbydere av ekomtjenester pålegges å behandle personopplysninger i EU-rettslig forstand:[83]

> *« [..] the Court has held that Article 15(1) of Directive 2002/58, read in conjunction with Article 3 thereof, must be interpreted as meaning that the scope of that directive*

[74] LQN avsnitt 117.
[75] LQN avsnitt 118.
[76] LQN avsnitt 119.
[77] LQN avsnitt 120-121.
[78] LQN avsnitt 124.
[79] LQN avsnitt 129-130.
[80] LQN avsnitt 131.
[81] LQN avsnitt 132.
[82] LQN avsnitt 133.
[83] PI avsnitt 39-40.

extends not only to a legislative measure that requires providers of electronic communications services to retain traffic data and location data, but also to a legislative requiring them to grant the competent national authorities access to that data. Such legislative measures necessarily involve the processing, by those providers, of the data and cannot, to the extent that they regulate the activities of those providers, be regarded as activities characteristic of states [..]."

Motsetningsvis vil tiltak som implementeres direkte av statene uten å pålegge ekomtilbyderne en behandlingsplikt, falle utenfor direktivets virkeområde.[84]

Flere stater fremmet tredjepartsinnlegg for EU-domstolen knyttet til tolkningsspørsmålene, deriblant Norge. Et sentralt tema var kommunikasjonsverndirektivets virkeområde sett i lys av EU-traktaten artikkel 4(2) om at nasjonal sikkerhet er statenes eneansvar. Flertallet av statene hevdet at statlige tiltak av hensyn til nasjonal sikkerhet måtte falle utenfor kommunikasjonsverndirektivet i lys av artikkel 4(2) og kommunikasjonsverndirektivet artikkel 1(3), som i norsk oversettelse lyder:

«Dette direktiv får ikke anvendelse på virksomhet som ikke omfattes av virkeområdet til traktaten om opprettelse av Det europeiske fellesskap, som den nevnt i avdeling V og VI i traktaten om Den europeiske union, og ikke i noe tilfelle på virksomhet som gjelder offentlig sikkerhet, forsvar, statens sikkerhet (herunder statens økonomiske interesser når virksomheten er forbundet med spørsmål om statens sikkerhet) eller statens virksomhet på det strafferettslige området.»

EU-domstolen var imidlertid ikke enig med statene i en slik avgrensning av direktivets virkeområde. Etter å ha dratt skillet mellom tiltak som innebærer at tjenestetilbydere må behandle data på den ene siden og ren statlig aktivitet på den andre, understreket domstolen at: [85]

«the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law."

Norske myndigheter har hittil holdt fast ved prinsippet om at nasjonal sikkerhet er et eneansvar for nasjonalstatene, og ikke et EU/EØS-anliggende. EØS-avtalen har ingen bestemmelse som tilsvarer EU-traktaten artikkel 4(2), men det er klart at ivaretakelse av den nasjonale sikkerhet faller utenfor EØS-avtalens saklige virkeområde. På bakgrunn av domstolens begrunnelse som redegjort for over, kan det ikke utelukkes at EFTA-domstolen vil kunne komme til at direktivets saklige virkeområde er det samme i EØS som i EU.

3.3.2. Tolkingen av kommunikasjonsverndirektivets artikkel 15(1) i EØS

Direktivets artikkel 15(1) krever at alle tiltak som innføres må være i overensstemmelse med generelle prinsipper i EU-retten, herunder artikkel 6(1) og (2) i EU-traktaten, som bl.a. viser til EUs Charter. Charteret er ikke en del av EØS-avtalen, og ved innlemmelsen av direktivet i EØS ble artikkel 15(1) tilpasset ved at henvisningen til prinsippene i EU-retten og traktaten artikkel 6 ble erstattet med en henvisning til «de allmenne prinsippene i EØS-retten».[86] Det betyr at ordlyden i artikkel 15(1) ikke er identisk i EØS og EU.

[84] PI avsnitt 48, LQN avsnitt 103.
[85] PI avsnitt 44.
[86] EØS-komiteens beslutning 80/2003.

I henhold til EØS-avtalen artikkel 6 skal bestemmelser i EU og EØS som i sitt innhold er like, tolkes likt. Dette homogenitetsprinsippet får ikke samme betydning der bestemmelser i EU og EØS ikke er like. For å avklare hvilke forpliktelser EØS/EFTA-statene har etter direktivet artikkel 15(1), kan man altså ikke automatisk legge tolkningen av denne i EU til grunn. Man må se på hva som ligger i «allmenne prinsipper i EØS-retten».

Det kan ikke gis et generelt svar på hva som ligger i disse prinsippene, og deres innhold må vurderes konkret. Det er nærliggende å anta at man med «allmenne prinsipper i EØS-retten» i direktivets artikkel 15(1) sikter til de grunnleggende rettigheter som berøres i direktivet, særlig retten til respekt for privatlivet, retten til et kommunikasjonsvern og til dels ytringsfriheten. Det er etablert EØS-rett at EØS-avtalen skal tolkes i lys av slike grunnleggende rettigheter, jf. bla. sak E-4/11 Clauder avsnitt 49. I mange tilfeller vil innholdet i disse grunnleggende rettighetene korrespondere med Norges forpliktelser etter EMK, jf. referansen over.

Det finnes eksempler på at EFTA-domstolen har utviklet EØS-rettslige prinsipper i tilfeller hvor EMK ikke inneholder bestemmelser som korresponderer til Charteret.[87] Begrunnelsen som ble gitt av EFTA-domstolen var at denne friheten var i kjernen av EØS-avtalen. Også på andre områder (unionborgerdirektivet) har EFTA-domstolen de siste årene tolket EØS-retten slik at rettstilstanden blir lik i EU og EØS, også der det rettslige grunnlaget ikke har vært identisk.[88] I denne saken anså EFTA-domstolen det som nødvendig å tolke unionsborgerdirektivet annerledes i EØS enn i EU for å oppnå formålet med direktivet som er å legge til rette for og styrke utøvelsen av den grunnleggende retten til fri personbevegelse i EØS. Det er imidlertid ikke gitt at EØS-retten skal tolkes på samme måte som EU-retten når det gjelder retten til vern av personopplysninger, som ligger lenger unna kjernen i EØS-samarbeidet (de fire friheter). Som nevnt over faller ivaretakelse av nasjonal sikkerhet utenfor EØS-avtalens saklige virkeområde. Suverenitetshensyn tilsier også at statene har et visst handlingsrom her.

Det er utfordrende å trekke grensen mellom EU og EØS-retten der det er gjort materielle tilpasninger ved innlemmelse av en rettsakt i EØS-avtalen. Dette er, naturlig nok, ikke tilpasninger som EU-domstolen adresserer i saker som kun gjelder EU-stater. Når tilpasningen i tillegg, som her, ikke har et klart avgrenset innhold, blir vurderingen ytterligere utfordrende. Det kan anføres at Charterets bestemmelser har vært et utslagsgivende moment i tolkningen av artikkel 15(1) og dermed for vilkårene i LQN, og at bestemmelsen skal tolkes annerledes for Norge som EØS-stat, med de tilpasninger vi har og fordi vi ikke er bundet av EUs Charter. Samtidig er det vanskelig å isolere bidraget fra Charteret som eget og avgjørende tolkningsmoment i EU-domstolens argumentasjon.

Oppsummert er det knyttet rettslig usikkerhet til hvilken konkret betydning det har for vurderingen av tilrettelagt innhenting etter EØS-retten at direktivets artikkel 15(1) ble tilpasset ved innlemmelse i EØS og at Norge ikke er bundet av EUs Charter. Det presiseres imidlertid at det ikke ble foretatt noen andre materielle tilpasninger til direktivet ved innlemmelse i EØS enn for artikkel 15(1), og at Norge er bundet av direktivets øvrige regler slik de er i EU.

[87] Sak E-10/14 Devici avsnitt 64 (friheten til å opprette og drive egen virksomhet, sml. Charteret artikkel 16).
[88] Sak E-4/19 Campbell avsnitt 57

3.3.3. Behandling av personopplysninger som kriterium for direktivets anvendelse

Som nevnt over legger EU-domstolen i LQN og PI til grunn at all *behandling* av personopplysninger som foretas av tilbydere av elektroniske kommunikasjonstjenester, faller inn under direktivets virkeområde, herunder behandling som følge av plikter pålagt av det offentlige.[89] Hvis derimot statene selv direkte gjennomfører tiltak som fraviker regelen om kommunikasjonsfortrolighet, faller dette utenfor direktivets rammer.[90]

Hva som menes med «behandling» defineres i personvernforordningen artikkel 4 nr. 2:

> «enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.»

En plikt for tilbyderne til selv å lagre metadata[91] eller en plikt til selv å overføre metadata[92] omfattes av eksemplene i legaldefinisjonen, og omfattes således av direktivet.

I etterretningstjenesteloven er tilbydere pålagt en plikt til å speile og gjøre tilgjengelig utvalgte kommunikasjonsstrømmer og på annen måte legge til rette for utvalg, filtrering, testing, innhenting, lagring og søk, jf. § 7-2 første ledd.

Spørsmålet er om *speiling* er å anse som en «operasjon […] som gjøres med personopplysninger» slik at tilbyderne pålegges en plikt til å behandle personopplysningene i EU-rettens (GDPRs) forstand. Vurderingen må ta utgangspunkt i lovens ordlyd. Begrepet «speile» er ikke definert i loven, men kan gi inntrykk av en plikt til å foreta seg noe aktivt med kommunikasjonsstrømmen, slik at den blir tilgjengelig for E-tjenesten. Det er klart at en plikt til å *overføre* data faller inn under direktivets virkeområde, jf. PI. Å *speile* er imidlertid etter en alminnelig språklig forståelse ikke synonymt med å overføre. I praksis vil speiling tilsvare kopiering av datastrømmen i sanntid, uten at det innebærer at dataene lagres hos ekomtilbyder. E-tjenesten vil selv kunne operere systemene som sørger for at de speilede dataene overføres til og lagres hos tjenesten. Det er også vanskelig å se at tjenestetilbyderne vil være behandlingsansvarlige etter GDPR for deres begrensede tilretteleggingstiltak. Tjenestetilbyderne vil dermed ikke gjennomføre de samme aktivitetene som tilbyderne i hhv britisk, fransk og belgisk lovgivning.

På den annen side er opplistingen i personvernforordningen 4 nr. 2 ikke uttømmende, og det kan argumenteres for at kopiering av datastrømmen må sidestilles med en «operasjon som gjøres med personopplysninger» på lik linje med de øvrige eksemplene. Videre omfatter behandlingsbegrepet «spredning eller andre former for tilgjengeliggjøring». Det følger av ordlyden i etterretningstjenesteloven § 7-2 at ekomtilbyderne er forpliktet til å «gjøre tilgjengelig» kommunikasjonsstrømmene. Uavhengig av en ordlydsfortolkning av *speiling* opp mot personvernforordningen artikkel 4 nr. 2, legger imidlertid etterretningstjenesteloven § 7-2 uansett opp til en behandlingsplikt for tilbyder og systemet for tilrettelagt innhenting faller innenfor kommunikasjonsverndirektivets anvendelsesområde for så vidt gjelder enkelte av de handlinger som tilbyderne pålegges.

---

[89] LQN avsnitt 101.

[90] LQN avsnitt 103: «directly implement measures»/«mettent directement en oeuvre».

[91] LQN avsnitt 104.

[92] PI avsnitt 49: «forward»/»transmettre».

Det kan i så fall vurderes om det er hensiktsmessig og praktisk mulig at staten foretar den faktiske speilingen av data og andre tiltak som innebærer behandling av kommunikasjonsdata, slik at tilbyderne ikke pålegges noen plikter som omfattes av direktivet.

En slik ordning vil uansett måtte ivareta forsvarlig sikkerhet i norske ekomnett som pålegges tilbyder etter ekomploven § 2-10. Tilretteleggingen for en bulklagring fra E-tjenestens side uten medvirkning fra tilbyder, medfører høyere risiko for utfall og kan forringe kvaliteten i ekom- nett eller tjenester, med mindre det treffes særskilte tiltak som sikrer mot slik risiko.

Det vises i denne forbindelse til at tilretteleggingsplikten i § 7-2 ble utformet blant annet under hensynstagen til at det ville være i tilbydernes og samfunnets interesse at tilbyder selv forestår speilingen, både fordi de kjenner egne systemer best og for å unngå at E-tjenestens personell på egenhånd går inn i tilbydernes kjernenett. Arbeidsgruppen går derfor ikke videre i å anbefale en slik løsning.

3.3.4. Betydningen av eventuelle forskjeller mellom tilrettelagt innhenting og de britiske, franske og belgiske ordninger

I hvilken utstrekning LQN og PI er relevante for reguleringen i etterretningstjenesteloven kapittel 7 og 8, kan også bero på hvor mye systemene i disse to sakene ligner på tilrettelagt innhenting, og hvor generelt EU-domstolen har formulert seg i premissene.

Det britiske etterretningssystemet i PI skiller seg fra tilrettelagt innhenting på flere sentrale punkter. Overføringen omfattet data fra *alle* brukere, myndighetene fikk *direkte* tilgang til dataene, og det var *ingen begrensninger* på videre bruk av dataene.[93] At et slikt system ble ansett uforenlig med direktivet, var ingen stor overraskelse. Dommen gir lite konkret veiledning om hvilke systemer for innhenting av metadata som EU-domstolen vil kunne godta.

I LQN åpner EU-domstolen for at tilbydere kan pålegges en plikt til å lagre metadata av hensyn til nasjonal sikkerhet. Flere vilkår må imidlertid være oppfylt, se nærmere om dette nedenfor. Tilsvarende må legges til grunn for overføring av de samme data for nasjonale sikkerhetsformål, uten at tilbyderne pålegges å lagre dataene selv. Ved tilrettelagt innhenting vil det være en statlig aktør som står for overføringen av data etter at speilingen har funnet sted, samt for lagringen av dataene. Siden E-tjenesten ikke får aksess/tilgang til dataene før det foreligger tillatelse fra domstolen, jf. etterretningstjenesteloven kapittel 8, kan det anføres at systemene i praksis vil være nokså sammenlignbare og at det ikke har betydning *hvem* som står for lagringen, så lenge lagringssystemene hindrer at uvedkommende får tilgang. På den annen side kan det hevdes at etterretningstjenesteloven og sikkerhetsloven oppstiller særlig strenge krav knyttet til sikkerheten til lagrede data hos E-tjenesten, og at disse er strengere enn de krav som stilles til lagring hos tjenestetilbyderne.[94] Dessuten skal E-tjenesten iverksette systematiske tiltak for å sikre at tilrettelagt innhenting gjennomføres i samsvar med loven, og all bruk skal logges og vil være gjenstand for uavhengig kontroll av EOS-utvalget. Slike tiltak vil ha en disiplinerende effekt på tjenesten og innebære etablering av prosedyrer og interne kontrollmekanismer, for å sikre at avvik oppdages og redusere misbruksfaren ved lagring.

[93] PI avsnitt 52.

[94] Se krav til informasjonssikkerhet i blant annet etterretningstjenesteloven § 7-15 og sikkerhetsloven kapittel 5. Informasjon som E-tjenesten innhenter for etterretningsformål vil normalt være høygradert og behandlingen er underlagt strenge sikkerhetstiltak.

En forskjell som kan få større betydning, er at LQN gjaldt lagring av metadata fra *alle* brukere av kommunikasjonstjenester.[95] Tilrettelagt innhenting er begrenset til grensekryssende kommunikasjon, jf. etterretningstjenesteloven § 7-1. For å sikre at denne begrensningen får effekt, er E-tjenesten forpliktet til å søke å hindre lagring av metadata om kommunikasjon mellom avsender og mottaker som begge befinner seg i Norge,[96] jf. § 7-6. De tekniske mulighetene for å filtrere ut innenlandsk kommunikasjon fungerer godt for enkelte typer kommunikasjon, der det er mulig å angi geografisk plassering/tilhørighet, slik som prefikset +47 ved telefoni. For de typer kommunikasjon der geografi ikke lar seg bestemme, vil filtreringen ikke fungere på samme måte. Metadata om kommunikasjon mellom avsender og mottaker som begge befinner seg i Norge, skal imidlertid slettes dersom det gjøres treff på slik informasjon i forbindelse med søk. Slik intern kommunikasjon vil kategoriseres som overskuddsinformasjon, altså informasjon som er uten interesse for etterretningsformål, jf. § 1-3 bokstav g. Det følger av § 9-2 sett i sammenheng med sletteplikten i § 9-8 at overskuddsinformasjon som er personopplysninger skal slettes. Før sletting gjennomføres, kan som hovedregel slik overskuddsinformasjon deles med andre norske myndigheter når vilkårene for utlevering etter § 10-2 er oppfylt, jf. § 10-4. For overskuddsinformasjon som stammer fra tilrettelagt innhenting stiller dette seg annerledes. Det følger av § 7-13 at E-tjenesten ikke skal utlevere overskuddsinformasjon fra tilrettelagt innhenting, med mindre det er nødvendig for å forhindre alvorlig fare for noens liv, helse eller frihet eller at noen blir uriktig tiltalt eller domfelt for en straffbar handlinger. Lovens system sikrer følgelig at treff på søk som er intern kommunikasjon må slettes, og at slik kommunikasjon ikke vil kunne benyttes til etterretningsproduksjon eller utlevering til andre aktører.

Det er også viktig å merke seg at EMD i *Centrum för rättvisa* tilla begrensningen til grensekryssende kommunikasjon etter svensk rett vekt, og uttalte at begrensningen «*must be seen as a significant limitation on the authorities' discretion and as a safeguard against abuse*».[97] Spørsmålet ble ikke prøvd av EU-domstolen.

Tilrettelagt innhenting er strengt avgrenset til utenlandsetterretning. Det er en viktig avgrensning. Det betyr at de mest inngripende tiltakene en stat kan gjennomføre overfor egne borgere faller utenfor (overvåkning av personer på eget territorium er særlig inngripende pga. statens sanksjonsmuligheter innenfor egen jurisdiksjon). Foruten formålsavgrensningen i lovens kapittel 3 og innhentingsforbudene i kapittel 4 vises det også til forbudet i § 7-14 mot å benytte informasjon som fremkommer gjennom tilrettelagt innhenting som grunnlag for ileggelse av straff eller andre strafferettslige sanksjoner (med unntak for saker som gjelder terrorhandlinger etter straffeloven § 131).

Til sammenligning omfattet den franske lovgivningen som ble prøvd i LQN – *Code de la sécurité intérieure (Internal Security Code)* – avverging av bl.a. kollektive voldshandlinger som kan forårsake alvorlige forstyrrelser for opprettholdelsen av lov og orden («*collective violence liable to cause serious disruption to the maintenance of law and order*»), organisert kriminalitet og andre forhold som bærer mer preg av kriminalitetsbekjempelse enn utenlandsetterretning.

[95] LQN avsnitt 137-138: «all users»/«l'ensemble des utilisateurs».

[96] Med mindre en av dem opptrer på vegne av fremmed stat eller statslignende aktør, jf. etterretningstjenesteloven § 4-2 første ledd.

[97] CfR avsnitt 308.

På denne bakgrunn kan det argumenteres for at vurderingene i EU-dommene ikke uten videre lar seg overføre til et system som kun gjelder grensekryssende kommunikasjon, strengt avgrenset til utenlandsetterretning og hvor det ikke skjer en altomfattende lagring av personopplysninger. Det kan også stilles spørsmål ved om EU-domstolens uttalelse om at unntaket i artikkel 15(1) ikke kan bli hovedregelen,[98] er like treffende i slike saker. I alle tilfeller er det klart at tilrettelagt innhenting på dette punktet skiller seg fra de systemer som ble behandlet i EU-domstolens avgjørelser.

Det kan samtidig problematiseres om begrensningen til grensekryssende kommunikasjon er tilstrekkelig til at det kan oppstilles lempeligere vilkår for tilrettelagt innhenting, sammenlignet med kravene som stilles i LQN. Eksempelvis kan det hevdes at lagringen i seg selv er såpass omfattende at det er av underordnet betydning hvilke bruksbegrensninger som gjelder og at treff på ren innenlands kommunikasjon er underlagt sletteplikt. Ved tilrettelagt innhenting vil det bli lagret store mengder data uten at det er påvist noen forbindelse mellom dataene og etterretningsformålet.[99] Dette kan tale for at tilrettelagt innhenting vil bli vurdert på samme måte som lagring av metadata i LQN. Beskrivelsen av lagringen i LQN som «preventiv lagring»[100] støtter også opp under en slik forståelse. En slik forståelse kan tilsi at det er fraværet av mistanke eller lignende mot de personene som rammes som er det sentrale, ikke hvor mange personer som omfattes eller hvor disse befinner seg (innenlands/utenlands).

Avslutningsvis bemerkes det at tolkingsavgjørelsene fra EU-domstolen ikke går nærmere inn og vurderer utfordringer knyttet til truslene i cyberdomenet og grunnleggende tekniske forutsetninger som ligger til grunn for bulkinnsamling. Dette gjør det vanskeligere å operasjonalisere kriteriene i dommene i praksis. Til sammenligning foretok EMD en grundig analyse av konteksten som den svenske og britiske lovgivningen anvendes i.

Samlet sett er det mulig å argumentere for at systemet for tilrettelagt innhenting må vurderes etter en annen standard enn altomfattende systemer som i PI og LQN. Ingen avgjørelser avsies i et vakuum, og EU-domstolens tolkingsavgjørelser synes å basere seg tungt på inntrykket fra det franske, belgiske og britiske systemet, som på vesentlige områder skiller seg fra kapittel 7 og 8 i etterretningstjenesteloven.

3.4. Vurdering av om kapittel 7 og 8 er i overensstemmelse med EU-domstolens krav til bulklagring

3.4.1. Krav om alvorlig trussel som er reell og aktuell eller forutsebar

Dersom man, til tross for de rettslige usikkerhetsmomentene som det er pekt på i vurderingene i pkt. 3.3 ovenfor, kommer til at vilkårene i LQN gjelder for tilrettelagt innhenting etter EØS-retten og for et system som det norske, blir det neste spørsmålet hvordan disse vilkårene skal forstås.

For det første presiserer domstolen at den ikke tidligere har tolket kommunikasjonsverndirektivet i saker som angår tiltak for å beskytte nasjonal sikkerhet.[101] I denne sammenheng viser domstolen til EU-traktaten artikkel 4(2), og slår fast at statenes eneansvar for nasjonal sikkerhet etter denne bestemmelsen korresponderer med de primære interessene statene har i å verne essensielle statlige funksjoner, herunder å avverge og straffe

[98] LQN avsnitt 111, PI avsnitt 59.
[99] LQN avsnitt 133 og 137.
[100] LQN avsnitt 138.
[101] LQN avsnitt 134.

aktivitet som er egnet til å destabilisere fundamentale konstitusjonelle, politiske, økonomiske eller sosiale statlige strukturer eller som er egnet til å direkte true samfunnet, befolkningen eller staten selv, slik som terrorisme.[102]

Videre presiserer domstolen at tiltak med formål å beskytte nasjonal sikkerhet er viktigere enn de øvrige formålene som kan begrunne unntak etter artikkel 15(1), herunder kriminalitetsbekjempelse og beskyttelse av offentlig sikkerhet. På grunn av deres natur og høye alvorlighetsgrad kan truslene som omfattes av nasjonal sikkerhet distingveres fra den generelle risikoen som intern spenning og uro – også der denne er av en alvorlig karakter – kan forårsake. Tiltak for å beskytte nasjonal sikkerhet kan dermed rettferdiggjøre mer alvorlige inngrep i grunnleggende rettigheter enn de øvrige formålene i artikkel 15(1).[103]

På denne bakgrunn konkluderer domstolen med at artikkel 15(1), lest i lys av Charteret artikkel 7, 8, 11 og 52(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, forutsatt 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 judgment, to national security which is shown to be genuine and present or foreseeable.»*[104]

Domstolen oppstiller her grunnvilkårene 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 er en *alvorlig trussel mot den nasjonale sikkerhet*. For det andre må trusselen anses *reell og aktuell eller mulig å forutse*. Ordlyden «reell og aktuell» henspeiler på at trusselen må være genuin, mens alternativet om forutsebarhet henspeiler på at trusselen i det minste må være påregnelig med en viss grad av sannsynlighet. Kravene til bevis framstår som vage og ikke spesielt strenge *(«sufficiently solid grounds for considering»/«circonstances suffisamment concrètes permettant de considérer»*), og truslene som kan gi grunnlag for lagring av metadata er også formulert nokså bredt *(«activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country»*).[105] Uttalelsen viser videre at det trolig er tilstrekkelig at trusselen er av generell art, også fordi fremtidige trusler er omfattet dersom de kan forutses/er påregnelige («*which is shown to be genuine and present or foreseeable»/«qui s'avère réelle et actuelle ou prévisible*»).

Domstolen uttaler videre:[106]

> *«Even if such a measure is applied indiscriminately to all users of electronic communications systems, without there being at first sight any connection, within the meaning of the case-law cited in paragraph 133 of the present judgment, with a threat to the national security of that Member State, it must nevertheless be considered that the existence of that threat is, in itself, capable of establishing that connection.»*

[102] LQN avsnitt 135.
[103] LQN avsnitt 136.
[104] LQN avsnitt 137.
[105] LQN avsnitt 137, jf. avsnitt 135.
[106] LQN avsnitt 137.

Dette må forstås slik at selv om et tiltak gjelder for alle brukere av elektroniske kommunikasjonstjenester, uten at det i utgangspunktet synes å være noen sammenheng med en trussel mot nasjonal sikkerhet, må eksistensen av en slik trussel i seg selv anses egnet til å etablere en slik forbindelse. Videre kan det ikke være nødvendig at trusselen har konkretisert seg, i den forstand at man må kjenne navnet på personer eller grupper som antas å være involvert i trusselaktivitet. EU-domstolens bemerkning om at det ikke kreves noen forbindelse mellom de dataene det er snakk om å lagre, og trusselen mot nasjonal sikkerhet, ville ellers ikke gi noen mening.

En slik plikt til preventiv lagring av alle brukeres opplysninger må begrenses i tid til det strengt nødvendige. Tiltaket kan forlenges hvis trusselen fortsatt er til stede («*owing to the ongoing nature of such a threat*»/«*en raison de la persistance d'une telle menace*»), men bare innenfor en tidshorisont som kan forutses. Lagringen må være gjenstand for begrensninger, og være rammet inn av strenge minstekrav som gjør det mulig å effektivt beskytte opplysningene mot misbruk, se nærmere nedenfor. Lagringen kan derfor ikke være av systematisk karakter.[107] Det ligger i dette at det ikke vil være adgang til å ha et permanent system for generell og udifferensiert lagring av metadata, som ikke er direkte knyttet til potensielt alvorlige trusler mot nasjonal sikkerhet.

EU-domstolen understreker også at det må sikres at bruk av slike tiltak faktisk begrenses til der hvor det er en slik trussel mot den nasjonale sikkerhet. Det er derfor avgjørende at beslutninger om slike tiltak undergis effektiv kontroll, enten av domstolene eller tilsvarende uavhengig organ.[108]

Trusselen må være genuin og påregnelig. Domstolen går ikke nærmere inn på hva som ligger i disse begrepene. Det er nærliggende å tolke domstolens uttalelse om at det ikke kreves noen forbindelse mellom dataene det er tale om å lagre (altså for alle brukere) og trusselen, dithen at trusselen kan være av generell art. I lys av at et av formålene med etterretningsvirksomhet er å avdekke hittil ukjente trusler, er det vanskelig å forstå kravene som noe annet enn at E-tjenesten må besitte informasjon som etter en nærmere etterretningsfaglig analyse tilsier at et gitt forhold innebærer et trusselpotensial for den nasjonale sikkerheten. En praktisk tilnærming til kriteriet vil være å innfortolke et krav om at det må være mulig å saklig begrunne at trusselpotensialet vil eller kan realiseres dersom ulike forutsetninger er til stede. Videre tilsier nødvendighets- og effektivitetshensyn at man må følge personer, grupper og fenomener over tid for å kunne avdekke og motvirke truslene i tide.

Grunnvilkåret i etterretningstjenesteloven for innhenting av rådata i bulk i § 5-3 første ledd må være oppfylt for at tilrettelagt innhenting skal kunne benyttes. Det oppstilles her et krav om at innhentingen må være «nødvendig for å få tilgang til et relevant og tilstrekkelig informasjonsgrunnlag.» Hva som vil være nødvendig i det enkelte tilfellet må vurderes konkret. Der Norges internasjonale forpliktelser stiller særlige krav til innhentingen, må dette tas høyde for i lovtolkingen.

E-tjenesten må fremme begjæring for Oslo tingrett om tillatelse til å gjennomføre søk i metadata som lagres gjennom tilrettelagt innhenting. Etterretningstjenesteloven § 8-2 oppstiller krav til begjæringen, herunder at tjenesten må angi oppdraget som søket knytter seg til og det faktiske og rettslige grunnlaget for søket, jf. bokstav a og b. Begjæringen skal gjøres kjent for EOS-utvalget, jf. § 8-1 siste ledd andre punktum. Både domstolen og utvalget vil

[107] LQN avsnitt 138.
[108] LQN avsnitt 139.

dermed kunne vurdere E-tjenestens tilnærming til kravene over, og ettergå disse i henhold til egen kompetanse, dersom det oppfattes at tjenesten legger en uriktig tolkning til grunn.

I tillegg til den løpende overprøvingen fra domstolen i forbindelse med begjæringer om søk i lagrede metadata, og den løpende kontrollen fra EOS-utvalget, vil også regjeringen regelmessig revurdere om potensielle trusler mot rikets sikkerhet tilsier bruk av tilrettelagt innhenting. Dette gjøres minimum årlig gjennom behandling av E-tjenestens og PSTs graderte trusselvurderinger. Trusselvurderingene forelegges også for offentligheten i ugraderte versjoner. Lovens ordlyd gjengir imidlertid ikke LQN-kriteriene direkte, og arbeidsgruppen mener det kan være grunn til å vurdere dette nærmere i forbindelse med en videre utredning av beslutningsprosedyren i § 7-3. I denne forbindelse bør det etter arbeidsgruppens syn vurderes om det er behov for å knytte beslutningen om tilrettelegging opp mot en vurdering av trusselsituasjonen og dermed behovet for tilrettelegging.

Frankrikes høyesterett (Le Conseil d'Etat) har i sin avgjørelse av 21. april 2021 kommet til at det franske systemet som ble prøvd i LQN er forenlig med EU-retten, fordi det på tidspunktet for avgjørelsen fantes flere trusler, som ikke bare kunne forutses, men som også var aktuelle.[109] Det ble vist til følgende trusler: terrorisme, spionasje og annen innblanding fra utlandet, og en økning i radikale og ekstremistiske grupper. Domstolen kom til at det manglet en bestemmelse om plikt til jevnlig å vurdere om trusselen fortsatt er til stede, men det var ikke nødvendig å gjøre andre endringer i det franske regelverket.[110]

Tilsvarende vurderinger legges til grunn av den danske regjeringen, i et forslag til lovskisse om datalagring som skal munne ut i lovbehandling senere i år eller neste år.[111] Det danske justisdepartementet viser i den forbindelse til at Center for Terroranalyse (CTA) årlig utgir vurderinger av terrortrusselen mot Danmark, og at denne sammen med andre analyseprodukter fra etterretnings- og sikkerhetstjenestene i Danmark er tilstrekkelige til å underbygge at kravene EU-domstolen oppstiller i LQN er tilfredsstilt:

> *«Det er således Justitsministeriets vurdering, at der bl.a. på baggrund af Vurderingen av Terortruslen mod Danmark og øvrige analyseprodukter, kan foretages en velunderbygget vurdering av truslen mot Danmarks nationale sikkerhed med henblik på at konstatere, om der er tilstrækkelige solide grunde til at antage, at Danmark står over for en alvorlig trussel mot den national sikkerhed, som er reel og aktuel eller forudsigelig.»*[112]

I det danske forslaget foreslås å innføre en ordning hvor justisministeren kan fastsette en forpliktelse for tjenestetilbyderne i opptil et år av gangen å lagre metadata i bulk av hensyn til beskyttelse av nasjonal sikkerhet. Justisministerens vurdering kan i prinsippet gjøres til gjenstand for domstolsprøvelse. Detaljeringsgrad i de ugraderte trusselvurderinger mv anses å utgjøre et tilstrekkelig grunnlag for effektiv rettslig prøving, og kan eventuelt suppleres med vitneforklaringer fra ledende medarbeidere som kan forklare metodikken og tilblivelsesprosessen bak de konkrete vurderingene.

---

[109] Avgjørelse i sak nr. 393099, 394922, 397844, 397851, 424717, 424718 French Data Network et autres, avsnitt 44.

[110] Ibid, avsnitt 45.

[111] *Justitsministeriet, 23. mars 2021: Skitse for revision av logningsreglerne mv*. Skissen omhandler primært datalagring for å bekjempe alvorlig kriminalitet, som etterforskningsredskap for politiet og Politets Efterretningstjeneste, men omhandler i kapittel 3 også krav til bulklagring av trafikkdata med formål å beskytte nasjonal sikkerhet.

[112] Pkt. 3.3.2 i lovforslaget.

3.4.2. Kravet til proporsjonalitet og streng nødvendighet

Som redegjort for over under punkt 3.4.1, kreves at unntak etter artikkel 15 fra prinsippet om kommunikasjonsfortrolighet må oppfylle proporsjonalitetskravet, herunder kravet til streng nødvendighet. Kravet innebærer at det må gjelde klare og presise regler som angir i hvilke situasjoner og på hvilke vilkår tiltak som medfører behandling av personopplysninger kan vedtas, og minstekrav som sikrer mot misbruk. Avslutningsvis må det foretas en samlet interesseavveining.

Rettssikkerhets- og kontrolltiltak som ikke omfatter tjenestetilbydernes behandling av kommunikasjonsdata faller utenfor EU/EØS-rettens virkeområde, jf. pkt. 3.3.2 ovenfor.

Formålet med etterretningstjenesteloven fremgår av § 1-1. Loven skal blant annet bidra til å trygge Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser, herunder forebygge, avdekke og motvirke utenlandske trusler mot Norge og norske interesser. Lovens kapittel 3 (§§ 3-1 til 3-5) konkretiserer E-tjenestens oppgaver og angir hvilke formål som kan begrunne innhenting og analyse av informasjon. Videre fremgår det uttrykkelig i kapittel 4 hvilken informasjon som ikke kan innhentes, blant annet forbudet mot innhenting i Norge og forbudet mot å innhente for politiformål.

Det vurderes at formålsangivelsen i kapittel 3 sett i sammenheng med kravet til behandlingsgrunnlag etter § 9-2 og med forbudene og begrensningene i kapittel 4 på en tilstrekkelig klar og presis måte angir hvilke situasjoner som kan medføre at data innhentes og behandles. Det samme gjelder en klar og presis angivelse av hvilke vilkår som må være oppfylt for at innhenting og behandling skal kunne finne sted, se særlig grunnvilkårene i kapittel 5, særreglene for tilrettelagt innhenting i kapittel 7 og 8, samt reglene for behandling av personopplysninger i kapittel 9 og reglene for utlevering i kapittel 10. Loven er skrevet innenfor rammen av det menneskerettslige lovskravet etter EMK, hvoretter det også kreves klare og presise lovregler.

EU-domstolen drøfter ikke proporsjonaliteten og det strenge nødvendighetskravet i LQN avsnitt 137-139, der vilkårene for datalagring i bulk for nasjonale sikkerhetsformål fremgår. Domstolen er heller ikke tydelig på hva som ligger i streng nødvendighet utover de ovenfor nevnte kravene til lovgivningen og at det må foretas en samlet interesseravveining. I avsnitt 136 understreker domstolen at nasjonale sikkerhetsformål «*goes beyond*» de andre formålene som kan begrunne unntak etter artikkel 15(1). Det kan dermed argumenteres for at så lenge lovskravet er oppfylt, trusselsituasjonen som beskrives i avsnitt 135-137 er til stede og innhentingen/lagringen er gjenstand for uavhengig kontroll, så vil proporsjonalitetskravet og kravet til streng nødvendighet også være oppfylt.

Når det gjelder reglene for tilrettelagt innhenting i etterretningsloven kapittel 7 og 8, finnes det ikke uttrykkelige bestemmelser som sikrer at selve innhentingen begrenses til det som er strengt nødvendig. Men et nødvendighetskrav – som blir strengere jo mer inngripende tiltak det er tale om – følger likevel av forholdsmessighetsprinsippet, jf. loven § 5-4, jf. § 5-3, som også gjelder for en beslutning om innhenting etter §§ 7-2 og 7-7. I forarbeidene heter det at:[113]

> «Departementet er enig med NIM i at Etterretningstjenesten bare skal kunne kreve tilrettelegging i den grad det er nødvendig ut fra formålet. Departementet mener at

[113] Prop. 80 L (2019-2020) pkt. 11.8.7.3

> dette kravet er tilstrekkelig regulert gjennom lovforslaget § 5-3 om innhenting av rådata i bulk og plikten til utvalg etter lovforslaget § 7-6.»

I tillegg kommer uttalelser i forarbeidene om at «Etterretningstjenesten skal prioritere innhenting fra de kommunikasjonsbærerne som antas å transportere mest mulig etterretningsrelevant kommunikasjon».[114] Det må også tas i betraktning at EU-domstolen åpner for innhenting av kommunikasjon knyttet til samtlige brukere av kommunikasjonstjenestene, og at tilrettelagt innhenting er mer begrenset enn dette. Samtidig må den teknologiske realitet tas i betraktning, i den forstand at utenlandske trusler i det digitale rom som har til hensikt å ramme norske personer og virksomheter i Norge vil kunne ta svært ulike veier inn i Norge. Det vil dermed i utgangspunktet være strengt nødvendig å innhente mest mulig av de utenlandske kommunikasjonsstrømmene, som grunnlag for autoriserte målrettede søk i strømmene.

Etter en samlet avveining taler ovennevnte for at tilrettelagt innhenting oppfyller kravet til proporsjonalitet og streng nødvendighet.

3.4.3. Avgrensningen til trusler mot nasjonal sikkerhet

I LQN åpnes det bare for tiltak knyttet til trusler mot den nasjonale sikkerheten. Hva som menes med nasjonal sikkerhet er bredt formulert:[115]

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

Beskrivelsen overlapper i stor utstrekning med formålsbestemmelsen i etterretningstjenesteloven § 1-1 bokstav a. Også opplistingen av etterretningsformål i § 3-1 synes å være innenfor denne rammen. I tillegg angir EU-domstolen at straff («punishment») for aktiviteter som nevnt er en del av statens eneansvar for den nasjonale sikkerheten. På dette punktet er formålet med etterretningstjenesteloven mer avgrenset enn det EU-retten tillater, ettersom loven er avgrenset til innhenting og analyse for å avdekke og motvirke at utenlandske trusler mot Norge og norske interesser aktualiseres.

Tilrettelagt innhenting kan bare brukes for etterretningsformål etter lovens kapittel 3. Dette kapitlet omfatter utenlandske trusler (§ 3-1) og forhold (§ 3-2), okkupasjonsberedskap (§ 3-3), internasjonalt etterretningssamarbeid (§ 3-4) og evneinformasjon (§ 3-5). Adgangen til å innhente informasjon med hjemmel i en av bestemmelsene i kapittel 3 beror ikke på en tolkning av bestemmelsen alene, men må leses i sammenheng med vilkår i loven for øvrig, herunder kravet til forholdsmessighet etter § 5-4. Formålet med innhentingen er et sentralt moment i denne vurderingen. Dette har igjen betydning for hvilke metoder som E-tjenesten kan benytte seg av, herunder om søk i metadata fra tilrettelagt innhenting er forholdsmessig. Jo viktigere formålet er, jo mer inngripende metodebruk kan aksepteres.

LQN åpner som nevnt kun for tiltak knyttet til trusler mot den nasjonale sikkerheten. Det kan dermed argumenteres for at bruk av tilrettelagt innhenting bør avgrenses mot §§ 3-2 til 3-5, som ikke direkte gjelder trusler mot Norge og norske interesser. På den andre siden er disse

[114] Prop. 80 L (2019-2020) pkt. 11.8.2.3
[115] LQN avsnitt 135.

etterretningsformålene i praksis så nært knyttet til formålet om å avdekke og motvirke utenlandske trusler i § 3-1, at de i EØS-rettslig sammenheng må anses som en del av det overordnede formålet om å motvirke utenlandske trusler. I forarbeidene ble særlig forholdet mellom §§ 3-1 og 3-2 belyst, og således tatt stilling til ved stortingsbehandlingen:[116]

> «Paragraf 3-1 kommer først til anvendelse dersom man står overfor en *trussel*. Lovforslaget gir ingen nærmere beskrivelse av *når* noe regnes som en trussel. Det må avgjøres konkret i den enkelte situasjon. Likevel er det klart at forholdet må være av en viss alvorlighetsgrad for å kunne utgjøre en trussel. Dersom Etterretningstjenesten utelukkende skal innhente informasjon om etablerte trusler og kjent truende aktivitet, vil den ikke evne å avdekke fremtidens trusselbilde. Etterretningsvirksomhet er predikativ i sin natur, og det å detektere avvik fra normalen er en viktig oppgave. For å kunne varsle om avvik fra det normale, må normaltilstanden være kjent. Forholdet mellom §§ 3-1 og 3-2 kan illustreres med et eksempel fra våre nærområder. Norges forhold til Russland er i stor grad preget av forutsigbarhet. Russland utgjør ingen militær trussel mot Norge i dag. Vår geografiske plassering i forhold til russiske strategiske kapasiteter betyr likevel at utviklingen i Russland og nordområdene har vedvarende stor betydning for norsk og alliert sikkerhet. God og tidsriktig situasjonsforståelse, herunder inngående kunnskap om utviklingen i russisk utenriks- og sikkerhetspolitikk og om moderniseringen av den russiske militærmakten i våre nærområder, er dermed avgjørende forutsetninger for å kunne utforme norsk utenriks-, forsvars- og sikkerhetspolitikk. Uten hjemmel til å innhente informasjon om disse forholdene, som ikke kan karakteriseres som en trussel, men som et prioritert område, vil man ikke besitte den dybdekunnskapen som kreves for å evne å varsle om endringer av betydning. Litt forenklet sagt vil derfor informasjonsinnhenting etter § 3-2 ofte være en avgjørende forutsetning for å kunne innhente informasjon om trusler etter § 3-1.»

Tilsvarende argumentasjon er relevant i forholdet mellom § 3-1 og E-tjenestens øvrige oppgaver (§§ 3-3 til 3-5).

Tilrettelagt innhenting vil inkludere en evne til å gjøre retrospektive søk i datagrunnlaget der Oslo tingrett har tillatt dette. Tatt i betraktning mengden informasjon som går via tjenestetilbyderne, vil tilrettelagt innhenting først og fremst utgjøre en viktig kapasitet for å avdekke trusler etter § 3-1. Det kan samtidig tenkes tilfeller hvor sentral informasjon om forhold som ikke enda utgjør en trussel, men hvor en slik utvikling er påregnelig, også vil kunne detekteres gjennom søk i data fra tilrettelagt innhenting. I alle tilfeller vil det være opp til Oslo tingrett å avgjøre om den faktiske og rettslige begrunnelsen, herunder E-tjenestens forholdsmessighetsvurdering, er tilstrekkelig konkret til at søk kan tillates. Domstolskontrollen vil dermed ytterligere sikre at tilrettelagt innhenting ikke benyttes for formål som ikke møter terskelen.

På denne bakgrunn anføres at tilrettelagt innhenting oppfyller kravet om å være avgrenset til trusler mot nasjonal sikkerhet.

3.4.4. Kontrollmekanismer

Beslutningen om å pålegge tjenestetilbyderne tilretteleggingsplikt av hensyn til nasjonal sikkerhet må være gjenstand for effektivt tilsyn enten av en domstol eller en tilsvarende uavhengig instans med beslutningsmyndighet. Formålet med tilsynet må være å verifisere at det er tilstrekkelig konkrete grunner til å anta at en trussel eksisterer, og at vilkårene og sikkerhetsmekanismene respekteres.

[116] Prop. 80 L (2019-2020) pkt. 7.3.4.3

EOS-utvalget oppfyller kravene til uavhengighet fra den utøvende myndigheten, og er tillagt oppgaven å kontrollere E-tjenestens bruk av tilrettelagt innhenting både i sanntid (§ 7-11) og gjennom ordinær etterfølgende kontroll etter EOS-kontrolloven. EOS-utvalget har ikke beslutningsmyndighet, men særordningen etter etterretningstjenesteloven § 7-12 gir utvalget anledning til å begjære stans i pågående innhenting og sletting av innhentede data overfor Oslo tingrett. Det kan argumenteres for at kravet om et en uavhengig instans med beslutningsmyndighet er oppfylt som følge av samspillet mellom EOS-utvalget og tingretten i slike saker. EOS-utvalget skal meddeles beslutninger om tilrettelegging, og vil dermed være orientert i sanntid om E-tjenestens pålegg overfor ekomtilbyderne og være i stand til å gjennomgå og vurdere begrunnelsen, herunder om pålegget er nødvendig og forholdsmessig og for øvrig i tråd med lovens vilkår. Tilsvarende vil EOS-utvalget bli meddelt hvilke begjæringer E-tjenesten fremmer for tingretten om å utføre søk i lagrede metadata. Utvalget vil således være i stand til å ettergå hvordan tjenesten blant annet tilnærmer seg det ovenfor nevnte forholdet mellom § 3-1 og §§ 3-2 til 3-5. Videre vil Nasjonal kommunikasjonsmyndighet (Nkom) meddeles beslutninger om tilrettelegging jf. § 7-3 tredje ledd, og vil ha en særlig anledning til å gjennomføre uavhengig tilsyn på tilbydersiden. Nkom kan som ledd i dette ta opp saker hvor man mener at tilrettelegging pålegges i større utstrekning enn loven og våre folkerettslige forpliktelser tillater.

Det vises til drøftelsen om autorisasjon i pkt. 2.3.3 ovenfor. Her vurderes det at ettersom E-tjenesten ikke har direkte *tilgang* til de innhentede data før domstolen har tatt stilling til om vilkårene for å gjøre søk er oppfylt, kan det anføres at beslutningsprosedyren i § 7-3, sett i lys av EOS-utvalgets løpende kontroll og anledning til å fremme begjæring om stans til Oslo tingrett, er forholdsmessig og tilfredsstiller EMKs krav. Det samme kan anføres her. Dette bør likevel etter arbeidsgruppens syn utredes nærmere, før endelig konklusjon trekkes. Ikrafttredelse av § 7-3 bør avvente en slik ytterligere utredning, som muligens kan resultere i forslag til lovendringer, se også pkt. 3.5.4 nedenfor.

3.4.5. Tidsavgrensning

Tjenestetilbyderne kan ikke pålegges å iverksette tiltak av hensyn til nasjonal sikkerhet for lenger tid enn det som er strengt nødvendig, med mulighet for en tidsbegrenset forlengelse dersom trusselen vedvarer. Etterretningstjenesteloven § 7-3 legger opp til at beslutninger om tilrettelegging kan gjelde for inntil tre år av gangen. Det kan hevdes at en maksimal frist på tre år i alle tilfeller vil overstige det som er strengt nødvendig, og at det vil stå i et spenningsforhold til EU-domstolens uttalelse om at tiltaket ikke må være systematisk. Det bør følgelig vurderes om fristen kan nedjusteres til for eksempel ett år. Som nevnt i punkt 2.3.3 og 3.5.4 er det grunn til å se nærmere på utformingen av § 7-3 i en separat utredning. Det er derfor tilrådelig å utsette ikraftsettelse av denne bestemmelsen til resultatet av en slik utredning foreligger og en eventuell revisjon av bestemmelsen er gjennomført. En nærmere vurdering av tidsavgrensningen vil i så fall inngå i dette arbeidet.

Etterretningstjenesteloven § 7-2 fastlegger hva som nærmere ligger i tilretteleggingsplikten. Arbeidsgruppen noterer seg at det i bestemmelsen første ledd bokstav b heter at tilbyderne skal tillate at E-tjenesten installerer utstyr og etablerer «midlertidig eller permanent» tilstedeværelse for å drifte utstyr på steder som kontrolleres av tilbyder. Arbeidsgruppen bemerker at begrepet «permanent» kan stå i et spenningsforhold til den tidsbegrensing av tiltaket som EU-domstolen legger til grunn. Samtidig er det lagringen/overføringen av datastrømmer som behandles i EU-domstolens avgjørelser, og ikke etterretnings- og sikkerhetstjenestenes eventuelle tilstedeværelse hos tilbyder. Arbeidsgruppen mener likevel at det bør tas stilling til om ordet «permanent» bør fjernes fra bestemmelsen i forbindelse med

den nærmere utredningen av § 7-3. Spørsmålet er imidlertid ikke av en slik karakter at det tilsier fortsatt utsatt ikrafttredelse av § 7-2. Inntil videre legger arbeidsgruppen til grunn at begrepet tolkes innskrenkende.

3.5. Helhetsvurdering

Det er rettslig usikkerhet knyttet til hvilken anvendelse og betydning EU-domstolens avgjørelser har for norsk lovgivning. Oppsummert er usikkerheten særlig forbundet med hvilken relevans dommene har for systemet for tilrettelagt innhenting, samt med tilpasningsteksten i direktivets artikkel 15 («de allmenne prinsippene i EØS-retten»).

Europakommisjonen har til nå ikke truffet tiltak i noe EU-land som arbeidsgruppen kjenner til for å forfølge/ettergå regelverk som anføres å ikke være i tråd med tolkingsuttalelsene i PI og LQN. Det samme gjelder ESA, for så vidt gjelder EØS/EFTA-statene.

Det tilføyes at EUs Råd i forslaget til ny kommunikasjonsvernforordning, som skal erstatte direktivet, ønsker å tydeliggjøre at forordningen ikke skal regulere tjenestetilbydernes behandling av data som ledd i utlevering for nasjonale sikkerhetsformål. Samtidig er forhandlingene med Europakommisjonen og Parlamentet om ny forordning ikke sluttført, og det kan ta lang tid før forordningen er vedtatt og trådt i kraft. En avgjørelse om hvorvidt etterretningstjenesteloven kapittel 7 og 8 skal tre i kraft bør derfor ikke avvente dette.

I LQN tillates bulkinnhenting/-lagring når det foreligger en alvorlig trussel mot nasjonal sikkerhet som er reell og aktuell eller kan forutses. Cybertruslene mot Norge, som illustrert ved ulike operasjoner den siste tiden mot en rekke mål i Norge – herunder Stortinget – og som er attribuert til ulike utenlandske trusselaktører, underbygger dette alene. Truslene mot nasjonal sikkerhet er i dag høy og vedvarende, og beskrives tydelig av samtlige vestlige etterretnings- og sikkerhetstjenester.

Arbeidsgruppen har etter en vurdering kommet til at LQN-kriteriene trolig bør komme klarere til uttrykk i etterretningstjenesteloven § 7-3. Det er behov for å utrede problemstillingen ytterligere, noe som taler for at denne paragrafen ikke settes i kraft nå. Dette er ikke til hinder for at de øvrige bestemmelsene i kapittel 7 og 8 trer i kraft nå, inntil en slik utredning er gjennomført. Det fremgår klart av etterretningstjenesteloven § 12-1 at bestemmelsene i loven kan tre i kraft til ulik tid.

4. Konklusjoner og tilrådninger

Tilrettelagt innhenting vurderes å være i overenstemmelse med de menneskerettslige kravene som følger av EMDs storkammeravgjørelser 25. mai 2021, med de presiseringer om ytterligere utredninger som er omtalt i denne analysen. Behovet for utredning knytter seg i hovedsak til spørsmålet om forhåndsautorisasjon og dermed beslutningsprosedyren i § 7-3.

Loven anses også forenlig med avgjørelsene fra EU-domstolen, med forbehold for at LQN-kriteriene trolig bør komme klarere til uttrykk i § 7-3.

Etter en samlet vurdering legges det til grunn at det er rettslig forsvarlig å treffe en beslutning om å sette i kraft kapittel 7 og 8 i etterretningstjenesteloven nå, med følgende presiseringer:

- Ettersom E-tjenesten ikke har tilgang til de innhentede data før domstolen har tatt stilling til om vilkårene er oppfylt, herunder om tilgangen er nødvendig og forholdsmessig, kan det anføres at beslutningsprosedyren i § 7-3 sett i lys av EOS-

utvalgets løpende kontroll og anledning til å fremme begjæring om stans til Oslo tingrett, er forholdsmessig og tilfredsstiller både EMKs og EØS-rettens krav. Det er imidlertid knyttet rettslig usikkerhet til et slikt standpunkt og spørsmålet bør utredes nærmere. Ikrafttredelse av § 7-3 bør avvente en slik ytterligere utredning, som kan resultere i forslag om lovendringer. Utredningen bør sendes på offentlig høring. Det følger av lovens § 12-1 at bestemmelsene kan settes i kraft til ulik tid.

- Det bør utredes om uavhengig forhåndsautorisasjon av målrettet innhenting overfor journalister eller målrettet innhenting som vil medføre tilgang til kildeidentifiserende materiale i etterretningstjenesteloven kapittel 5 er i overensstemmelse med EMK. Det bør også utredes om bestemmelsen i kapittel 9 om beslutningsmyndigheten for unntaksvis bruk av kildeidentifiserende materiale er i overensstemmelse med EMK. Utredningen bør sendes på offentlig høring. Begrunnelsen for eventuelle lovendringsforslag er ikke primært av hensyn til tilrettelagt innhenting, men av hensyn til at de deler av etterretningstjenesteloven som allerede er ikraftsatt, skal være fullt ut i samsvar med Norges menneskerettslige forpliktelser. Eventuelle lovendringer bør likevel tre i kraft før tilrettelagt innhenting settes i operativ drift.

Arbeidsgruppen vil tilføye at konsekvensen av at § 7-3 ikke settes i kraft er at det ikke kan finne sted noen etterretningsproduksjon med hjemmel i kapittel 7 og 8. Når det ikke kan fattes beslutning om tilrettelegging etter § 7-3, kan det heller ikke finne sted noen speiling av data for etterretningsformål. Ikrafttredelse av de øvrige bestemmelsene i kapittel 7 og 8 innebærer imidlertid at utviklingen av systemet for tilrettelagt innhenting kan fortsette. Tilrettelagt innhenting er et system det tar tid å få på plass – både utviklingen av de tekniske løsningene og kontrollmekanismene. Ikrafttredelse av bestemmelsene skaper nødvendig forutsigbarhet i denne utviklingsfasen.