UiT Norges arktiske universitet

Det juridiske fakultet

Tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon og forholdet til utvalgte overordnede rettighetsnormer

Bjørn Aslak Juliussen

Stor masteroppgave i rettsvitenskap våren 2021

Innholdsfortegnelse

1 Innledning 1

1.1 Tema og problemstilling 1

1.2 Aktualitet 2

1.3 Historikken bak den nye etterretningstjenesteloven 5

1.4 Kort om Etterretningstjenesten 6

1.4.1 Etterretningstjenestens formål og organisering 6

1.4.2 Forholdet mellom e-tjenesten og de andre hemmelige tjenestene 7

1.4.3 Kort om etterretningstjenestens historie 8

1.5 Avgrensninger 9

1.6 Den videre fremstillingen 10

2 Metode 11

2.1 Utgangspunkter 11

2.2 EMK-rettslig metode 11

2.3 EU-rettslig metode 13

2.3.1 Utgangspunkter 13

2.3.2 EU-domstolens metode 14

2.3.3 EU-domstolens prøving av forelagte spørsmål i prejudisielle avgjørelser 15

2.3.4 Uttalelser fra EUs generaladvokater- en rettskilde ved tolkningen av dommer fra EU-domstolen 16

2.3.5 EØS-avtalen 17

3 Tilrettelagt innhenting: teknologisk rammeverk 19

3.1 Innledning 19

3.2 Det norske ekomnettet 19

3.3 Hvilken datatrafikk passerer landegrensen? 20

3.4 Hvorfor har lovgiver vurdert at det er behov for tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon? 22

3.5 Metadata og innholdsdata 23
3.5.1 Skillet mellom metadata og innholdsdata i etterretningstjenesteloven 23
3.5.2 Hvorfor har metadata etterretningsverdi? 24
3.6 Kryptering 25
4 Materielle vilkår for tilrettelagt innhenting 26
4.1 Introduksjon 26
4.2 Innhentingen må begrunnes i etterretningsformål 26
4.3 Kommunikasjonen må krysse den norske landegrensen 27
4.4 Kommunikasjonsbegrepet 28
4.5 Grunnvilkår for metodebruk i etterretningstjenesteloven kapittel 5 28
4.6 Innhentingen skjer i form av en tilretteleggingsplikt 28
4.6.1 Hvem gjelder tilretteleggingsplikten for? 28
4.6.2 Hva omfatter tilretteleggingsplikten for ekomtilbyderne? 30
4.6.3 Tilretteleggingsplikt trer i kraft etter pålegg fra E-tjenesten 31
4.7 Testinnhenting og testanalyser 32
4.8 Utvalg og filtrering 34
4.9 Innhenting og lagring i bulk 36
4.10 Søk i lagrede metadata 37
4.11 Målrettet innhenting og lagring av innholdsdata 38
4.12 Forutgående domstolskontroll 39
4.12.1 Innledning 39
4.12.2 Etterretningstjenestens begjæring 39
4.12.3 Rettens forhåndskontroll 40
4.12.4 Anke 42
4.12.5 Hastekompetanse 42
4.12.6 Ordningen med særskilt advokat 43
4.13 Kontroll 44

4.14 Overvåkningssamarbeid med andre hemmelige tjenester 45
4.15 Overskuddsinformasjon 46
5 Skranker for tilrettelagt innhenting etter EMK 47
5.1 Innledning 47
5.2 I hvilken grad utgjør bulklagring et inngrep i EMK art. 8? 47
5.3 Kravet til klart rettsgrunnlag 49
5.3.1 Utgangspunkter 49
5.3.2 Rettsgrunnlagets tilgjengelighet 51
5.3.3 Virkeområdet til den nasjonale overvåkningsloven 52
5.3.4 Overvåkningens varighet 54
5.3.5 Prosedyrer for forhåndsgodkjennelse 55
5.3.6 Prosedyrer for lagring, tilgang, analyse og sletting av data 57
5.3.7 Delingsadgang 58
5.3.8 Regler for etterfølgende kontroll 59
5.3.9 Underretning til berørte personer 60
5.3.10 Rettsmidler 61
5.4 Legitimt formål 62
5.4.1 Generelle utgangspunkter 62
5.4.2 EMDs vurderinger av legitimt i Centrum för rättvisa mot Sverige og Big Brothers Watch mot Storbritannia 62
5.5 Nødvendighet 62
5.6 Proporsjonalitet 63
5.6.1 Utgangspunkter 63
5.6.2 EMDs vurderinger av nødvendighet i *Centrum för rättvisa mot Sverige* og *Big Brothers Watch mot Storbritannia* 64
5.7 Hvorfor ble resultatet krenkelse av EMK art. 8 i *Big Brothers Watch mot Storbritannia*, men ikke i *Centrum för rättvisa mot Sverige*? 65
5.8 Er tilrettelagt innhenting utformet i tråd med EMK art. 8? 66

5.8.1 Utgangspunkter for analysen 66
5.8.2 Følger tilrettelagt innhenting av et tilstrekkelig klart rettsgrunnlag? 66
5.8.3 Legitimt formål 72
5.8.4 Nødvendighet 74
5.8.5 Proporsjonalitet 75
5.9 Avsluttende bemerkninger 75
6 EU-rettslige skranker for tilrettelagt innhenting 75
6.1 De rettslige grunnlagene og forholdet mellom dem 75
6.1.1 Innledning 75
6.1.2 EUs Charter om grunnleggende rettigheter 76
6.1.3 GDPR 78
6.1.4 Kommunikasjonsvernsdirektivet 79
6.1.5 Forholdet mellom GDPR og kommunikasjonsvernsdirektivet 80
6.1.6 Datalagringsdirektivet 81
6.2 EU-rettens virkeområde for nasjonale regler om etterretning 82
6.3 Den videre analysen 85
6.4 Inngrep i privatlivets fred og personopplysningsvernet 86
6.5 Legitimt formål 89
6.6 Forholdsmessighetsvurderingen etter Charteret art. 52 91
6.6.1 Utgangspunkter for EU-domstolens forholdsmessighetsvurdering 91
6.6.2 Nødvendighet 92
6.6.3 Proporsjonalitet 94
7 Er etterretningstjenesteloven kapittel 7 utformet i samsvar med EØS-retten? 97
7.1 Er de analyserte dommene fra EU-domstolen EØS-relevante? 97
7.2 Konfrontasjon mellom norsk rett og EØS-retten 100
7.2.1 Utgangspunkt: Det gjelder forskjellige regler avhengig av om bulklagringen skjer hos myndighetene eller hos ekomtilbyderne 100

7.2.2 Innebærer tilrettelagt innhenting en generell og udifferensiert innhenting av metadata? ... 101
8 Forslag til regulering av bulklagring i tråd med EØS-retten ... 103
8.1 Innledning ... 103
8.2 Er det mulig å oppnå lagring av metadata uten å implementere EØS-rettens minstekrav? ... 103
8.3 Lagringstiden må fastsettes individuelt i hvert tilfelle ... 105
8.4 Bulklagring av ulike metadatakategorier ... 106
8.5 Bulklagring ved ekstraordinære trusler mot riket ... 108
8.5.1 Generell og udifferensiert bulklagring ... 108
8.5.2 Målrettet bulklagring ... 109
9 Avsluttende refleksjoner ... 113
Referanseliste ... 114

1 Innledning

1.1 Tema og problemstilling

I et av etterkrigstidens mest kjente litterære verk om overvåkning, George Orwells "1984"[1], presenterer forfatteren et samfunn der staten bruker teknologiske overvåkningsmetoder for å kontrollere befolkningen. I romanen blir også semantikk og språket brukt som en kontrollmetode. Overvåkningen har ikke nødvendigvis effekt på grunn av teknologien som blir brukt, men fordi staten gjennom lovgivning kontrollerer sannheten.[2] I overvåkningssammenheng brukes ofte eufemismer og omskrivninger i lovteksten, for eksempel bruken av betegnelsen kommunikasjonskontroll i stedet for telefonavlytting.[3] I etterretningstjenesteloven[4] kapittel 7 har Etterretningstjenesten fått hjemmel til tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon. Systemet gikk tidligere under navnet digitalt grenseforsvar og har blitt foreslått kalt digital masseovervåkning av Datatilsynet.[5]

Avhandlingens tema er en rettsdogmatisk undersøkelse av reglene om tilrettelagt innhenting. En slik rettsdogmatisk analyse reiser følgende problemstillinger: Hvilken adgang til tilrettelagt innhenting gir etterretningstjenesteloven? Er de materielle reglene om tilrettelagt innhenting i etterretningstjenesteloven utformet i samsvar med EMK- og EØS-retten? Hvordan kan et system for tilrettelagt innhenting utformes for å tilfredsstille kravene etter EMK og EØS-avtalen?

Tilrettelagt innhenting av grenseoverskridende elektronisk informasjon foregår ved at Etterretningstjenesten lagrer metadata i bulk om elektronisk kommunikasjon i fiberoptiske kabler som krysser den norske grensen.[6] Metadataen vil lagres i Etterretningstjenestens servere i 18 måneder.[7]

Elektronisk kommunikasjon og internett er globalt og grenseoverskridende. På grunn av plasseringen av utenlandske servere og andre forhold,[8] vil også innenlandsk kommunikasjon

---

[1] George Orwell 1984, (Oslo 1991).
[2] https://naob.no/ordbok/newspeak (03.03.2021).
[3] Se Lov 22 mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven) kap 16 a).
[4] Lov 19. juni 2020 nr. 77 om etterretningstjenesten (etterretningstjenesteloven).
[5] Se Prop. 80 L (2019-2020) Lov om etterretningstjenesten pkt. 11.2.3.
[6] Se etterretningstjenesteloven § 7-7.
[7] Se etterretningstjenesteloven § 7-7 tredje ledd
[8] Se pkt. 2.3

krysse grensen. Etterretningstjenestens lagring av metadata om grenseoverskridende elektronisk kommunikasjon i bulk i 18 måneder vil derfor i stor grad føre til at metadata om innenlandsk kommunikasjon blir gjenstand for lagring på Etterretningstjenestens servere. Alle internettbrukere i Norge vil derfor bli berørt av den nye etterretningstjenesteloven uavhengig av om de har noen tilknytning til etterretningsmessig interessant informasjon.[9]

1.2 Aktualitet

Etterretningstjenesteloven ble vedtatt av Stortinget sommeren 2020. Ved innføringen av tilrettelagt innhenting er en lagring av personopplysninger uten sidestykke i norsk historie vedtatt ved lov. I forbindelse med høringen av en rapport om Digitalt grenseforsvar, som var termen tilrettelagt innhenting tidligere gikk under, uttalte Datatilsynet at forslaget, som nå er vedtatt, innebærer at Etterretningstjenesten masseinnsamler "data om borgernes kommunikasjon- fullstendig løsrevet fra mistanke og individuelle sikkerhetsbekymringer-for å skaffe en database å søke på i jakt etter trusler (...)". Tilsynet uttalte videre at en slik datalagringen innebærer at vi alle havner under lupen og at det er en krenkelse av EMK art. 8 og Grunnloven § 102.[10]

Tilrettelagt innhenting innebærer lagring av metadata fra store mengder kommunikasjon som ikke er relevant for formålet, etterretning og nasjonal sikkerhet. I etterkant av internasjonale avsløringer om masseovervåkning i USA og i europeiske land på midten av 2010-tallet utarbeidet EUs byrå for grunnleggende rettigheter en kartleggingsrapport for å undersøke hvorvidt nasjonale sikkerhetstjenester i EUs medlemsland hadde masseovervåkningssystemer.[11] Karleggingen slo fast at Storbritannia og Sverige hadde hjemmel for masseinnhenting av teledata i nasjonale lover og gjennomførte slik innhenting. Rapporten konkluderte videre med at andre EU-land som Frankrike og Danmark hadde nasjonale lover som åpnet for slik masseovervåkning, men at det var uklart i hvilken grad disse landene gjennomførte slik innhenting.[12] Kartleggingsrapporten avsluttet med at beskyttelse av utenlandske trusler mot rikets sikkerhet involverer en vanskelig balanse mot

[9] Se lovens forarbeider Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 10.
[10] Se Datatilsynets høringsuttalelse 18.01.2017 til Forsvarsdepartementet.
[11] Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume I: Members States´legal framework.
[12] Kartleggingsrapporten side 77.

beskyttelse av grunnleggende menneskerettigheter og at slik lovgivning fordrer "thorough and candid discussion".[13]

I en liberal rettsstat må inngrep i grunnleggende menneskerettigheter knyttet til privatlivet til alle som benytter elektronisk kommunikasjon begrunnes. Begrunnelsen for tilrettelagt innhenting er å beskytte den liberale rettsstaten og vårt demokrati fra utenlandsk påvirkning og utenlandske trusler slik som terror, spionasje, påvirkningsoperasjoner og digitale angrep mot digital infrastruktur.[14] Den europeiske menneskerettighetsdomstolen har i flere avgjørelser om hemmelig overvåkning fremhevet risikoen for at "(...) a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it."[15]

Vedtakelsen av tilrettelagt innhenting i etterretningstjenesteloven har ført til flere rettslige kontroverser i Norge. Hele den nye etterretningstjenesteloven var planlagt å tre i kraft 1. januar 2021.[16] Den 10. november 2020 varslet Regjeringen Stortinget[17] om at ikrafttredelsen av lovens kapittel 7 og 8 om tilrettelagt innhenting utsettes på ubestemt tid på grunn av EU-domstolens dommer av 6. oktober 2020 i sakene Privacy International[18] og La Quadrature du Net[19].[20]

Stortingets vedtakelse av ny etterretningstjenestelov i juni 2020 skjedde før EMDs storkammerdommer i sakene *Big Brothers Watch mot Storbritannia*[21] og *Centrum för rättvisa mot Sverige*[22] om lignede systemer i Sverige og Storbritannia er avsagt.[23] Videre ble også loven vedtatt før EU-domstolens dom i saken Privacy International konkluderte med at kommunikasjonsverndirektivet og EUs charter er til hinder for generell og vilkårlig bulklagring for å beskytte nasjonal sikkerhet. Etterretningstjenesteloven og tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon ble altså vedtatt i Norge i en

---

[13] Karleggingsrapporten side 3.
[14] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 92-93.
[15] Se *Big Brothers Watch mot Storbritannia* [J], ECHR:2018:0913JUD005817013 avsnitt 308).
[16] FOR-2020-06-19 1231 Ikrafts. av lov 2020:77 etterretningstjenesteloven.
[17] Prop. 1 S Tillegg 1 (2020–2021).
[18] Dom av 6. oktober 2020 [GC], *Privacy International, C-623/17,* EU:C:2020:790.
[19] Dom av 6. oktober 2020, La Quadrature du Net,French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, C-511/18, C-512/18 og C-520/18, EU:C:2020:791.
[20] Prop. 1 S Tillegg 1 (2020–2021) side 103 og 104.
[21] *Big Brothers Watch mot Storbritannia* [J], ECHR:2018:0913JUD005817013.
[22] *Centrum för rättvisa mot Sverige* [J], ECHR:2018:0619JUD003525208.
[23] Storkammerdommene er ikke avsagt per 3. mai 2021.

tid der det er stor usikkerhet om et system med bulklagring av metadata er i tråd med EMK og EU-retten.

I etterkant av terrorangrepene i London i 2005 ble datalagringsdirektivet[24] vedtatt av EU-lovgiver. Gjennomføringen av datalagringsdirektivet i norsk rett, skjedde ved lov 15. april 2011 nr. 11 (lagringsloven). I lagringsloven ble ekomtilbydere pålagt å lagre data fra telefoni, internettaksess og e-post i seks måneder for at politi og påtalemyndighet skulle ha tilgang til dataen for etterforskning av kriminalitet. EU-domstolen kom 8. april 2014 til at direktivet var i strid med EUs charter artikkel 7 og 8 om retten til privatliv og personopplysningsvern. Lagringsloven trådte derfor aldri i kraft i Norge.

I motsetning til den nye etterretningstjenesteloven, brakte lagringsloven med seg stor offentlig omtale og debatt. En av grunnene til at jeg har valgt å skrive min masteroppgave om tilrettelagt innhenting, er at etterretningstjenesteloven ble vedtatt sommeren 2020 uten noe særlig offentlig ordskifte sammenlignet med datalagringsdirektivet og lagringsloven. Det har heller ikke blitt skrevet noen omfattende juridiske artikler om tilrettelagt innhenting, selv om etterretningstjenesteloven til tider går lenger enn lagringsloven.

I et av våre nærmeste naboland er en etterretningsskandale under opprulling. Det danske kontrollorganet for etterretningstjenesten, tilsvarende det norske EOS-utvalget, har i en rapport konkludert med at den danske etterretningstjenesten kan ha begått en rekke lovbrudd og tjenesten er blant annet anklaget for å ha overvåket sitt eget kontrollorgan.[25] Selv om eksempelet er fra Danmark og ikke Norge, viser det at de hemmelige tjenestene er sårbare for internt misbruk. Det er derfor viktig at Etterretningstjenesten er underlagt effektivt tilsyn og kontroll og at Etterretningstjenestens metodebruk er beskyttet av tilstrekkelige materielle og prosessuelle rettssikkerhetsgarantier. Denne avhandlingen skal undersøke rettssikkerhetsgarantiene knyttet til tilrettelagt innhenting, herunder om garantiene gir et tilstrekkelig vern mot faren for misbruk.

---

[24] Europaparlaments- og rådsdirektiv 2006/24/EF av 15. mars 2006 om lagring av data som fremkommer ved bruk av offentlig elektronisk kommunikasjon, samt endring i europaparlaments- og rådsdirektiv 2002/58/EF.

[25] https://www.aftenposten.no/verden/i/vAl14j/dansk-etterretning-drev-ulovlig-overvaaking-av-dansker (lastet ned 15.03.2021)

1.3 Historikken bak den nye etterretningstjenesteloven

Den gamle etterretningstjenesteloven er fra 1998.[26] Etterretningstjenestens metodebruk har endret seg stort siden 1998, fordi metoder som tjenesten benytter ikke var mulig på tidspunktet for vedtakelsen av den gamle etterretningstjenesteloven.

Den nye etterretningstjenesteloven ble til blant annet på bakgrunn av et anmodningsvedtak[27] fra Stortinget der Stortinget ba regjeringen om å legge frem et forslag til revidert lov om etterretningstjenesten. Dette anmodningsvedtaket ble vedtatt av Stortinget på grunn av en særskilt melding[28] fra EOS-utvalget[29] til Stortinget. I meldingen stilte EOS-utvalget spørsmål om etterretningstjenestens hjemmelsgrunnlag var i tråd med lovkravet i EMK, blant annet på grunn av utviklingen i e-tjenestens metoder for innhenting av elektronisk kommunikasjon.[30]

En slik særskilt melding er et virkemiddel som EOS-utvalget sjelden bruker.

I meldingen fra EOS-utvalget fremkom det at Etterretningstjenesten foretok selektorsøk (søk etter søkeord og søkebegreper) i lagret og innhentet metadata knyttet til norske rettssubjekter for å finne informasjon om etterretningsmessige interessante objekter i utlandet. EOS-utvalget mente at hjemmelsgrunnlaget for slik innhenting og søk var for svakt, og at Stortinget derfor måtte informeres.[31]

I februar 2016 nedsatte regjeringen et utvalg ledet av professor i informatikk Olav Lysne. Utvalget fikk som mandat å utrede faktiske og rettslige problemstillinger knyttet til Etterretningstjenestens mulige tilgang til elektronisk informasjon som kommuniseres i fiberoptiske kabler inn og ut av Norge (digitalt grenseforsvar).

Utvalget leverte en rapport som gikk inn for å anbefale å etablere et digitalt grenseforsvar som skulle kontrolleres av et eget tilsyn og gis forhåndstillatelser til søk og analyse i innhentet data av en egen særdomstol. Utvalgets rapport ble sendt på høring og møtte kritikk fra et flertall av høringsinstansene, herunder Datatilsynet, Advokatforeningen, Den norske dommerforening,

---

[26] Lov 20.03.1998 nr. 11 om etterretningstjenesten.
[27] Anmodningsvedtak av 21.02.2017 nr. 466 (2016-2017).
[28] DOK 7:2 (2015-2016) Særskilt melding til Stortinget fra Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-utvalget).
[29] EOS-utvalget er Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjenesten og skal føre kontroll over de hemmelige tjenestene for passe på at tjenestene utfører sin virksomhet innen rammen av lov og menneskerettigheter, jf. EOS-loven § 2.
[30] DOK 7:2 (2015-2016) Særskilt melding til Stortinget fra Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-utvalget) side 17.
[31] DOK 7:2 (2015-2016) side 21.

International Commision of Jurists Norge, NRK, Norges Institusjon for menneskerettigheter, Riksadvokaten, Direktoratet for forvaltning og IKT og omtrent 80 privatpersoner.[32]

Rapporten fra Lysne-utvalget ble brukt som mal for forsvarsdepartementets forslag til regulering av bulklagring i norsk rett.[33] I forarbeidene til etterretningstjenesteloven[34] ble betegnelsen digitalt grenseforsvar lagt bort siden termen ble ansett som lite beskrivende. Fordi bulktilgangen til grenseoverskridende fiberoptiske data innebærer en tilretteleggingsplikt for ekomtilbydere, ble navnet tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon valgt.

Etterretningstjenesteloven ble vedtatt av Stortinget i juni 2020. Lovens formål er blant annet å "bidra til å trygge Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser".[35] En av nyvinningene med loven er at etterretningstjenestens metodebruk fremgår mer spesifikt og konkretisert av loven, sammenlignet med etterretningstjenesteloven fra 1998.

1.4 Kort om Etterretningstjenesten

1.4.1 Etterretningstjenestens formål og organisering

Etterretningstjenesten er Norges nasjonale utenlandsetterretningstjeneste. Tjenesten er en del av Forsvaret og underlagt forsvarssjefens kommando, jf. etterretningstjenesteloven § 2-1 første ledd. På sine egne nettsider beskriver Etterretningstjenesten seg selv og sine tre hovedoppgaver slik:

1. Den første er å understøtte norske myndigheter med informasjon og vurderinger om utenriks- sikkerhets- og forsvarspolitiske forhold. (...)
2. Tjenestens andre hovedoppgave er å fremskaffe informasjon og varsle om forhold som kan true Norge og norske interesser. (...) Internasjonal terrorisme og trusler i det digitale rom er grenseoverskridende. Disse truslene endres raskt, kan befinne seg langt borte og samtidig true norske interesser hjemme og ute.

---

[32] Høringssvarene er tilgjengelig her: https://www.regjeringen.no/no/dokumenter/horing-av-rapport-avgitt-av-lysne-ii-utvalget-om-digitalt-grenseforsvar/id2513635/?expand=horingssvar&lastvisited=b6c6e5c6-167a-421f-97d6-6f032afba031
[33] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 85.
[34] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 86.
[35] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 9.

3. Sist, men ikke minst, skal Etterretningstjenesten støtte Forsvarets operasjoner hjemme og ute.[36]

Etterretningstjenesten er en utenlandsetterretningstjeneste og har ikke som oppgave å innhente informasjon om norske borgere i Norge, jf. etterretningstjenesteloven § 4-1 første ledd. Overvåkning og innhenting av informasjon om norske statsborgere i Norge skjer i regi av de andre hemmelige tjenestene, Politiets Sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet.

1.4.2 Forholdet mellom e-tjenesten og de andre hemmelige tjenestene

De hemmelige tjenestene i Norge er Etterretningstjenesten, Politiets sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet.[37] Politiets sikkerhetstjeneste er en avdeling i politiet som har ansvaret for å forebygge, motvirke og etterforske kriminalitet og trusler mot rikets sikkerhet. PSTs oppbygging og oppgaver fremgår av Instruks for politiets sikkerhetstjeneste[38] gitt i medhold av politiloven[39] § 29.

Nasjonal sikkerhetsmyndighet er et direktorat underlagt Justis- og beredskapsdepartementet som også rapporterer til Forsvarsdepartementet. Nasjonal sikkerhetsmyndighet skal forebygge spionasje, sabotasje og terror mot skjermingsverdige objekter og informasjon. NSM er ansvarlig for sikkerhetstilstanden i staten og kommunene og i private selskaper som leverer viktige tjenester til det offentlige, for eksempel IT-systemer.[40]

Samarbeidet mellom Etterretningstjenesten og PST reguleres av instruks[41] om samarbeidet mellom Etterretningstjenesten og PST fastsatt i kongelig resolusjon med hjemmel i Kongens instruksjonsmyndighet. Etter instruksen § 3 skal PST og Etterretningstjenesten særlig samarbeide og utveksle informasjon om terrorisme, kontraproliferasjon[42], fremmed etterretningsvirksomhet og andre prioriterte forhold som berører norske interesser. Samarbeidsinstruksen oppretter også et felles kontraterrorsenter, jf. instruksen § 9.

---

[36] Etterretningstjenestens nettsider: https://forsvaret.no/organisasjon/etterretningstjenesten (besøkt 01.07.2020)
[37] https://snl.no/de_hemmelige_tjenester (22.09.2020).
[38] FOR-2005-08-19-920.
[39] Lov 4. august 1995 nr. 53 om politiet (politiloven).
[40] https://nsm.no/om-oss/dette-er-nsm/ (22.09.2020).
[41] FOR-2006-10-13-1151.
[42] Motarbeiding av spredning av masseødeleggelsesvåpen.

Etterretningstjenestens adgang til å dele etterretningsinformasjon med de andre hemmelige tjenestene fremgår av etterretningstjenesteloven kapittel 10. I etterretningstjenesteloven kapittel 7 er det gitt bestemmelser om hvilke vilkår som må være oppfylt for at Etterretningstjenestens skal kunne dele overskuddsinformasjon fra tilrettelagt innhenting, det vil si informasjon som ikke er relevant for etterretningsformål, med politiet og andre rettshåndhevende myndigheter. Avhandlingen behandler informasjonsdeling mellom Etterretningstjenesten og PST nærmere i kapittel 4.

1.4.3 Kort om etterretningstjenestens historie

Etterretningstjenesteloven fra 1998 ble vedtatt to år etter Stortingets granskingskommisjon leverte sin rapport om de hemmelige tjenestene til Stortinget.[43] Høyesterettsdommer Ketil Lund ledet en parlamentarisk granskingskommisjon oppnevnt av Stortinget[44] som skulle undersøke påstander om at de hemmelige tjenestene hadde drevet ulovlig og irregulær overvåkning av egne borgere i tiden etter 1945. Kommisjonen konkluderte i sin granskningsrapport med at de hemmelige tjenestene hadde utført ulovlig overvåkning av egne borgere i etterkrigstiden, spesielt av politiske partier. Kommisjonen konkluderte også med at forsvarets etterretningstjeneste hadde samlet inn ulovlig informasjon om norske borgere. Forsvaret i Nord-Norge hadde blant annet registrert, samlet og lagret informasjon om hvilke norske borgere som hadde kommunistiske sympatier og var med i partier på ytterste venstrefløy.[45]

Etterretningstjenestens historie og Lund-kommisjonens historiske gjennomgang av de hemmelige tjenestene viser at de hemmelige tjenestene særpreges av én ting, de er hemmelige. I motsetning til andre deler av offentlig forvaltning er de ikke underlagt kontrollen som følger av allmennhetens innsynsrett. Etterretningstjenesten har også tette bånd til den enhver tid sittende regjering. Lund-kommisjonen pekte på at disse forholdene kan føre til at det utvikler seg en kultur der rettslige skranker i lov, forskrift og instruks ikke følges.[46]

I de avsluttende bemerkningene i Lund-kommisjonens rapport har kommisjonen følgende betraktning som er relevant i relasjon til tilrettelagt innhenting:

---

[43] Dokument nr. 15 (1995-1996).
[44] Opprettet i Lov 25. mars 1994 nr. 6.
[45] DOK 15 (1995-1996) side 1127.
[46] DOK 15 (1995-1996) side 1130.

> "Kommisjonen vil avslutningsvis peke på at selv om tjenestene inngjerdes av regler og gjøres til gjenstand for en mer effektiv kontroll, og selv om tjenestenes virksomhet åpnes mer mot omverden i tråd med alminnelige prinsipper i forvaltningen, er det ikke utenkelig at vi står foran en tid der den moderne teknologi vil gi nytt potensiale for rykter og spekulasjoner. Et samfunn der befolkningens gjøren og laden overvåkes i minste detalj er ingen fjern teknologisk mulighet. I en slik tid er det fremfor noe viktig at ansvarlige politikere er villige til å håndtere forholdet mellom tjenestene og offentligheten med oppriktighet, uansett om spørsmålene måtte være ømtålige".[47]

Det er den teknologiske utviklingen som har gjort at lovgiver har sett behovet for en ny etterretningstjenestelov. Selv om tilrettelagt innhenting ikke innebærer at "befolkningens gjøren og laden overvåkes i minste detalj", vil systemet innebære at metadata om store deler av befolkningen i Norge lagres på Etterretningstjenestens servere i 18 måneder.

1.5 Avgrensninger

Avhandlingen avgrenses av plasshensyn mot andre menneskerettslige bestemmelser som verner privatlivets fred og behandling av personopplysninger enn EMK art. 8 og EUs Charter art. 7 og 8. Avhandlingen vil derfor ikke behandle Grunnloven § 102, FNs internasjonale konvensjon om sivile og politiske rettigheter[48] art. 17 eller Verdenserklæringen for menneskerettigheter[49] art. 12.

Tilrettelagt innhenting har problematiske sider opp mot Grunnloven § 100 og EMK art. 10 om ytringsfrihet. Av hensyn til avhandlingens omfang avgrenses det også mot rettighetsbestemmelser om ytringsfrihet.

Avhandlingen avgrenses til å ikke behandle internasjonal soft law som for eksempel internasjonale anbefalinger som Report on the democratic oversight of the Security Services og Report on the democratic oversight of signals Intelligence agencies fra Den europeiske

[47] DOK 15 (1995-1996) side 1130.
[48] De forente nasjoners internasjonale konvensjon 16. desember 1966 om sivile og politiske rettigheter
[49] FNs erklæring om menneskerettigheter av 10. desember 1948.

kommisjonen for demokrati gjennom lovgivning (Veneziakommisjonen)[50]. Det avgrenses også mot Europarådets personvernkonvensjon[51] av hensyn til oppgavens omfang.

EMK art. 1 fastslår at EMK gjelder innenfor konvensjonsstatenes jurisdiksjon. Etterretningstjenesten skal gjennom tilrettelagt innhenting overvåke utenlandske borgere som truer norske sikkerhetsinteresser, det vil si borgere i andre konvensjonsstater og borgere av stater som ikke er en del av EMK. Avhandlingen vil ikke problematisere jurisdiksjonsspørsmålet slik det fremgår av EMK art. 1 særskilt.

Søk i lagret metadata og tilrettelagt innhenting av innholdsdata skal skje etter en forutgående domstolsprøving av Oslo tingrett, jf. etterretningstjenesteloven § 8-1. Denne forutgående domstolsprøvingen har en side til EMK art. 6 og "fair-trial"-standarden slik den er utformet av EMD. Det ville imidlertid sprenge oppgavens rammer dersom EMK art. 6 skulle bli behandlet til det fulle. Avhandlingen avgrenses derfor også opp mot EMK art. 6.

1.6 Den videre fremstillingen

En fullstendig analyse av EMK art. 8 og fundamentale rettigheter i EU og sekunddærrett om kommunikasjonsvern forutsetter en undersøkelse av metodiske særtrekk i EMK- og EU-retten og implementering av disse rettssystemene i norsk rett. Kapittel 2 inneholder en slik analyse av metodiske særtrekk i de to rettssystemene.

Kapittel 3 undersøker tekniske forutsetninger for tilrettelagt innhenting og hvorfor lovgiver har vurdert at det er behov for en slik innhentingsmetode i norsk rett.

Kapittel 4 er en rettsdogmatisk analyse av tilrettelagt innhenting i etterretningstjenesteloven kapittel 7 og 8. Loven blir analysert ut fra tilgjengelige rettskilder i forarbeidene til loven for å få klarlagt hvordan innhentingssystemet skal fungere og hvilke materielle og prosessuelle vilkår innhentingssystemet er underlagt.

I kapittel 5 klarlegges først gjeldende EMK-rett ved en analyse av to kammeravgjørelser om bulkinnhenting som etterretningsmetode, før avhandlingen foretar en analyse av hvorvidt tilrettelagt innhenting er et rettmessig inngrep i EMK art. 8.

---

[50] European Commission for Democracy through law.
[51] Convention for the Protection of Individuals with regard to the Automatic Prosessing for Personal Data av 28. januar 1981 nr. 108.

Deretter foretas det en analyse av hvilke skranker EU-retten har for en nasjonal regulering av generell lagring av metadata som et verktøy for beskyttelse av nasjonal sikkerhet i kapittel 6. Etter denne analysen foretas det en vurdering av hvorvidt disse reglene gjelder for Norge på grunn av EØS-avtalen og om etterretningstjenesteloven ivaretar EØS-rettens krav i kapittel 7.

Kapittel 8 inneholder et forslag til en regulering av generell og målrettet bulklagring som ivaretar EØS-retten overordnede krav. Denne delen av avhandlingen bygger på regelverksutvikling til en arbeidsgruppe i EU og forutsetninger i nylige avsagte dommer fra EU-domstolen.

Etterretningstjenesteloven kapittel 7 er vedtatt, men ikke trådt i kraft. Avhandlingen avsluttes med noen rettspolitiske refleksjoner av hvilke veivalg lovgiver burde foreta videre i kapittel 9.

2 Metode

2.1 Utgangspunkter

Avhandlingen vil for det meste anvende en rettsdogmatisk metode. Hovedformålet til den rettsdogmatiske metoden er å samle, bearbeide og analysere rettskilder for å klargjøre hva som er gjeldende rett.[52] Avhandlingen vil derfor søke å samle, systematisere og analysere rettskilder for å først foreta en rettsdogmatisk analyse av tilrettelagt innhenting i etterretningstjenesteloven. Deretter skal avhandlingen analysere de materielle reglene om tilrettelagt innhenting opp mot EMK art. 8 og EØS-avtalen, for å avgjøre om reguleringen er i overensstemmelse med EMK art. 8 og EØS-avtalen. Avhandlingen avsluttes med refleksjoner i kapittel 9 som inneholder noen rettspolitiske betraktinger om den videre lovgivningsprosessen av tilrettelagt innhenting i norsk rett.

Avhandlingen vil analysere internasjonale rettskilder fra EMK- og EU-retten. Det er derfor nødvendig med to korte redegjørelser av metodiske særpreg ved henholdsvis EMK- og EU-retten, og om norsk retts forhold til disse internasjonale rettssystemene.

2.2 EMK-rettslig metode

Internasjonale menneskerettigheter blir dannet gjennom internasjonale konvensjoner og håndheves av internasjonale overvåkningsordninger eller internasjonale domstoler. Den

[52] Hans Petter Graver, "Vanlig juridisk metode? Om rettsdogmatikken som juridisk sjanger" *Tidsskrift for Rettsvitenskap,* vol. 121, 2/2008, s. 149 –178 på side 154.

europeiske menneskerettighetskonvensjonen ble vedtatt 4. november 1950 og trådte i kraft 3. september 1953. Konvensjonen art. 19 oppretter en egen domstol for å sikre at forpliktelsene de kontraherende stater har påtatt seg blir ivaretatt. Konvensjonen ble ratifisert av Norge i 1952. I perioden fra ikrafttredelsen og fram til 1999 var konvensjonen folkerettslig bindende for Norge. I 1999 ble menneskerettsloven[53] vedtatt, etter § 2 skal EMK gjelde som norsk lov, og etter § 3 skal EMK gis forrang ved direkte motstrid med annen norsk rett. Vernet etter EMK utgjør et mimimumsvern.[54] Det innebærer at EMK ikke kan brukes som argument for å tolke nasjonal rett på en snevrere måte slik at individet får et svakere vern.

EMD bygger sin tolkning av EMK på Wienkonvensjonen om traktattolkning.[55] Etter Wienkonvensjonen art. 31 er utgangspunktet for traktattolkning at traktater skal tolkes i god tro, at det kan tas hensyn til konteksten til ordlyden i traktaten og at traktattolkningen kan ta hensyn til traktens gjenstand og formål.[56] EMD har utviklet sin egen rettsanvendelse der artikkel 31 i Wienkonvensjonen er utgangspunktet for en samlet helhetlig metode der alle rettskildene i Wienkonvensjonen art. 31 er likeverdige.[57]

Verden er en annen i dag enn ved vedtakelsen av konvensjonen av EMK i 1950. I 1950 var ikke forholdsmessigheten ved bulklagring av metadata et menneskerettslig tema fordi teknologien ikke eksisterte. Det tar lang tid å endre en konvensjonstekst fordi alle konvensjonsstatene skal enes om konvensjonens eventuelle nye ordlyd. De til enhver tid gjeldende samfunnsforhold er derfor relevant ved tolkningen av EMK.[58]

I vurderingen av om et inngrep i EMK art. 8 er nødvendig i et demokratisk samfunn, tildeler EMD medlemsstatene en skjønnsmargin der medlemsstatene til en viss grad selv kan vurdere om inngrepet er nødvendig og forholdsmessig uten at disse vurderingene blir overprøvd av EMD. Anvendelsesområde til en slik skjønnsmargin avhenger av hvilket formål inngrepet

---

[53] Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven).
[54] DOK. nr. 16 (2011-2012) Rapport fra Menneskerettighetsutvalget om menneskerettigheter i Grunnloven side 87.
[55] Se *Golder mot Storbritannia* [P], ECHR:1975:0221JUD000445170 avsnitt 29).
[56] Se Wienkonvensjonen om traktattolkning art. 31.
[57] Solheim, Stig Harald "Rettsanvendelsesprosessen på EMK-rettens område" i Alf Petter Høgberg (red.) og Jørn Øyrehagen Sunde (red.), *Juridisk metode og tenkemåte, Universitetsforlaget*, 2019 s. 361, Juridika
[58] *Tyrer mot Storbritannia* [J], ECHR:1978:0425JUD000585672.

skal ivareta og intensiteten av EMDs prøving avhenger av intensiteten av inngrepet i EMK art. 8. I saken M.M. mot Storbritannia uttrykte EMD det slikt:

> "The greater the scope of the recording system, and thus the greater the amount and sensitivity of data held and available for disclosure, the more important the content of the safeguards to be applied at the various crucial stages in the subsequent processing of the data".[59]

Ved anvendelsen av EMK i norske domstoler har Høyesterett uttalt at "(...) norske domstoler skal foreta en selvstendig tolkning av konvensjonen. Herunder skal de benytte samme metode som EMD".[60]

Den nasjonale skjønnsmarginen er begrunnet med at menneskerettighetene primært skal sikres og håndheves av konvensjonstatene selv og at konvensjonsstatene ofte har størst innsikt i lokale forhold i det enkelte land.[61] Etter EMDs storkammerdom av 19. februar 2009 i saken A mot Storbritannia avsnitt 194) gjelder denne skjønnsmarginen kun mellom konvensjonsstatene og EMD og ikke mellom nasjonale myndigheter og nasjonale domstoler. Oppgaven vil legge til grunn at kontrollen utført av EMD er en subsidiær kontroll over om konvensjonsstatene har gitt individene minimumsvernet etter EMK-bestemmelsene. Siden nasjonale domstoler ikke skal tilkjenne nasjonale myndigheter en statlig skjønnsmargin, vil heller ikke avhandlingen vurdere tilrettelagt innhenting i tråd med en slik skjønnsmargin.

2.3 EU-rettslig metode

2.3.1 Utgangspunkter

Den Europeiske Union (EU) er et økonomisk og politisk fellesskap mellom 27 land i Europa.[62] Unionen er opprettet i folkerettslige avtaler mellom medlemslandene hvor Traktat om den Europeiske Union (TEU)[63] og Traktat om den Europeiske Unions Virkemåte (TEUV)[64] er to av de grunnleggende traktatene. EU har et indre marked med fri flyt av varer, tjenester, kapital og arbeidskraft.[65] Medlemslandene i EU har delegert lovgivningskompetanse

---

[59] *M.M. mot Storbritannia* [J], ECHR:2012:1113JUD002402907 avsnitt 200).
[60] Rt. 2005 s. 883 avsnitt 45).
[61] Jens Edvin A. Skoghøy, "Nasjonal skjønnsmargin etter EMK" i *Lov og rett* 2011,4, årgang 4, side 189-190 på side 189.
[62] EUs hjemmesider: https://europa.eu/european-union/about-eu/eu-in-brief_en (25.03.2021).
[63] Traktat om den Europeiske Union av 7. februar 1992.
[64] Traktat om den Europeiske Unions virkemåte av 25. mars 1957.
[65] Se TEU art. 3 nr. 2.

til institusjoner i EU som skal lage rettsakter i form av direktiver og forordninger som skal sørge for fungeringen til det indre markedet. I traktene i EU er EU-domstolen opprettet for å sørge for at EU lovgivningen tolkes og anvendes likt i alle medlemslandene.[66]

2.3.2 EU-domstolens metode

Traktatene i EU er folkerettslige avtaler. Folkeretten inneholder tolkningsregler og tolkningsprinsipper som til sammen utgjør folkerettslig metode. Disse tolkingsreglene er traktatfestet i enkelte tilfeller i for eksempel Wien-konvensjonen om traktattolkning.[67] EU-domstolen har gjennom egen praksis lagt grunnlaget for en egen EU-rettslig metode.[68]

I EU skilles det mellom primærrett og sekunddærrett. Primærretten er den grunnleggende EU-retten, og her inngår traktaten om Den europeiske union (TEU), traktaten om Den europeiske Unions Virkemåte (TEUV), EUs Charter om grunnleggende rettigheter (Charteret) og grunnleggende prinsipper om EU-retten utviklet av EU-domstolen.[69]

Direktiver og forordninger vedtatt av institusjonene i EU i tråd med kompetansen tildelt institusjonene i traktatene, er sekunddærrett. EUs kommunikasjonsvernsdirektiv vedtatt av Europaparlamentet og Rådet i medhold av TEU art. 95, er et eksempel på sekunddærrett. Primærretten er lex superior over sekunddærretten. Sekunddærretten må derfor tolkes i samsvar med primærretten. Hvis slik tolkning ikke er mulig, må primærretten gis forrang.[70]

Det fremgår av TEU art. 1 nr. 2 at TEU utgjør "a new stage in the process of creating an even closer union among the peoples of Europe (…)." Etter denne bestemmelsen er et av de grunnleggende formålene med EU og EU-retten europeisk integrasjon. I 2014 uttalte EU-domstolen følgende om dette overordnede formålet:

> "(…) —the implementation of the process of integration (…) is the raison d'être of the EU itself."[71]

---

[66] Publication office of the European Union, "How the European Union Works", DOI:10.2775/11255
[67] Vienna Convention on the Law of Treaties, Wien, 23 mai 1969.
[68] Haukeland Fredriksen og Mathisen, *EU-rett som norsk rettskilde*, side 390.
[69] Haukeland Fredriksen og Mathisen, *EU-rett som norsk rettskilde* side 396.
[70] Haukeland Fredriksen og Mathisen, *EU-rett som norsk rettskilde* side 396.
[71] Dom av 18. desember 2014 [GC*], Adhésion de l'Union à la CEDH*, C-2/13, EU:C:2014:2454 avsnitt 172)

EU-domstolen uttalte at europeisk integrasjon er *raison d'être* (hovedformålet) med EU. Integrasjon og harmoniserte regler på tvers av EUs medlemssland er derfor en svært viktig tolkningsfaktor for EU-domstolen ved tolkning av primær- og sekunddærrett.

Det finnes 24 offisielle EU-språk. Traktatene og rettsaktene skal tolkes likt uavhengig hvilken språkversjon som legges til grunn. Tolkningen av primær- og sekunddærrett skal ta utgangspunkt i en alminnelig språkbruk.[72] Videre skal EU-retten tolkes i lys av konteksten og formålet til bestemmelsen som tolkes.[73] Dette er relevante tolkningsfaktorer særlig fordi traktatene og rettsaktene finnes i 24 ulike språkversjonene som alle har lik gyldighet.

Direktiver og forordninger skal som beskrevet ovenfor tolkes i samsvar med primærretten, herunder Charteret. Dersom en rettighetsbestemmelse i Charteret har en tilsvarende bestemmelse i EMK, følger det av Charterets art. 52 nr. 3 at bestemmelsen skal tolkes i samsvar med EMK. Praksis fra EMD blir derfor en relevant rettskilde ved tolkning og anvendelse av bestemmelser i Charteret som har en tilsvarende EMK bestemmelse, for eksempel Charterets art. 7 som tilsvarer EMK art. 8.

2.3.3 EU-domstolens prøving av forelagte spørsmål i prejudisielle avgjørelser

De ulike former for saker som EU-domstolen kan ha til behandling fremgår av TEUV art. 258 flg. Dommene som er gjenstand for analyse i avhandlingens kapittel 6 er prejudisielle avgjørelser, jf. TEUV art. 267. Prejudisielle avgjørelser er EU-domstolens besvarelse av EU-rettslige spørsmål forelagt av nasjonale domstoler i EUs medlemsland. Dersom det oppstår tvil om et EU-rettslig tolkningsspørsmål i en sak for nasjonale domstoler, kan enhver nasjonal domstol i et av EUs medlemsland forelegge spørsmålet for EU-domstolen, jf. TEUV art. 267 andre ledd. Etter TEUV art. 267 tredje ledd har en nasjonal domstol i siste instans en plikt til å forelegge uavklarte EU-rettslig spørsmål for EU-domstolen. Ordningen med prejudisielle avgjørelser er EU-rettens forsøk på å tilrettelegge for en desentralisert håndhevelse av EU-retten gjennom nasjonale domstoler uten at målsetningen om europeisk integrasjon blir skadelidende.[74]

---

[72] Dom av 3. september 2014 [GC], *Johan Deckmyn and Vrijheidsfonds VZW*, C-201/13, EU:C:2014:2132 avsnitt 19).
[73] For eksempel Dom av 22. oktober 2015 [C5], *Skatteverket mot David Hedqvist*, C-264/14, EU:C:2015:718 avsnitt 47).
[74] Haukeland Fredriksen og Mathisen, EØS-rett side 168.

Den nasjonale domstolen avgjør om et spørsmål skal forelegges EU-domstolen selv, og partene i saken kan ikke fremtvinge en slik foreleggelse. Den foreleggende domstolen trekker opp rammen for EU-domstolens behandling ved spørsmålsstillingen og redegjørelsen for faktum og nasjonale regler.[75] EU-domstolen forholder seg som regel til de forelagte spørsmålene uten å trekke inn annen EU-rett enn den påberopte. En prejudisiell avgjørelse må derfor alltid leses i lys av spørsmålet fra den foreleggende domstolen.[76]

Partene i saken fra den foreleggende domstolen har rett til å inngi innlegg under EU-domstolens saksbehandling av det forelagte spørsmålet. Den samme retten har alle EUs medlemsstater og institusjonene i EU, ESA og EFTA-landene.[77]

Svaret på det forelagte spørsmålet skjer i form av en dom fra EU-domstolen. Denne dommen er bindende for den nasjonale domstolen for tolkningen av EU-retten. Fortolkning av nasjonal rett av betydning for saken, bevisbedømmingen og anvendelsen av EU-retten på faktum hører til domstolsbehandlingen i den nasjonale domstolen.[78] Delingen mellom fastleggelsen av EU-retten og subsumsjonen er likevel ikke som to vanntette skott, og det er EU-domstolen selv som avgjør hvor langt i faktumprøvingen de går i hver enkelt sak.[79]

Når EU-domstolen blir forelagt spørsmål fra nasjonale domstoler om nasjonal lovgivning er i tråd med EU-retten, kan EU-domstolen kun fastslå at den nasjonale loven ikke er i tråd med EU-retten. Det er opp til nasjonale domstoler og nasjonale myndigheter eventuelt å underkjenne en nasjonal lov på grunn av manglende samsvar.[80]

2.3.4 Uttalelser fra EUs generaladvokater- en rettskilde ved tolkningen av dommer fra EU-domstolen

Etter TEUV[81] art. 252 skal dommerne i EU-domstolen bistås av åtte generaladvokater. Generaladvokatene er ansatt i EU-domstolen og skal være uavhengige og upartiske, jf. TEUV art. 252 andre ledd. Generaladvokatene har ikke til oppgave å dømme, men de skal skrive en

[75] Broberg og Fenger *Præjudicielle forelæggelser for EF-domstolen* (2008) side 403.
[76] Haukeland Fredriksen og Mathisen, EØS-rett side 169.
[77] EU-domstolens vedtekter art. 23.
[78] Haukeland Fredriksen og Mathisen, EØS-rett side 170.
[79] Haukeland Fredriksen og Mathisen, EØS-rett side 170.
[80] Se TEUV art. 267.
[81] Traktat om Den Europeiske Unions Virkemåte.

uttalelse og foreslå et resultat for dommerne før EU-domstolen treffer avgjørelse. Uttalelsen er rådgivende og følges ofte av dommerne, men ikke alltid.[82]

EU-domstolens forhandlinger og avstemninger er hemmelige, og eventuelle dissenser skrives og publiseres ikke.[83] Generaladvokatens innstilling kan av den grunn være med på å kaste lys over domstolens avgjørelser.[84] Den rettsskildemessige vekten til uttalelsene fra EUs generaladvokater må likevel vurderes opp mot EU-domstolens dom i hver enkelt sak.[85] I de tilfellene der EU-domstolen ikke har sluttet seg til generaladvokatens innstilling i dommen, må det vises varsomhet med å bruke innstillingen som rettskilde ved tolkning av den. Motsatt kan innstillingen fra generaladvokaten være med på å vise hvilke argumentasjonsmønstre domstolen har bygget sin avgjørelse på i de tilfellene domstolen har fulgt generaladvokatens innstilling.[86]

2.3.5 EØS-avtalen

Norge er ikke medlem av EU, men er tilknyttet EUs indre marked gjennom EØS-avtalen.[87] EØS-avtalen og gjennomførte rettsakter fra EØS i norsk rett kan sette begrensninger for reguleringen av tilrettelagt innhenting i etterretningstjenesteloven. Innledningsvis vil det derfor foretas en kort presentasjon av EØS-avtalen.

Norge, sammen med tre andre EFTA-land[88], undertegnet EØS-avtalen i mai 1992. Formålet med EØS-avtalen er å opprette et "dynamisk og ensartet Europeisk Økonomisk Samarbeidsområde, som er grunnlagt på felles regler og konkurransevilkår (...)".[89]

Tre av EFTA-landene, Norge, Island og Liechtenstein, har seg imellom inngått avtale om opprettelse av et overvåkningsorgan og en domstol (ODA-avtalen). ODA-avtalen oppretter EFTAs overvåkningsorgan, ESA, og EFTA-domstolen, som er institusjoner som skal kontrollere og sørge for at EØS-avtalens rettslige forpliktelser blir ivaretatt av EFTA-landene.

---

[82] Fredrik Sejersted mfl., EØS-rett, 3. utgave, Universitetsforlaget, 2011 s. 135.
[83] Fredrik Sejersted mfl., EØS-rett, 3. utgave, Universitetsforlaget, 2011 s. 136.
[84] Fredrik Sejersted mfl., EØS-rett, 3. utgave, Universitetsforlaget, 2011 s. 236.
[85] Haukeland Fredriksen, Halvard og Gjermund Mathisen, EØS-rett, 2. utgave 2014 side 246.
[86] Ibid. side 245.
[87] Avtale om Det europeiske økonomiske samarbeidsområde.
[88] Norge, Island, Liechtenstein og Sveits er medlemmer av EFTA (European Free Trade Association), kun de tre første landene er medlemmer av EØS-avtalen.
[89] EØS-avtalens fortale femte ledd.

Høyesterett har gjennom veletablert rettspraksis betraktet EØS-avtalen som en særegen mellomstatlig avtale og ikke en ordinær folkerettslig avtale.[90] Høyesterett har sluttet seg til en uttalelse fra EFTA-domstolen om at EØS-avtalen er "an international treaty sui generis which contains a distinct legal order of its own".[91]

EØS-avtalens rettslige innhold er nesten utelukkende EU-rett.[92] I en offentlig utredning om Norges forhold til EU hevder utvalget bak utredningen at "det er lite treffende å tale om en egen EØS-rett".[93] Uavhengig om man ser EØS-retten som et eget rettssystem, et tilknytningssystem mellom EFTA og EU eller som en kopi av det EU-rettslige system, har EU-retten stor betydning for EØS-rettslige forpliktelser, og det er derfor avgjørende å identifisere hvordan en EU-regel må tolkes og anvendes i egenskap av å være EU-rett for å klarlegge den EØS-rettslige forpliktelsen. Etter EØS avtalen art. 6 er praksis fra EU-domstolen gjort til tungtveiende argumenter for løsning av EØS-rettslige spørsmål, noe som også stadfester relevansen til dommer fra EU-domstolen som rettskilde i EØS-retten.

EØS-avtalens hoveddel er gjort til en del av norsk rett og skal gjelde som norsk lov, jf. EØS-loven[94] § 1. Etter EØS-loven § 2 skal lovbestemmelser som skal oppfylle en forpliktelse etter EØS-avtalen gå foran andre lovbestemmelser som regulerer samme forhold. Dersom tilrettelagt innhenting viser seg å stride mot forpliktelsene etter kommunikasjonsvernsdirektivet som i norsk rett er gjennomført i ekomloven, foreligger det motstrid mellom ekomloven og etterretningstjenesteloven. Slik motstrid kan løses direkte etter EØS-loven § 2 med det resultat at bestemmelsene i ekomloven, som er EØS-rettslig forpliktelser, må gis forrang.

---

[90] Se for eksempel HR-2016-296 A avsnitt 47).
[91] HR-2016-296-A avsnitt 47) med videre henvisninger til EFTA-domstolens rådgivende uttalelse i sak E-9/97 Sveinbjörnsdottir.
[92] Haukeland Fredriksen og Mathisen, EU-rett som norsk rettskilde side 389.
[93] NOU 2012: 2 *Utenfor og innenfor- Norges avtale med EU* kapittel 3.2.
[94] Lov 27. november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske samarbeidsområde (EØS) m.v. (EØS-loven).

3 Tilrettelagt innhenting: teknologisk rammeverk

3.1 Innledning

Etterretningstjenesteloven kapittel 7 åpner for lagring av metadata i bulk. Forut for en analyse av det teknologiske rammeverket rundt en slik form for lagring, er det nødvendig med et par forklaringer av begrep brukt i etterretningstjenesteloven.

Metadata er i proposisjonen til etterretningstjenesteloven[95] definert som "data som beskriver annen data eller som inneholder ekstra informasjon knyttet til data, herunder data som beskriver typen eller formatet på innholdet, hvem som er avsender og mottaker, og størrelse, tidspunkt og varighet for kommunikasjonen".[96] Metadata avgrenses mot innholdsdata som er all data som ikke er metadata, for eksempel innholdet i en e-post.

"Bulk" er legaldefinert i etterretningstjenesteloven § 1-3 bokstav i) som "informasjonssamlinger og datasett hvorav en vesentlig andel av informasjonen antas å være irrelevant for etterretningsformål".

Avhandlingen vil senere i kapittel 5 og 6 vurdere nødvendigheten og forholdsmessigheten av tilrettelagt innhenting. Vurderinger av nødvendighet og proporsjonalitet forutsetter forståelse for det livsområde som er regulert og de tekniske systemene som er vedtatt. Før en teknisk gjennomgang av hvordan bulklagringssystemet er ment å fungere, er det derfor nødvendig å presentere hvordan tele- og internettet er bygd opp i Norge og hvordan norske nettstrukturer kommuniserer med utenlandske nett.

Dette kapittelet vil også presentere hvorfor lovgiver har vurdert at det er et etterretningsmessig behov for et system med bulklagring av metadata i Norge. I forlengelsen av undersøkelsen av det etterretningsmessige behovet for tilrettelagt innhenting, vil trusselsituasjonen og utenlandsk påvirkning av riket bli presentert.

3.2 Det norske ekomnettet

Internett er antageligvis verdens viktigste infrastruktur.[97] Internett er desentralisert og ingen internasjonal eller statlig myndighet, organisasjon eller selskap kontrollerer "hele" internett.

---

[95] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 108.
[96] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 109.
[97] Min egen påstand.

Et kommunikasjonsnett for overføring av teledata og annen elektronisk kommunikasjon deles tradisjonelt inn i tre deler, transportnett, aksessnett og støttesystemer som styrer nettverket.[98] Transportnettet er ekomnettets motorvei og frakter datatrafikken over lange avstander fra sentrale knutepunkter og frem til aksessnettet.[99] Aksessnettet frakter datatrafikken fra transportnettet og frem til den enkelte databruker. Støttesystemene overvåker datatrafikken og styrer for eksempel taksering og abonnementsdatabaser.[100]

Ekomtilbydere har behov for å lagre metadata om telekommunikasjon og internettbruk for kommunikasjons- og faktureringsformål. Slik lagring skjer i støttesystemene til ekomnett.[101] Denne lagring utført av ekomtilbyderne muliggjør at politimyndigheter og etterretningstjenester kan benytte lagret metadata for bekjempelse og iretteføring av kriminalitet og til etterretningsformål.

I Norge har Telenor et landsdekkende transportnett som knytter regionene i Norge sammen. Dette kjernenettet kan sammenlignes med en motorvei og mobiloperatører som ikke eier egne basestasjoner benytter denne infrastrukturen. Ekomnettet består også av regionale nett, og også noen fiberoptiske interregionale transportnett eid av for eksempel Altibox.[102]

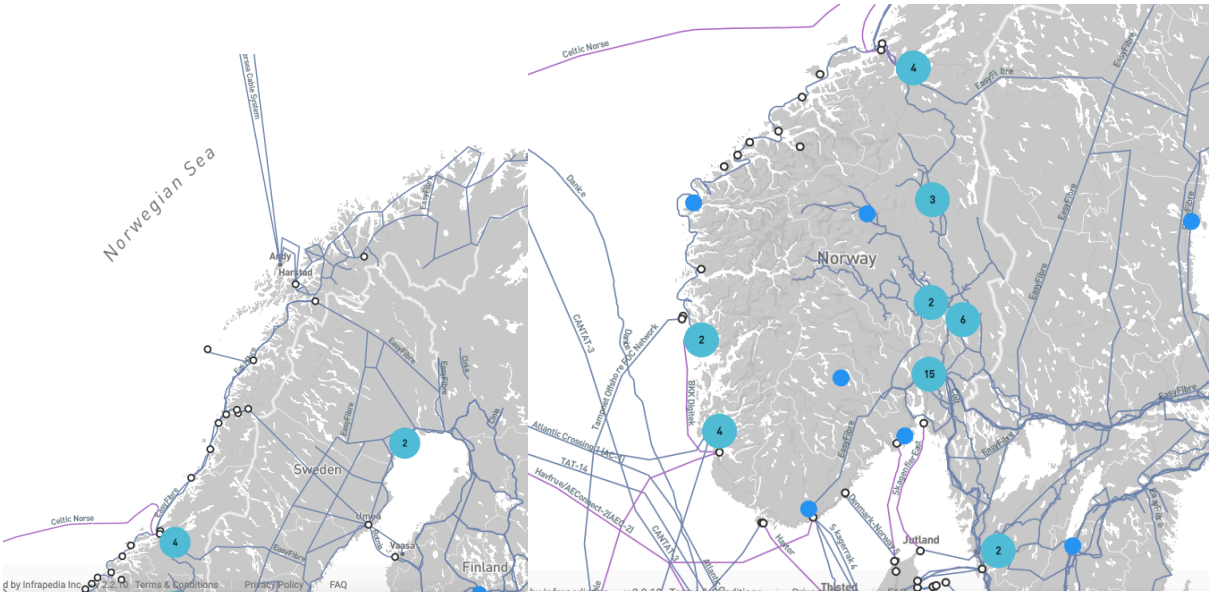
3.3 Hvilken datatrafikk passerer landegrensen?

Tilrettelagt innhenting gjelder kun grenseoverskridende kommunikasjon, der er derfor av betydning å fastslå hvor mye av datatrafikken som passerer landegrensen. Internett er globalt. Det norske transportnettet er derfor koblet sammen med utenlandske nettstrukturer. Denne sammenkoblingen er stort sett kabelbasert via fiberoptiske land- og sjøkabler. En liten andel av internettrafikken går via satellitt. Tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon gjelder ikke denne satellittkommunikasjonen. Begrunnelse for dette er at satellittkommunikasjonen utgjør en liten del av den totale grenseoverskridende elektroniske kommunikasjonen.[103]

Figuren under viser tilkoblingspunkter mellom norske og utenlandske nettstrukturer:

---

[98] NOU 2015:13 Digital sårbarhet-sikkert samfunn side 16.
[99] NOU 2015:13 Digital sårbarhet-sikkert samfunn side 16 og 17.
[100] NOU 2015:13 Digital sårbarhet-sikkert samfunn side 16 og 17.
[101] Se ekomloven § 2-7 femte ledd nr. 1).
[102] Digitalt grenseforsvar (DGF) Lysne II-utvalgets utredning til forsvarsdepartementet side 48.
[103] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 62.



*Figur 1: Oversikt over tilkoblingspunkter mellom norske og utenlandske fiberoptiske land- og sjøkabler. Kilde: live.infrapedia.com (*21.09.2020)

Dersom en e-post, en SMS eller annen korrespondanse sendes fra Norge til utlandet, eller fra utlandet til Norge, vil korrespondansen som utgangspunkt bli gjenstand for lagring, jf. etterretningstjenesteloven § 7-2. På grunn av plasseringen av servere, vil internettrafikken til for eksempel store sosiale medier også passere landegrensen, fordi de sosiale mediene har servere i utlandet.[104]

Norske internettleverandører har inngått avtaler med utenlandske operatører om bruk av utenlandske fibernett. Det innebærer at norske brukere av internett kan få rutet sine nettsøk og annen internettbruk via utenlandske kabler selv om man surfer på en nettside som har servere plassert i Norge og selv om to norske internettbrukere kommuniserer med hverandre. Det avhenger av tidspunkt på døgnet, lokasjon og hvor belastet linjene er om et norsk nettsøk blir omrutet via utlandet.[105] Dette er av avgjørende betydning siden tilrettelagt innhenting bare omhandler grenseoverskridende elektronisk kommunikasjon.

Kommunikasjon på internett foregår etter et sett med regler som kalles *Internet Protocol* (IP). Denne protokollen inneholder regler og framgangsmåter for pakking og ruting av elektronisk kommunikasjon.[106] Det innebærer at hvis man for eksempel sender et bilde som et vedlegg til

[104] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 104.
[105] https://nrkbeta.no/2019/02/14/slik-kan-den-nye-etterretningsloven-pavirke-deg/ (13.09.2020).
[106] https://www.cloudflare.com/learning/network-layer/internet-protocol/ (13.09.2020)

en e-post, vil bildet bli delt opp i mange små datapakker etter IP-protokollen. Disse pakkene blir deretter rutet raskeste vei fra avsender til mottaker, før datapakkene settes sammen igjen hos mottakeren. Denne oppdelingen og rutingen data kan innebærer at en e-post fragmenteres og tar forskjellige *veier* på sin rute frem til mottakeren. Oppdelingen kan igjen innebære at en del av meldingen går via Norge, mens en annen del av meldingen går over landegrensen og at metadata tilknyttet meldingen dermed blir gjenstand for lagring.[107]

Det som vanligvis ikke oppfattes som nettbruk, for eksempel automatisk lagring av bilder og dokumenter i Icloud på en Apple- enhet eller ved bruk av andre lignende skytjenester for lagring, vil også passere landegrensen og e-tjenestens filtre på grunn av plassering av servere.[108] Datamaskiner, mobiltelefoner og andre enheter koblet til internett vil også kommunisere over internett uten at det skyldes aktiv bruk av brukeren. På denne måten kan for eksempel datamaskinen motta automatiske oppdateringer. Slik databruk vil også være gjenstand for lagring dersom datatrafikken krysser landegrensen og kabelen er underlagt tilretteleggingsplikt av Etterretningstjenesten.[109]

I sitt høringssvar til ny lov om etterretningstjenesten uttalte Telenor seg om hvor mye av den norske datatrafikken Telenor anser som grenseoverskridende. I høringssvaret presiserte Telenor at "grenseoverskridende elektronisk kommunikasjon" i stor grad innbefatter innenlands kommunikasjon, med unntak av innenlands talekommunikasjon og SMS. I et uoffisielt estimat med mange forenklinger har Telenor overfor NRK anslått at om lag 70 % av den totale datatrafikken i Norge er grenseoverskridende i form av at den krysser landegrensen til Sverige.[110]

3.4 Hvorfor har lovgiver vurdert at det er behov for tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon?

I forarbeidene[111] til etterretningstjenesteloven viser lovgiver til høringsnotatet[112] til loven der Forsvarsdepartementet trekker frem tre hovedgrunner for at det foreligger et behov for

---

[107] https://snl.no/internettprotokoll (01.10.2020).
[108] Digitalt grenseforsvar (DGF) Lysne II-utvalgets utredning til forsvarsdepartementet side 48.
[109] Digitalt grenseforsvar (DGF) Lysne II-utvalgets utredning til forsvarsdepartementet side 48-49.
[110] https://nrkbeta.no/2019/02/14/slik-kan-den-nye-etterretningsloven-pavirke-deg/ (13.09.2020).
[111] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 92 og 93.
[112] Høringsnotat fra Forsvarsdepartementet av 12. november 2018 side 193

bulklagring av metadata. For det første fremhever departementet at statlige og private aktører gjennomfører truende operasjoner i det digitale rom, for eksempel angrep, påvirkningsoperasjoner og spionasje. For det andre blir det fremhevet at trusselaktører benytter digitale plattformer til planlegging og koordinering av terrorisme. For det tredje blir behovet for systemet begrunnet i at etterretningsmål kommuniserer på digitale plattformer.[113]

Departementet skriver videre i høringsnotatet at dersom Norge ikke har et eget system for tilrettelagt innhenting, vil Etterretningstjenesten være avhengig av å få informasjon fra allierte og samarbeidende land. I forbindelse med dette blir det fremhevet at samarbeidende tjenester i andre land har ikke har norske interesser som sin øverste prioritet.[114] Departementet skriver også at ved slik informasjonsinnhenting fra andre land har ikke Etterretningstjenesten noen garanti for at innhentingen har skjedd i samsvar med norsk lov og Norges folkerettslige forpliktelser.[115]

Ikke-statlige og statlige aktører bruker internett til for eksempel å påvirke politiske prosesser og offentlig opinion i et annet land. Etterretningstjenesten gir ut en avgradert trusselvurdering hvert år. I trusselvurderingen for 2021, Fokus 2021, skriver Etterretningstjenesten at de faktorene som i størst grad påvirker trusselbildet mot Norge er knyttet til Russland og Kina. I valgåret 2021 er særlig utenlandsk valgpåvirkning i digitale kanaler ansett som en trussel mot Norge. E-tjenesten skriver i sin trusselvurdering at pandemien har ført til at nettverksoperasjoner har "blitt en viktigere metode for innhenting av informasjon (...) En større del av aktiviteten i samfunnet skjer på digitale plattformer, og muligheten for å hente ut store mengder informasjon har økt".[116]

3.5 Metadata og innholdsdata

3.5.1 Skillet mellom metadata og innholdsdata i etterretningstjenesteloven

Metadata[117] er som nevnt under pkt. 3.1 data som beskriver annen data eller inneholder ekstra informasjon om data. Hvis man overfører betegnelsene metadata og innholdsdata over til et

---

[113] Høringsnotatet side 193.
[114] Høringsnotatet side 193.
[115] Høringsnotatet side 193.
[116] https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Fokus2021-web.pdf/_/attachment/inline/b9d52b53-0abe-4d1c-9c51-bf95796560bf:8dd66029b7efb38aab37d13e8b387d2e6ed0bd05/Fokus2021-web.pdf (09.02.2021).
[117] Meta kommer fra gresk og betyr "mellom, etter, ved siden av".

analogt brev, er innholdsdata brevets innhold på innsiden av konvolutten. Metadata er det som står utenpå konvolutten, mottakeren på forsiden, avsender på baksiden, frimerket og poststempelet.[118]

Det finnes ikke noen omforent og enhetlig internasjonal definisjon om hva som skiller metadata fra innholdsdata.[119] I etterretningstjenesteloven er skillet mellom metadata og innholdsdata regulert ved at Etterretningstjenesten selv oppretter en liste over hvilke typer data som utgjør metadata og dermed kan lagres, jf. etterretningstjenesteloven § 7-7 andre ledd. Denne listen skal også være tilgjengelig for EOS-utvalget og Nasjonal kommunikasjonsmyndighet, men vil mest sannsynlig være gradert etter sikkerhetsloven[120] for allmennheten.

3.5.2 Hvorfor har metadata etterretningsverdi?

Etterretningstjenesten ønsker å lagre metadata for å sammenstille kommunikasjonsmønstre ved cyberangrep, internasjonal terrorisme eller for andre etterretningsformål. Ved å sammenstille metadata fra telefonnumre eller IP-adresser kan man danne seg et bilde av for eksempel et terrornettverks størrelse og omfang.[121]

Metadata er tradisjonelt ansett som mindre sensitivt enn innholdsdata. Sammenstilling av metadata kan likevel si mye om et enkelt individ, selv om man ikke har tilgang til innholdsdata. Etterretningsverdien av metadata kan sammenlignes med et eksempel fra straffeprosessen. Dersom politiet ønsker å få kartlagt omfanget av et mulig narkotikanettverk, kan de henvende seg til retten med begjæring om kommunikasjonskontroll på en kjent narkotikaselger. Ved å sammenstille hvem denne selgeren kommuniserer med, kan politiet skaffe seg oversikt over et narkotikanettverk.

Dersom Etterretningstjenesten for eksempel får et tips fra en samarbeidende tjeneste om et kjent etterretningsmål, kan de sende en begjæring til Oslo tingrett med begjæring om å søke i metadatalagreret for å finne ut hvem denne personen har kommunisert med. På denne måten kan man sammenstille kommunikasjonsmønstre og skaffe seg oversikt over mulige nettverk av personer som er interessante fra et etterretningsperspektiv. Dersom et slikt målsøk etter

---

[118] Digitalt grenseforsvar (DGF) Lysne II-utvalgets utredning til forsvarsdepartementet side 25.
[119] Datatilsynets høringssvar av 06.02.2019 side 30 med videre henvisninger til praksis fra EU-domstolen og EMD.
[120] Lov 1. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven).
[121] Digitalt grenseforsvar (DGF) Lysne II-utvalgets utredning til forsvarsdepartementet side 25.

metadata gir resultater, kan disse resultatene fra målsøket utgjøre grunnlaget for at Etterretningstjenesten begjærer målrettet innhenting av innholdsdata for å få tilgang til hva som blir kommunisert.

Innholdet i elektronisk kommunikasjon kan ofte være skrevet på en måte som kun mottaker og avsender forstår, den kan være kryptert eller skrevet indirekte eller i en kodet form. Metadata er ofte numerisk i formen og derfor lettere gjenstand for automatisk samling, sortering og analyse, også analyse ved bruk av algoritmer og kunstig intelligens. Metadata kan derfor ha større etterretningsmessig verdi enn innholdsdata fra elektronisk kommunikasjon.[122] Lagring av metadata kan derfor beskrives som sensitivt på en annen måte enn innholdsdata heller enn at metadata er mindre sensitivt enn innholdsdata.[123]

3.6 Kryptering

Formålet med tilrettelagt innhenting er å beskytte norske interesser mot utenlandsk påvirkning og utenlandske trusler. Dersom de med onde hensikter bruker krypterte og sikre kommunikasjonsmåter og ikke benytter kommunikasjonsveier som er gjenstand for Etterretningstjenestens lagring og analyse, kan det problematiseres om fordelene ved tilrettelagt innhenting ikke oppveier for inngrepet systemet medfører i den enkelte internettbrukers personopplysningsvern.

Dette avsnittet skal derfor knyttet noen kommentarer til kryptert kommunikasjon og om slik kommunikasjon vil oppdages av tilrettelagt innhenting. Elektronisk kommunikasjon via internett kan enten være i) ukryptert, ii) kryptert, men på en slik måte at etterretningstjenesten lett kan forsere krypteringen eller iii) være kryptert på en måte som etterretningstjenesten ikke kan forsere.[124]

Det er lite norsk empiri om hvordan for eksempel terrorister kommuniserer med hverandre eller hvordan en fremmed stat kommuniserer med representanter for fremmede etterretningstjenester plassert i Norge. I artikkelen "The Investigatory Powers Act 2016" inntatt i boken Terrorism and State Surveillance of Communications[125] er det undersøkt

---

[122] Paul Bernal, "Data Gathering, surveillance and human rights: recasting the debate (2016)" I *Journal of Cyber Policy*, 1: 2 side 243-264 på side 247.
[123] Bernal, side 248.
[124] Digitalt grenseforsvar (DGF) Lysne II-utvalgets utredning til forsvarsdepartementet side 26.
[125] Simon Hale-Ross, The Investigatory Powers Act 2016 The human rights conformist, Terrorism and State Surveillance of Communications, Routledge (London) 2019, s. 44.

hvordan terrorister bruker kommunikasjonsteknologi i den digitale tidsalderen. Artikkelen benytter terrororganisasjon IS som casestudium og undersøker hvordan slike organisasjoner benytter kryptering og "det mørke nettet" til kommunikasjon.

Et eksempel fra artikkelen er kommunikasjonen mellom en utro ansatt i British Airways og den kjente al Qaida- toppen Anwar al- Awaki om planleggingen av et terrorangrep. Denne kommunikasjonen gikk gjennom gjentatte avanserte krypteringer. Den originale meldingen ble skrevet inn i Excel der den ble kryptert ved makrokryptering, deretter ble den overført til Word og passordbeskyttet. Denne filen ble komprimert og kryptert en gang til før den gikk gjennom krypteringsprogrammetet RAR. Deretter ble denne filen postet på internett og internettadressen ble forkortet for å anonymisere metadataen til internettadressen. Storbritannias hemmelige tjenester brukte ni måneder på å dekryptere kommunikasjonen.[126]

Dette eksempelet viser at de med onde hensikter i stor grad vet hvordan man kan kommunisere kryptert uten å komme i myndighetenes og etterretningstjenestens søkelys. Avhandlingen vil komme tilbake til den økende bruken av kryptering i forbindelse med forholdmessighetsvurderingen etter EMK og EU-retten i kapittel 5 og 6.

4 Materielle vilkår for tilrettelagt innhenting

4.1 Introduksjon

Hjemmelsgrunnlaget for tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon er etterretningstjenesteloven kapittel 7. Tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon omfatter lagring av metadata, søk i lagrede metadata og tilrettelagt innhenting av innholdsdata.

Etter etterretningstjenesteloven § 7-1 er vilkårene for tilrettelagt innhenting at i) den elektroniske kommunikasjonen krysser landegrensen, ii) grunnvilkårene i kapittel 5 er oppfylt og iii) at de prosessuelle vilkårene for innhenting i kapittel 7 og 8 følges.

4.2 Innhentingen må begrunnes i etterretningsformål

Etter etterretningstjenesteloven § 7-1 første ledd kan etterretningstjenesten benytte tilrettelagt innhenting som metode "for etterretningsformål." Etterretningsformål er legaldefinert i

[126] Hale-Ross side 47.

etterretningstjenesteloven § 1-3 bokstav c) som "formål om å ivareta en eller flere av etterretningstjenestens oppgaver etter kapittel 3". For en gjennomgang av etterretningstjenestens oppgaver vises det til punkt 1.4.

I etterretningstjenesteloven § 2-2 er det fastslått at Forsvarsdepartementet årlig skal koordinere og prioritere myndighetenes etterretningsbehov i et prioriteringsdokument. Videre kan forsvarssjefen prioritere de sivile etterretningsbehovene som ikke fremgår av prioriteringsdokumentet, jf. etterretningstjenesteloven § 2-2 andre ledd første punktum. Selv om etterretningstjenesteloven § 2-2 inneholder regler om departementets og forsvarssjefens oppdragsstyring, avgrenser ikke det vilkåret om at tilrettelagt innhenting kan skje "for etterretningsformål". Det vil si at etterretningstjenesten kan foreta tilrettelagte søk hvis vilkårene for det er oppfylt, uten at formålet for søket fremgår av prioriteringsdokumentet.[127]

Etterretningstjenesteloven § 4-8 første ledd har slik ordlyd: "etterretningstjenesten skal ikke innhente eller medvirke til å innhente informasjon for å utføre oppgaver som tilligger politiet eller andre rettshåndhevende myndigheter". I etterretningstjenesteloven § 10-7 er det presisert at etterretningstjenesten kan yte bistand til politiet etter politiets begjæring i medhold av politiloven § 27 a, men at slik bistand ikke kan omfatte tilrettelagt innhenting eller målsøking.

4.3 Kommunikasjonen må krysse den norske landegrensen

Etter etterretningstjenesteloven § 7-1 første ledd er det et vilkår for lagring av metadata at kommunikasjonen "transporteres over den norske grensen." Ordlyden sier ikke noe om hvordan kommunikasjonen kan krysse landegrensen, og i forarbeidene er det presisert at det er uten betydning hvorvidt "kommunikasjonen transporteres inn og ut av Norge på land, sjøveien eller i luften".[128] I forarbeidene er det likevel presisert at metadata fra satellittkommunikasjon ikke foreslås lagret fordi det utgjør en liten del av den samlende grenseoverskridende kommunikasjonen.[129]

[127] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 220.
[128] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 212.
[129] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 62.

4.4 Kommunikasjonsbegrepet

Etter etterretningstjenesteloven § 7-1 kan etterretningstjenesten innhente grenseoverskridende elektronisk *kommunikasjon.* En vanlig ordlydfortolkning av *kommunikasjon* er meddelelser mellom to eller flere personer, eller meddelelser mellom to eller flere dataenheter.

Etter bestemmelsens forarbeider skal ikke bestemmelsens forstås slik.[130] Etter lovgivers vurdering foreligger det også *kommunikasjon* ved ensidig overføring av lyd, tekst, bilder eller andre data. Det anses derfor som kommunikasjon å laste ned et bilde fra internett, å se på videooverføring og ved ordinær surfing på internett.

4.5 Grunnvilkår for metodebruk i etterretningstjenesteloven kapittel 5

Grunnvilkåret for tilrettelagt innhenting av rådata i bulk etter etterretningstjenesteloven § 5-3 er at innhentingen er "nødvendig for å få tilgang til et relevant og tilstrekkelig informasjonsgrunnlag".

Ordlyden er svært skjønnsmessig, og det er Etterretningstjenesten selv som avgjør når det er nødvendig å innhente rådata i bulk. I forarbeidene er bestemmelsen kommentert slik "(...) rådata i bulk ikke kan hentes inn dersom mindre inngripende alternativer vil gi tilgang til et adekvat informasjonsgrunnlag".[131]

Videre er det er det et forholdsmessighetsvilkår i etterretningstjenesteloven § 5-4. Det fremgår av bestemmelsen at "innhenting og utlevering av informasjon skal ikke gjennomføres dersom det vil være uforholdsmessig inngrep overfor den enkelte". Vilkåret gjelder generelt overfor alle innhentingsmetoder, og ikke bare tilrettelagt innhenting.

4.6 Innhentingen skjer i form av en tilretteleggingsplikt

4.6.1 Hvem gjelder tilretteleggingsplikten for?

Tilrettelagt innhenting, lagring av rådata av metadata i bulk, skjer i form av en tilretteleggingsplikt for ekomtilbydere, jf. etterretningstjenesteloven § 7-2.

Denne plikten til å legge til rette for innhenting gjelder for tilbydere av elektroniske kommunikasjonsnett eller kommunikasjonstjenester, jf. etterretningstjenesteloven § 7-2.

---

[130] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 104.
[131] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 206.

Etterretningstjenesteloven § 7-2 viser til ekomloven[132] § 1-5 tredje og fjerde ledd for definisjonen av elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste.

Et elektronisk kommunikasjonsnett er et system for signaltransport som muliggjør overføring av lyd, tekst, bilder eller andre data ved hjelp av elektromagnetiske signaler i fritt rom eller kabel, jf. ekomloven § 1-5 andre ledd.

En elektronisk kommunikasjonstjeneste er en tjeneste som helt eller i det vesentlige omfatter formidling av signaler i elektroniske kommunikasjonsnett og som normalt ytes mot vederlag, jf. ekomloven § 1-5 tredje ledd.

Telenors kjernenett er et eksempel på et kommunikasjonsnett i Norge. Når en annen leverandør av telefoni leier Telenors nett for å selge sine tjenester, for eksempel hvis Telia leier Telenors nett, driver Telia en elektronisk kommunikasjonstjeneste på Telenors kommunikasjonsnett.

Etter ekomforskriften § 1-2 skal tilbydere av elektroniske kommunikasjonsnett og kommunikasjonstjenester registrere seg hos Nasjonal kommunikasjonsmyndighet. Per 22.02.2021 er det registrert 456 tilbydere av elektroniske kommunikasjonsnett og kommunikasjonstjenester i Norge.[133] Etter tilbyderoversikten vil tilretteleggingsplikten etter etterretningstjenesteloven § 7-2 både gjelde for allment kjente ekomtilbydere som Telenor og Telia, men aktører som Fitjar Kraftlag SA og en lang rekke kommuner fremgår også av tilbyderoversikten og kan underlegges tilretteleggingsplikt. Forutsetningen er at tilbyderne leverer grenseoverskridende elektronisk kommunikasjon, jf. etterretningstjenesteloven § 7-1.

I tillegg til tilbyderne som fremgår av ekomloven § 1-5, gjelder tilretteleggingsplikten for "tilbydere av kommunikasjons- eller meldingstjenester som er tilgjengelige for allmennheten", jf. etterretningstjenesteloven § 7-2 første ledd. Slike tjenester blir kalt "over the top"- tjenester (OTT-tjenester).[134]

Slike tjenester har ikke noen enhetlig eller omforent definisjon, men tjenester som for eksempel leverer telefoni-tjenester via internett og ikke via det tradisjonelle telenettet,

---

[132] Lov av 4. juli 2007 nr. 83 om elektronisk kommunikasjon (ekomloven).
[133] Tilbyderoversikt fra NKOM, tilgjengelig: https://www.nkom.no/files/ekomstat/Tilbyderoversikt.pdf (Lastet ned 22.02.2021).
[134] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 213.

VoIP,[135] er eksempler på en slik tjeneste. Lovens ordlyd stiller krav om at OTT-tjenesten må ha meldings- eller kommunikasjonsfunksjonalitet, jf. etterretningstjenesteloven § 7-2 første ledd.

Ved at tilretteleggingsplikten også omfatter tilbydere av kommunikasjons- eller meldingstjenester som er tilgjengelig for allmennheten, skaper det vanskelige grensedragningsspørsmål. Det kan stilles spørsmål om for eksempel aktører som Finn.no som har meldingsfunksjonalitet i sin nettplattform omfattes av definisjonen. Loven er heller ikke klar på om tilretteleggingsplikten også omfatter internasjonale OTT-tjenester slik som Facebook eller WhatsApp. Slike grensedragningsspørsmål er ikke løst i forarbeidene til etterretningstjenesteloven og må derfor avgjøres ved tolkning i hvert enkelt tilfelle.

4.6.2 Hva omfatter tilretteleggingsplikten for ekomtilbyderne?

Tilretteleggingsplikten omfatter en plikt til å "speile og gjøre tilgjengelig for Etterretningstjenesten utvalgte kommunikasjonsstrømmer og på annen måte tilrettelegge for utvalg, filtrering, testing, innhenting, lagring og søk (...)", jf. etterretningstjenesteloven § 7-2 første ledd.

Videre er tilretteleggingsplikten konkretisert i bestemmelsens andre ledd, ekomtilbyderne plikter også å:

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

Ordlyden "speile og gjøre tilgjengelig" i første ledd innebærer at tilbyderne av elektroniske kommunikasjonstjenester ikke selv blir pålagt en plikt til å lagre metadataen. Lagringen vil skje på servere som eies og vedlikeholdes av Etterretningstjenesten. Etter

[135] Voice over Internet Protocol.

etterretningstjenesteloven § 7-2 er ekomtilbyderne pålagt en plikt til å la etterretningstjenesten installere utstyr på kommunikasjonsnettene og til å medvirke til drift og vedlikehold av dette utstyret.

Lysne II-utvalget som først foreslo et digitalt grenseforsvar, skjønte at økende kryptering var en vei utviklingen gikk og at dette kunne vanskeliggjøre etterretningsmessig innhenting av metadata.[136]

Tilretteleggingsplikten inneholder derfor også en plikt for tilbyder til å sørge for tilgang til kommunikasjonen uten hensyn til kryptering som tilbyderen selv kan kontrollere. Etterretningstjenesteloven § 7-2 pålegger ikke tilbyderen en plikt til å forsøke å omgå brukergenerert kryptering. Dersom dataen som går gjennom Telenors kommunikasjonsnett er brukergenerert, for eksempel kryptering tilknyttet banktjenester fra en finansinstitusjon, har ikke Telenor en plikt til å forsøke å trenge gjennom bankens kryptering.

Videre får ekomtilbyderne en plikt til å sørge for sikre og forsvarlige løsninger. Det innebærer hemmelighold innad i leverandøren og at færrest mulig ansatte har kjennskap til de tekniske løsningene og lignende.[137] Bestemmelsen om tilretteleggingsplikt er utformet på en teknologinøytral måte og er heller ikke uttømmende. Lovgiver har valgt en slik reguleringsmåte for å hensynta fremtidig teknologisk utvikling for å hindre at lovbestemmelsen blir utdatert.[138]

4.6.3 Tilretteleggingsplikt trer i kraft etter pålegg fra E-tjenesten

Lovens system er at tilretteleggingsplikt besluttes av sjefen for Etterretningstjenesten etter at tilbyderen har fått anledning til å uttale seg, jf. etterretningstjenesteloven § 7-3 første ledd. En slik beslutning gjelder for maksimalt tre år av gangen, men kan forlenges i ytterligere tre år ved utløpet av treårsperioden.

Vedtaket om tilretteleggingsplikt besluttet av sjefen for E-tjenesten er ikke et enkeltvedtak etter forvaltningsloven, jf. etterretningstjenesteloven § 11-1, men vedtaket kan påklages til forsvarsdepartementet, jf. etterretningstjenesteloven § 7-3 andre ledd. Departementet kan på

[136] Digitalt grenseforsvar (DGF) Lysne II-utvalgets utredning til forsvarsdepartementet side 112.
[137] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 112.
[138] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 114.

anmodning fra klageren beslutte at klagen skal gis oppsettende virkning, jf. etterretningstjenesteloven § 7-3 andre ledd siste punktum.

Det er straffbart for ekomtilbyderne å ikke oppfylle tilretteleggingsplikten, jf. etterretningstjenesteloven § 11-8.

Forut for etterretningstjenestelovens vedtakelse uttalte mange av høringsinstansene seg kritisk til at Etterretningstjenesten selv skulle kunne pålegge en tilretteleggingsplikt som ekomtilbyderne måtte rette seg etter. Noen av høringsinstansene mente at tilretteleggingsplikt for ekomtilbydere burde bli pålagt av en uavhengig myndighet eller domstol.[139]

4.7 Testinnhenting og testanalyser

I etterretningstjenesteloven § 7-5 er E-tjenesten gitt en mulighet til å gjennomføre testinnhenting og testanalyser av "trafikk og nett" som omfattes av etterretningstjenesteloven kapittel 7. Det vil si grenseoverskridende trafikk og grenseoverskridende kommunikasjonsnett og grenseoverskridende kommunikasjon på "internettbaserte kommunikasjons- og meldingstjenester", jf. etterretningstjenesteloven § 7-2 første ledd.

Etter etterretningstjenesteloven § 7-5 første ledd andre punktum skal "testinnhenting og testanalyser (...) utelukkende brukes for å muliggjøre utvalg, filtrering, lagring, søk, reprossesering, forståelse av signalmiljø og gjenkjenning av tjenester og dataformater, samt annen teknisk understøttelse".

Testinnhenting foregår ved uttrekk av ufiltrert kommunikasjon fra én eller flere kommunikasjonsstrømmer. Ett uttrekk skal ikke overstige 30 sekunder. Det kan ikke gjøres mer enn ett uttrekk hver time, jf. etterretningstjenesteloven § 7-5 andre ledd. Uttrekkene skal lagres i et kortidslager som er avskilt fra data som lagres etter lovens §§ 7-7 og 7-9, jf. etterretningstjenesteloven § 7-5 tredje ledd.

I siste ledd i etterretningstjenesteloven § 7-5 er det slått fast at "testinnhenting, testanalyser og annen teknisk undersøkelse skal bare utføres av tekniske spesialister" som ikke har "etterretningsanalyse som oppgave". For å unngå misbruk skal det som en sikkerhetsordning

[139] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 113.

alltid være to slike spesialister til stede ved uttrekk, jf. etterretningstjenesteloven § 7-5 femte ledd andre punktum.

Begrunnelsen for behovet for gjennomføring testinnhenting og testanalyse er teknisk drift av systemet og for å bygge opp en database som skal filtrere bort innenlandsk kommunikasjon.[140] I forarbeidene fremgår det at misbrukspotensialet ved testinnhenting og testanalyse er begrenset, blant annet under henvisning til at det er tilfeldig hva som fanges opp av uttrekkene og fordi det kun er tekniske personell uten etterretningsanalyse som oppgave som gjennomfører testinnhentingen.[141]

I motsetning til ved lagring av metadata i bulk, jf. etterretningstjenesteloven § 7-7, lagres både metadata og innholdsdata ved testinnhenting og testanalyse. 24 ganger i døgnet har etterretningstjenesten hjemmel til å innhente øyeblikksbilder av tilfeldige nordmenns internetttrafikk og teledata som krysser landegrensen. Denne datatrafikken blir ikke innhentet på grunn av etterretningshensyn, men utelukkende for å bygge opp en database som skal brukes til å filtrere bort norsk innenlandsk kommunikasjon.

Det er ikke et krav om forutgående godkjennelse før det kan innhentes data for testinnhenting og analyse etter lovens § 7-5. Denne dataen er ikke begrenset til metadata, innholdsdata vil også innhentes, opp mot 24 ganger i døgnet i 30 sekunder av gangen.

Det vil kanskje ikke føles inngripende for den gjengse nordmann at 30 sekunder internettbruk og telekommunikasjon kan innhentes tilfeldig av teknisk personale i e-tjenesten og lagres i opp mot 14 dager før sletting.

Det er likevel interessant å sammenligne de materielle og prosessuelle vilkårene for E-tjenestens tilgang til data for testinnhenting og testanalyse med det straffeprosessuelle tvangsmidlet dataavlesning i straffeprosessloven kapittel 16 d. Etter en slik sammenligning ser vi at det er store forskjeller på de materielle og prosessuelle vilkårene i de to regelsettene.

Ved dataavlesning får imidlertid politiet adgang til datasystemene til bestemte individer, mens det etter etterretningstjenesteloven § 7-5 er tilfeldig hvilken datatrafikk som blir plukket ut.

---

[140] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 106.
[141] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 106.

Innhenting etter etterretningstjenesteloven § 7-5 er også avgrenset til 30 sekunder 24 ganger i døgnet.

I straffeprosessloven § 216 O er vilkårene for at politiet skal kunne foreta dataavlesning at siktede med skjellig grunn kan mistenkes for et straffbart forhold med strafferamme på over 10 år, eller noen av straffebestemmelsene som er opplistet i straffeprosessloven § 216 O første ledd. Videre er det retten som har adgang til å beslutte dataavlesning etter begjæring fra politiet.

Testinnhenting og testanalyse etter etterretningstjenesteloven og dataavlesning etter straffeprosessloven kapittel 16 d har forskjellige formål. Mens testinnhenting og testanalyse skal bidra til drift av systemene som skal drifte tilrettelagt innhenting, er formålet med dataavlesning å skaffe bevis i straffesaker. Likevel sier de ulike vilkårene for innhenting av data fra datasystemer i de to lovene, noe om hvor strengt lovgiver har regulert tilgangen til datasystemer i straffeprosessloven, og hvor få materielle og prosessuelle rettssikkerhetsgarantier lovgiver har innført i etterretningstjenesteloven § 7-5.

4.8 Utvalg og filtrering

I etterretningstjenesteloven § 7-6 er det oppstilt en plikt for Etterretningstjenesten til å søke "å hindre lagring" av metadata i bulk om kommunikasjon der avsender og mottaker befinner seg i Norge. Etterretningstjenesten skal hindre slik lagring ved "utvalg og filtrering", jf. etterretningstjenesteloven § 7-6 første ledd første punktum. Plikten til å søke å unngå lagring av metadata fra innenlands kommunikasjon gjelder ikke dersom enten sender eller mottaker er en utenlandsk statsborger eller statsløs i Norge som driver etterretningsvirksomhet for fremmed stat, jf. etterretningstjenesteloven § 4-2.

Plikten til "utvalg" innebærer at E-tjenesten skal vurdere hvilke kabler som antas å bære mest mulig etterretningsrelevant informasjon før ekomtilbyderen pålegges tilretteleggingsplikt.[142]

Plikten til filtrering innebærer at Etterretningstjenesten skal utvikle filtre som filtrer bort mest mulig innenlandsk kommunikasjon. I forarbeidene fremgår følgende om vilkåret:

> "At tjenesten skal «søke å» hindre lagring, synliggjør at det ikke alltid vil være mulig å filtrere bort irrelevant data. Det vil ofte måtte lagres store mengder irrelevante data fra

[142] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 215.

> enkelte kommunikasjonsstrømmer, fordi det ikke er mulig å filtrere bort informasjonen som er uten interesse".[143]

I høringsrunden uttalte mange av høringsinstansene seg kritisk til hvorvidt det i det hele tatt er teknisk mulig å opprette et filter som på en effektiv måte skiller elektronisk kommunikasjon der avsender og mottaker befinner seg i Norge, og kommunikasjon ut av Norge. Dette særlig på bakgrunn av at elektronisk kommunikasjon splittes etter IP-protokoll, der de ulike delene av kommunikasjonen tar ulike veier. Det vises her tilbake til kapittel 3.

Dette ble også uttalt av Forsvarsdepartementet selv i høringsnotatet: "Hva gjelder Etterretningstjenestens oppbevaring av uevaluerte data som kan være overskuddsinformasjon, vektlegger departementet at det ikke finnes realistiske alternativer for å filtrere ut ikke-relevant informasjon fra datasettene".[144]

I proposisjonen er det ikke drøftet inngående hvordan slik filtrering foregår. I Lysne II-utvalgets fremgår det at det i hovedsak finnes to måter å filtrere på, den ene metoden går ut på at det foretas en maskinell filtrering der alt som ikke blir filtrert bort, lagres. Den andre metoden kalles positiv filtrering der det på forhånd angitt hva som skal anses relevant for etterretningsformål og det tas vare på, mens alt annet slettes.[145]

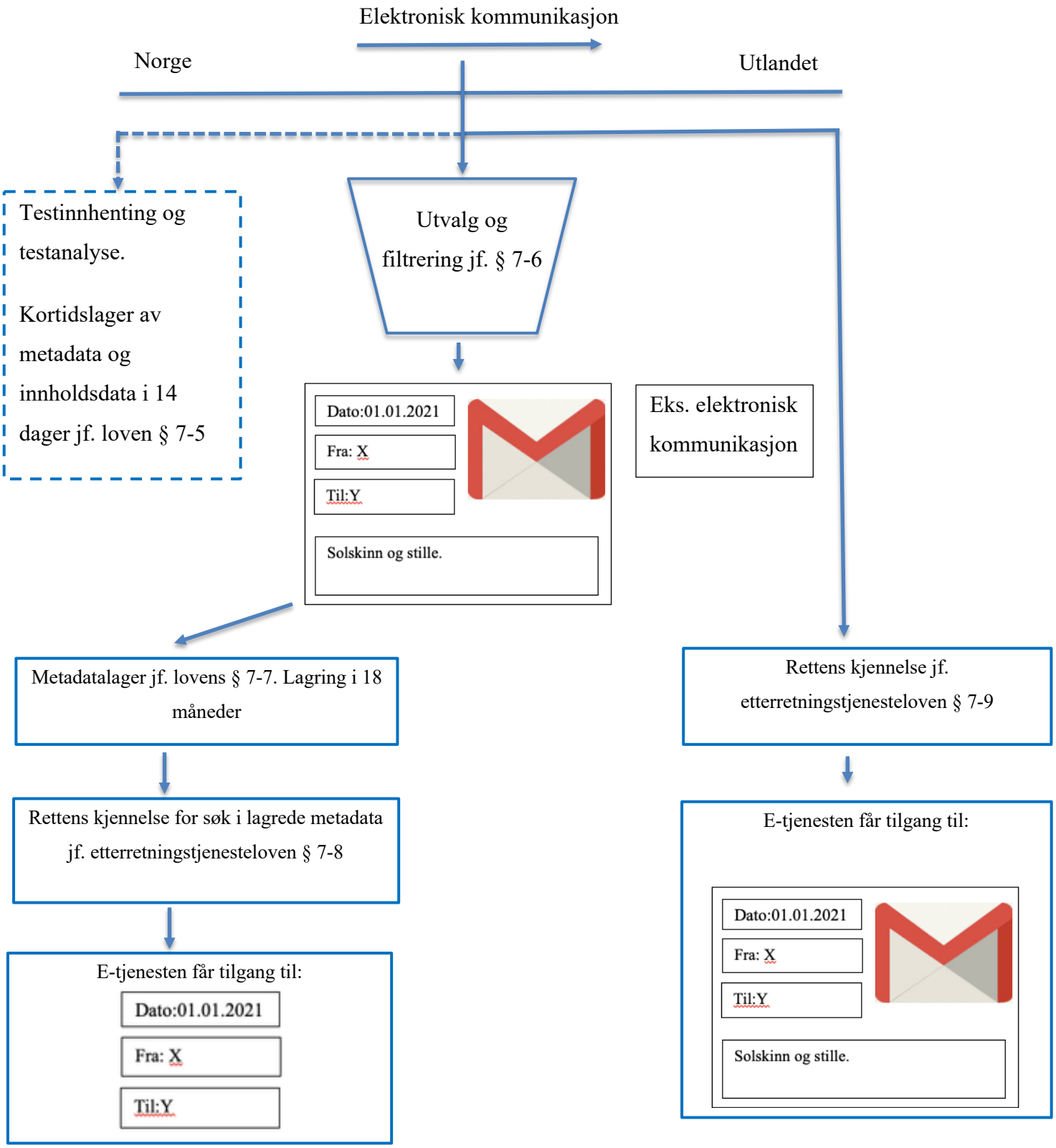
I etterretningstjenesteloven § 7-5 er etterretningstjenesten gitt et vidtgående skjønn til å filtrere ut hva som skal havne i metadatalagreret. Det er ikke oppstilt noen plikt til å filtrere metadataen utover å "søke" å filtrere bort innenlands kommunikasjon. Det vil si at Etterretningstjenesten med et forsøk på et filter kan sies å ha oppfylt vilkåret i § 7-5.

---

[143] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 215.
[144] Høringsnotatet pkt. 8.6.3.
[145] Digitalt grenseforsvar (DGF) Lysne II-utvalgets utredning til forsvarsdepartementet side 50.

4.9 Innhenting og lagring i bulk

Innhenting av metadata for lagring i bulk kan illustreres slik:



Figur 2: Egen illustrasjon over målsøking i lagret metadata og målrettet innhenting av innholdsdata.

Hjemmelen for lagring av metadata i bulk er etterretningstjenesteloven § 7-7. Etter utvalg og filtrering etter § 7-6, kan "Etterretningstjenesten innhente og lagre metadata i bulk om elektronisk kommunikasjon som transporteres over den norske grensen". Det er Etterretningstjenesten selv som beslutter lagring av metadata i bulk, jf. § 7-7. Selve lagringen er ikke avhengig av en forutgående prøvelse i Oslo tingrett.

Etterretningstjenesten skal lage og vedlikeholde en liste over hvilke typer metadata som kan lagres, jf. § 7-7 andre ledd. Denne listen har som formål å hindre lagringen av innholdsdata. Listen skal være tilgjengelig for EOS-utvalget og Nasjonal kommunikasjonsmyndighet, jf. etterretningstjenesteloven § 7-7 andre ledd andre punktum.

Lagringen kan skje i opptil 18 måneder, jf. § 7-7 tredje ledd. Deretter slettes rådataen. Etterretningsmessig interessant data kan lagres i 15 år, jf. etterretningstjenesteloven § 9-8 første ledd.

4.10 Søk i lagrede metadata

Etter etterretningstjenesteloven § 7-8 første ledd kan Etterretningstjenesten foreta søk i metadatalageret etter § 7-7 "innenfor rammen av rettens kjennelse etter kapittel 8". Slike søk skal baseres på søkebegreper. Materielle og prosessuelle vilkår for den forutgående domstolskontrollen vil bli behandlet sammen under pkt. 4.12.

Søk i lagrede metadata kan foretas av skikkede ansatte i Etterretningstjenesten som er utpekt av Etterretningssjefen. Søk kan kun foregå innenfor oppdragsporteføljen til vedkommende ansatt, jf. etterretningstjenesteloven § 7-7 andre ledd.

Det er to hovedtyper søkebegreper som kan brukes til søk i lagrede metadata, jf. etterretningstjenesteloven § 7-8. Disse er søk etter personselektor og søk etter modusselektor.[146]

En personselektor er en identifikator som kan benyttes for å søke frem til en person. Dette kan for eksempel være en IP-adresse, et brukernavn på Facebook eller lignende sosiale media, navn på en person, et kjent alias eller et telefonnummer. Hvis rettens kjennelse åpner for at

[146] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 217.

det kan søkes etter en bestemt person, vil det kunne søkes etter alle identifiserbare personselektorer knyttet til den bestemte personen i metadatalageret.

Verken lovteksten eller forarbeidene inneholder noen begrensninger i hvor mange ledd ut fra en personselektor det kan søkes etter i lagret metadata. En bruker av elektroniske kommunikasjonstjenester er i kontakt med en lang rekke andre brukere. I en undersøkelse gjennomført ved Stanford i 2016[147] indikeres det at søk i bulklagret metadata etter personselektor der søket gjøres to ledd ut fra personen det søkes etter, potensielt kan inkludere metadata om 25 000 individer. I etterettningstjenesteloven er slike søk ikke avgrenset til to ledd, og det er opp til rettens skjønn å avgrense antall ledd i personselektorsøket.[148]

Et modusselektorsøk er mer omfattende enn personselektorsøk. Modusselektor er en "selektor knyttet til et bestemt handlemønster, eksempelvis all kommunikasjon som orginerer fra en nærmere avgrenset geografisk lokasjon".[149]

Ved rettens kjennelse kan Etterretningstjenesten få hjemmel til målrettet søk i metadata i for eksempel elektronisk kommunikasjon fra et spesielt konfliktområde eller personer som har vært i kontakt med et telefonnummer eller IP-adresse til en nylig avslørt terrorist som den norske etterretningstjenesten har fått fra en samarbeidende tjeneste i et annet land.[150]

4.11 Målrettet innhenting og lagring av innholdsdata

I etterretningstjenesteloven § 7-9 er E-tjenesten gitt hjemmel til målrettet innhenting og lagring av innholdsdata. Slik målrettet innhenting fordrer en forutgående domstolsprøvelse av Oslo tingrett, jf. etterretningstjenesteloven § 7-9 første ledd første punktum.

Hjemmelen gir også adgang til å innhente og lagre metadataen som medfølger innholdsdataen.

---

[147] Mayer, J., Mutchler, P., & Mitchell, J. C. (2016). *Evaluating the privacy properties of telephone metadata. Proceedings of the National Academy of Sciences of the United States of America*, 113 (20), 5536-5541. https://doi.org/10.1073/pnas.1508081113
[148] Prop. 80 L (2019-2020) Lov om etterretningstjenesten pkt. 11.8.5.3 side 110).
[149] Digitalt grenseforsvar (DGF) Lysne II-utvalgets utredning til forsvarsdepartementet side 89.
[150] Høringsnotatet side 149

Innholdsdata er definert som data som ikke er metadata. Innholdsdata vil derfor være data som ikke fremgår av Etterretningstjenestens opplisting i listen E-tjenesten skal opprette og vedlikeholde etter etterretningstjenesteloven § 7-7 andre ledd.

Vilkårene i etterretningstjenesteloven i 5-2 må være oppfylt for at Etterretningstjenesten skal kunne innhente innholdsdata med tilhørende metadata.[151] Det vil si at Etterretningstjenesten må ha "konkrete holdepunkter" som "gir grunn til å undersøke om innhenting kan frembringe informasjon som er relevant for etterretningsformål", jf. etterretningstjenesteloven § 5-2. Ved målrettet innhenting etter loven § 7-9 brukes også personselektorer og modusselektrorer som søkebegreper.[152] Målrettet innhenting kan skje både mot identifiserte og uidentifiserte mål, men vilkåret i § 5-2 om "konkrete holdepunkter" må være oppfylt.

4.12 Forutgående domstolskontroll

4.12.1 Innledning

Både ved målsøk i metadatalageret etter etterretningstjenesteloven § 7-8 og ved målrettet innhenting av innholdsdata med tilhørende metadata etter lovens § 7-9, er det et krav om forutgående domstolskontroll etter etterretningstjenesteloven kapittel 8. Dette kapittelet vil gjennomgå materielle og prosessuelle vilkår for forhåndsgodkjennelsen.

Det presiseres at det ikke er et krav for forutgående domstolskontroll for selve lagring av metadata i bulk, jf. etterretningstjenesteloven § 7-7.

Oslo tingrett den eneste tingretten i Norge som behandler begjæringer etter etterretningstjenesteloven kapittel 8.[153] Kompetansen til å behandle slike begjæringer er samlet i Oslo tingrett for å legge til rette for en viss form for dommerspesialisering.[154]

4.12.2 Etterretningstjenestens begjæring

Etter etterretningstjenesteloven § 8-1 første ledd kan retten, det vil si Oslo tingrett, Borgarting lagmannsrett og Høyesterett, ved kjennelse gi Etterretningstjenesten adgang til søk i lagrede metadata, jf. etterretningstjenesteloven § 7-8 eller tilrettelagt innhenting og lagring av

[151] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 111.
[152] Høringsnotatet side 150.
[153] Se etterretningstjenesteloven § 8-2.
[154] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 118.

innholdsdata, jf. etterretningstjenesteloven § 7-9. Det kan gis vilkår i kjennelsen. Kjennelsen skal begrunnes og retten kan omgjøre kjennelsen.

Begjæringen for søk i lagrede metadata etter etterretningstjenesteloven § 7-8 eller målrettet innhenting av innholdsdata etter etterretningstjenesteloven § 7-9 skal være skriftlig og fremmes for Oslo tingrett av Etterretningstjenestesjefen eller den sjefen for E-tjenesten gir fullmakt, jf. etterretningstjenesteloven § 8-2 første ledd.

En slik begjæring skal etter etterretningstjenesteloven § 8-2 andre ledd oppgi hvilket oppdrag søket eller innhentingen gjøres som en del av, det faktiske og rettslige grunnlaget for begjæringen, hvilke søkebegreper eller kategorier av søkebegreper det dreier seg om hvis begjæringen gjelder søk i lagrede metadata, hvem innhentingen retter seg mot hvis begjæringen gjelder målrettet innhenting av innholdsdata og hvor lenge tillatelsen bør vare, jf. etterretningstjenesteloven § 8-6.

Retten skal treffe avgjørelse så raskt som mulig, jf. etterretningstjenesteloven § 8-1 andre ledd. En person som rammes av tilrettelagt innhenting skal ikke vite at han blir overvåket, da det kan føre til at kommunikasjonen blir tilpasset. Retten skal derfor ikke meddele kjennelsen for den søket eller innhentingen gjelder og berørte personer har heller ikke adgang til å uttale seg, jf. § 8-1 andre ledd andre punktum.

Kjennelsen skal meddeles E-tjenesten av retten og E-tjenesten skal gjøre kjennelsen og begjæringen tilgjengelig for EOS-utvalget, jf. etterretningstjenesteloven § 8-1 tredje ledd.

4.12.3 Rettens forhåndskontroll

Rettens prøving av begjæringen følger av etterretningstjenesteloven § 8-4. Etter første ledd "skal retten prøve om vilkårene etter denne loven er oppfylt".

Retten skal prøve om søket eller innhentingen ligger innenfor E-tjenestens oppgaver etter etterretningstjenesteloven kapittel 3, om forbudene i §§ 4-1, 4-8, 4-9 eller 9-4 er til hinder for søket eller innhentingen og om vilkårene for søk eller innhenting i kapittel 5 er oppfylt, jf. etterretningstjenesteloven § 8-4 andre ledd.

I forarbeidene antas det at siden Etterretningstjenestens har mange oppgaver etter kapittel 3 og fordi Etterretningstjenesten selv har best kontroll over sine oppgaver, så er det "ikke grunn til å tro at retten ofte vil overprøve tjenestens vurdering på dette punktet".[155]

Etterretningstjenesteloven oppstiller innhentingsforbud i § 4-1 (forbud mot innhenting mot personer i Norge), § 4-8 (forbud mot innhenting for politiformål), § 4-9 (forbud mot innhenting for å gi selskaper konkurransemessige fortrinn) og § 9-4 (diskrimineringsforbud).

Bestemmelsene i § 4-8 og § 4-9 er en negativ avgrensning av det som følger positivt av etterretningstjenesteloven kapittel 3. Det følger av etterretningstjenesteloven kapittel 3 at Etterretningstjenestens oppgaver er å drive utenlandsetterretning og ikke å være politi eller annen rettshåndhevende myndighet og heller ikke å drive med industrispionasje for norsk næringsliv.

Retten skal ikke gi tillatelse til søk i lagrede metadata eller tilrettelagt innhenting av innholdsdata hvis søket eller innhentingen strider mot diskrimineringsforbudet i etterretningstjenesteloven § 9-4. Hvis E-tjenesten i sin begjæring kun har angitt søkebegreper som utelukkende omhandler for eksempel etnisitet, religiøs bakgrunn eller seksuell orientering, skal ikke retten ta begjæringen til følge, jf. etterretningstjenesteloven § 9-4.[156]

Tilrettelagt innhenting av innholdsdata og søk i lagrede metadata må tilfredsstille grunnvilkårene for søk og for innhenting i etterretningstjenesteloven kapittel 5. Ved søk i lagrede metadata skal retten etter etterretningstjenesteloven § 8-4 prøve om "det er saklig grunn til å undersøke om innhenting kan frembringe informasjon som er relevant for etterretningsformål", jf. etterretningstjenesteloven § 5-1.

Ved målrettet innhenting av innholdsdata med tilhørende metadata skal retten prøve om det foreligger "konkrete holdepunkter" som gir grunn "til å undersøke om innhenting kan frembringe informasjon som er relevant for etterretningsformål", jf. etterretningstjenesteloven § 5-2.

I tillegg skal retten prøve om søket eller innhentingen er "et uforholdsmessig inngrep overfor den enkelte", jf. etterretningstjenesteloven § 5-4. I denne vurderingen skal det vurderes om

---

[155] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 220.
[156] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 221.

mindre inngripende tiltak kan ivareta formålet, inngrepets virkning for den som rammes, sakens betydning og forholdene ellers, jf. § 5-4 første ledd andre punktum.

4.12.4 Anke

Saksbehandlingen av begjæringer om målsøking etter metadata og tilrettelagt innhenting av innholdsdata reguleres verken av tvisteloven eller straffeprosessloven. Den rettslige prøvingen som ligner mest på begjæringer etter etterretningstjenesteloven, er forhåndsgodkjennelsen av straffeprosessuelle tvangsmidler som kommunikasjonskontroll og dataavlesning. Det fremgår derfor av etterretningstjenesteloven 8-9 andre ledd at reglene i straffeprosessloven kapittel 26 om anke over kjennelse "gjelder tilsvarende så langt de passer".

4.12.5 Hastekompetanse

I etterretningstjenesteloven § 8-10 er sjefen for Etterretningstjenesten gitt hjemmel for å treffe beslutning som kan tre i stedet for rettens kjennelse. Vilkårene for å treffe slik beslutning er at det "ved opphold er stor fare for at informasjon av vesentlig betydning for utførelsen av Etterretningstjenestens oppgaver etter kapittel 3, kan gå tapt." I motsetning til andre bestemmelser i kapittel 8, er kompetansen etter § 8-10 kun gitt til Etterretningstjenestesjefen og kompetansen kan ikke delegeres til andre tjenestepersoner i etterretningstjenesten.[157]

I forarbeidene presiserer at § 8-10 er ment å være "en meget snever unntaksregel som skal brukes med stor varsomhet".[158]

Dersom etterretningstjenestesjefen velger å benytte seg av denne hastekompetansen skal saken forelegges for retten for etterfølgende godkjennelse innen 24 timer, jf. etterretningstjenesteloven § 8-10 første ledd andre punktum.

Dersom retten ved slik etterfølgende kontroll kommer til at søket i metadatalageret eller innhentingen av innholdsdata var ulovlig, skal retten meddele dette til EOS-utvalget, jf. § 8-10 andre ledd andre punktum. Retten kan også pålegge Etterretningstjenesten å slette innhentet data dersom retten kommer til at innhentingen var ulovlig, jf. § 8-10 andre ledd tredje pkt.

---

[157] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 223.
[158] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 223.

4.12.6 Ordningen med særskilt advokat

I etterretningstjenesteloven § 8-5 første ledd første punktum er utgangspunktet og hovedregelen at retten etter å ha mottatt en begjæring skal "oppnevne en advokat som skal ivareta den enkeltes rettigheter og samfunnets interesser i saken". Oppnevnelse kan unnlates hvis retten finner det "ubetenkelig", jf. etterretningstjenesteloven § 8-5 første ledd andre punktum. I forarbeidene[159] fremgår det at "det må avgjøres konkret i hvilke situasjoner det er ubetenkelig å unnlate oppnevning". Forarbeidene nevner som et eksempel at det vil være ubetenkelig å ikke oppnevne en advokat for å verne samfunnet og den berørtes interesser dersom begjæringen gjelder innhenting av elektronisk kommunikasjon om en fremmed stat eller en fremmed statlig aktør.[160]

Advokaten må være sikkerhetsklarert etter sikkerhetsloven, og kan derfor kun oppnevnes fra en særskilt krets av sikkerhetsklarerte advokater, jf. § 8-5 første ledd tredje punktum.

Advokaten skal sette frem faktiske og rettslige argumenter, og kan peke på svakheter i Etterretningstjenestens begjæring.[161] Advokaten skal gjøres kjent med begjæringen og skal varsles før det avholdes rettsmøter og har rett til å uttale seg før det treffes avgjørelse i saken, jf. § 8-5 andre og tredje ledd.

Søk i metadatalageret og tilrettelagt innhenting og lagring av innholdsdata er svært teknisk og saken blir belyst gjennom en begjæring fra Etterretningstjenesten som også har en egeninteresse i at domstolen tar begjæringen til følge. Et flertall av høringsinstansene[162] tok derfor til orde for at retten burde ha mulighet til å kunne oppnevne en sakkyndig for å belyse tekniske forhold i begjæringen. En slik oppnevning skulle sørge for at domstolen hadde et bedre faktisk beslutningsgrunnlag og at domstolskontrollen derfor ble mer reell og uavhengig.

Forsvarsdepartementet avslo forslaget om mulighet for rettsoppnevnte sakkyndige som skulle bidra til sakens opplysning under denne henvisningen:

---

[159] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 221.
[160] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 221.
[161] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 221.
[162] Høringsinnstansene som ga uttrykk for et slikt syn var Advokatforeningen, Borgarting lagmannsrett, Den norske dataforening – IT-politisk råd, ICJ-Norge, dommerne Julsrud, Flaterud, Baumann, Horn, Heggdal og Selfors, Elektronisk Forpost Norge og Norges institusjon for menneskerettigheter (NIM), jf. Prop. 80 L (2019-2020) Lov om Etterretningstjenesten side 117.

"Det bør etter departementets syn holdes fast ved at det er Etterretningstjenesten som skal sørge for sakens opplysning. Teknisk innhenting innenfor utenlandsetterretning er en høyt spesialisert disiplin som av legitime grunner er skjermet, og det vil derfor være vanskelig å finne egnet sakkyndighet. Sikkerhetshensyn taler også mot å involvere flere aktører i saksbehandlingen. (...) Departementet legger til grunn at retten vil få et forsvarlig faktisk avgjørelsesgrunnlag gjennom den skriftlige begjæringen og uttalelsen fra den særskilte advokaten, eventuelt i kombinasjon med den supplerende informasjon fra tjenesten (...)".[163]

4.13 Kontroll

Stortingets kontrollutvalg for etterretnings-overvåknings- og sikkerhetstjenesten (EOS-utvalget) skal føre løpende kontroll over E-tjenestens innhenting av grenseoverskridende elektronisk kommunikasjon, jf. etterretningstjenesteloven § 7-11 første ledd.

Denne kontrollen skal blant annet undersøke om søk i lagret metadata kun skjer etter og i tråd med rettens kjennelser og at kortidslageret etter § 7-5 kun brukes til teknisk understøtte, jf. etterretningstjenesteloven § 7-11 første ledd.

EOS-utvalget skal ha tilgang til "all informasjon, interne retningslinjer og prosedyrer, lokaler, utstyr, programvare, filteroppdateringer, aktivitetslogger" som brukes i forbindelse med innhenting, jf. etterretningstjenesteloven § 7-11 andre ledd.

Hvis EOS-utvalget oppdager at det skjer innhenting eller søk i lagrede metadata i strid med bestemmelsene i etterretningstjenesteloven, kan EOS-utvalget fremme en begjæring til Oslo tingrett om stansing av innhentingen og at innhentet informasjon slettes. Før en slik begjæring fremmes for retten, skal E-tjenesten informeres og gis mulighet til selv å rette seg etter EOS-utvalgets syn, jf. etterretningstjenesteloven § 7-12.

EOS-utvalget skal også overprøve at Etterretningstjenesten opprettholder plikten til utvalg og filtrering, jf. etterretningstjenesteloven § 7-6. Utvalget skal meddeles rettens kjennelser av Etterretningstjenesten, jf. § 8-1 tredje ledd andre punktum for å kontrollere om innhentingen og målsøkene gjennomføres i samsvar med rettens forhåndstillatelse.

[163] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 118.

4.14 Overvåkningssamarbeid med andre hemmelige tjenester

I etterretningstjenesteloven § 4-8 er det oppstilt et forbud mot innhenting eller medvirkning til innhenting av grenseoverskridende elektronisk kommunikasjon for "å utføre oppgaver som tilligger politiet eller andre rettshåndhevende myndigheter". I etterretningstjenesteloven § 10-7 er det presisert at Etterretningstjenesten kan gi bistand til politiet i medhold av politiloven § 27 a, men at slik bistand ikke kan omfatte tilrettelagt innhenting.

Dette underkapittelet skal undersøke hvor grensen går mellom Etterretningstjenestens oppgaver etter kapittel 3, og "oppgaver som tilligger politiet eller andre rettshåndhevende myndigheter". Hvis for eksempel Etterretningstjenesten oppdager at et terrorangrep eller annen alvorlig kriminalitet er under planlegging, hvor går grensen mellom E-tjenesten og politiets ansvars- og oppgaveområder?

Etterretningstjenesten og PST har samarbeidet i mange år, og er etter den någjeldende samarbeidsinstruksen[164] pålagt å samarbeide på visse områder. Etter instruksen er PST og E-tjenesten pålagt å samarbeide om blant annet kontraterror og kontraetterretning.

Det er uklart hvor grensen mellom etterretningsformål etter kapittel 3 og forbudet mot innhenting for politiformål etter § 4-8 går. Klassiske straffbare handlinger som for eksempel narkotikasmugling vil klart være et politiformål og ikke et etterretningsformål. Ved andre mer tilgrensende områder mellom etterretning- og politiformål blir det vanskeligere. Etter etterretningstjenesteloven § 3-1 d) skal E-tjeneste forebygge og motvirke fremmed etterretningsvirksomhet i Norge. Etter politiloven § 17 b) nr. 2 skal PST også forebygge ulovlig etterretningsvirksomhet. Samme avgrensende oppgaveområde gjør seg også gjeldende ved grenseoverskridende terrorisme jf. etterretningstjenesteloven § 3-1 bokstav f) og politiloven § 17 b) nr. 5.

En mulig løsning på denne problemstillingen er at oppgaver som både tilligger Etterretningstjenesten og PST ikke er oppgaver med politiformål etter etterretningstjenesteloven § 4-8, men at oppgaver som kun tilligger PST er oppgaver med politiformål som ikke kan brukes som grunnlag for tilrettelagt innhenting.

---

[164] Instruks av 13. oktober 2006 nr. 1151 om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste (Samarbeidsinstruksen).

4.15 Overskuddsinformasjon

Hvis Etterretningstjenesten ved tilrettelagt innhenting for eksempel oppdager at en utenlandsk terrororganisasjon finansierer sin virksomhet ved salg av narkotika, salg av ulovlige kopier av merkeklær i Norge og hallikvirksomhet, oppstår spørsmålet om Etterretningstjenesten kan overlevere informasjon om den ulovlige virksomheten til politiet.

I etterretningstjenesteloven § 7-13 er det oppstilt et forbud mot utlevering av overskuddsinformasjon fra målsøking eller innhenting etter etterretningstjenesteloven kapittel 7. Hovedregelen er at etterretningstjenesten "ikke [skal] utlevere overskuddsinformasjon fra innhenting etter dette kapittelet", jf. etterretningstjenesteloven § 7-13 første ledd første punktum. Slik informasjon utløser ikke avvergings- eller opplysningsplikter etter annen lov, for eksempel avvergingsplikten etter barnevernloven, jf. 7-13 første ledd andre punktum.

Dette forbudet gjelder kun overskuddsinformasjon, det vil si informasjon som ikke er relevant for etterretningsformål. Informasjon relevant for etterretningsformål kan deles med PST og NSM etter vilkårene for informasjonsdeling i etterretningstjenesteloven kapittel 10.

I etterretningstjenesteloven § 7-13 andre ledd er det oppstilt et unntak fra utgangspunktet om forbud om deling av overskuddsinformasjon. Overskuddsinformasjon kan likevel utleveres i den utstrekning "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 handling". EOS- utvalget skal varsles om utlevering av slik overskuddsinformasjon, jf. etterretningstjenesteloven § 7-13 andre ledd.

I etterretningstjenesteloven § 7-14 er det også et bevisforbud i straffesaker. Det innebærer at informasjon innhentet etter kapittel 7 ikke kan brukes som grunnlag for ileggelse av straff eller andre strafferettslige reaksjoner. Et unntak fra dette er ved overtredelse av straffeloven § 131 (terrorhandlinger), jf. etterretningstjenesteloven § 7-14 siste pkt.

5 Skranker for tilrettelagt innhenting etter EMK

5.1 Innledning

Dette kapittelet skal behandle den norske etterretningstjenestelovens bestemmelser om tilrettelagt innhenting om grenseoverskridende elektronisk kommunikasjon opp mot EMK art. 8 og relevant rettspraksis fra EMD, for å undersøke om lovens kapitler om bulklagring av metadata for etterretningsformål er et rettmessig inngrep i EMK art. 8 som verner offentlige inngrep i privat- og familielivet.

EMK art. 8 har slik ordlyd:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.".

Kapittelet vil i først behandle spørsmålet om i hvilken grad bulklagring av metadata for etterretningsformål utgjør et inngrep i EMK art. 8. Deretter vil vilkårene som må være oppfylt for at inngrepet i EMK art. 8 likevel er rettmessig etter EMK art. 8 nr. 2 presenteres. Det vil først redegjøres generelt om vilkårene om klart rettsgrunnlag, legitimt formål og nødvendighet i EMK art. 8 nr. 2, før det vil foretas en sammenligning av EMDs vurdering av hvert av disse vilkårene i to kammeravgjørelser om bulklagring, *Centrum för rättvisa mot Sverige* og *Big Brothers Watch mot Storbritannia.* Begge disse kammeravgjørelsene om bulklagring er anket inn til storkammer, men storkammerdommene er ennå ikke avsagt. Det er derfor nødvendig med inngående analyser av disse to kammeravgjørelsene. Etter redegjørelsen for vilkårene om klart rettsgrunnlag, legitimt formål og at inngrepet må være nødvendig i et demokratisk samfunn, vil avhandlingen behandle disse vilkårene opp mot de materielle reglene om tilrettelagt innhenting i etterretningstjenesteloven.

5.2 I hvilken grad utgjør bulklagring et inngrep i EMK art. 8?

EMK art. 8 slår fast at enhver har krav på respekt for sitt privat- og familieliv, sitt hjem og sin korrespondanse. EMK inneholder ikke noe eget særskilt vern for behandling av

personopplysninger, men EMD har utviklet EMK art. 8 slik at bestemmelsen også inneholder et slikt vern.[165] Etter EMDs praksis skal ikke ordlyden "privatliv" i EMK art. 8 tolkes restriktivt, men tolkes slik at vernet etter bestemmelsen inkluderer beskyttelsen av opplysninger som kan knyttes til et identifisert eller identifiserbart individ.[166]

Overvåkning utført av hemmelige tjenester inkluderer innsamling og systematisering av opplysninger og personopplysninger av et individ. Innsamling og lagring av metadata har tradisjonelt vært ansett som mindre personvernsensitivt enn innsamling og lagring av innholdsdata, men EMD har uttalt at ikke bare personopplysninger i tradisjonell forstand som er vernet etter EMK art. 8, det er tilstrekkelig at opplysningen muliggjør identifiseringen av et individ.[167] Vernet av metadata under EMK art. 8 ble særskilt behandlet av EMD i Big Brothers Watch-saken. I kammeravgjørelsen kom EMD til at metadata kan være like så sensitivt som innholdsdata og uttalte at metadata:

> "(…) could reveal the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. In bulk, the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location, tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with".[168]

EMD uttalte også at innholdsdata kan være kryptert og at metadata derfor ofte er eneste mulighet til å finne ut avsender og mottaker av kommunikasjonen i vurderingen av vernet av metadata under EMK art. 8.[169]

Omfattende statlig lagring av metadata om elektronisk kommunikasjon i 18 måneder, der brukerne av ekomnett ikke har visshet om deres kommunikasjon er underlagt lagring eller ikke, utgjør klart et inngrep i EMK art. 8. Dette ble lagt til grunn av EMD i både *Centrum för rättvisa*[170] og *Big Brothers Watch mot Storbritannia*[171]. Siden disse avgjørelsene er henvist til storkammerbehandling og storkammeravgjørelsene ikke er avsagt, hersker det en viss

---

[165] Se for eksempel EMDs dom i saken *Rotaru mot Romania* [GC], ECHR:2000:0504JUD002834195.
[166] Se *Amann mot Sveits* [GC], ECHR:2000:0216JUD002779895 avsnitt 65).
[167] Se *P. og S. mot Polen* [J], ECHR:2012:1030JUD005737508 avsnitt 130).
[168] *Big Brothers Watch* avsnitt 356).
[169] *Big Brothers Watch* avsnitt 356).
[170] *Centrum för rättvisa* mot Sverige (J).
[171] *Big Brothers Watch mot Storbritannia*.

uklarhet om hvilket vern EMD kommer til å legge til grunn i storkammerdommene. På grunnlag av tidligere EMD-praksis[172] er det likevel høyst sannsynlig at EMD vil legge samme vurderingstema til grunn i storkammerdommene og avhandlingen vil derfor vurdere de norske reglene om tilrettelagt innhenting i etterretningstjenesteloven kapittel 7 opp mot vurderingstemaene som ble lagt til grunn i de to kammeravgjørelsene.

5.3 Kravet til klart rettsgrunnlag

5.3.1 Utgangspunkter

Etter EMK art. 8 nr. 2 må et inngrep i EMK art. 8 være "in accordance with the law". Det fremgår av EMDs praksis at EMK art. 8 nr. 2 ikke inneholder et krav om at inngrepet må følge av et vedtak fra det lovgivende organet i medlemsstaten, lovkravet innebærer at inngrepet må være hjemlet i et rettsgrunnlag som oppfyller nasjonale krav til hjemmelsgrunnlag for et slikt type inngrep.[173] I vilkåret om at et inngrep må være "in accordance with the law" har EMD i veletablert rettspraksis stilt opp minimumskrav som skal sikre at inngrepet er i tråd med rettsstatlige grunnprinsipper.[174] Dette kravet innebærer at rettsgrunnlaget for inngrepet må være tilgjengelig og forutberegnelig.[175]

Krav om at et rettsgrunnlag som åpner for inngrep i EMK art. 8 må være tilgjengelig og forutberegnelig innebærer et krav om at det skal være mulig å forutse i hvilke tilfeller man blir utsatt for et inngrep fra en offentlig myndighet. Når inngrepet i EMK art. 8 har et atferdsregulerende formål, der ikke-oppfyllelse av inngrepet får en negativ konsekvens for et individ, gjør kravene til et tilgjengelig og forutberegnelig rettsgrunnlag seg særskilt gjeldende.[176] Når inngrepet ikke har et atferdsregulerende formål, slik som informasjonsinnhenting, er kravet til et tilgjengelig og forutberegnelig rettsgrunnlag først og fremst begrunnet i behovet for legalitetskontroll med inngrepet.[177]

---

[172] Se for eksempel *Roman Zakharov mot Russland* og *Weber og Saravia mot Tyskland* [J], ECHR:2006:0629DEC005493400.
[173] *Silver mot Storbritannia* [J], ECHR:1983:0325JUD000594772 avsnitt 86).
[174] Se *Roman Zakharov mot Russland* avsnitt 227 med videre henvisninger.
[175] *Roman Zakharov mot Russland* avsnitt 227).
[176] Se Fause, Anett Beatrix Osnes «Kravet til legalitet, nødvendighet og proporsjonalitet når det utøves polisiær eller påtalemessig myndighet som griper inn i vernet etter EMK art. 8 nr. 1», *Tidsskrift for strafferett* 2014/1, Juridika https://juridika.no/tidsskrifter/tidsskrift-for-strafferett/2014/1/artikkel/fause
[177] Se Aall, Jørgen "Rettsstat og menneskerettigheter" side 105.

Ved etterretning og annen informasjonsinnhenting i hemmelige tjenester er det et naturlig behov for hemmelighold. EMDs har derfor uttalt at det gjelder egne krav til forutberegnelighet i relasjon til hemmelig overvåkning.[178] En hjemmel for hemmelig overvåkning skal ikke gjøre det mulig for borgerne å forutberegne i hvilke tilfeller myndighetene vil overvåke kommunikasjon til hvert enkelt individ, da det ville det gjøre det mulig å tilpasse kommunikasjonen.[179] EMD uttaler likevel at ved hemmelig overvåkning er risikoen for misbruk til stede, og hjemmelen for overvåkning må derfor ha klare, detaljerte bestemmelser om når slik overvåkning kan skje for å gi individet et tilstrekkelig vern mot vilkårlige inngrep.[180]

For å forhindre vilkårlige inngrep i EMK art. 8 har EMD i langvarig og konsistent rettspraksis om hemmelig overvåkning stilt opp seks mimimumsvilkår en lov om hemmelig tvangsbruk, herunder hemmelig informasjonsinnhenting må oppfylle. Disse seks vilkårene ble første gang formulert i dommen *Huvig mot Frankrike*[181], og kalles derfor Huvigvilkårene. Vilkårene benyttes også ved innhenting av metadata i bulk.[182]

Etter Huvigvilkårene må et rettsgrunnlag som hjemler hemmelig informasjonsinnhenting ha bestemmelser som klargjør hvilke personkategorier som kan bli utsatt for overvåkning og bestemmelser om hvilke etterretningsgrunner som kan gi grunnlag for å starte overvåkning. Videre må hjemmelsgrunnlaget avgrense overvåkningens varighet og ha regler om hvilke prosedyrer og hvilken prosess som kan gi grunnlag for overvåkning. Til sist må slike lover ha bestemmelser om sletting av overvåkningsdata og bestemmelser om uavhengig kontroll og varsling til berørte personer.[183]

I det følgende vil disse vilkårene for klart rettsgrunnlag analyseres med utgangspunkt i de to kammeravgjørelsene om bulklagring, *Centrum för rättvisa mot Sverige* og *Big Brothers Watch mot Storbritannia.* I begge disse avgjørelsene har menneskerettighetsorganisasjoner i Sverige og Storbritannia klaget nasjonale bulklagringsregler inn for EMD fordi

---

[178] Se *Roman Zakharov mot Russland* avsnitt 299).
[179] *Roman Zakharov mot Russland* avsnitt 299-300).
[180] *Roman Zakharov mot Russland* avsnitt 299-300).
[181] *Huvig mot Frankrike* [J], ECHR:1990:0424JUD001110584
[182] Se *Weber og Saravia mot Tyskland* der EMD for første gang anvendte Huvigvilkårene for innformasjonsinnhenting i bulk. Se videre *Roman Zakharov mot Russland*, *Centrum för rättvisa mot Sverige* og *Big Brothers Watch mot Storbritannia* som alle henviser til disse retningslinjene.
[183] *Huvig mot Frankrike* avsnitt 34)

organisasjonene mener at deres organisasjonsvirksomhet kan være berørt av bulklagring.[184] I begge avgjørelsene ble innføringen av et bulklagringssystem ansett som et inngrep i EMK art. 8, men at innføringen av slike regler lå innenfor statenes skjønnsmargin.[185] De svenske reglene ble ansett for å være et rettmessig inngrep i EMK art. 8, mens dommen i saken *Big Brothers Watch mot Storbritannia* endte med at Storbritannia ble dømt for å ha krenket EMK art. 8. Avhandlingen vil foreta en deskriptiv innrettet undersøkelse av hvorfor kravet om klart rettsgrunnlag ble vurdert forskjellig av EMD i de to dommene. En sammenligning av faktum i de to dommene er nødvendig for å identifisere hvorfor det ble to ulike utfall i sakene, og en sammenligning av disse to dommene er helt nødvendig for en presis undersøkelse av det norske systemet. Den britiske loven som medførte at Storbritannia ble dømt for å ha krenket EMK art. 8 er senere endret og vil derfor bli omtalt i preteritum i det følgende.

5.3.2 Rettsgrunnlagets tilgjengelighet

5.3.2.1 EMDs vurdering i *Centrum för rättvisa mot Sverige*

I Centrum för rättvisa var ikke lovens tilgjengelighet problematisert av partene, og EMD konstaterte derfor bare at loven var publisert og tilstrekkelig tilgjengelig for allmennheten.[186]

5.3.2.2 EMDs vurdering i *Big Brothers Watch mot Storbritannia*

I Big Brothers Watch-saken anførte klagerne at britisk bulklovgivning var fragmentarisk regulert i forskjellige lover, svært komplisert og bulkovervåkning i realiteten var regulert i ikke-offentlige direktiver og instrukser. EMD anerkjente i sin vurdering av lovgivningens tilgjengelighet at konvensjonsstatene har et berettiget behov for hemmelighold av detaljer, men at hovedtrekkene av et bulkovervåkningsregime må fremgå av offentlig lovgivning.[187] EMD sa seg enig med klagerne at den britiske bulkovervåkningsloven, RIPA, var ekstremt komplisert, men at dette hadde mer å gjøre med lovens forutberegnelighet og hvorvidt loven var nødvendig, heller en at lovens fragmentariske karakter og kompleksitet var relevant i relasjon til rettsgrunnlagets tilgjengelighet.[188]

---

[184] Se *Centrum för rättvisa* avsnitt 6) og *Big Brothers Watch* avsnitt 8).
[185] *Centrum för rättvisa* avsnitt 104 og *Big Brothers Watch* avsnitt 308).
[186] *Centrum för rättvisa* avsnitt 115).
[187] *Big Brothers Watch* avsnitt 325).
[188] *Big Brothers Watch* avsnitt 325).

5.3.3 Virkeområdet til den nasjonale overvåkningsloven

5.3.3.1 EMDs vurdering i *Centrum för rättvisa mot Sverige*

EMD begynte sin vurdering av den svenske lovens virkeområde, med å slå fast at en lov om hemmelig informasjonsinnhenting må ha et angitt virkeområde som gir befolkningen forutberegnelighet om i hvilke tilfeller de kan bli utsatt for overvåkning, herunder også bulklagring.[189]

Etter den svenske loven om försvarsunderrättelsesverksamhet[190] og den svenske loven om signalspaning i fôrsvarsunderrättelsesverksamhet[191] kan den svenske signaletterretningstjenesten bruke signaletterretning og lagring om metadata i bulk som etterretningsmetode for utenlandsetterretning. Grenseoverskridende metadata kan lagres i bulk i 12 måneder etter svensk rett. Søk og analyse i lagret metadata kan ikke brukes som metode av hensyn til kriminalitetsbekjempelse eller iretteføring av straffbare handlinger, slik analyse kan kun benyttes for ivaretakelse av nasjonale sikkerhetsinteresser. Bare elektronisk kommunikasjon som krysser grensen ut av Sverige kan bulklagres. Myndigheten til å foreta signaletterretning er lagt til Forsvarets radioanstalt (FRA). FRA kan foreta signaletterretning på lagret metadata etter en kjennelse fra den svenske signaletterretningsdomstolen.[192] Signaletterretning kan kun skje innenfor rammene av denne kjennelsen, som kan omhandle et fenomen, situasjon eller spesielt utvalgte personer.[193] Etter den svenske signaletterretningsloven kan slik signaletterretning kun skje på grunnlag av typiske etterretningstrusler som militære trusler mot Sverige, internasjonal terrorisme, og fremmede etterretningsoperasjoner mot svenske interesser.[194] Den svenske signaletterretningsdomstolen kan bare ta begjæringen til følge dersom oppdraget ligger innenfor formålene i den svenske signaletterretningsloven, dersom formålet med etterretningsopperasjonen ikke kan oppfylles på en mindre inngripende måte og hvis oppdraget kan resultere i informasjon som har større verdi enn de negative konsekvensene av innhentingen.[195] Den svenske signaletterretningsloven inneholder bestemmelser om uavhengig etterfølgende kontroll av at

[189] *Centrum för rättvisa* avsnitt 118).
[190] Lagen om försvarsunderrättelsesverksamhet (2000:130).
[191] Lagen om signalspaning i fôrsvarsunderrättelsesverksamhet (2008:717).
[192] *Centrum för Rättvisä* avsnitt 9).
[193] *Centrum för rättvisä* avsnitt 9) med videre henvisninger.
[194] *Centrum för Rättvisä* avsnitt 12).
[195] *Centrum för Rättvisä* avsnitt 19).

FRA ikke har innhentet metadata og annen data utenfor tillatelsen de er gitt og at innhentingstillatelser er gitt av signaletterretningsdomstolen i tråd med svensk lov.[196]

Den svenske loven åpner for bulkovervåkning i åtte tilfeller. Selv om noen av disse tilfellene har en generell ordlyd, er formålene utdypet i forarbeidene til loven. EMD kom derfor til at formålene som kunne åpne for bulkovervåkning var tilstrekkelig angitt i svensk rett.[197] I vurderingen av om den svenske loven avgrenset bulkovervåkning i tilstrekkelig grad, hensyntok EMD at kun metadata om grenseoverskridende elektronisk kommunikasjon kunne lagres.[198] EMD konkluderte derfor med at svensk rett avgrenset virkeområde til bulklagringen med tilstrekkelig klarhet.[199]

5.3.3.2 EMDs vurdering i *Big Brothers Watch mot Storbritannia*

I EMDs vurdering om britisk lov definerte virkeområdet til bulkinnhenting i tilstrekkelig grad i Big Brothers Watch, tok EMD utgangspunkt i forskjellen på målrettet innhenting og bulkinnhenting. Ved målrettet innhenting må adgangen til å innhente informasjon fra kommunikasjonsnettverk være strengt avgrenset fordi det er nærliggende å anta at all den innhentede informasjonen vil være gjenstand for etterretningsanalyse.[200] Ved bulkinnhenting la EMD til grunn at adgangen til å innhente informasjon fra kommunikasjonsnettverk kan angis bredere enn ved målrettet innhenting fordi det knytter seg strengere vilkår til bruk og analyse av bulkinnhentet informasjon. EMD la videre til grunn at det britiske bulklagringssystemet besto av fire faser: i) innhenting av kommunikasjon fra internettkabler som har størst sannsynlighet for å inneholde utenlandsk kommunikasjon med etterretningsverdi, ii) automatisk filtrering av den innhente kommunikasjonen for å filtrere ut innenlandsk data, iii) automatisk selektorsøk i den resterende dataen der data som inneholder relevante søkeord blir lagret, mens irrelevant data blir slettet, iv) undersøkelse av etterretningsrelevant data av etterretningsanalytikere.[201]

EMD vurderte først hvorvidt britisk lov inneholdt tilstrekkelig klare vilkår for når den britiske signaletterretningstjenesten kunne utstede et direktiv for søk i lagret metadata. Etter britisk lov kunne søk i lagret metadata kun skje hvis en minister i den britiske regjeringen godkjente

---

[196] *Centrum för rättvisä* avsnitt 36).
[197] Centrum *för* rättvisa avsnitt 120).
[198] *Centrum för rättvisä* avsnitt 121).
[199] *Centrum för rättvisä* avsnitt 124).
[200] *Big Brothers Watch* avsnitt 329).
[201] *Big Brothers Watch* avsnitt 329).

at et slikt søk var nødvendig av hensyn til nasjonal sikkerhet, bekjempelse av alvorlig kriminalitet eller beskyttelse av kritisk infrastruktur. Søket måtte være proporsjonalt, i denne proporsjonalitetsvurderingen skulle det vurderes om informasjonen kunne innhentes på en mindre inngripende måte.[202] I vurderingen om disse vilkårene for søk i lagret metadata ga individ tilstrekkelig forutberegnelighet, kom EMD under henvisning til tidligere praksis at trusler mot nasjonal sikkerhet ofte er vanskelige å definere uttømmende på forhånd. EMD kom derfor til at den britiske loven ga individene en tilstrekkelig og adekvat indikasjon om i hvilke tilfeller den britiske signaletterretningstjenesten kunne søke i lagret metadata.[203]

EMD vurderte deretter om britisk rett regulerte hvilke persongrupper som kunne bli utsatt for bulklagring- og bulkinnhenting med tilstrekkelig klarhet. Den britiske loven åpnet kun for signaletterretning mot utenlandsk kommunikasjon og det ekskluderte i prinsippet kommunikasjon mellom to personer der begge oppholdt seg på de britiske øyer. EMD uttalte at britisk lov i realiteten åpnet for innhenting av innenlandsk kommunikasjon på grunn av plassering av servere i utlandet. EMD vektla likevel at det ikke var vilkårlig hvilken kommunikasjon som ble innhentet. Signaletterretningstjenesten hadde ikke ubegrenset myndighet til å innhente hvilken som helst kommunikasjon, og bulkinnhenting skulle kun etableres på grenseoverskridende kabler, innhentingen måtte begrunnes i et legitimt formål og inngrepet måtte være proporsjonalt.[204] EMD kom til at det er en naturlig regulering av et bulklagringssystem at etterretningstjenesten har bred myndighet til å selv avgjøre hvilke kommunikasjonsnettverk som skal være gjenstand for lagring og rutiner for filtrering av innenlandsk kommunikasjon. EMD konkluderte deretter med at inngrepet i EMK art. 8 er mer alvorlig ved selektorsøk i lagret metadata og ved analyse i innhentet data. EMD kom derfor til at det må stilles strengere krav individets rettssikkerhetsgarantier ved selektorsøk og etterretningsanalyse på lagret metadata enn ved lagring og filtrering av metadata.[205]

5.3.4 Overvåkningens varighet

5.3.4.1 EMDs vurdering i *Centrum för rättvisa mot Sverige*

Etter svensk lovgivning kan signaletterretningsdomstolen godkjenne søk i lagret metadata etter søkebegreper i til sammen seks måneder. Tillatelsen kan forlenges av domstolen etter

[202] *Big Brothers Watch* avsnitt 331).
[203] *Big Brothers Watch* avsnitt 336).
[204] *Big Brothers Watch* avsnitt 337).
[205] *Big Brothers Watch* avsnitt 338).

disse seks månedene i ytterligere seks måneder, men det fordrer en ny prøvelse av om vilkårene er oppfylt.[206] EMD kom til at varigheten av en overvåkningstillatelse er en del av konvensjonsstatenes skjønnsmargin så lenge nasjonal lovgivning inneholder tilstrekkelige rettssikkerhetsgarantier knyttet til fornyelse og avbrudd av tillatelser.[207] EMD konkluderte med at svensk rett hadde tilstrekkelige rettssikkerhetsgarantier knyttet til varighet, fornyelse og avbrudd av overvåkningstillatelser.[208]

5.3.4.2 EMDs vurdering i *Big Brothers Watch mot Storbritannia*

Etter britisk rett kunne en forhåndsgodkjennelse for søk i lagret metadata av hensyn til nasjonal sikkerhet vare i seks måneder, og en forhåndsgodkjennelse med kriminalitetsbekjempelse som formål kunne ha en varighet på tre måneder.[209] Godkjennelsen kunne fornyes før de gikk ut. Signaletterretningstjenesten måtte avbryte et søk dersom søket ikke lenger var nødvendig. EMD fant at plikten til å avbryte søket når det ikke lenger var nødvendig medførte at overvåkningstillatelsene var under kontinuerlige vurdering. EMD fant derfor at britisk rett hadde tilstrekkelige rettsikkerhetsgarantier knyttet til overvåkningstillatelsenes varighet.

5.3.5 Prosedyrer for forhåndsgodkjennelse

5.3.5.1 EMDs vurdering i *Centrum för rättvisa mot Sverige*

Etter svensk rett må den svenske signaletterretningsdomstolen gi forhåndstillatelse før signaletterretningstjenesten kan søke i lagret metadata. Lederen av signaletterretningsdomstolen er fast ansatt dommer, mens de andre medlemmene er utnevnt av den svenske regjeringen i en fireårsperiode. Signaletterrettningsdomstolen er uavhengig av den svenske regjeringen, parlamentet og forsvaret.[210] Alle rettsmøter i den svenske domstolen og alle avgjørelser er underlagt absolutt hemmelighet og blir ikke offentliggjort, heller ikke statistikk på antallet gjennomførte rettsmøter eller tildelte overvåkningstillatelser.[211] I de fleste saker i den svenske etterretningsdomstolen er en juridisk representant for offentligheten tilstede, en såkalt "privacy protection representative", denne representanten representer ikke

[206] *Centrum för rättvisa* avsnitt 128).
[207] *Centrum för rättvisa* avsnitt 127).
[208] *Centrum för rättvisa* avsnitt 130).
[209] *Big Brothers Watch* avsnitt 358).
[210] *Centrum för rättvisa* avsnitt 134).
[211] *Centrum för rättvisa* avsnitt 135).

enkeltpersoner, kan kun uttale seg under rettsmøte og har ikke rett til å anke en overvåkningstillatelse.[212]

Begjæringen fra den svenske etterretningstjenesten til signaletterretningsdomstolen om forhåndsgodkjennelse må inneholde opplysninger om hvilke operasjon søket skal skje som en del av, behovet for søk i lagret metadata, hvilke ekomtilbydere som blir berørt og hvilke søkeord etterretningstjenesten skal benytte.[213] Etterretningstjenesten i Sverige har også en hastekompetanse til å selv beslutte søk i lagret metadata i, men må snarest mulig sende inn denne tillatelsen til domstolen for etterfølgende kontroll. Domstolen kan omgjøre tillatelsen og beordre sletting av resultatene av søket gjennomført på grunnlag av hastekompetansen.[214]

EMD begynte sin vurdering av de svenske reglene om forhåndsgodkjennelse med å vise til tidligere rettspraksis om at det ikke er et krav om uavhengig juridisk forhåndsgodkjennelse av en domstol for overvåkningstillatelser.[215] En uavhengig forhåndskontroll ved en domstol er likevel etter menneskerettighetsdomstolens oppfatning den beste typen kontroll, fordi den sikrer uavhengighet og upartiskhet. Forhåndskontroll ved en uavhengig domstol minimerer etter EMDs syn best risikoen for vilkårlig overvåkning og at etterretningstjenesten går utenfor sine hjemler.[216]

EMD var kritisk til at offentlighetens representant ikke hadde ankeadgang over en overvåkningstillatelse, men mente at tilstedeværelsen av en slik representant i rettsmøtene er med på å minimere risikoen for uhjemlede tillatelser.[217] EMD mente videre at de svenske reglene for forhåndskontroll av overvåkningstillatelser var en viktig rettssikkerhetsgaranti for misbruk av innhentet metadata og fant at de svenske reglene om forhåndskontroll ga individet et tilstrekkelig vern for misbruk. EMD mente også at den etterretningstjenestens hastekompetanse var legitim fordi en slik midlertidig tillatelse måtte sendes inn til etterretningsdomstolen for etterfølgende kontroll snarest mulig.[218]

---

[212] *Centrum för rättvisa* avsnitt 137).
[213] *Centrum för rättvisa* avsnitt 139).
[214] *Centrum för rättvisa* avsnitt 140).
[215] *Centrum för rättvisa* avsnitt 133).
[216] *Centrum för rättvisa* avsnitt 133).
[217] *Centrum för rättvisa* avsnitt 138).
[218] *Centrum för rättvisa* avsnitt 138).

5.3.5.2 EMDs vurdering i *Big Brothers Watch mot Storbritannia*

Britisk rett inneholdt ikke regler om uavhengig forhåndsgodkjennelse av søk i lagret metadata, og en minister i den britiske regjeringen kunne autorisere slike søk på begjæring fra den britiske signaletterretningstjenesten.

EMD var svært kritisk til at forhåndsgodkjennelser av søk i lagret metadata ofte var svært generelt utformet, for eksempel kunne etterretningstjenesten få autorisasjon til å søke i innhentet metadata etter "material providing intelligence on terrorism".[219] EMD mente at slik generelle søkeord gjorde forhåndskontrollen til en lite effektiv rettssikkerhetsgaranti. EMD uttalte deretter: "In a bulk interception regime, where the discretion to intercept is not significantly curtailed by the terms of the warrant, the safeguards applicable at the filtering and selecting for examination stage must necessarily be more robust".[220] EMD hadde tidligere funnet at rettssikkerhetsgarantiene knyttet til filtrering av innhenting data ikke var robust. EMD konkluderte deretter med at den britiske forhåndskontrollen var for avhengig av etterretningstjenesten selv til å utgjør en effektiv rettssikkerhetsgaranti mot misbruk.[221]

5.3.6 Prosedyrer for lagring, tilgang, analyse og sletting av data

5.3.6.1 EMDs vurdering i *Centrum för rättvisa mot Sverige*

I vurderingen av om svensk rett inneholdt tilstrekkelige klare regler for lagring, tilgang, analyse og sletting av innhentet metadata vektla EMD at etterretningspersonellet som håndterte dataen var sikkerhetsklarert, hadde en straffesanksjonert taushetsplikt og hadde lang opplæring.[222] EMD vektla videre at den svenske overvåkningsloven inneholder regler om umiddelbar sletting av personlige data som var irrelevant for etterretningsoperasjonen, data underlagt pressens kildevern, advokatkorrepondanse og data gitt under religiøst skriftemål.[223] EMD kom videre til at svensk rett åpnet for lagring av rådata i bulk i ett år, men at denne dataen var ubehandlet informasjon som EMD mente det var nødvendig å lagre av hensyn til at bulklagrinssystemet skulle fungere effektivt. EMD fant etter en helhetlig vurdering at svensk

[219] *Big Brothers Watch* avsnitt 342).
[220] *Big Brothers Watch* avsnitt 346).
[221] *Big Brothers Watch* avsnitt 347).
[222] *Centrum för rättvisa* avsnitt 144).
[223] *Centrum för rättvisa* avsnitt 145).

rett inneholdt tilstrekkelig rettssikkerhetsgarantier vedrørende lagring, tilgang, analyse og sletting av innhentet data.[224]

5.3.6.2 EMDs vurdering i *Big Brothers Watch mot Storbritannia*

Etter britisk lov kunne bare analyse av innhentet data skje etter at metadataen hadde vært gjenstand for automatisk filtrering. Hvilke søketermer som kunne brukes måtte fremgå av forhåndsgodkjennelsen av en minister i den britiske regjeringen.[225] Før en etterrettningsanalytiker kunne analysere lagret metadata, måtte analytikeren skrive et notat der det ble redegjort for hvorfor det var nødvendig med tilgang, hvorvidt oppdraget kunne skje på en mindre inngripende måte og om inngrepet var proporsjonalt.[226] I likhet med svensk rett, måtte personalet som skulle analysere innhentet metadata være sikkerhetsklarert og var underlagt en streng straffesanksjonert taushetsplikt. Britisk lov inneholdt vilkår om at metadataen skulle lagres så sikkert som mulig.[227] EMD kom til at de britiske reglene om lagring, tilgang, analyse og sletting av metadata var tilstrekkelig klare og utgjorde en effektiv rettssikkerhetsgaranti.[228]

5.3.7 Delingsadgang

5.3.7.1 EMDs vurdering i *Centrum för rättvisa mot Sverige*

Etter svensk rett kan innhentet metadata deles med andre land og internasjonale organisasjoner når den svenske regjeringen mener det er nødvendig, så lenge det ikke skader svenske interesser.[229] EMD var bekymret fordi denne delingsadgangen var vidt angitt og ga lite forutberegnelighet, likevel mente EMD at en slik regulering lå innenfor det akseptable.[230]

5.3.7.2 EMDs vurdering i *Big Brothers Watch mot Storbritannia*

Etter den britiske overvåkningsloven skulle informasjondeling av innhentet metadata holdes på et absolutt minimum, det vil si at kun etterretningstjenesten som utgangspunkt skulle ha tilgang. Innhentet data kunne deles med påtalemyndigheten dersom det var grunn til å tro at en person ikke ville få en rettferdig rettergang hvis etterretningstjenesten unnlot å dele

---

[224] *Centrum för rättvisa* avsnitt 147).
[225] *Big Brothers Watch* avsnitt 361).
[226] *Big Brothers Watch* avsnitt 361).
[227] *Big Brothers Watch* avsnitt 363).
[228] *Big Brothers Watch* avsnitt 364).
[229] *Centrum för rättvisa* avsnitt 150).
[230] *Centrum för rättvisa* avsnitt 150).

informasjonen.[231] Innhentet data kunne deles med allierte land hvis det var nødvendig av hensyn til Storbritannias interesser. EMD fant at britisk lov hadde tilstrekkelige rettssikkerhetsgarantier knyttet til deling av innhentet data.

5.3.8 Regler for etterfølgende kontroll

5.3.8.1 EMDs vurdering i *Centrum för rättvisa mot Sverige*

EMD begynte sin vurdering av de svenske reglene om etterfølgende kontroll ved bulkinnhenting med å oppstille en regel om at etterfølgende kontroll helst bør skje ved en uavhengig domstol, men at slik kontroll også kan skje ved et administrativt organ hvis dette organet er uavhengig av etterretningstjenesten og har tilstrekkelige kompetanse og myndighet til å foreta en effektiv kontroll.[232] I EMDs kontroll over et slik kontrollorgans uavhengighet, undersøker EMD særskilt på hvordan medlemmer av kontrollorganet blir utnevnt og hvilken kompetanse slike medlemmer har. Aller helst ser EMD at medlemmer av et slik kontrollorgan blir utnevnt av parlamentet. Videre kontrollerer EMD hvorvidt etterretningstjenesten gir kontrollorganet tilgang til all relevant informasjon og hvilke handlingsalternativer og kompetanse organet har hvis det oppdager ulovligheter.[233]

Etter svensk rett blir medlemmene av kontrollorganet utnevnt av det svenske parlamentet, og lederen og nestledere av kontrollorganet må ha juridisk kompetanse. EMD fant at organet derfor var tilstrekkelig uavhengig av etterretningstjenesten. Kontrollorganet har som oppgave å kontrollere hvilke søkebegreper som blir brukt for søk i lagret metadata, sletting av innhenting data og deling av innhentet data. Kontrollorganet har tilgang til alle dokumenter som etterretningstjenesten har tilgang til og skal føre kontroll over at søk ikke foretas utenfor det kjennelsen fra etterretningsdomstolen åpner for.[234] EMD fant at denne kontrollen var effektiv og reell både i teori og i praksis, og at de svenske reglene ga individet et tilstrekkelig vern for misbruk av innhentet metadata i bulk.[235]

5.3.8.2 EMDs vurdering i *Big Brothers Watch mot Storbritannia*

I Storbritannia foregikk kontrollen over bulkinnhenting på flere nivåer. Det første kontrollnivået besto av advokater og tjenestemenn i departementet som ga forhåndstillatelser

---

[231] *Big Brothers Watch* avsnitt 365).
[232] *Centrum för rättvisa* avsnitt 153).
[233] *Centrum för rättvisa* avsnitt 154 og 155).
[234] *Centrum för rättvisa* avsnitt 157).
[235] *Centrum för rättvisa* avsnitt 158).

til søk i lagret metadata. Dette var en løpende kontroll der tjenestemenn kontrollerte at overvåkningstillatelser ikke ble gitt dersom de ikke var nødvendig og forholdsmessige.[236] Videre ble overvåkningstillatelsene kontrollert av et ombud som rapporterte til statsministeren dersom det ble oppdaget at signaletterretningstjenesten gjennomførte søk i lagret metadata uten tillatelse.[237]

EMD har gjennom langvarig praksis om etterfølgende kontroll av overvåkning stilt krav om at kontrollorganet må være tilstrekkelig uavhengig av den utøvende makt. I Big Brothers Watch uttalte EMD at vurderingen av kontroll over overvåkningstillatelser må ta utgangspunkt i innhentingssystemet som en helhet, herunder om det eksisterer noen bevis på at systemet faktisk blir misbrukt eller benyttet tilfeldig og vilkårlig.[238] Deretter vurderte EMD britisk rett dithen til at det ikke var noen bevis for at overvåkning skjedde ulovlig eller irregulært. EMD godtok derfor det britiske kontrollsystemet og uttalte at kontrollnivået i Storbritannia ga individet tilstrekkelig vern mot misbruk, selv om EMD var kritisk til kontrollsystemets uavhengighet.[239]

5.3.9 Underretning til berørte personer

5.3.9.1 EMDs vurdering i *Centrum för rättvisa mot Sverige*

Etter svensk lov er det et krav om at personer som har blitt utsatt for et søk i lagret metadata skal underrettes om hvilke søkebegreper som er brukt, når søket fant sted og hvorfor det ble gjennomført et slikt søk. En slik underretning skal gis når slik underretning ikke lenger vil ødelegge etterretningsoperasjonen. Kravet om underretning gjelder ikke når den svenske signaletterretningstjenesten har et berettiget behov for hemmelighold. Dette siste vilkåret har ført til at det aldri har blitt gitt en slik underretning.[240]

EMD uttalte at det ikke eksisterer et absolutt krav om at det må gis underretning til berørte personer etter en etterretningsoperasjon og begrunnet dette med at slike operasjoner ofte er svært langvarige, at underretning kan avsløre hemmelige metoder og agenter og i ytterste konsekvens ødelegge etterretningsoperasjoner.[241] EMD var likevel kritisk til at svensk rett

---

[236] *Big Brothers Watch* avsnitt 375).
[237] *Big Brothers Watch* avsnitt 378).
[238] *Big Brothers Watch* avsnitt 377).
[239] *Big Brothers Watch* avsnitt 381).
[240] *Centrum för rättvisa* avsnitt 165).
[241] *Centrum för rättvisa* avsnitt 164).

hadde et krav om underretning til berørte personer, men at slik underretning aldri hadde blitt gitt. EMD uttalte at en prosessuell rettssikkerhetsgaranti skal være praktisk og effektiv og ikke teoretisk og illusorisk.[242] EMD bestemte seg derfor for å behandle kravet om underretning til berørte personer sammen med kravet om at berørte personer må ha tilstrekkelige rettsmidler til å få behandlet spørsmålet om det har blitt utsatt for hemmelig overvåkning. EMDs behandling av dette spørsmålet i *Centrum för rättvisa* presenteres under pkt. 5.3.10.

Britisk rett inneholdt ikke et krav om underretning til personer som hadde blitt utsatt for et søk i lagret metadata. Spørsmålet ble derfor ikke behandlet i Big Brothers Watch-saken.

5.3.10 Rettsmidler

5.3.10.1 EMDs vurdering i *Centrum för rättvisa mot Sverige*

I EMDs vurdering av om svensk rett inneholdt tilstrekkelige rettsmidler for dem som mener seg utsatt for ulovlig overvåkning vurderte EMD både rettsmidler særskilt for bulkinnhenting og generelle rettsmidler på overvåkningsområdet. I praksis var det ikke mulig for et individ å bli informert om de hadde blitt utsatt for bulklagring eller etterfølgende etterretningsanalyse i Sverige. Individet kunne likevel klage til kontrollorganet for bulkinnhenting og få svar på om innhentingen var lovlig eller ikke. I totalvurderingen av rettsmidler i Sverige hensyntok EMD også klageadgangen til sivilombudsmannen og det svenske datatilsynet. EMD fant at disse rettsmidlene til sammen var tilstrekkelig. EMD støttet denne konklusjonen ved å vise til rettssikkerhetsgarantiene knyttet til hele bulkinnhentingssystemet og særlig til at rettssikkerhetsgarantiene knyttet til autorisasjon i søk var robuste.[243]

5.3.10.2 EMDs vurdering i *Big Brothers Watch mot Storbritannia*

Etter britisk rett kan enhver som mener seg utsatt for ulovlig overvåkning klage til ombudet ansvarlig for å kontrollere overvåkningstillatelsene for søk i lagret metadata. Dette ombudet hadde myndighet til å gjennomføre offentlige høringer og gi kompensasjon i form av erstatning dersom de fant at et individ har vært utsatt for uhjemlede søk i lagrede metadata.[244]

---

[242] *Centrum för rättvisa* avsnitt 166).
[243] *Centrum för rättvisa* avsnitt 178).
[244] *Big Brothers Watch* avsnitt 379).

EMD konkluderte med at denne ordningen var et tilstrekkelig rettsmiddel og ga individet vern mot misbruk.[245]

5.4 Legitimt formål

5.4.1 Generelle utgangspunkter

For at et inngrep i EMK art. 8 ikke skal føre til at konvensjonsstaten har krenket EMK art. 8, må inngrepet forfølge et av de legitime formålene oppstilt i EMK art. 8 nr. 2. I EMK art. 8 nr. 2 er ivaretakelse av nasjonal sikkerhet nevnt som et legitimt formål. "The prevention of disorder or crime" er opplistet i EMK art. 8 nr. 2 som et annet legitimt formål.

5.4.2 EMDs vurderinger av legitimt i Centrum för rättvisa mot Sverige og Big Brothers Watch mot Storbritannia

EMK art. 8 nr. 2 nevner beskyttelse av nasjonal sikkerhet som et legitimt formål som kan begrunne inngrep i EMK art. 8. Hverken i *Centrum för rättvisa mot Sverige* eller *Big Brothers Watch mot Storbritannia* behandler EMD kravet om at inngrepet må forfølge et legitimt formål. EMDs manglende fokus på dette kan begrunnes i at EMD foretar en mer prosessuell prøving i saker om hemmelig overvåkning, der den tradisjonelle tretrinns-testen med prøving av rettsgrunnlagets klarhet, legitimt formål og en nødvendighetsvurdering heller blir formulert som en prosessuell vurdering av om det eksisterer tilstrekkelige prosessuelle rettssikkerhetsgarantier mot misbruk.[246]

5.5 Nødvendighet

Et inngrep i EMK art. 8 må være "necessary in a democratic society", jf. EMK art. 8 nr. 2 for at inngrepet skal være rettmessig.

Etter EMDs rettspraksis må et inngrep i EMK art. 8 være nødvendig ut fra et "pressing social need"[247] Videre følger det av rettspraksis fra EMD at inngrepet må være "proportionate to the legitimate aim pursued".[248] Vurderingen av om inngrepet er nødvendig i et demokratisk samfunn tas først av konvensjonsstaten, EMDs kontroll er først og fremst en kontroll over om

---

[245] *Big Brothers Watch* avsnitt 383).
[246] Vogiatzoglou, Plixavra. "Centrum for Rattvisa v Sweden: Bulk Interception of Communications by Intelligence Services in Sweden Does Not Violate the Right to Privacy." European Data Protection Law Review (EDPL), vol. 4, no. 4, 2018, p. 563-567. HeinOnline.
[247] Se for eksempel *Yefimenko mot Russland* [J], ECHR:2013:0212JUD000015204 avsnitt 142).
[248] *Yefimenko mot Russland* avsnitt 142).

begrunnelsen konvensjonsstaten har gitt for inngrepet i EMK art. 8 er "relevant and sufficient".[249]

I saken Big Brothers Watch uttalte EMD at på området for hemmelig overvåkning er tradisjonelt EMD forsiktig med å overprøve konvensjonsstatenes vurderinger av om overvåkningsloven er nødvendig i et demokratisk samfunn. Samtidig uttalte EMD at: "a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it (…)".[250] EMDs kontroll er derfor særlig fokusert på om de nasjonale reglene om overvåkning inneholder tilstrekkelige rettssikkerhetsgarantier slik at inngrepet avgrenses på en slik måte at overvåkning kun skjer i den grad det er nødvendig i et demokratisk samfunn.[251]

5.6 Proporsjonalitet

5.6.1 Utgangspunkter

I EMK art. 8 nr. 2 fremgår det at inngrepet må være "nødvendig i et demokratisk samfunn". I denne ordlyden har EMD i sin praksis tolket nødvendighetskravet slik at det også inneholder et krav om at inngrepet må være proporsjonalt. I saken *Sporrong og Lönnroth mot Sverige* fremhevet EMD at det i alle de relative rettighetsbestemmelsene i EMK foreligger en "fair balance" mellom "the demands of the general interest of the community and the requirements of the protection of the individual's fundamental rights".[252]

I 2015 ble endringsprotokoll nr. 15[253] til EMK åpnet for ratifikasjon av Europarådets medlemsland, endringsprotokollen trer i kraft 1. august 2021.[254] Etter ratifikasjon av denne endringsprotokollen inneholder EMK subsidiaritetsprinsippet og prinsippet om en statlig skjønnsmargin. Denne protokollen skal tydeliggjøre at EMD ikke er en fjerdeinstansdomstol. I etterkant av ratifikasjonen av denne protokollen har det skjedd et skifte i EMDs praksis der EMD i større grad har beveget seg mot en mer prosessuell kontroll i vurderingen av et

[249] *Yefimenko mot Russland* avsnitt 142).
[250] *Big Brothers Watch* avsnitt 308).
[251] Big Brothers Watch avsnitt 308-309).
[252] *Sporrong og Lönnroth mot Sverige* [J] ECHR:1982:0923JUD000715175 avsnitt 69).
[253] Protocol No. 15 amending the Convention on the Protection of Human Rights and Fundamental Freedoms.
[254] EMDs nettsider: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/213 (30.04.21)

inngreps proporsjonalitet.[255] Når EMD vurderer rettmessigheten av en nasjonal lov som utgjør et inngrep i EMK art. 8, følger det av rettspraksis fra EMD at EMD må vurdere de legislative grunnene bak inngrepet.[256] I denne vurderingen tildeler EMD statene en skjønnsmargin. I vurderingen av om konvensjonsstaten har holdt seg innenfor denne skjønnsmarginen foretar EMD en kontroll av om lovgivningsprosessen bak inngrepet har vært rettferdig og om denne prosessen har tatt tilstrekkelig hensyn til individets rettigheter etter EMK art. 8. I denne vurderingen prøver EMD spesielt om individet har tilstrekkelige prosessuelle rettssikkerhetsgarantier.[257]

EMDs kontroll over proporsjonalitet til et inngrep under vilkåret "nødvendig i et demokratisk samfunn" har derfor utviklet seg fra å være en kontroll over om det foreligger en rettferdig balanse mellom individets rettigheter og allmennhetens behov for inngrep, til i større grad bli en prosessuell kontroll over hvilke rettssikkerhetsgarantier konvensjonsstaten har tildelt den enkelte. Til dette vil jeg bemerke at den statlige skjønnsmarginen ikke kan brukes av konvensjonsstatene selv for å begrunne inngrep i EMK art. 8, det er kun EMD som kan hensynta den statlige skjønnsmarginen.[258]

5.6.2 EMDs vurderinger av nødvendighet i *Centrum för rättvisa mot Sverige* og *Big Brothers Watch mot Storbritannia*

EMD foretok en særskilt vurdering om bulkinnhenting er nødvendig i et demokratisk samfunn i Big Brothers Watch-saken. I Centrum för rättvisa behandlet EMD svenske regler om bulkinnhenting opp mot de seks Huvigkriteriene uten å behandle nødvendighet og proporsjonalitet særskilt.

I proporsjonalitetsvurderingen i Big Brothers Watch-saken viste EMD til Veneziakommisjonens vurdering av bulkovervåkning. Veneziakommisjonen er et permanent organ i Europarådet som gir rådgivende anbefalinger til utvikling av lover til Europarådets medlemsland.[259] Veneziakommisjonen har anerkjent bulkovervåkning som nødvendig i et demokratisk samfunn fordi et slikt system proaktivt kan fange opp ukjente trusler mot

---

[255] Se Huijbers, Leonie M, " The European Court of Human Rights' procedural approach in the age of subsidiarity" i Cambridge International Law Journal, 2017, Vol. 6 No. 2, side. 177–201
[256] Se for eksempel *A.-M.V. mot Finland* ECHR:2017:0323JUD005325113 avsnitt 82).
[257] Se *A.-M.V. mot Finland* avsnitt 83-84).
[258] EMDs storkammerdom av 19. februar 2009 i saken A mot Storbritannia avsnitt 194).
[259] https://snl.no/Europarådet#-Venezia-kommisjonen (30.03.2021)

nasjonalstatenes sikkerhet.[260] EMD sa seg enig i Veneziakommisjonens vurderinger og anerkjente bulklagring som nødvendig i et demokratisk samfunn på grunn av truslene fra internasjonal terrorisme og alvorlig kriminalitet.[261]

5.7 Hvorfor ble resultatet krenkelse av EMK art. 8 i *Big Brothers Watch mot Storbritannia*, men ikke i *Centrum för rättvisa mot Sverige*?

I Centrum för rättvisa kritiserte EMD noen deler av det svenske bulklagringssystemet. EMD var kritisk til at advokaten oppnevnt for å tale allmennhetens sak i rettsmøter om bulkinnhenting ikke hadde rett til å anke overvåkningstillatelsene. Videre mente EMD at vilkåret om underretning i den svenske loven var en ineffektiv rettssikkerhetsgaranti på grunn av at underretning aldri hadde blitt gitt til noen berørte personer. Til tross for disse manglene anerkjente EMD den svenske loven som et rettmessig inngrep i EMK art. 8 fordi helheten av systemet ikke hadde alvorlige mangler. EMD fant at den svenske loven hadde klare og detaljerte regler om innhenting, at det var en viktig rettssikkerhetsgaranti at overvåkningstillatelser ble gitt av en uavhengig domstol og at det ble ført uavhengig kontinuerlig kontroll over slike tillatelser.[262]

I Big Brothers Watch fant EMD også at innføringen av et bulkinnhentingssystem lå klart innenfor Storbritannias skjønnsmargin. EMD hadde heller ingen konkrete holdepunkter for å konkludere med at Storbritannia misbrukte systemet eller innhentet metadata og kommunikasjonsdata i større omfang enn det loven åpnet for. Ved undersøkelsen av om rettsgrunnlaget som hjemlet bulkinnhenting oppfylte Huvigvilkårene fant EMD likevel flere mangler. Gjennomgående mente EMD at det var for lite uavhengig kontroll av tillatelser om søk i lagret metadata. Det britiske bulkinnhentingssystemet sett som en helhet inneholdt for få og for få effektive prosessuelle rettssikkerhetsgarantier til at EMD kunne anerkjenne inngrepet i EMK art. 8 som nødvendig i et demokratisk samfunn. Resultatet ble derfor at EMD dømte Storbritannia for å ha krenket EMK art. 8.[263]

Dommen i *Big Brothers Watch mot Storbriannia* ble avsagt tre måneder etter dommen i saken *Centrum för rättvisa mot Sverige*. Likevel henviser ikke Big Brothers Watch til den tidligere

---

[260] *Big Brothers Watch* avsnitt 385).
[261] *Big Brothers* Watch avsnitt 386).
[262] *Centrum för rättvisa* avsnitt 180).
[263] *Big Brothers Watch* avsnitt 387-388).

dommen om samme tema en eneste gang. På grunn av en mulig inkonsekvens mellom de to dommene er begge dommene henvist til storkammerbehandling, og slik behandling er gjennomført uten at det er avsagt dom per 3. mai 2021. Det er likevel trolig at storkammerdommene vil behandle de nasjonale lovene opp mot Huvigvilkårene. Hvilket beskyttelsesnivå som blir resultatet etter behandling av EMD i storkammer gjenstår å se.

5.8 Er tilrettelagt innhenting utformet i tråd med EMK art. 8?

5.8.1 Utgangspunkter for analysen

Både Big Brothers Watch og Centrum för rättvisa behandler spørsmålet om en nasjonal lov som sådann er et rettmessig inngrep i EMK art. 8. Disse lovene er vedtatt av demokratiske forsamlinger i henholdsvis Storbritannia og Sverige. Dommerne i EMD er ikke demokratisk valgt. For at EMDs behandling skal ha legitimitet, har EMD i sin overprøving foretatt en prosessuell prøving av om de nasjonale rettsgrunnlagene har tilstrekkelige rettssikkerhetsgarantier til å forhindre misbruk av overvåkningsordningene.

Ivaretakelsen av forpliktelsene EMK legger på konvensjonsstatene skal først og fremst skje på nasjonalt nivå. EMDs kontroll er en subsidiær kontroll.[264] Den resterende delen av analysen vil ha konvensjonsstatens fokus. Det vil si at de prosessuelle minstegarantiene oppstilt av EMD på overvåkningsområdet vil utgjøre utgangspunktet for analysen av etterretningstjenesteloven kapittel 7, men at analysen vil hensynta at disse kravene er minimumskrav oppstilt av en domstol som har foretatt en subsidiær kontroll av demokratiske valgte lover. Et inngrep i EMK art. 8 er likefullt et inngrep uavhengig av om inngrepet er omringet av prosessuelle rettssikkerhetsgarantier.

5.8.2 Følger tilrettelagt innhenting av et tilstrekkelig klart rettsgrunnlag?

5.8.2.1 Er rettsgrunnlaget som hjemler tilrettelagt innhenting tilstrekkelig tilgjengelig?

I Centrum för rättvisa slo EMD fast at den svenske loven var tilstrekkelig tilgjengelig. Tilrettelagt innhenting er vedtatt i lovs form i Etterretningstjenesteloven kapittel 7 og anses derfor for å være tilstrekkelig tilgjengelig for allmennheten.

[264] *Big Brothers Watch* avsnitt 244).

5.8.2.2 Angir etterretningstjenesteloven kapittel 7 virkeområdet til tilrettelagt innhenting tilstrekkelig?

En nasjonal overvåkningslov skal gi borgerne en adekvat indikasjon om i hvilke tilfeller de kan bli utsatt for informasjonsinnhenting.[265] Den forutgående analysen av *Big Brothers Watch mot Storbritannia* og *Centrum för rättvisa mot Sverige* har vist at EMD har en ulik tilnærming til vurderingen av angivelsen av virkeområdet i de to overvåkningsloven. I Big Brothers Watch foretok EMD en vurdering av forutberegneligheten til overvåkningssystemet basert på de fire fasene i et bulkovervåkningssystem. I Centrum för rättvisa foretok EMD en mer overordnet vurdering av de svenske reglene vurdert som en helhet. I det følgende vil forutberegneligheten til de norske reglene bli vurdert ut fra om reglene gir norske borgere en adekvat indikasjon av i hvilke tilfeller de kan bli utsatt for innhenting. Analysen vil ha sitt hovedfokus på hjemmelen for lagring av metadata og hjemmelen for tilgang til lagret metadata.

Etter etterretningstjenesteloven § 7-2 første ledd gjelder tilretteleggingsplikten for ekomtilbydere og for "tilbydere av internettbaserte kommunikasjons- eller meldingstjenester som er tilgjengelige for allmennheten". Denne ordlyden overlater i stor grad opp til Etterretningstjenestens skjønn hvilke tilbydere som kan bli underlagt tilretteleggingsplikt. Et stort antall apper og internett-tjenester kan sies å ha kommunikasjonsformål, for eksempel kan allmennkringkastere og nettaviser omfattes av ordlyden i etterretningstjenesteloven § 7-2 første ledd.[266] Forarbeidene presiserer ikke om denne ordlyden omfatter både nasjonale og internasjonale tilbydere og avgrenser i liten grad hva som menes med internettbaserte kommunikasjons- og meldingstjenester. Slik etterretningstjenesteloven § 7-2 første ledd er vedtatt gir den borgerne liten forutberegnelighet for hvilke datastrømmer som kan bli underlagt tilretteleggingsplikt.

I etterretningstjenesteloven § 4-1 første ledd fremgår det et utgangspunkt om at etterretningstjenesten ikke har som oppgave å drive informasjonsinnhenting og etterretning mot personer i Norge. Etter etterretningstjenesteloven § 7-1 kan Etterretningstjenesten iverksette tilrettelagt innhenting i form av lagring av metadata i bulk om kommunikasjon som transporteres over den norske grensen. Drøftelsen i kapittel 3 viser at om lag 70 % av innenlandsk kommunikasjon passerer landegrensen. Selv om etterretningstjenesten har en

[265] Se *Roman Zakharov mot Russland* avsnitt 243).
[266] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 113.

lovbestemt plikt til å filtrere ut innenlandsk kommunikasjon, eksisterer det per lovens vedtakstidspunkt ingen effektiv måte å foreta slik filtrering på. Disse forholdene sett i sammenheng fører til at Etterretningstjenesten vil innhente store datamengder om individer i Norge, selv om etterretningstjenesten ikke har som oppgave å innhente informasjon om norske borgere. Det avhenger av tilfeldigheter om metadata om internettbruk fra norske borgere blir lagret i bulk, slik som om internettbruken blir rutet om Sverige. Slik loven er utformet, er det derfor grunnlag for å hevde at det er vanskelig for et individ i Norge å forutberegne hvilke persongrupper og i hvilke situasjoner man kan bli utsatt for innhenting i form av bulklagring av metadata. Slik tilrettelagt innhenting er forutsatt å fungere kan loven støte an mot kravet til forutberegnelighet oppstilt i EMDs praksis under EMK art. 8 nr. 2.

Slik tilrettelagt innhenting er vedtatt i etterretningstjenesteloven kapittel 7 innebærer det en selvmotsigelse. Etterretningstjenesteloven § 4-1 første ledd slår fast at E-tjenesten ikke skal innhente, det vil også si lagre, informasjon om norske borgere. Likevel fremgår det av forarbeidene til kapittel 7 at det allikevel skjer fordi det "ikke finnes realistiske alternativer for å filtrere ut ikke-relevant informasjon fra datasettene".[267] Et skille mot grenseoverskridende data er et kunstig skille som gir liten forutberegnelighet for om man blir utsatt for informasjonsinnhenting.

Etterretningstjenesteloven inneholder regler om forhåndskontroll ved Oslo tingrett før etterretningstjenesten kan søke i lagret metadata. Oslo tingrett skal prøve om søket ligger innenfor e-tjenestens oppgaver og om det er saklig grunn til å undersøke om innhenting kan frembringe informasjon som er relevant for etterretningsformål", jf. etterretningstjenesteloven § 5-1. Ordlyden "saklig grunn til å undersøke" og "frembringe informasjon som er relevant" er vag og overlater mye av rettsanvendelse til Etterretningstjenestens skjønn. Ordlyden gir ikke et klart svar på hvilken sannsynlighetsovervekt som må foreligge for at retten kan autorisere søket. Metadataen er lagret av Etterretningstjenesten selv og e-tjenesten må derfor søke om å få tilgang til noe de allerede har tilgang til. Når etterretningstjenestens begjærer tilgang til noe de allerede har tilgang til, kan det skape en risiko for misbruk. Forhåndskontrollen skal minimere denne risikoen. Når denne forhåndskontrollen knytter seg til et vagt grunnvilkår, kan det stilles spørsmål ved om kontrollen vil utgjøre en reell kontroll. Dette skjønnsmessige grunnvilkåret kan også gjøre at inngrepet i EMK art. 8, lagring av

[267] Høringsnotatet- Forslag til ny etterretningstjenestelov av 12.11.2018 pkt. 8.6.2, side 137.

metadata og søk og analyse i den lagrede dataen, ikke følger av et forutberegnelig rettsgrunnlag.

5.8.2.3 Avgrenser etterretningstjenesteloven overvåkningstillatelsenes varighet på en tilstrekkelig forutberegnelig måte?

Kjernen av EMDs kontroll av overvåkningstillatelsers varighet er om tillatelsene har tilstrekkelige forutberegnelige regler for avbrudd og forlengelse av tillatelsene. Etter etterretningstjenesteloven § 8-6 kan rettens kjennelse for søk i lagret metadata ikke overstige ett år. Siden etterretningstjenesteloven inneholder klare regler for fornyelse og avbrudd av tillatelser i kapittel 8 og siden EMD i Centrum för rättvisa kom til at overvåkningstillatelsenes varighet var opp til statenes skjønnsmargin så lenge varigheten var innrammet av klare regler, konkluderes det med at de norske reglene om overvåkningstillatelsenes varighet gir et tilstrekkelig vern mot misbruk.

5.8.2.4 Inneholder norsk rett tilstrekkelige prosedyrer for forhåndsgodkjennelse av søk i lagret metadata?

I analysene av *Big Brothers Watch mot Storbritannia* og *Centrum för rättvisa mot Sverige* ser man at EMD foretrekker en uavhengig og upartisk forhåndskontroll av overvåkningstillatelser ved en domstol. Samtidig uttaler EMD at en prosessuell rettssikkerhetsgaranti skal være praktisk og effektiv og ikke teoretisk og illusorisk.[268] I artikkelen "Noen utviklingstrekk i norsk kriminalpolitikk basert på 40 år i påtalemyndigheten" omtaler tidligere riksadvokat Tor-Aksel Busch forhåndskontroll av straffeprosessuelle tvangsmidler, han skriver: "Ingen vil formentlig protestere på at domstolskontroll er av avgjørende betydning i en rettsstat. Men det er ikke tilstrekkelig å etablere slike ordninger; det avgjørende vil være domstolenes mulighet for realitetskontroll. Inngrepshjemler må lages og utformes slik at domstolsprøvningen blir effektiv og reell."[269]

Etter etterretningstjenesteloven § 8-4 skal forhåndskontrollen av målsøk i lagret metadata ved Oslo tingrett prøve om søket ligger innenfor etterretningstjenestens oppgaver, om søket hindres av et innhentingsforbud og om "det er saklig grunn til å undersøke om innhenting kan frembringe informasjon som er relevant for etterrettningsformål", jf. etterretningstjenesteloven § 5-3 jf. § 5-2.

---

[268] *Centrum för rättvisa* avsnitt 166).
[269] Busch, Tor-Aksel «Noen utviklingstrekk i norsk kriminalpolitikk basert på 40 år i påtalemyndigheten», Tidsskrift for strafferett 2018/4, Juridika

De alminnelige domstolene er ikke ukjent med forhåndskontroll av tvangsmidler, heller ikke hemmelige tvangsmidler. I forhåndskontrollen av tvangsmidler etter straffeprosessloven prøver domstolen om det er skjellig grunn til mistanke. Det er en kjent størrelse for domstolene å overprøve. Vilkåret "saklig grunn til å undersøke" legger etter sin ordlyd ikke opp til en kjent terskel som er lett å overprøve. Forarbeidene inneholder heller ingen konkretisering eller veiledning om hva som utgjør "saklig grunn til å undersøke".

Når Oslo tingrett for første gang skal overprøve om det foreligger "saklig grunn til å undersøke om innhenting kan frembringe informasjon som er relevant for etterretningsformål" har de en vag inngrepshjemmel, lite veiledning i forarbeidene for hvor terskelen skal ligge og de blir opplyst av Etterretningstjenesten som har interesse av at begjæringen blir tatt til følge. Selv om domstolskontroll er den mest uavhengige formen for forhåndskontroll, er den norske etterretningstjenesteloven § 8-4 mer en teoretisk og illusorisk enn reell og effektiv forhåndskontroll.

5.8.2.5 Har norsk rett tilstrekkelige prosedyrer for lagring, tilgang, analyse og sletting av innhentet data?

Kjernen i EMDs kontroll over nasjonale regler om lagring, tilgang, analyse og sletting er at de nasjonale regler skal verne mot vilkårlig tilgang til lagret metadata, usikker lagring og misbruk som for eksempel snoking i innhentet data. Etterretningstjenesteloven inneholder regler om straffesanksjonert taushetsplikt, logging, sletting av innhentet data og sikker lagring av data. De norske reglene om lagring, tilgang, analyse og sletting av innhentet metadata anses derfor for å gi tilstrekkelig vern mot misbruk og vilkårlighet.

5.8.2.6 Har etterretningstjenesteloven tilstrekkelige regler for etterfølgende kontroll av overvåkningstillatelser?

Hoveddelen av EMDs overprøving av nasjonale regler om etterfølgende kontroll av overvåkningstillatelser er om kontrollen er lagt til et organ tilstrekkelig uavhengig av Etterretningstjenesten og at dette organet har tilstrekkelig kompetanse og tilgang til informasjon til å foreta en effektiv kontroll. Som et ledd av vurderingen av kontrollorganets effektivitet hensyntas også hvilken myndighet kontrollorganet har, for eksempel om organet har myndighet til å beordre stans eller sletting av innhenting.

Etter etterretningstjenesteloven § 7-11 skal EOS-utvalget foreta løpende kontroll over tilrettelagt innhenting og etterfølgende kontroll. EOS-utvalget er et parlamentarisk organ underlagt Stortinget og anses for å være tilstrekkelig uavhengig av E-tjenesten. Videre skal

EOS-utvalget ha tilgang til all informasjon E-tjenesten har tilgang til, jf. etterretningstjenesteloven § 7-11 andre ledd. EOS-utvalget kan begjære stans av innhenting og sletting av innhentet data overfor Oslo tingrett som videre kan beordre slik stans og sletting, jf. etterretningstjenesteloven § 7-12 første ledd. En betenkelighet med at EOS-utvalget skal føre løpende kontroll med tilrettelagt innhenting er at utvalget ikke er et permanent utvalg, men at utvalget møtes til sporadiske møter og kun er beslutningsdyktig med fem medlemmer samlet, jf. EOS-kontrolloven § 13 første ledd. Den løpende kontrollen vil derfor mest sannsynlig være en form for stikkprøvekontroll.

Samlet sett når EOS-utvalgets uavhengighet og myndighet hensyntas fremstår kontrollordningen i etterretningstjenesteloven for å gi en effektiv kontroll som gir vern mot misbruk og vilkårlighet.

5.8.2.7 Har etterretningstjenesteloven tilstrekkelige regler for underretning og inneholder loven tilstrekkelige rettsmidler?

Det fremgår av den forutgående analysen av *Centrum för rättvisa mot Sverige* og *Big Brothers Watch mot Storbritannia* at underretning til personer som har blitt berørt av overvåkning og tilgjengelige rettsmidler for å overprøve om man har blitt utsatt for ulovlig overvåkning er viktige prosessuelle rettssikkerhetsgarantier i EMDs overprøving av en overvåkningslov. Rettssikkerhetsgarantiene henger sammen, dersom man ikke blir gitt underretning, så må rettsmidlene være effektive og reelle.[270]

Etter Etterretningstjenesteloven § 11-7 plikter ikke E-tjenesten "å gi underretning til den som har vært gjenstand for informasjonsinnhenting som kan innebære et menneskerettslig inngrep." I forarbeidene fremgår det at E-tjenesten kan gi slik underretning, men at det sjelden vil være aktuelt.[271]

Kravet om underretning skal vurderes sammen med tilgjengelige rettsmidler. I Big Brothers Watch mot Storbritannia vektla EMD at det britiske ombudet ansvarlig for bulkinnhenting hadde anledning til å tilkjenne erstatning til personer utsatt for ulovlig innhenting.[272]

Tilgjengelige rettsmidler reguleres av EOS-kontrolloven, jf. etterretningstjenesteloven § 11-7 første ledd. EOS-utvalget kan etter klage fra et individ få tilgang til alle opplysninger, holde

---

[270] *Centrum för rättvisa* avsnitt 166).
[271] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 223).
[272] *Big Brothers Watch* avsnitt 379).

høringer og gi etterretningstjenesten kritikk, men har ikke myndighet til å gi individer erstatning. Dersom et individ mener seg utsatt for ulovlig overvåkning og ønsker å ta saken inn for de alminnelige domstoler eksisterer det et bevisforbud etter tvisteloven § 22-1 for opplysninger av betydning for rikets sikkerhet.

Underretning og tilgjengelige rettsmidler skal vurderes samlet etter EMDs praksis. I den norske etterretningstjenesteloven er det ikke et krav om underretning til berørte personer og det eneste reelle rettsmiddelet er parlamentarisk kontroll i EOS-utvalget. Sammenholdt bærer ikke de norske reglene om underretning og rettsmidler preg av å være en effektiv prosessuelle rettssikkerhetsgaranti.

5.8.3 Legitimt formål

I EMDs dom i saken *Weber og Saravia mot Tyskland* kom EMD til at en dersom informasjon er innhentet av hensyn til et legitimt formål, for eksempel hensynet til nasjonal sikkerhet, innebærer det et nytt inngrep i EMK art. 8 dersom disse innhentede opplysningene benyttes til et annet formål, for eksempel kriminalitetsbekjempelse.[273] Hvis innhentede opplysninger skal benyttes til et annet formål enn det de er innhentet for, må det foretas en ny vurdering av om en slik informasjondeling oppfyller vilkårene i EMK art. 8 nr. 2.[274]

Formålet med tilrettelagt innhenting er å innhente informasjon for etterretningsformål, jf. etterretningstjenesteloven § 5-1. Når informasjon er innhentet for et formål innebærer det et ytterligere inngrep i EMK art. 8 at informasjonen benyttes til et annet formål.[275] Det innebærer igjen at bruk av innhentet data til et annet formål enn innhentingsformålet må følge av et klart rettsgrunnlag, forfølge et legitimt formål og være nødvendig i et demokratisk samfunn, jf. EMK art. 8 nr. 2.

Etterretningstjenesteloven kapittel 7 inneholder to tilfeller der innhentet informasjon kan benyttes for et annet formål enn etterretning, det kan brukes som bevis i straffesaker for iretteføring av straffeloven § 131 (terror), jf. etterretningstjenesteloven § 7-14 første ledd andre pkt. og overskuddsinformasjon kan utleveres i "den utstrekning det er nødvendig for å

[273] *Weber og Saravia mot Tyskland* [J] avsnitt 103-106).
[274] Se *Weber og Saravia mot Tyskland* avsnitt 105).
[275] *Weber og Saravia mot Tyskland* [J] avsnitt 103-106).

forhindre alvorlig fare for noens liv, helse eller frihet eller at noen blir uriktig tiltalt eller domfelt for en straffbar handling", jf. etterretningstjenesteloven § 7-13.

EMDs fokus i saker der innhentet informasjon har blitt brukt til et annet formål enn innhentingsformålet er om informasjonsinnhentingen er nødvendig for å ivareta det nye formålet informasjonen blir brukt til.[276] Dette kan illustreres med et eksempel fra EMDs storkammerdom i saken S. and Marper om lagring i en fingeravtrykksdatabase. Klagerens fingeravtrykk hadde blitt innhentet for å utgjøre bevis i en straffesak og senere lagret i en nasjonal fingeravtrykksdatabase av identifiseringsformål og for å bygge opp en slik database.[277] Klageren var ikke dømt i straffesaken og var også mindreårig.[278] Det opprinnelige formålet med å ta klagerens fingeravtrykk var å utgjøre bevis i den konkrete straffesaken, det nye formålet var å bygge opp fingeravtrykksdatabasen. I EMDs vurderingen av rettmessigheten av det nye formålet, uttalte EMD at det nye formålet ikke hadde et "pressing social need" og at formålet derfor ikke gjorde det nødvendig å ta klagerens fingeravtrykk for å bygge opp en database.[279]

Tankegangen bak informasjondelingsadgangen i etterretningstjenesteloven § 7-13 er at Etterretningstjenesten i sin informasjonsinnhenting kommer over informasjon som andre offentlige myndigheter kan få bruk for, og at det ville være lite hensiktsmessig å ikke dele informasjonen med disse myndighetene. I forarbeidene fremgår det at begrunnelsen bak denne adgangen til å dele informasjon er pragmatisk, dersom Etterretningstjenesten kommer over informasjon om at noen blir utsatt for vold, overgrep eller justismord vil det være vanskelig å ikke handle.[280] Etter EMDs praksis er ikke dette vurderingstemaet, vurderingstemaet er om det er nødvendig i et demokratisk samfunn på grunn av et presserende samfunnsbehov å lagre metadata i bulk i 18 måneder om grenseoverskridende elektronisk kommunikasjon for i) forhindre alvorlig fare for noens liv, helse eller frihet ii) for å forhindre uriktige domfellelser eller iii) for å innhente bevis for overtredelse av straffeloven § 131.

Forholdsmessigheten av en slik informasjondeling er ikke drøftet eller vurdert i forarbeidene og lovgivers begrunnelse lyder slik: "Hvis en slik situasjon likevel skulle oppstå, mener

---

[276] Se *S. and Marper mot Storbritannia* [GC], ECHR:2008:1204JUD003056204 avsnitt 86).
[277] *S. and Marper* avsnitt 9-13).
[278] *S. and Marper* avsnitt 86).
[279] *S. and Marper* avsnitt 123-125).
[280] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 136.

departementet at forbudet mot å utlevere overskuddsinformasjon ikke kan stå i veien for å handle."

Etterretningstjenesteloven §§ 7-13 og 7-14 fremstår derfor som en formålsutglidning uten at forholdsmessigheten av en slik formålsutglidning er vurdert etter EMK art. 8 nr. 2 av lovgiver.

5.8.4 Nødvendighet

I forarbeidene til etterretningstjenesteloven blir fordelene ved tilrettelagt innhenting vurdert og drøftet opp mot de store personvernsmessige ulempelene med systemet. Lovgiver konkluderer på bakgrunn av de prosessuelle rettssikkerhetsgarantiene ved systemet og fordi systemet styrker "Norges selvstendige etterretningsevne" med at tilrettelagt innhenting ikke er et uforholdsmessig inngrep i EMK art. 8.[281]

Den grunnleggende forutsetningen for utfallet av lovgivers forholdsmessighets vurdering er at de etterretningsmessige fordelene ved systemet oppveier for inngrepet i personvernet.

I en høring i det britiske parlamentet om den britiske loven for bulklagring i 2016 uttalte tidligere teknisk direktør i signaletterretningstjenesten i USA William Binnley følgende:

> "(…) over the last fifteen years, the bulk collection approach has cost lives, including lives in Britain, because it inundates analysts with too much data. It is 99 per cent useless, as attacks occur when intelligence and law enforcement lose focus on previously suspected terrorists and fail to find accomplices or others enabling fresh attacks".[282]

Uttalelsen er om et bulklagrinssystemer i et annet land og også om eldre bulklagringssystemer enn det norske, men uttalelsen kan likevel være med på å nyansere de etterretningsmessige fordelene ved systemet, noe som har betydning i nødvendigetsvurderingen av inngrepet.

---

[281] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 97.
[282] JPCIPB. 2016. Written Evidence to the Joint Parliamentary Committee on the Investigatory Powers Bill.Tilgjengelig:http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26854.html

5.8.5 Proporsjonalitet

EMDs kontroll over nasjonale overvåkningskontroller er prosessuelle kontroller av om lovene inneholder tilstrekkelige rettssikkerhetsgarantier som gir individet vern mot misbruk og vern mot vilkårlighet. Det er derfor lite trolig at EMD vil sette privatlivets fred opp mot vernet av nasjonal sikkerhet i en proprosjonalitetsvurdering. Selv om dette ikke blir gjort av Den Europeiske menneskerettighetsdomstolen i Strasbourg, blir slike proporsjonalitsvurderinger foretatt av en annen Europeisk domstol, EU-domstolen. Dette er tema i kapittel 6.

5.9 Avsluttende bemerkninger

Tilrettelagt innhenting ble vedtatt i etterretningstjenesteloven fordi E-tjenesten ble kritisert av EOS-utvalget for å drive med innhenting som ikke tilfredsstilte lovkravet til EMK. En lov som skal kodifisere en uhjemlet innhentingsform er ikke det beste utgangspunktet for en bred debatt om forholdsmessighet. Samlet bærer lovgivningsarbeidet preg av at forholdsmessighetsvurderingene ikke er transparente. Hva som blir resultatet av storkammerdommene i Strasbourg i *Centrum för rättvisa* og *Big Brothers Watch mot Storbritannia* vites ikke. Storkammerdommene bør i alle tilfellene føre til at tilrettelagt innhenting tas opp i Stortinget på nytt. Drøftelsene i pkt. 6 vil vise at også grunnleggende rettigheter i EU-retten setter skranker for hvordan tilrettelagt innhenting kan reguleres. Disse skrankene har ført til at tilrettelagt innhenting er vedtatt, men ikke trådt i kraft, noe som igjen muliggjør en ny vurdering der også EMK-retten kan hensyntas.

6 EU-rettslige skranker for tilrettelagt innhenting

6.1 De rettslige grunnlagene og forholdet mellom dem

6.1.1 Innledning

I EU har EU-lovgiver innført flere reguleringer som både skal sørge for fri utveksling av personopplysninger i EUs indre marked og sikre privatlivets fred for den enkelte bruker av kommunikasjonstjenester.[283] Nasjonale lover om lagring av metadata i bulk for kriminalitetsbekjempelse og etterretningsformål må utformes i samsvar med disse EU-reglene. I det følgende skal det klarlegges hvilke EU-regler som regulerer bulklagring av metadata for etterretningsformål. På området for elektronisk kommunikasjon reguleres privatlivets fred og prinsippet om fortrolig elektronisk kommunikasjon både i Charteret, i

[283] Se for eksempel GDPR art. 1 nr. 1 og 3).

kommunikasjonsvernsdirektivet og i GDPR. Innledningsvis, før reglene om fortrolig kommunikasjon tolkes opp mot regler om bulklagring, må det derfor redegjøres for forholdet mellom de rettslige grunnlagene som gir vern for fortrolig kommunikasjon.

Både kommunikasjonsvernsdirektivet[284] og GDPR[285] som vil bli gjenstand for analyse i det følgende er en del av EØS-avtalen og også en del av norsk rett gjennom ekomloven[286] og personopplysningsloven.[287] Dette kapittelet skal analysere rettsgrunnlagene på EU-nivå, mens rettsgrunnlagenes forhold til EØS og norsk rett behandles i kapittel 7.

6.1.2 EUs Charter om grunnleggende rettigheter

Den reguleringen som har høyest rang av reguleringene av privatlivets fred i kommunikasjonsnett i EU, er EUs Charter om grunnleggende rettigheter.[288] Charteret er en del av den rettslige bindende primærretten i EU etter at det ble vedtatt ved Lisboatrakten som trådte i kraft i 2009. EUs charter er bindende for EUs organer og EUs medlemsstater "when they are implementing Union law", jf. Charterets artikkel 52 nr. 5. Charteret inneholder sivile, politiske og økonomiske rettigheter og inspirert av EMK. Etter Charterets art. 52 nr. 3 skal bestemmelser i Charteret som har en tilsvarende bestemmelse i EMK samsvare med EMK-rettigheten slik at minstevernet etter EMK-retten alltid ligger til grunn. Likevel kan rettighetene i Charteret gå lenger enn rettighetsvernet etter EMK.[289]

I Charterets artikkel 7 er det oppstilt et vern for privatliv: "everyone has the right to respect for his or hers private and family life, home and communication". Charterets art. 7 tilsvarer EMK art. 8, likevel slik at ordlyden korrespondanse i EMK art. 8 er byttet ut med "communication". Ordlyden er bevisst annerledes for å hensynta den teknologiske

---

[284] Europaparlaments- og rådsdirektiv 2002/58/EF av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon (direktivet om personvern og elektronisk kommunikasjon), engelsk: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
[285] Regulation (EU) 2016/679 of the Parliament and of the Council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directiv 94/46/EC (GDPR).
[286] Lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven).
[287] Lov 15. juni 2018 nr. 31 om behandling av personopplysninger (personopplysningsloven).
[288] EU Charter of Fundamental Rights. Det kgl. Norske Utenriksdepartementet har "døpt" Charteret *EUs Pakt om grunnleggende rettigheter* og det er det navnet som er brukt i henvisninger i norske EØS-rettsakter. Ingen av EUs medlemsland betegner Charteret som en pakt, så avhandlingen vil heretter betegne Charteret om grunnleggende rettigheter som "*Charteret*".
[289] Charterets art. 52 nr. 3 siste pkt.

utviklingen.[290] Charterets art. 7 er en kvalifisert rettighet, det vil si at alle inngrep i rettigheten i utgangspunktet er forbudt, med mindre inngrepet likevel er lovlig etter Charterets art. 52.[291]

Charterets art. 8 inneholder et eget vern for personopplysninger og bestemmelsen får betydning i vurderingen av lovligheten av bulklagring. Charterets art. 8 nr. 1 oppstiller et vern for "everyone" for "protection of personal data concerning him or her". Art. 8 nr. 2 og nr. 3 inneholder vilkår for når det kan gjøres inngrep i den enkeltes personopplysningsvern. Personopplysninger må "be processed fairly for specific purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law". I tillegg må vilkårene i Charterets art. 52 være oppfylt for at inngrepet i art. 8 skal være lovlig.

En grunnleggende menneskerettighet beskytter som oftest en generell eller spesifikk frihetsrett. For eksempel ytringsfrihet etter Charteret art. 11 som beskytter retten til å ytre seg fritt uten risiko for forfølgning av det offentlige. I juridisk teori[292] har det vært diskutert hvilken frihetsrett personopplysningsvernet etter Charteret art. 8 beskytter. Den tyske konstitusjonsdomstolen har knyttet sammen personopplysningsvernet med eiendomsretten, slik at individet må samtykke til andres bruk av egne personopplysninger på lik linje med at en eier må samtykke til andres bruk av en eiendom.[293]

En mer anerkjent måte å kategorisere vernet etter art. 8 enn eiendomsrett til opplysninger, er at personopplysningsvernet ikke utgjør en egen materiell rettighet, men heller forsterker og en konkretiserer allerede eksisterende grunnleggende menneskerettigheter.[294] Mens en rettighet som rett til privat- og familieliv i Charteret art. 7 kun beskytter mot faktiske krenkelser av rettighetene eller en konkret risiko for krenkelse,[295] forsterket personopplysningsvernet i Charteret art. 8 andre grunnleggende rettigheter fordi personopplysningsvernet etablerer et preventivt vern mot risikoen for misbruk som følger av omfattende innsamling, lagring og

---

[290] Steve Peers og Sacha Prechal, Scope and Interpretation of Rights and Priciples, The EU Charter of Fundamental Rights: A commentary side 153.
[291] Peers side 155.
[292] Se for eksempel Ralf Poscher *The Right to Data Protection- A No-Right Thesis* inntatt i Russell A. Miller Privacy and Power- A transatlantic Dialogue in the Shadow of the NSA- Affair (2017) Cambridge University Press side 132.
[293] Se for eksempel BverfG, 1 BvR 209/83. Dom av 15. desember 1983. Tilgjengelig på http.//www.servat.unibe.ch/dfr/bv065001.html.
[294] Ralf Poscher "The Right To Data Protection- A No-Right Thesis" i Russell A. Miller *Privacy And Power- A transatlantic Dialogue in the Shadow of the NSA- Affair* (2017) Cambridge University Press side 133.
[295] Se Orla Lynskey, "Deconstructing Data Protection" side 63, i *International & Comparative Law Quartely* (2014) Cambridge University Press.

analyse av personopplysninger og metadata.[296] Denne klassifiseringen av Charteret art. 8 får betydning når avhandlingen skal vurdere betydningen Charterets betydning for EØS-avtalen i kapittel 7.

6.1.3 GDPR

EUs Charter art. 8 tar sikte på å verne fysiske personer i forbindelse med behandling av personopplysninger. EUs forordning 2016/679 GDPR (General Data Protection Regulation) tar sikte på å utdype og konkretisere vernet som følger av Charteret art. 8.[297]

Personvernforordningen trådte i kraft i EUs medlemsland 25. mai 2018 etter langvarige forhandlinger i Rådet for den europeiske union og Europaparlamentet. GDPR er gjennomført i norsk rett gjennom personopplysningsloven som inkorporerer forordningen som norsk lov.

GDPR gir individet en rekke rettigheter som vil ha betydning for medlemsstatenes adgang til å benytte bulklagring av metadata som etterretningsmetode. GDPR har som mål å sikre vern av personopplysninger, og å etablere et likt og harmonisert vern i hele EU for å sikre fri utveksling av personopplysninger mellom EU- og EØS-land.[298] GDPR inneholder et svært detaljert regelverk om personopplysningsvern. Reglene er gjennomført i en forordning og ikke et direktiv for å begrense EU-landenes handlingsrom for å oppnå mest mulig harmoniserte regler i hele EU.

GDPR regulerer etter art. 4 nr. 2 "any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collecting, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure (…)". Bulklagring innebærer lagring av store mengder metadata. Metadata er vernet av GDPR. jf. art. 4 nr. 1. GDPR art. 4 tilsier derfor at forordningen regulerer bulklagring av metadata.

Personopplysningsvernet i offentlige tilgjengelige kommunikasjonsnett[299] er også regulert i kommunikasjonsvernsdirektivet fra 2002. Spørsmålet om hvilken rettsakt av kommunikasjonsvernsdirektivet og GDPR som regulerer bulklagring av metadata for

---

[296] Se Lynskey side 63.
[297] Se GDPRs fortale pkt. (1) til (4).
[298] Prop. 56 LS Lov om behandling av personopplysninger (2017-2018) side 10.
[299] Se pkt. 2.12.1 for definisjon av ekomnett og offentlige tilgjengelige kommunikasjonsnett.

etterretningsformål oppstår derfor og vil bli behandlet etter at reglene i kommunikasjonsvernsdirektivet er analysert.

6.1.4 Kommunikasjonsvernsdirektivet

EUs kommunikasjonsverndirektiv også betegnet e-databeskyttelsesdirektivet har som formål å harmonisere EU- og EØS-landenes reguleringer av elektronisk kommunikasjon for å sikre likeverdig vern av grunnleggende rettigheter knyttet til personopplysninger og personvern.[300] Kommunikasjonsvernsdirektivet er ment å være en inngående regulering av personopplysningsvernet for å sikre at Charterets grunnleggende rettigheter blir fulgt ved databehandling i offentlig tilgjengelig kommunikasjonsnett.[301]

Direktivet har også som formål å harmonisere regelverk om fri bevegelighet for personopplysninger og for elektroniske kommunikasjonstjenester i EU og EØS.[302] I Norge er direktivet gjennomført gjennom ekomloven og ekomforskriften[303] etter at direktivet ble en del av EØS-avtalen ved beslutning fra EØS-komiteen.[304]

Etter direktivets artikkel 4 er tilbyderne av ekomnett[305] pålagt en plikt til å sørge for sikker elektronisk kommunikasjon i sine nett. Videre pålegger artikkel 5 i direktivet medlemsstatene en plikt til å ha nasjonal lovgivning som sikrer fortrolighet "for trafikkopplysninger knyttet til slik kommunikasjon".[306] Trafikkopplysninger er en annen betegnelse på metadata.[307]

Videre i artikkel 5 fremgår følgende plikt som er særlig relevant for tilrettelagt innhenting: "De [medlemsstatene] skal særlig forby enhver annen person enn brukerne, uten samtykke fra vedkommende bruker, å avlytte, oppfange, lagre eller på andre måter oppfange eller overvåke kommunikasjonen og tilhørende trafikkopplysninger, unntatt dersom denne virksomheten er tillatt i henhold til lov [og] i samsvar med artikkel 15 nr. 1."

I direktivet artikkel 15 nr. 1 er det gitt hjemmel for inngrep i bestemmelsene i direktivet når det er ″nødvendig, egnet og rimelig i et demokratisk samfunn av hensyn til nasjonal sikkerhet

---

[300] Se fortalepunkt 1 og 2) til kommunikasjonsvernsdirektivet.
[301] Se fortalepunkt 2) til kommunikasjonsvernsdirektivet.
[302] Kommunikasjonsvernsdirektivet artikkel 1.
[303] Forskrift 16.02.2004 nr. 401 om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften).
[304] Beslutning fra EØS-komiteen nr. 80/2003 av 20. juni 2003.
[305] Se pkt. 2.12.1 for forklaring av ekomnett.
[306] Kommunikasjonsverndirektivet art. 5.
[307] Se kommunikasjonsvernsdirektivet art. 2 andre ledd litra b).

(dvs. statens sikkerhet), forsvar, offentlig sikkerhet og forebygging, etterforskning, avsløring og rettslig forfølging av straffbare handlinger eller ulovlig bruk av det elektroniske kommunikasjonssystemet (...)". Etter direktivets ordlyd i EU fremgår det av kommunikasjonsvernsdirektivet art. 15 nr. 1 siste punktum at et inngrep i kommunikasjonsvernet må vedtas i samsvar med "de allmenne prinsippene i fellesskapsretten, herunder prinsippene art. 6 nr. 1 og 2 i traktaten om den Europeiske union". TEU art. 6 nr. 1 og 2 henviser til Charteret og EMK. I EØS-retten er denne delen av direktivets ordlyd erstattet med "de allmenne prinsippene i EØS-retten".[308]

6.1.5 Forholdet mellom GDPR og kommunikasjonsvernsdirektivet

Forholdet mellom GDPR og kommunikasjonsvernsdirektivet reguleres av GDPR art. 95. Det fremgår av bestemmelsen at GDPR ikke inneholder noen ytterligere forpliktelser for fysiske og juridiske personer ved levering av offentlig tilgjengelige elektroniske kommunikasjonstjenester i offentlige kommunikasjonsnett enn det som fremgår av kommunikasjonsvernsdirektivet. Ved databehandling i offentlig tilgjengelige kommunikasjonsnett er reglene i kommunikasjonsvernsdirektivet lex specialis.[309]

Ekomtilbydere som prosesserer kommunikasjonsdata og behandler personopplysninger må forholde seg til GDPR. Dersom lovgivere i EUs medlemsland og i EØS vedtar forskjellige regler om bulklagring vil det kunne føre til forskjellige beskyttelsesnivå for personopplysninger i EUs medlemsland. Et slikt forskjellig beskyttelsesnivå kan være problematisk opp mot GDPRs målsetning som er å skape like felleseuropeiske regler og homogenitetsmålsetningen i EØS-avtalen art. 6

Tema for dette kapittelet er rettmessigheten av nasjonale lover om bulklagring i EU-retten. Kommunikasjonsvernsdirektivet inneholder spesiallovgivning om lagring av metadata fra offentlig tilgjengelige kommunikasjonsnett. Tilrettelagt innhenting slik det er regulert i etterretningstjenesteloven knytter seg til tilbydere av offentlig tilgjengelige kommunikasjonsnett. Det tilsier at tilrettelagt innhenting heller reguleres av kommunikasjonsvernsdirektivet enn GDPR. Avhandlingen vil derfor i det følgende

[308] Se EØS-komiteens beslutning nr. 80/2003 20. juni 2003.
[309] Se GDPR art. 95, fortalen til GDPR pkt. 173 og uttalelse 5/2019 fra Det europeiske Personvernrådet (EDPB), tilgjengelig på: https://edpb.europa.eu/our-work-tools/our-documents/styrelsens-yttrande-art-64/opinion-52019-interplay-between-eprivacy_en.

utelukkende benytte reguleringen av persopplysningsvernet slik det fremgår av kommunikasjonsvernsdirektivet.

6.1.6 Datalagringsdirektivet

Datalagringsdirektivet[310] er et historisk direktiv som ble underkjent av EU-domstolen i Digital Rights-dommen.[311] Av hensyn til sammenhengen i den videre analysen må også det nå underkjente datalagringsdirektivet nevnes under rettsgrunnlag som er relevante i relasjon til bulklagring av metadata av hensyn til nasjonal sikkerhet.

På bakgrunn av kommunikasjonsvernsdirektivet artikkel 15 nr. 1, som åpner for inngrep i kommunikasjonsvernet på nærmere bestemte vilkår, innførte flere av EUs medlemssland lovgivning om lagring av innholdsdata og metadata for å forhindre, etterforske, oppdage og irretteføre straffbare handlinger og trusler mot nasjonal sikkerhet i de første årene av 2000-tallet.[312] Slike reguleringene skulle særlig forhindre terrorisme. For å harmonisere medlemsstatenes lovgivning om når inngrep i kommunikasjonsvernet var lovlig etter kommunikasjonsvernsdirektivet art. 15 nr. 1, ble datalagringsdirektivet vedtatt av EU-lovgiver i 2006.[313]

Datalagringsdirektivet påla medlemslandene en plikt til å ha nasjonal lovgivning som forpliktet ekomtilbyderne å lagre data som var prosessert av tilbyderne. Etter direktivets art. 1 nr. 2 gjaldt direktivet trafikk- og lokasjonsdata knyttet til fysiske og juridiske personer. Etter datalagringsdirektivet art. 5 måtte medlemsstatene ha nasjonal lovgivning som påla ekomtilbydere å lagre kategorier av data nødvendig for å spore avsender og mottaker for kommunikasjonen. Innholdsdata skulle ikke lagres, jf. datalagringsdirektivet art. 5 nr. 2. Lagringen skulle skje innenfor et tidsrom på seks måneder og to år, jf. direktivets art. 6. Saksbehandlingsregler og materielle vilkår for medlemsstatenes tilgang til den lagrede dataen var opp til lovgivningen i hvert enkelt medlemssland, jf. direktivets artikkel 4.

I sakene C-293/12 og C-594/12 ble datalagringsdirektivets gyldighet prøvd av EU-domstolen. Foranledningen var at organisasjonen Digital Rights Ireland Ltd. reiste sak i Irland om

---

[310] Europaparlaments- og rådsdirektiv 2006/24/EF av 15. mars 2006 om lagring av data som fremkommer ved bruk av offentlig elektronisk kommunikasjon, samt endring i europaparlaments- og rådsdirektiv 2002/58/EF.
[311] Dom av 8. april 2014 [GC], *Digital Rights Ireland Ltd og Kärtner Landesregierung* mfl., C-293/12 og C-594/12, EU:C:2014:238.
[312] Det vises til datalagringsdirektivets fortale pkt. 5.
[313] Se datalagringsdirektivets fortale pkt. 21 og datalagringsdirektivet art. 1 nr. 1.

lovligheten av irske regler om datalagring vedtatt på grunn av direktivet. Irsk høyesterett henviste behandlingen av spørsmålet om datalagringsdirektivets gyldighet til EU-domstolen for prøving, jf. TEU art. 267. EU-domstolen ble forelagt spørsmålet om direktivet var i strid med grunnleggende rettigheter i Charteret om privatlivets fred og personopplysningsvern.[314]

EU-domstolen konkluderte med at datalagringsdirektivet var et uforholdsmessig inngrep i Charteret art. 7 og 8 og dermed ugyldig. EU-domstolens dom i Digital Rights-saken og datalagringsdirektivet er relevant i relasjon til tilrettelagt innhenting fordi analysen i kapittel 6 og 7 viser at etterretningstjenesteloven må tolkes i samsvar med kommunikasjonsvernsdirektivet som igjen må tolkes i lys av EUs grunnleggende rettigheter i Charteret. I Digital Rights-dommen tolker EU-domstolen et direktiv direkte opp mot Charteret og dommen sier derfor noe om hva som er gjeldende rett etter Charteret. Dommen vil bli nærmere behandlet senere i dette kapitlet.

6.2 EU-rettens virkeområde for nasjonale regler om etterretning

EU har som formål å opprette et fritt indre marked for fri flyt av varer og tjenester.[315] EU-retten pålegger derfor medlemslandene forpliktelser for å ivareta dette indre markedet. Forsvar, etterretning og ivaretakelse av nasjonal sikkerhet er svært grunnleggende for en stat. EU-retten inneholder som utgangspunkt ikke forpliktelser for medlemsstatene om essensielle statsfunksjoner og det følger av Traktat om Den Europeiske Union art. 4 (2) at ivaretakelse av nasjonal sikkerhet "remains the sole responsibility of each Member State". Det må derfor drøftes om rettighetene i Charteret og reglene i kommunikasjonsvernsdirektivet får anvendelse på nasjonale reguleringer om bulklagring av metadata for ivaretakelse av nasjonal sikkerhet.

Kommunikasjonsvernsdirektivet inneholder en tvetydighet som har skapt usikkerhet om hvorvidt direktivet regulerer nasjonale regler om etterretning. Etter kommunikasjonsvernsdirektivets artikkel 1 nr. 3 får direktivet ikke anvendelse på virksomhet som er unnlatt fra traktatene som utgjør primærretten i EU sine virkeområder, og "ikke i noe tilfelle på virksomhet som gjelder offentlig sikkerhet, forsvar, statens sikkerhet (herunder

[314] Charteret art. 7 og 8.
[315] Se TEU art. 3 (2).

statens økonomiske interesser når virksomheten er forbundet med spørsmål om statens sikkerhet) eller statens virksomhet på det strafferettslige området."[316]

Samtidig som art. 1 nr. 3 unntar virksomhet som gjelder nasjonal sikkerhet fra direktivets virkeområde, åpner kommunikasjonsvernsdirektivet art. 15 for unntak fra direktivet for regler begrunnet i nasjonal sikkerhet.

Kommunikasjonsvernsdirektivets anvendelsesområde opp mot regler om bulklagring av metadata av hensyn til nasjonal sikkerhet ble behandlet av EU-domstolen i Privacy International- dommen og i La Quadrature du Net-dommen. Den franske interesseorganisasjonen La Quadrature du Net gikk i 2015 til sak ved den franske forvaltningsdomstolen med påstand om at den franske lovgivningen om bulklagring for etterretningsformål var i strid med den franske grunnloven, EMK og kommunikasjonsvernsdirektivet lest i lys av Charterets art. 7, 8, 11 og 47.[317] Den franske forvaltningsdomstolen forela EU-domstolen spørsmålet om en plikt i nasjonal lovgivning for ekomtilbydere til å foreta en generell og udifferensiert lagring av metadata sett i lys av alvorlige og vedvarende trusler mot nasjonal sikkerhet er et rettmessig inngrep i kommunikasjonsvernet og Charteret art. 7 og 8.

Storbritannia, Tsjekkia, Estland, Irland, Frankrike, Kypros, Ungarn, Polen og Sverige intervenerte i La Quadrature du Net-saken og anførte at kommunikasjonsvernsdirektivet ikke gjaldt nasjonal lovgivning om bulklagring for etterretningsformål.[318] De begrunnet dette med at nasjonal sikkerhet og medlemsstatenes territorielle integritet er et ansvarsområde som tilhører den enkelte nasjonalstat og ikke EU, jf. TEU art. 4 nr. 2.[319]

I Privacy International-saken gikk en britisk menneskerettighetsorganisasjon til søksmål ved en britisk domstol med påstand om at britiske bulklagringsregler var i strid med Charteret art. 7 og 8. Den britiske domstolen henviste saken til EU-domstolen for prøving av prejudisielle spørsmål. Norge intervenerte i EU-domstolens behandling i saken og inngi skriftlig innlegg og deltok i den muntlige høringen i Luxembourg i september 2019.[320] Norge argumenterte for

[316] Kommunikasjonsvernsdirektivet art. 1 nr. 3).
[317] *La Quadrature du Net* avsnitt 56).
[318] *La Quadrature du Net* avsnitt 31-32).
[319] *La Quadrature du Net* avsnitt 32).
[320] Se *Privacy International* avsnitt 1).

at kommunikasjonsvernsdirektivet ikke regulerer en nasjonal lov som forplikter ekomtilbydere til å tilgjengeliggjøre metadata av hensyn til nasjonal sikkerhet.[321]

Forskjellen på bulklagringsreglene i Frankrike og i Storbritannia var at de britiske reglene pålå ekomtilbydere å tilgjengeliggjøre metadata til etterretningstjenestene av hensyn til nasjonal sikkerhet, mens de franske reglene påla ekomtilbydere en generell og udifferensiert lagringsplikt av metadata av hensyn til nasjonal sikkerhet.[322] I Storbritannia skjedde lagringen av myndighetene, mens ekomtilbyderne ble pålagt lagringsplikt i Frankrike. Privacy International-dommen og La Quadrature du Net-dommen er avsagt på samme dag og har samme prinsipielle utgangspunkt vedrørende EU-rettens virkeområde for nasjonal sikkerhet.

Medlemsstatene som intervenerte i EU-domstolens behandling av sakene gjorde gjeldende at ivaretakelse av nasjonal sikkerhet er essensielt for en stats fungering og dermed EU-retten uvedkommen. Medlemstatene anførte at kommunikasjonsvernsdirektivet ikke kan regulere nasjonal lovgivning som har nasjonal sikkerhet som formål da det ville føre til at TEU art. 4 (2) ikke ville ha praktisk effekt.[323]

EU-domstolen var ikke enig i medlemsstatenes argumentasjon og støttet seg til ordlyden i kommunikasjonsvernsdirektivet art. 1 (3) om at "activites of the state" er unnlatt direktivets anvendelsesområde.[324] EU-domstolen tolket denne ordlyden dithen at kun statlige aktiviteter som ikke involverer nasjonale individer er unntatt anvendelsesområde, for eksempel en stats beskyttelse mot spionasje fra en annen stat. EU-domstolen mente videre at "activites of state" heller ikke involverer lovgivning.[325] EU-domstolen støttet denne tolkningen med å vise til at formålet til direktivet er å harmonisere medlemsstatenes lovgivning for å sikre likt kommunikasjonsvern i hele EU, og at statene dermed ikke står fritt til å ha sin egen lovgivning som ikke er i tråd med dette vernet.[326]

EU-domstolen viste også til at kommunikasjonsvernsdirektivet art. 15 (1), som åpner for unntak fra direktivet på visse vilkår av hensyn til nasjonal sikkerhet, forutsetter at nasjonal lovgivning, inkludert lovgivning med nasjonal sikkerhet som formål, faller inn under

---

[321] Se Written observations by The Kingdom of Norway av 14.02.2018 til EU-domstolen i sak C-623/17 Privacy International inntatt som vedlegg 1 til avhandlingen.
[322] *Privacy International* avsnitt 16) og *La Quadrature du Net* avsnitt 34-38).
[323] *La Quadrature du Net* avsnitt 33).
[324] *Privacy International* avsnitt 35 og *La Quadrature du Net* mfl. avsnitt 92).
[325] *Privacy International* avsnitt 38 og *La Quadrature du Net* mfl. avsnitt 95).
[326] *Privacy International* avsnitt 46 og *La Quadrature du Net* mfl. avsnitt 101).

direktivets virkeområde.[327] Når direktivet art. 15 (1) åpner for unntak av hensyn til nasjonal sikkerhet, må nødvendigvis en lov om nasjonal sikkerhet falle inn under direktivet. EU-domstolen kom etter dette også til at direktivet omfatter både statlig lagring av metadata og et statlig pålegg til ekomtilbydere om å lagre metadata.[328]

EU-domstolen behandlet medlemsstatenes anførsel om at kommunikasjonsvernsdirektivet ikke regulerer nasjonal sikkerhet fordi TEU art. 4 (2) gjør ivaretakelse nasjonal sikkerhet til medlemsstatenes prerogativ ved å vise til tidligere rettspraksis om at EU-retten ikke er irrelevant kun fordi en medlemsstat har gjort et tiltak for ivaretakelse av nasjonal sikkerhet.[329]

EU-domstolen kom på bakgrunn av dette til at en nasjonal lovgivning som enten forplikter ekomtilbydere å tilgjengeliggjøre metadata til nasjonale sikkerhetstjenester eller forplikter ekomtilbydere til å generelt og udifferensiert å lagre metadata av hensyn til nasjonal sikkerhet i en nærmere angitt tidsperiode faller inn under kommunikasjonsvernsdirektivets anvendelsesområde og derfor også innen EU-rettens anvendelsesområde.[330]

6.3 Den videre analysen

I det følgende skal rettmessigheten av bulklagring som etterretningsmetode analyseres. Analysen av EU-rettens anvendelsesområde viser at kommunikasjonsvernsdirektivet og Charteret omfattet bulklagring som etterretningsmetode. Slik lagring eller tilgjengeliggjøring må derfor tilfredsstille unntakshjemlene fra utgangspunktet om sikker og fortrolig elektronisk kommunikasjon i kommunikasjonsvernsdirektivet art. 15 og Charteret art. 52. Disse unntakshjemelene har forskjellige ordlyd. Et inngrep i kommunikasjonsvernsdirektivet må være nødvendig, egnet og rimelig i et demokratisk samfunn av hensyn til nasjonal sikkerhet, jf. direktivet art. 15 (1). Et inngrep i Charteret må følge av lov, ivareta et legitimt formål og være nødvendig og proporsjonalt, jf. Charteret art. 52. Et inngrep i kommunikasjonsvernsdirektivet må også oppfylle vilkårene i Charteret art. 52, jf. direktivet art. 15 siste pkt. I det følgende skal det først drøftes om bulklagring utgjør et inngrep i kommunikasjons- og personopplysningsvernet. Deretter vil rettmessigheten av et slik inngrep

[327] *Privacy International* avsnitt 39 og *La Quadrature du Net* mfl. avsnitt 96).
[328] *Privacy International* avsnitt 40 og *La Quadrature du Net* mfl. avsnitt 96-97).
[329] *Privacy International* avsnitt 44 og *La Quadrature du Net* mfl. avsnitt 99).
[330] *Privacy International* avsnitt 49 og *La Quadrature du Net* mfl. avsnitt 104).

analyseres ut fra om inngrepet ivaretar et legitimt formål og om det er nødvendig og proporsjonalt.

6.4 Inngrep i privatlivets fred og personopplysningsvernet

Dersom en nasjonal lov er i strid med et direktiv som skal sørge for ivaretakelse av en grunnleggende Charterrettighet, kan det etter omstendighetene utgjøre et inngrep i Charteret. Dette fordi kommunikasjonsvernsdirektivet er ment å være en regulering som skal utdype og sikre vernet etter Charteret art. 7 og 8.[331] Nasjonale reguleringer i EUs medlemsland om ekomnett og elektronisk kommunikasjon kan ikke være i strid med kommunikasjonsvernsdirektivet. En nasjonal lov i et medlemsland vedtatt i strid med direktivet innebærer derfor både et brudd på nasjonalstatens plikt til direktivtkonform lovgivning[332] og en potensiell krenkelse av Charteret.

I Digital Rights-dommen ble datalagringsdirektivet vurdert som et inngrep i Charterets rettigheter om privatlivets fred og personopplysningsvern i Charteret art. 7 og 8 av EU-domstolen. I vurderingen av hva som utgjør et inngrep i Charteret art. 7 og 8, viste domstolen til tidligere rettspraksis og uttalt at lagring av data er et inngrep i privatlivet etter Charteret art. 7 uavhengig om dataene som blir lagret er sensitive eller om de berørte personen har blitt utsatt for en ulempe ved lagringen.[333] Datalagringsdirektivet artikkel 3 og 6 utgjorde derfor et inngrep i Charteret art. 7.[334]. EU-domstolen kom videre til at medlemsstatenes tilgang til den lagrede dataen et ytterligere inngrep i privatlivet enn selve lagringen.[335] Det er interessant at EU-domstolen kom til dette fordi medlemsstatenes tilgang til lagret data ikke var regulert av datalagringsdirektivet, men av nasjonal rett jf. datalagringsdirektivet art. 4. Digital Rights-dommen slår derfor tydelig fast at generell lagring av metadata fra elektronisk kommunikasjon er et inngrep i Charteret.

EU-domstolen uttalte seg også om hvor inngripende slik lagring er. Siden data ble lagret i henhold til datalagringsdirektivet generelt og udifferensiert uten at de enkelte brukerne av elektroniske kommunikasjonsnett ble informert, mente EU-domstolen at det kunne det gi brukerne av elektroniske kommunikasjonstjenester en følelse av konstant overvåkning.[336] EU-

[331] Se fortalepunkt 2 til kommunikasjonsvernsdirektivet.
[332] Se TEU art. 249.
[333] *Digital Rights* avsnitt 33).
[334] *Digital Rights* avsnitt 34).
[335] *Digital Rights* avsnitt 35).
[336] *Digital Rights* avsnitt 37).

domstolen uttalte at metadataen som ble lagret i tråd med datalagringsdirektivet gjorde det mulig å kartlegge personers vaner, oppholdssteder, reiser, relasjoner og hvilke miljøer personer frekventerte. Sammenstilling og kartlegging av metadata muliggjorde å lage profiler av personer som var like så personvernsensitivt, om ikke mer personvernsensitivt, som innholdsdataen til kommunikasjonene.[337] EU-domstolen uttalte likevel at lagring av metadata var mindre inngripende enn lagring av innholdsdata fra elektronisk kommunikasjon. EU-domstolen kom til at metadatalagring ikke var et inngrep i kjernen av rettigheten i Charteret art. 7.[338]

I Tele2-dommen[339] vurderte EU-domstolen både svensk og britisk lovgivning om lagring av metadata i bulk for kriminalitetsbekjempelse. Både den svenske og britiske lovgivningen inneholdt krav om lagring av metadata om avsender og mottaker av elektronisk kommunikasjon, lokasjon til avsender og mottaker og identifikatorer som telefonnummer og IP-adresse.[340] I likhet med i Digital Rights- dommen mente EU-domstolen at slik omfattende lagring av metadata gjør det mulig å trekke svært presise konklusjoner om individers liv, vaner, oppholdssteder og sosiale miljøer.[341] Men i motsetning til i Digital Rights dommen mente EU-domstolen at slik lagring utgjorde et inngrep i Charteret art. 7 og 8 som var like alvorlig som lagring av innholdsdata.[342]

Ved vurdering av om den svenske loven om bulklagring av trafikk- og lokasjonsdata om telekommunikasjon for etterforskning og iretteføring av kriminalitet var et rettmessig inngrep i Charteret art. 7 og 8 og kommunikasjonsvernsdirektivet, vektla EU-domstolen at generell og udifferensiert datalagring var hovedregelen i den svenske loven om bulklagring av metadata, mens kommunikasjonsvernsdirektivet art. 15 nr. 1 åpner for datalagring som et begrenset unntak.[343] Videre rammet den svenske loven alle brukere av elektronisk kommunikasjon i Sverige, også personer som ikke var under mistanke for straffbare overtredelser. Svensk lovgivning inneholdt ingen unntak for lagrings- og tilgjengeliggjøringsplikten,[344] og hadde heller ikke som vilkår at det måtte være sammenheng mellom de dataene som ble lagret og

---

[337] *Digital Rights* avsnitt 99).
[338] *Digital Rights* avsnitt 27 og 28).
[339] Dom av 21. desember 2016 [GC], Tele2 Sverige AB og Tom Watson mfl.,C-203/15 og C-698/15, EU:C:2016:970 avsnitt 18).
[340] *Tele2* avsnitt 18).
[341] *Tele2* avsnitt 99).
[342] *Tele2* avsnitt 99).
[343] *Tele2* avsnitt 105).
[344] Tele2 avsnitt 105).

straffbare overtredelser, for eksempel at data fra et visst tidsrom eller geografisk område som knyttet seg til alvorlige straffbare handlinger ble lagret.[345] EU-domstolen kom derfor til at den svenske loven klart var et inngrep i Charteret art. 7 og 8.

Lignende vurderinger ble gjort av EU-domstolen i Privacy International-dommen som gjaldt det britiske systemet for bulklagring av metadata for etterretningsformål. EU-domstolen viderefører argumentasjonen fra Tele2-dommen om at generell og udifferensiert bulkaksess og bulklagring gjorde inngrepet i kommunikasjonsvernet til regelen, mens i kommunikasjonsvernsdirektivet er et slikt inngrep unntaket.[346] EU-domstolen presiserte i Privacy International-dommen at deling av data med en tredjepart utgjør et inngrep i art. 7 og 8 i Charteret uavhengig av hva dataene blir brukt til av tredjeparten.[347] EU-domstolen uttalte at bulklagring og bulkaksess kan ha en nedkjølende effekt på bruk av elektronisk kommunikasjon, fordi taushetsbelagt informasjon og annen sensitiv informasjon også blir gjenstand for lagring. Opplysninger underlagt taushetsplikt og journalistisk materiale som er vernet etter pressens kildevern blir lagret, noe som etter EU-domstolens oppfatning kan ha en nedkjølende effekt på ytringsfriheten og utgjøre et inngrep også i Charteret art. 11.[348]

Gjennomgående i EU-domstolens dommer om bulklagringsregimer, er at den etterfølgende bruken av den lagrede dataen ikke har betydning for vurderingen av om lagringen utgjør et inngrep i kommunikasjons- og personopplysningsvernet.[349]

I La Quadrature du Net-dommen avsagt i oktober 2020 ble inngrepet metadatalagring utgjør nyansert. Lagring av metadata og annen teledata deles opp i kategorier, der rettmessigheten av lagring avhenger av ulike kategorier av teledata og hvilke formål det lagres for.[350] Til forskjell fra Privacy International-dommen gjaldt denne dommen en plikt for ekomtilbyderne til å lagre metadata og ikke statlig lagring av metadata. Teledata kan grovt sett deles opp i to kategorier, innholdsdata og metadata. Metadata kan igjen deles opp i trafikkdata, lokaliseringsdata, IP-adresser og brukeridentitetopplysninger. Trafikkdata er data om for eksempel avsender og mottaker av en SMS eller varighet av en telefonsamtale. Lokaliseringsdata er opplysninger om hvilken basestasjon eller hvilket bredbånd elektronisk kommunikasjon går gjennom som

---

[345] T*ele2* avsnitt 106.
[346] *Privacy International* avsnitt 69).
[347] *Privacy International* avsnitt 70).
[348] *Privacy International* avsnitt 72).
[349] Se *Digital Rights* avsnitt 33) og *Privacy International* avsnitt 70).
[350] *La Quadrature du Net* avsnitt 117 til 119).

kan gi opplysninger om avsender og mottakers lokasjon. En IP-adresse er en identifikator som tildeles en kommunikasjonsenhet, for eksempel en mobiltelefon eller en datamaskin, når enheten kobler seg på nettverket. Flere enheter på samme nettverk vil ha samme IP-adresse. Brukeridentitetopplysninger er navn og adresse på for eksempel et mobil- eller bredbåndsabonnement.[351]

I La Quadrature du Net-dommen oppstiller EU-domstolen forskjellige terskler for lagring av forskjellige kategorier av metadata. Dette tilsier at EU-domstolen anser lagring ulike metadatakategorier som mer inngripende enn andre. Lagring av trafikk- og lokaliseringsdata er mest inngripende og underlagt en strengere vurdering av EU-domstolen enn lagring av IP-adresser. Lagring av trafikk- og lokaliseringsdata kan derfor bare skje i en generell og udifferensiert form når det er strengt nødvendig av hensyn til nasjonal sikkerhet.[352]

6.5 Legitimt formål

Etter Charterets art. 52 nr. 1 er et inngrep i en rettighet i Charteret lovlig dersom formålet med inngrepet enten er i) "objectives of general interest recognised by the Union" eller ii) "the need to protect the rights and freedoms of others".

I Steve Peers kommentarutgave til Charteret[353] fremgår det at det i prinsippet er uendelig mange formål som kan legitimere inngrep i Charterrettighetene, jf. Charterets art. 52. Hovedmekanismen for EU-domstolens kontroll av inngrep i Charterrettigheter er derfor kontroll av hjemmelen for inngrepet og balansetesten av inngrepet.[354]

I Digital Rights-dommen behandlet EU-domstolens inngrepets formål i bedømmelsen av om inngrepet var lovlig etter Charteret art. 52. I vurderingen av om datalagringsdirektivet hadde et legitimt formål viste EU-domstolen at formålet med direktivet var å sikre at data var tilgjengelig for å etterforske og irretteføre kriminalitet. EU-domstolen viste til tidligere praksis og konkluderte med at bekjempelse av alvorlig kriminalitet og terrorisme klart er et legitimt formål.[355] EU-domstolen vurderte det dithen at direktivet oppfylte formålet med

[351] Se *La Quadrature du Net* avsnitt 52 og 182).
[352] *La Quadrature du Net* avsnitt 135).
[353] Peers side 1476.
[354] Peers pkt. 52.50.
[355] *Digital Rights* avsnitt 41).

rettsakten, kriminalitetsbekjempelse, fordi den lagrede dataen ga politiet et viktig verktøy i bekjempelsen av kriminalitet.[356]

EU-domstolen foretok også en formålsvurdering av et inngrep i Charteret i Privacy International-dommen. Som nevnt gjaldt denne dommen bulklagring av hensyn til nasjonal sikkerhet og ikke bekjempelse av kriminalitet. Ved bruk av bulklagring som etterretningsmetode gjør noen andre hensyn seg gjeldende enn ved bulklagring for kriminalitetsbekjempelse. Ved etterforskning og iretteføring av kriminalitet, har den kriminelle handlingen allerede skjedd og det er derfor mulig å etablere et bulklagrings- og bulkaksesssystem som minimerer og avgrenser metadata som blir lagret og myndighetenes tilgang til lagret data.[357]

Ved bulklagring av hensyn til etterretning og nasjonal sikkerhet, brukes systemet som en preventiv metode for å oppdage trusler mot rikets sikkerhet før hendelsene har skjedd og truslene har materialisert seg. Differensiert bulklagring og bulktilgang er derfor vanskeligere ved slik lagring. Rettmessigheten av slike systemer blir ofte begrunnet i alvorligheten av trusler mot rikets sikkerhet og systemets preventive effekt mot slike trusler.

I Privacy International-dommen viste EU-domstolen til at det fremgår av TEU art. 4 nr. 2 at nasjonal sikkerhet er de enkelte medlemsstatenes prerogativ. Beskyttelse av nasjonal sikkerhet er etter EU-domstolens oppfatning viktigere enn de andre formålene opplistet i kommunikasjonsvernsdirektivet art. 15 nr. 1, bekjempelse av kriminalitet og ivaretakelse offentlig sikkerhet. Nasjonal sikkerhet er derfor et formål som kan rettferdiggjøre mer alvorlige inngrep i privatlivets fred og personopplysningsvernet, enn de andre formålene opplistet i art. 15 nr. 1.[358]

Spørsmålet om forholdsmessigheten av bulklagring stiller seg annerledes når metadata lagres av hensyn til nasjonal sikkerhet enn ved bulklagring for kriminalitetsbekjempelse vil bli gjenstand for analyse under pkt. 6.6.

---

[356] *Digital Rights* avsnitt 49.
[357] Se EMDs dom av 12. januar 2016 Szabó og Vissy mot Ungarn [J], ECHR:2016:0112JUD003713814 avsnitt 18-20 hvor EMD har dette utgangspunktet.
[358] *Privacy International* avsnitt 75).

6.6 Forholdsmessighetsvurderingen etter Charteret art. 52

6.6.1 Utgangspunkter for EU-domstolens forholdsmessighetsvurdering

Når EMD foretar proporsjonalitetsvurderinger for å vurdere rettmessigheten av et inngrep i en rettighet etter EMK, tildeler EMD statene en "statlig skjønnsmargin".[359] Denne skjønnsmarginen skal hensynta at EMK er et rettighetsinstrument som skal fungere på tvers av Europarådet medlemssland i forskjellige rettskulturer og i forskjellige samfunn. Charteret er derimot et rettighetsinstrument som skal fungere i en jurisdiksjon, EU. EU-systemet hensyntar at det består av mange forskjellige medlemssland med forskjellige rettskulturer, ved at gjennomføringen av sekunddærretten i form av direktiver og forordninger skjer i hvert enkelt medlemssland ved vedtakelsen av nasjonal lovgivning.[360] EU-domstolen tildeler derfor ikke medlemslandene en statlig skjønnsmargin i vurderingen av et inngreps forholdsmessighet etter Charterets art. 52.[361] Ved prejudisielle avgjørelser skal EU-domstolen svare en nasjonal domstol på forelagte spørsmål om hvordan EU-retten skal forstås. Ved slike prejudisielle avgjørelser subsumerer som utgangspunkt ikke EU-domstolen nasjonal rett opp mot EU-retten og det er derfor heller ikke naturlig at det eksisterer en skjønnsmargin.

Forholdsmessighetstesten etter Charteret art. 52 går ut på å vurdere behovet for inngrep i Charteret opp mot rettigheten det gjøres inngrep i. Inngrep i en rettighet i Charteret kan kun skje hvis inngrepet "respect the essence of the Charter rights and freedoms, "if they are necassery and geuinly meet objectives of general interests or (...) the need to protect the rights and freedoms of others(...)" og hvis inngrepet ivaretar "the principle of proportionality".[362]

Balansetesten i Charteret art. 52 er et tveegget sverd, med det menes at testen både kan brukes for å beskytte individets Charterrettigheter, men også for å begrense individets rettigheter.[363] I EU blir balansetesten etter Charteret art. 52, som også kalles proporsjonalitetsprinsippet, ansett som et grunnleggende eller konstitusjonelt prinsipp.[364] Balansetesten bygger på at inngrep i en grunnleggende EU rett skal skje i færrest mulig tilfeller, og testen skal kontrollere at inngrep i grunnleggende EU-rettigheter ikke er uproporsjonale. Testen kan også

---

[359] Se pkt. 3.4.
[360] Peers side 1481.
[361] Peers side 1481.
[362] Charteret art. 52 første ledd andre punktum.
[363] Ester Herlin Karnell, Reflection Note: EU Data Protection Rules and the Lack of Compliance in Sweden, Nordic Journal of European Law Vol. 3 No. 2 (2020).
[364] Tor Inge Harbo, *The Function of the Proportionality Principle in EU Law, European law journal: review of European law in context, 2010-03, Vol.16 (2), p.158-185* side 159.

anses som et utslag av ren rimelighet. Dersom inngrepet i en Charterrettighet kunne ha skjedd på en mindre inngripende måte, kan ikke inngrepet sies å hverken være nødvendig eller egnet, og balansetesten slår i slike tilfeller ut til fordel for den grunnleggende rettigheten.[365]

Den videre analysen av dommer fra EU-domstolen skal belyse hvordan EU-domstolen har foretatt balansetester etter Charterets art. 52 nr. 1 i relevante dommer om bulklagring av metadata. I EU-domstolens rettspraksis deler som regel ikke EU-domstolen opp forholdmessighetsvurderingen etter nødvendighet og proporsjonalitet, domstolen foretar som oftest en overordnet helhetsvurdering som et ledd i besvarelsen av de forelagte spørsmålene.[366] Avhandlingen vil likevel forsøke å strukturere domstolens vurderinger i de forskjellige sakene etter nødvendighet og proporsjonalitet.

6.6.2 Nødvendighet

Etter Charteret art. 52 kan det vedtas unntak fra en rettighet i Charteret når det er nødvendig. På området på for personopplysningsvern og ved bulklagring av metadata følger det av rettspraksis fra EU-domstolen om bulklagring, at et slik inngrep kun kan skje når det er *strengt nødvendig.*[367]

En lovgivning om datalagring med formål om kriminalitetsbekjempelse må etter EU-domstolens dom i Tele2-saken begrenses til det som er strengt nødvendig.[368] Det innebærer at kun strengt nødvendig metadatakategorier kan lagres, kun metadata om strengt nødvendige kommunikasjonsmidler kan lagres, kun metadatadata omhandlende strengt nødvendige brukere av elektroniske kommunikasjonstjenester og at metadataen kan kun lagres så lenge det er strengt nødvendig.[369]

I Privacy International-dommen og La Quadrature du Net-dommen drøfter EU-domstolen om det gjelder en annen terskel for at et bulklagringsregime er i tråd med Charteret art. 52 når inngrepet er begrunnet i nasjonal sikkerhet enn kriminalitetsbekjempelse. Nasjonal sikkerhet er tradisjonelt ansett som et formål som ikke inngår i traktatene i EU. Videre er ivaretakelse

---

[365] Ester Herlin Karnell, Reflection Note: EU Data Protection Rules and the Lack of Compliance in Sweden, Nordic Journal of European Law Vol. 3 No. 2 (2020) side 101.
[366] I enkelte dommer, f.eks. Digital Rights-dommen foretar EU-domstolen drøftelser etter vilkårene i Charteret art. 52, mens i andre, f.eks. Privacy International, er dommen oppbygd etter spørsmålene som er stilt.
[367] Se *Digital Rights* avsnitt 52, *Tele2* avsnitt 96 og *Privacy International* avsnitt 67).
[368] *Tele2* avsnitt 109.
[369] *Tele2* avsnitt 109).

av nasjonal sikkerhet helt nødvendig for grunnleggende statsfunksjoner og svært viktig for en nasjonalstat.

Ivaretakelse av nasjonal sikkerhet er også et prinsipielt annet formål enn etterforskning og iretteføring av kriminalitet. Bulklagring som en metode for kriminalitetsbekjempelses blir brukt for å bekjempe interne trusler og handlinger som allerede er begått. Ytre trusler mot en stat som i siste instans kan materialisere seg i et angrep mot staten er ikke et forhold som reguleres i strafferetten. Det taler for at forholdmessighetsvurderingen vil være annerledes ved bulklagring for etterretningsformål enn ved bulklagring for kriminalitetsbekjempelse.

EU-domstolen anerkjenner at terskelen for at et bulklagringsregime anses som nødvendig kan stille seg annerledes når formålet er nasjonal sikkerhet, og at nasjonal sikkerhet og etterretning kan begrunne mer alvorlige inngrep i Charteret art. 7 og 8 enn andre formål forbeholdt at vilkårene i Charteret art. 52 er oppfylt.[370] Formålet med et bulklagringsregime har derfor stor betydning i vurderingen av balansetesten etter Charteret art. 52.

Et av de forelagte spørsmålene i Privacy International-dommen og La Quadrature du Net-dommen var om vilkåret fra Tele2-dommen om at bulklagring kun kan anses som et nødvendig inngrep i Charteret når det foreligger objektive holdepunkter for at bulklagring kan utgjøre et strengt nødvendig bidrag i etterforskning og iretteføring av alvorlig kriminalitet også gjelder ved bulklagring for etterretningsformål.[371]

Ved bulklagring av hensyn til etterretning og nasjonal sikkerhet brukes systemet som en preventiv metode for å oppdage trusler før de har materialisert seg. Hvordan skulle EU-domstolen knytte vilkårene fra Tele2-dommen om at bulklagring måtte være strengt nødvendig for å etterforske alvorlig kriminalitet opp mot bulklagringsregler begrunnet i nasjonal sikkerhet?

I vurderingen av hvordan EU-domstolen skulle forholde seg til sin egen rettspraksis om bulklagring for kriminalitetsbekjempelse i bedømmelsen av bulklagringsregler om nasjonal sikkerhet, vektla EU-domstolen i Privacy International-dommen at privatlivets fred og personopplysningsvernet er helt grunnleggende rettigheter i et moderne vestlig demokrati.[372]

---

[370] *Privacy International* avsnitt 75).
[371] *Privacy International* avsnitt 29).
[372] *Privacy International* avsnitt 67).

Unntak fra personopplysnings- og kommunikasjonsvernet må derfor også i slike tilfeller også begrenses til strengt nødvendige tilfeller.[373] På bakgrunn av dette utgangspunktet uttalte EU-domstolen at nasjonale regler om bulklagring for etterretningsformål må ha klare og presise vilkår og et minimum av materielle og prosessuelle rettssikkerhetsgarantier for å minimere risikoen for misbruk ved omfattende lagring av metadata i bulk. Nasjonal lovgivning om bulklagring av metadata av hensyn til nasjonal sikkerhet må indikere hvilke tilfeller og omstendigheter som kan gi grunnlag til metadatalagring for å sikre at inngrepet som bulklagring utgjør kun skjer når det er strengt nødvendig.[374]

6.6.3 Proporsjonalitet

Første gangen EU-domstolen behandlet forholdsmessigheten av bulklagring i Digital Rights-dommen kom EU-domstolen til at følgende forhold var spesielt problematisk med datalagringsdirektivet: direktivet åpnet for generell og udifferensiert metadatatalagring og inneholdt ikke noe vilkår om at det måtte være sammenheng mellom datalagringen og alvorlig kriminalitet.[375] Direktivet inneholdt ikke objektive kriterier for tilgang og bruk av lagret metadata av nasjonale myndigheter, og direktivet inneholdt heller ikke krav til materielle og prosessuelle rettssikkerhetsgarantier som for eksempel forhåndsgodkjennelse av bruk av lagret data av en domstol eller uavhengig administrativ myndighet.[376] Direktivet påla også medlemsstatene å innføre tidsbestemte lagringsperioder og inneholdt ikke mulighet for nasjonal lovgivning om individuelle lagringstider knyttet til lagring av forskjellige metadatakategorier.[377] EU-domstolen kom på bakgrunn av dette til at datalagringsdirektivet var i strid med Charteret og dermed ugyldig. Sammenholdt bærer avgjørelsen preg av at EU-domstolen fant det uforholdsmessig at alle borgere i EUs medlemsland ble utsatt for metadatalagring i 12 måneder, uavhengig av om de hadde noen forbindelse til alvorlig kriminalitet.

I Privacy International-dommen uttalte EU-domstolen seg om forskjellen på forholdsmessighetsvurderingene ved lagring av metadata og ved etterfølgende tilgang til lagret metadata og muligheten til å gjøre etterfølgende søk i lagret data. EU-domstolen uttalte at det er selve lagringen av metadata i bulk som utgjør inngrepet i de grunnleggende

---

[373] *Privacy International* avsnitt 67 og 68).
[374] *Privacy International* avsnitt 68).
[375] *Digital Rights* avsnitt 58-59)
[376] *Digital Rights* avsnitt 60)
[377] *Digital Rights* avsnitt 61-62)

Charterrettighetene,[378] og at dette inngrepet, lagringen, ikke blir forholdsmessig av at tilgangen til metadata som er lagret av myndighetene er underlagt materielle og prosessuelle vilkår. Når nasjonale myndigheter har hjemmel til å pålegge ekomtilbyderne å overføre metadata til myndighetene i bulk, innebærer det at dataene er tilgjengelig for de offentlige myndighetene med den risikoen for misbruk det innebærer. Dette utgangspunktet gjelder uavhengig av om tilgangen til metadatalagreret avhenger av forhåndsgodkjennelse av en uavhengig juridisk myndighet.[379]

Privacy International dommen omhandler nasjonale regler der ekomtilbydere blir pålagt en plikt til å tilgjengeliggjøre all metadata generelt og udifferensiert til nasjonale etterretningsmyndigheter for at disse myndighetene skal lagre metadataen. EU-domstolens vurdering av proporsjonaliteten til en slik lovgivning er at Charteret og kommunikasjonsvernsdirektivet utelukker en slik nasjonal lovgivning.[380] La Quadrature du Net-dommen omhandler nasjonal lovgivning der metadataen blir lagret generelt og udifferensiert av ekomtilbyderne og ikke nasjonale myndigheter, og der myndighetene får tilgang til dataene etter visse prosessuelle regler. EU-domstolen vurderte at direktivet og Charteret ikke utelukker et slikt regime. Som omtalt under pkt. 4.3 knyttet EU-domstolen i La Quadrature du Net-dommen opp vurderingen av forholdsmessigheten av bulklagring som etterretningsmetode opp mot hvilke metadatakategorier som lagres og for hvilke formål lagring skjer. Domstolen uttaler generelt at ivaretakelse av nasjonal sikkerhet er et så viktig formål, at det kan begrunne mer alvorlige inngrep i kommunikasjonsvernet.[381] Lagring av trafikk- og lokaliseringsdata er den mest inngripende formen for metadatalagring, og slik bulklagring av slike data av ekomtilbyderne kan derfor etter EU-domstolens oppfatning kun skje generelt og udifferensiert av hensyn til nasjonal sikkerhet på nærmere bestemte vilkår: i) bulklagring av trafikk- og lokaliseringsdata må kun skje generelt og udifferensiert i en begrenset tidsperiode som anses som strengt nødvendig, ii) et pålegg til ekomtilbydere om å lagre metadata må være avgrenset i tid, iii) for et slikt pålegg gis må det foreligge konkrete holdepunkter som gjør det mulig å anta at landet står overfor en alvorlig trussel mot nasjonal sikkerhet, iv) trusselen mot nasjonal sikkerhet må være reell og aktuell eller forutsigbar, v) bulklagringen må være underlagt tilstrekkelige prosessuelle rettssikkerhetsgarantier for å

[378] *Privacy International* avsnitt 69).
[379] *Privacy International* avsnitt 79 og 80).
[380] *Privacy International* avsnitt 83, slutningens pkt. 2.
[381] *La Quadrature du Net* avsnitt 135).

minske risikoen for misbrukt, vi) et pålegg om bulklagring eller av metadata rettet mot en ekomtilbyder skal kunne underlegges kontroll av et administrativt uavhengig organ eller en domstol. EU-domstolen oppstiller som et absolutt krav at slik generell og udifferensiert bulklagring av trafikk- og lokasjonsdata ikke kan ha en systematisk og forhåndsdefinert form.[382]

Årsaken til at EU-domstolen vurderer lagring hos etterretningstjenestene annerledes enn bulklagring som skjer hos ekomtilbyderne, kan være at et system der myndighetene selv lagrer metadata i enorme mengder og kun kan søke i disse dataene på visse vilkår, utgjør en mye større risiko for misbruk av de lagrede dataene enn når metadataen er lagret hos ekomtilbyderne. Inngrepet, lagringen av metadata, er likt i Storbritannia og i Frankrike, men proporsjonalitsvurderinger slår annerledes ut når lagringen skjer hos etterretningstjenesten selv og etterretningstjenesten er underlagt prosessuelle vilkår for å få tilgang til noe de allerede har tilgang til.

Til tross for at bulklagring kan gi et effektivt bidrag i bekjempelsen av terrorisme og andre ytre trusler mot en nasjonalstat, er EU-domstolen i både Privacy International-dommen og i La Quadrature du Net-dommen kort i sin vurdering av forholdsmessigheten til slike nasjonale regler i relasjon til behovet for bulklagring som etterretningsmetode. I etterkant av Tele2-dommen har EU-domstolen blitt kritisert i juridisk teori for at forholdsmessighetsvurderingene domstolen foretok var kort og ikke utførlig begrunnet.[383] EU-domstolen har blitt kritisert for å ikke vurdere forskjellen i forholdsmessigheten av omfattende statlig lagring av metadata opp mot lagring av metadata som foregår i stort omfang hver dag av andre aktører som for eksempel sosiale medier eller skytjenester. EU-domstolen foretok heller ikke slike forholdmessighetsvurderinger i Privacy International-dommen. Bulklagring ble vurdert som et uforholdsmessig inngrep i all hovedsak på grunn av den store risikoen for misbruk som følger av slik omfattende lagring[384] og EU-domstolen gikk ikke inn på vurderinger av medlemsstatenes behov for bulklagringssystemer.

---

[382] *La Quadrature du Net* avsnitt 137 til 139).
[383] Christopher Kuner, mfl., "An unstoppable force and an immoveable object? EU data protection law and national security" i *International Data Privacy Law*, 2018, Vol. 8, No. 1.
[384] *Privacy International* avsnitt 68 og 69).

EU-domstolens vurderinger av inngrepets forholdsmessighet må her tolkes i lys av generaladvokatens uttalelse i saken.[385] Generaladvokaten viste til at effektiviteten til bekjempelse av trusler mot rikets sikkerhet måles i hvor mange terrorangrep og trusselhendelser som blir oppdaget og avverget. Rettsstatens effektivitet på den andre siden måles ut fra om prosedyrer og garantier som gjør rettsstaten til en legitim samfunnsform er fulgt. Hvis kun effektiviteten i bekjempelsen av trusler mot rikets sikkerhet hensyntas, vil rettsstaten bli illegitim og i ytterste tilfelle selv utgjøre en trussel mot borgerne. Dersom myndighetene er utrustet med uforholdsmessige verktøy i bekjempelse av trusler mot rikets sikkerhet og vage hjemler som åpner for datalagring i vidt omfang, vil det ikke være noen garanti mot at staten selv skader den enkeltes rettigheter og friheter.[386]

7 Er etterretningstjenesteloven kapittel 7 utformet i samsvar med EØS-retten?

7.1 Er de analyserte dommene fra EU-domstolen EØS-relevante?

I Norges skriftlige innlegg til EU-domstolen[387] i Privacy International-saken avsnitt 2) gjorde Norge gjeldende overfor EU-domstolen at TEU art. 4 om at "national security remains the sole responsibility of each member state"[388] ikke har noe tilsvarende bestemmelse i EØS-avtalen, og viste samtidig til at EØS-avtalen art. 1 og 2 har et snevrere virkeområde enn TEU og TEUV. Siden EU-domstolen svarte på de forelagte spørsmålene med grunnlag i EU-rett, ble naturligvis ikke Norges EØS-rettslige anførsel kommentert. Spørsmålet blir derfor hvilken betydning det får at nasjonal sikkerhet er utelatt av EØS-avtalens saklige virkeområde.

I sakene La Quadrature du Net og Privacy International blir EU-retten i all hovedsak fastsatt på grunnlag av Charteret og kommunikasjonsvernsdirektivet. EU-domstolen uttaler at "Article 4(2) TEU (...) cannot invalidate that conclusion".[389] Selv om art. 4 i TEU spilte en rolle i EU-domstolens avgjørelser, og en slik bestemmelse ikke følger av EØS-avtalen, bygger EU-domstolens rettsanvendelse på at selv om et inngrep i en Charterrettighet er begrunnet i et formål som faller utenfor EU-traktatens virkeområde, så medfører ikke det at

---

[385] Generaladvokat Campos Sánches Bordonas uttalelse av 15. januar 2020 i C-511/18 og C512/18
[386] Generaladvokat Campos Sánches Bordonas uttalelse i C-511/18 og C512/18 avsnitt 130-131).
[387] Written observations by The Kingdom of Norway av 14.02.2018 til EU-domstolen i sak C-623/17 Privacy International inntatt som vedlegg 1 til avhandlingen.
[388] TEU art. 4.
[389] *Privacy International* avsnitt 44).

EU-retten er irrelevant. Selv om EØS-avtalen er en annen type multilateral avtale enn traktatene i EU, legges det samme utgangspunktet til grunn for EØS-rettens anvendelse på et inngrep i en grunnleggende rettighet når inngrepet er begrunnet i et formål som ikke er en del av EØS-avtalen.

EUs kommunikasjonsvernsdirektiv er inkorporert i norsk rett i ekomloven med tilhørende forskrift. Mange av de analyserte dommene fra EU-domstolen behandler kommunikasjonsvernsdirektivet opp mot Charteret. Charteret er ikke en del av EØS-avtalen, spørsmålet i det følgende er derfor om dommene fra EU-domstolen fra oktober 2020 får betydning for norsk rett siden Charteret ikke er en del av EØS-avtalen. I forarbeidene til etterretningstjenesteloven er det fremhevet at charteret ikke er "gjort til en del av EØS-avtalen, og dermed ikke bindende for Norge".[390]

Halvard Haukeland Fredriksen har behandlet spørsmålet om Charteret relevans i EØS-retten i artikkelen "Betydningen av EUs pakt om grunnleggende rettigheter for EØS-retten".[391] På den ene siden fremhever artikkelen at Charteret ble en del av EU-retten i 2009 lenge etter vedtakelsen av EØS-avtalen. Hvis Charteret skal legge føringer for norsk rett vil det innebære at Norges folkerettslige forpliktelser påvirkes av et rettighetsinstrument som Norge ikke har hatt noen innflytelse over. Det kan være problematisk opp mot Norges suverenitet og funksjonsfordeling mellom de øverste statsmaktene.

På den andre siden viser artikkelen til homogenitetsprinsippet i EØS som har som målsetning å skape felles regler og reguleringer i EU og EØS. I sin artikkel skiller Fredriksen mellom de tilfellene der Charteret utgjør en tolkningsfaktor i tolkningen av EU-regler som er innlemmet i EØS-avtalen og tilfeller der bestemmelsene i Charteret utgjør det rettslige grunnlaget for å prøve gyldigheten av EØS-relevant EU-lovgivning.[392] Fredriksen skriver at i tilfellene der Charteret blir brukt som tolkningsfaktor for EU-rettsakter som er innlemmet i EØS, så har Charteret betydning som tolkningsfaktor også i EØS.[393]

---

[390] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 101.
[391] Fredriksen, Halvard Haukeland, "Betydningen av EUs pakt om grunnleggende rettigheter for EØS-retten", *Jussens venner* 06/2013.
[392] Fredriksen, Halvar Haukeland, "Betydningen av EUs pakt om grunnleggende rettigheter for EØS-retten", *Jussens venner* 06/2013 side 378.
[393] Fredriksen, Halvar Haukeland, "Betydningen av EUs pakt om grunnleggende rettigheter for EØS-retten", *Jussens venner* 06/2013 side 380.

Kommunikasjonsvernsdirektivet er en EU-rettsakt innlemmet i EØS-avtalen og i norsk rett gjennom ekomloven. Hvis kommunikasjonsvernsdirektivet skal tolkes uten å ta hensyn til Charterets bestemmelser om privatlivets fred og personopplysningsvern i Charterets art. 7 og 8, vil det innebære at kommunikasjonsvernsdirektivet får et annerledes virkeområde i henholdsvis EU, i EØS og i Norge. Et slikt skille er ikke i tråd med homogenitetsmålsetningen i EØS-avtalen art. 6 og heller ikke i tråd med hovedformålet om europeisk integrasjon i EU.

Et annet argument mot å lese kommunikasjonsvernsdirektivet isolert uten å se hen til Charteret, er at Charterets bestemmelse om privatlivets fred er en tilsvarende bestemmelse som i EMK art. 8. EMK art. 8 gjelder som norsk lov, jf. menneskerettsloven art. 2. Hvis man tolker EØS-retten isolert, risikerer man å tolke kommunikasjonsvernsdirektivet, i motstrid med EMK art. 8 som skal gis forrang, jf. menneskerettsloven § 3.

Det har vært hevdet at på området for personopplysningsvern og ved datalagring, så gir Charteret art. 8 et bedre vern enn EMK.[394] Det kan derfor anføres at Charteret gir et vern mot datalagring som ikke følger av EMK som Norge er bundet av, noe som igjen taler for at Norge ikke er bundet at EU-domstolens dommer om bulklagring. Som drøftet under pkt. 6.1.2 kan Charteret art. 8 ses på som en konkretisering av andre grunnleggende rettigheter i Charteret, heller enn en egen materiell rettighet. Etter denne tankegangen er Charteret art. 8 mer et verktøy for å fremme andre rettigheter, for eksempel retten til privatliv og ytringsfrihet, heller enn en rettighet med et eget innhold. Ved en slik synsmåte får det ikke avgjørende betydning at en tilsvarende bestemmelse som Charteret art. 8 ikke eksisterer i EMK.

Min vurdering av kildematerialet er at når EUs Charter om grunnleggende rettigheter blir anvendt som tolkningsfaktor av EU-domstolen i tolkningen av rettsakter fra EU som er gjort til EØS-rettsakter, er Charteret også relevant for tolkningen av EØS-rettsaktene. I EU-domstolens avgjørelser om kommunikasjonsvernsdirektivet og Charteret er også analysen og anvendelsen av Charteret og direktivet sammenføyd, og det er vanskelig å skille rettighetsvernet i Charteret fra vernet i direktivet. På bakgrunn av den overordnende

[394] Kuner, Christopher, Fred Cate, Orla Lynskey, Christopher Millard, Nora Ni Loideain og Dan Svantesson, "An unstoppable force and an immoveable object? EU data protection law and national security", i *International Data Privacy Law*, 2018, Vol. 8, No. 1

målsetningen om homogenitet i EØS, kan kommunikasjonsvernsdirektivet vanskelige tolkes isolert uten å hensynta Charteret.

I dommene fra EU-domstolen er det svært vanskelig å skille mellom hvilke rettigheter og plikter som følger av Charteret og hvilke som følger av kommunikasjonsvernsdirektivet. Charteret og direktivet er direkte bindende for EUs medlemsland, det ville derfor ikke hatt noen funksjon for EU-domstolen å skille disse reguleringene fra hverandre. Dersom det faktum at Charteret ikke er bindende for Norge skal brukes som argument for at kommunikasjonsvernet skal være svakere i Norge enn i EU, vil det innebære en tankegang om at Charteret gir individet flere rettigheter enn kommunikasjonsvernsdirektivet, som Norge er bundet av. Kommunikasjonsvernsdirektivet skal være en mer detaljert regulering av personopplysningsvernet som følger av Charteret art. 7 og 8.[395] Det innebærer at Charteret ikke kan gi individet rettigheter som ikke følger direktivet, siden direktivet er en mer detaljert og uttømmende regulering av personopplysningsvernet. Rettighetsvernet kan derfor ikke være svakere i EØS og i Norge enn i EU. Det konkluderes derfor med at dommene fra EU-domstolen om bulklagring er EØS-relevante og relevante rettskilder i norsk rett.

7.2 Konfrontasjon mellom norsk rett og EØS-retten

7.2.1 Utgangspunkt: Det gjelder forskjellige regler avhengig av om bulklagringen skjer hos myndighetene eller hos ekomtilbyderne

Utgangspunktet i kommunikasjonsvernsdirektivet art. 5 er klart. Elektronisk kommunikasjon, og metadata fra slik elektronisk kommunikasjon, skal være fortrolig. Unntak fra dette utgangspunktet må oppfylle vilkårene i direktivets art. 15.

Spørsmålet om bulklagring av metadata er et slik rettmessig inngrep ble behandlet av EU-domstolen av EU-domstolen i Privacy International-saken. 6.oktober 2020 avsa EU-domstolen dom i Privacy International-saken med slik slutning:

> "Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Article 4(2) TEU and Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation enabling a State authority to require providers of electronic communications

[395] Se fortalepunkt 2) til kommunikasjonsvernsdirektivet.

services to carry out the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security." (Min understreking)

Samme dag avsa EU-domstolen dom i saken La Quadrature du Net, der andre vilkår gjelder når nasjonal lovgivning pålegger ekomtilbyderne en lagringsplikt til å lagre metadata generelt og udifferensiert av hensyn til nasjonal sikkerhet.

Etterretningstjenesteloven kapittel 7 etablerer et bulklagringsregime i Norge der lagringen skjer på Etterretningstjenestens servere, jf. etterretningstjenesteloven § 7-7 første ledd, og ekomtilbydere blir pålagt en plikt til å tilgjengeliggjøre metadata til Etterretningstjenesten, jf. etterretningstjenesteloven § 7-2 første ledd.

De norske reglene samsvarer derfor med det som var tilfellet i Privacy International-dommen siden lagringen foretas av Etterretningstjenesten selv og ikke det som var tilfellet i La Quadrature du Net-dommen. Vilkårene som åpner for bulkagringen i et begrenset tilfelle i La Quadrature du Net-dommen er forbeholdt der lagringen skjer av ekomtilbyderne.

Etterretningstjenesteloven kapittel 7 ble vedtatt av Stortinget i juni 2020, mens dommen fra EU-domstolen ble avsagt 6. oktober 2020. Lovens kapittel 7 er ikke trådt i kraft, fokuset i det følgende blir derfor om kapittelet kan tre i kraft uten at Norge bryter forpliktelser etter EØS-avtalen. For å avgjøre dette må det drøftes om tilretteleggingsplikten for ekomtilbyderne i etterretningstjenesteloven kapittel 7 omfatter en "general and indiscriminate transmission" av metadata.

7.2.2 Innebærer tilrettelagt innhenting en generell og udifferensiert innhenting av metadata?

Etter etterretningstjenesteloven § 7-1 første ledd kan Etterretningstjenesten kun treffe beslutning overfor ekomtilbyderne om å tilrettelegge for bulklagring av data som "transporteres over den norske grensen". Et argument for at tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon ikke innebærer en generell og udifferensiert datalagring er at loven kun åpner for tilrettelagt innhenting av elektronisk kommunikasjon som passerer grensen, og at grensepasseringen dermed utgjør en differensiering i seg selv.

Som forklart i kapittel 3 har Telenor i et uoffisielt estimat anslått at 70 % av internettrafikken i Norge er grenseoverskridende. Det taler i alle tilfelle for at skillet mellom innenlands og

grenseoverskridende data er en differensiering som ikke har noen særlig effekt for å forhindre generell datalagring. I Generaladvokatens uttalelse i forkant av La Quadrature du Net-dommen gjør Generaladvokaten gjeldende at datalagringen er generell og udifferensiert hvis den knytter seg til alle brukere når det ikke er noen sammenheng mellom brukerne og formålet med datalagringen.[396]

Siden etterretningstjenesteloven knytter seg til alle brukere av grenseoverskridende kommunikasjonsnett, uten at det er noen sammenheng mellom data som blir lagret og alvorlige trusler mot rikets sikkerhet, konkluderes det med at loven utgjør en generell plikt for ekomtilbydere til å tilgjengeliggjøre metadata til Etterretningstjenesten.

Videre må det drøftes det om tilrettelagt innhenting utgjør en udifferensiert innhenting av metadata. Etterretningstjenesteloven inneholder regler om differensiering av metadata, men denne differensieringen skjer etter at lagringen har skjedd når det søkes i lagret metadata, jf. etterretningstjenesteloven § 7-8. Etter dommene fra EU-domstolen må differensieringen knytte seg til selve lagringen, og ikke etterfølgende søk eller sammenstilling av metadata. På bakgrunn av dette utgjør tilrettelagt innhenting en udifferensiert plikt for ekomtilbydere til å tilgjengeliggjøre metadata til Etterretningstjenesten.

Siden etterrettningstjenesteloven kapittel 7 innebærer statlig lagring av metadata fra elektronisk kommunikasjon uten sammenheng mellom de dataene som lagres og etterretningsformål, og siden lagringen skjer av Etterretningstjenesten selv, innebærer det en generell og udifferensiert datalagring. Plikten for ekomtilbyderne til å tilgjengeliggjøre disse dataene generelt og udifferensiert er i strid med kommunikasjonsvernsdirektivet.

Min konklusjon er derfor at etterretningstjenesteloven kapittel 7 ikke kan tre i kraft uten at det innebærer ikrafttredelse av norsk lovgivning som strider mot en EØS-direktiv som er gjennomført i norsk rett i ekomloven. Det konkluderes videre med at ikrafttredelse etterretningstjenesteloven kapittel 7 vil utgjøre et brudd på EØS-avtalen art. 7.

[396] Generaladvokatens uttalelse av 15. januar 2020 i sak C-623/17 avsnitt 115).

8 Forslag til regulering av bulklagring i tråd med EØS-retten

8.1 Innledning

Det følgende kapittelet skal forsøke å oppstille et forslag til hvordan bulklagring for etterretningsformål kan reguleres for å tilfredsstille kravene som fremgår av EØS-retten. Grunnen til at kapittelet kun drøfter hvordan reguleringen kan utformes for å samsvare med EØS-retten og ikke også EMK, er at EØS-retten inneholder flere krav til nasjonale reguleringer enn EMK. Når EØS-retten gir individet et bedre personopplysningsvern enn EMK og når EØS-retten inneholder flere krav til materielle vilkår for nasjonal lovgivning om bulklagring enn EMK-retten, er det mest hensiktsmessig å beskrive hvordan bulklagring kan reguleres i samsvar med EØS-retten.

Kapittelet skal forsøke å beskrive et forslag til lovgivning som er utformet i samsvar med de krav EU-domstolen har oppstilt til nasjonale lover om bulklagring for etterretningsformål. Analysen av EU-retten resulterte i konklusjonen at Charteret og kommunikasjonsvernsdirektivet setter skranker for bulklagring av metadata for å sikre at lagringen er et forholdsmessig inngrep i kommunikasjonsvernet. La Quadrature du Net-dommen åpner likevel for bulklagring som et unntak i særskilte situasjoner når lagringen skjer av ekomtilbyderne.

De siste dommene fra EU-domstolen om temaet ble avsagt i oktober 2020, og det finnes lite empiri eller juridisk forskning om temaet. Dette kapittelet kan derfor kun angi konturene og hovedpunktene av en lovgivning om bulklagring som samsvarer med minstekravene oppstilt av EU-domstolen.

8.2 Er det mulig å oppnå lagring av metadata uten å implementere EØS-rettens minstekrav?

EØS-retten legger en rekke begrensninger på adgangen til nasjonal regulering av lagring av metadata i bulk. Spørsmålet i det følgende er om det er mulig å unngå implementeringen av EØS-rettens minstekrav ved lagring av metadata i bulk.

I de tilfellene der bulklagring av metadata foregår uten at ekomtilbydere blir pålagt noen tilretteleggingsplikter eller forpliktelser til å lagre metadata, reguleres slik lagring utelukkende

av nasjonal rett.[397] Slik statlig lagring må skje uten noen form for involvering av ekomtilbydere eller andre private rettssubjekt.[398] Ved tilrettelagt innhenting i etterretningstjenesteloven pålegges ekomtilbydere tilretteleggingsplikter. Slike plikter følger også nærmest uten unntak også av reguleringene av bulklagring av metadata i andre europeiske land.[399]

I etterretningstjenesteloven er bulklagring av metadata regulert ved at ekomtilbydere pålegges en plikt til å tilrettelegge for etterretningstjenestens lagring av grenseoverskridende data. Det kan tenkes at en regulering der staten eksproprierer den delen av kabelen som går over grensen og selv skaffer tilgang til de grenseoverskridende kommunikasjonsdataene går klar av kommunikasjonsvernsdirektivet og heller reguleres utelukkende av nasjonal rett. Ingen av EUs medlemsland har en slik regulering av bulklagring.

En fordel med en regulering av bulklagring der staten eksproprierer den grenseoverskridende delen av ekomtilbydernes fiberoptiske kabler er at private rettssubjekt ikke blir pålagt en rekke plikter som kan stride mot fellesskapsretten. I etterretningstjenesteloven er ekomtilbydere både pålagt en plikt til å dele metadata, men også en plikt til å forsere egne krypteringer. Ved at staten eksproprierer den grenseoverskridende delen av kabelen, blir ekomtilbyderne frigjort fra disse pliktene som i ytterste grad kan føre til ansvar for brudd på EU-retten for ekomtilbyderne.

En betenkelighet med en regulering der Norge eksproprierer den grenseoverskridende delen av fiberoptiske kabler fra ekomtilbydere for å selv besørge aksess og lagring av grenseoverskridende metadata, er at en slik ordning kan gå klar av kommunikasjonsvernsdirektivet, men stride mot grunnleggende rettigheter i Charteret. I EU-domstolens dom av 16. juli 2020 i saken C-311/18 Schrems II[400] vurderte EU-domstolen avtalen Privacy Shield som var hjemmel for å overføre personopplysninger fra EU til et

---

[397] Se unntaksbestemmelsen i GDPR art. 2 (2) litra d) og *Privacy International* avsnitt 48).
[398] Se directive (EU) 2016/680 of the European Parliament and of the Council of Europe of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA artikkel 1.
[399] Rapport fra 20. oktober 2017 fra European Union Agency for fundamental rights *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU Volume II. Field perscpectives and legal update.* Tilgjengelig på: https://fra.europa.eu/sites/defaul/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf (lastet ned 08.01.2021).
[400] Dom av 16. juli 2020 [GC], *Maximillian Schrems,* C-311/18, EU: ECLI:2020:559.

tredjeland. Dommen gjaldt direkte overføringer av personopplysninger mellom Facebook Ireland og Facebook Inc. i USA, men EU-domstolen benyttet også anledningen til å uttale seg om overføring av personopplysninger til tredjeland generelt. I dommen oppstiller EU-domstolen tilleggskrav for overføring av personopplysninger til tredjeland for å sikre at EU-borgeres personopplysninger er like godt beskyttet etter overførselen som de er i EU.[401] Dersom tredjelandet som importerer personopplysninger fra et land i EU har lokale overvåkningslover som strider mot grunnleggende rettigheter i EU og som derfor senker beskyttelsesnivået for personopplysninger, kan ikke personopplysningene overføres til tredjelandet.[402] Etter Schrems II-dommen har databehandlere i EØS forbud mot å overføre personopplysninger til tredjeland som har nasjonale lover som gir et svakere beskyttelsesnivå enn GDPR og Charteret.

Dersom Norge innfører et bulklagringssystem med langt mer omfattende lagring av metadata som på grunn av statlig aksess og lagring ikke reguleres av kommunikasjonsvernsdirektivet, vil det kunne innebære at databehandlere i EU har forbud mot å overføre data til norske databehandlere. Norge risikerer derfor å bli stående utenfor europeisk samarbeid om elektronisk kommunikasjon. Det konkluderes derfor med at bulklagring ikke kan reguleres uten å implementere EU-rettens minstekrav uten at det vil få store negative konsekvenser for Norge.

8.3 Lagringstiden må fastsettes individuelt i hvert tilfelle

EU-domstolen avsa 2. mars 2021 storkammerdom i C-746/18 Prokuratuur.[403] Saken var foranlediget av at metadata var brukt som bevis i en straffesak i Estland. I storkammerdommen uttalte EU-domstolen seg særskilt om hvordan lagringstid i nasjonal lov har betydning for forholdmessighetsvurderingen etter kommunikasjonsvernsdirektivet art. 15 og Charteret art. 52. I storkammerdommen uttalte EU-domstolen at lagring og statlig tilgang til lagret trafikk- og lokasjonsdata er et alvorlig inngrep i Charteret art. 7 og 8 uavhengig av hvor lenge dataen blir lagret.[404]

I etterretningstjenesteloven er lagringstiden satt til 18 måneder, jf. etterretningstjenesteloven § 7-7 tredje ledd. EU-domstolen praksis i Prokuratuur-dommen innebærer at lagringstiden til

---

[401] *Schrems II* avsnitt 105).
[402] *Schrems II* avsnitt 203) slutningens pkt. 2.
[403] Dom av 02.03.2021 [GC], *Prokuratuur,* C-746/18, EU:C:2021:152.
[404] *Prokuratuur* avsnitt 39).

metadata må fastsettes i hvert enkelt tilfelle ut ifra konkrete risikovurderinger. Når lagring ikke lenger er strengt nødvendig for etterretningsoperasjonen, må lagringen opphøre. En regulering av bulklagring kan derfor ikke ha en på forhånd fastsatt absolutt lagringstid slik etterretningstjenesteloven § 7-7 tredje ledd har.

8.4 Bulklagring av ulike metadatakategorier

I den norske etterretningstjenesteloven har etterretningstjenesten fått hjemmel for bulklagring av grenseoverskridende metadata. Metadata er ikke legaldefinert, men i forarbeidene er betegnelsen definert som "data som beskriver annen data eller som inneholder ekstra informasjon knyttet til data (...)".[405] I EU-domstolens praksis legges det opp til at lagring av metadata utgjør varierende grad av inngrep i kommunikasjons- og personopplysningsvernet avhengig av hvilken type metadatakategori som lagres.[406] I tråd med EU-domstolens praksis vil derfor avhandlingen i det følgende legge til grunn et forslag om forskjellige regler for bulklagring av trafikk- og lokasjonsdata, IP-adresser og brukeridentitetopplysninger.

Trafikk- og lokasjonsdata anses etter EU-domstolens praksis som de metadatakategoriene som kan gi mest informasjon om et individ, og bulklagring av slike data anses som mer inngripende enn lagring av IP-adresser og brukeridentitetopplysninger.

Både av hensynet til individets kommunikasjonsvern og av hensyn til ekomtilbydernes forutberegnelighet, burde lagringsplikt og tilgjengeliggjøringsplikt av metadata med formål å verne nasjonal sikkerhet konkretisere hvilke metadatakategorier ekomtilbydere skal bli pålagt å lagre. Fokus i det følgende vil være adgangen til bulklagring av trafikk- og lokasjonsdata, herunder hvilke materielle og prosessuelle EU-retten inneholder. Av hensyn til sammenhengen i analysen, vil det kort kommenteres i hvilke tilfeller EU-retten åpner for bulklagring av IP-adresser og brukeridentitetopplysninger. Tilrettelagt innhenting kan med noen unntak ikke benyttes i strafferettspleien. EU-domstolens drøftelser av bulklagring inneholder ikke noe klart skille mellom nasjonal sikkerhet og kriminalitetsbekjempelse. Den resterende delen av dette underkapittelet vil også kommentere noen forhold som omhandler bulklagring for kriminalitetsbekjempelse.

[405] Prop. 80 L (2019-2020) Lov om etterretningstjenesten side 108.
[406] Se pkt. 4.5.3 for en forklaring av de ulike metadatakategoriene.

Selv om det er et inngrep i kommunikasjonsvernet, anser EU-domstolen generell og udifferensiert bulklagring av IP-adresser som et forholdsmessig inngrep i kommunikasjonsvernet når det skjer av hensyn til nasjonal sikkerhet, bekjempelse av alvorlig kriminalitet og ved alvorlige trusler mot offentlig sikkerhet og når lagringen skjer hos ekomtilbyderne. Lagringstiden må ikke være lengre enn strengt nødvendig for å ivareta formålet og slik bulklagring av IP-adresser må ha være strengt regulert og ha prosessuelle rettssikkerhetsgarantier for å sikre at tilgangen til lagrede IP-adresser kun skjer for å ivareta formålene.[407]

Brukeridentitetopplysninger anses som den minst "avslørende" metadatakategorien av EU-domstolen. Slike opplysninger knytter sammen for eksempel en IP-adresse med et navn på en fysisk eller juridisk person og er typisk lagret av ekomtilbydere for faktureringsformål. EU-domstolen åpner for at brukeridentitetopplysninger kan bulklagres generelt og udifferensiert for alle brukere av et kommunikasjonsnett. Slik bulklagring kan begrunnes i bekjempelse av alminnelig kriminalitet.[408] Hvilke formål som kan begrunne lagring av forskjellige metadatakategorier kan illustreres med denne tabellen:

	Alvorlig trussel mot rikets sikkerhet	**Alvorlig kriminalitet**	**Alminnelig kriminalitet**
Trafikk- og lokasjonsdata (Generelt og udifferensiert)	✔	✘	✘
Trafikk- og lokasjonsdata (Målrettet)	✔	✔	✘
IP-adresser	✔	✔	✘
Brukeridentitetopplysninger	✔	✔	✔

I EU-domstolens praksis er selve lagringen av metadata ansett som et inngrep i kommunikasjonsvernet. Tilgang til lagrede metadata er et ytterligere inngrep. En formålsbegrensning av bulklagring knytter seg til selve lagringen. Ved generell og udifferensiert bulklagring, som EU-domstolen åpner for ved lagring av IP-adresser og

[407] Se La Quadrature du Net-dommen avsnitt 156).
[408] La Quadrature du Net-dommen avsnitt 158).

brukeridentitetopplysninger, rammer lagringen alle brukere av et ekomnett. Ved slik bulklagringen kommer formålsbegrensningen først til anvendelse ved tilgangen til bulklagret metadata.

EU-domstolen har videre åpnet for målrettet bulklagring av trafikk- og lokasjonsdata ved alvorlige trusler mot rikets sikkerhet når lagringen skjer hos ekomtilbyderne. I slike situasjoner vil formålsbegrensingen bli aktuell ved selve lagringen. En nasjonal lov som åpner for slik bulklagring, må derfor ha prosessuelle og materielle vilkår som sikrer at loven kun åpner for generell og udifferensiert lagring av metadata for å ivareta formålet om ivaretakelse av nasjonal sikkerhet.

8.5 Bulklagring ved ekstraordinære trusler mot riket

8.5.1 Generell og udifferensiert bulklagring

I La Quadrature du Net-dommen kom EU-domstolen til at siden etterretning og ivaretakelse av nasjonal sikkerhet er svært viktig for en nasjonalstat, utelukker ikke Charterets art. 7, 8, 11 og art. 52 nasjonal lovgivning som gir de hemmelige tjenestene adgang til å pålegge ekomtilbydere en datalagringsplikt for trafikk- og lokasjonsdata for en begrenset tidsperiode, når det foreligger objektive holdepunkter for å hevde at nasjonalstaten er i en alvorlig trusselsituasjon. Dette gjelder selv et pålegg om generell og udifferensiert datalagring hvis trusselen mot nasjonal sikkerhet er alvorlig nok.[409]

Dette utgangspunktet fremgår også av generaladvokatens uttalelse i La Quadrature du Net-saken.[410] Generaladvokaten uttalte at i situasjoner der sikkerhetstjenestene i en medlemsstat på bakgrunn av informasjon de besitter har en berettiget mistanke om planleggingen av et terrorangrep, så kan bulklagring som etterretningsmetode være et forholdsmessig inngrep i rettighetene etter Charteret. Generaladvokaten presiserte at mistanken må være sannsynlig og objektivt konstaterbar.[411]

EU-retten åpner ikke for nasjonal lovgivning som åpner for generell og udifferensiert bulklagring av trafikk- og lokasjonsdata begrunnet med den til enhver tid gjeldende

---

[409] *La Quadrature du Net* avsnitt 137).
[410] Uttalelse av 15. januar 2020 fra generaladvokat Campos Sánchez-Bordona i sakene C-511/18 og C-512/18.
[411] Uttalelse av 15. januar 2020 fra generaladvokat Campos Sánchez-Bordona i sakene C-511/18 og C-512/18 avsnitt 134).

terrortrusselen som eksisterer mot europeiske land.[412] Etterretningstjenesteloven burde derfor inneholde klare vilkår for når det foreligger en alvorlig trussel mot nasjonal sikkerhet. Slik generell og udifferensiert bulklagring burde i tråd med EU-domstolens praksis forhåndsgodkjennes av en domstol etter Etterretningstjenestens begjæring. Siden bulklagring i slike tilfeller skal forhindre en konkret trussel mot riket, burde loven inneholde en formålsbegrensning som hindrer deling av innhentet data med politi- og påtalemyndighet, med unntak av iretteføring og etterforskning av tilfellet som ga grunn til å starte bulklagringen. Bulklagringen må avgrenses i tid. I en slik situasjon innhentes trafikk- og lokasjonsdata av hensyn til en konkret trussel, loven må derfor inneholde en plikt til å slette innhentet data etter en viss tidsperiode. Av hensyn til demokratisk kontroll burde det også skje en offentlig kunngjøring av at det har skjedd en generell og udifferensiert bulklagring når en slik kunngjøring ikke vil ødelegge etterretningsoperasjonen.

8.5.2 Målrettet bulklagring

Etter EU-retten kan etterretningstjenesten foreta målrettet bulklagring knyttet til strengt nødvendige persongrupper og metadatakategorier av hensyn til nasjonal sikkerhet. Dette underkapittelet skal drøfte prosessuelle og materielle vilkår for avgrensning av målrettet bulklagring. En form for avgrensning av metadata er avgrensning mot personkrets, for eksempel at kun metadata om personer med direkte eller indirekte forbindelser til trusler mot rikets sikkerhet lagres. En annen avgrensningsmåte er at kun metadata fra et avgrenset geografisk område lagres.

Ved bulklagring som metode for etterforskning og iretteføring av kriminalitet kan lagringen begrenses fordi de kriminelle handlingene allerede er begått. Ved bulklagring som etterretningsmetode er dette vanskeligere siden systemet er tenkt å oppdage trusler mot rikets sikkerhet før truslene har materialisert seg i angrep, utenlandske etterretningsoperasjoner eller lignende hendelser. Etterretningsmål benytter seg i stor grad av kryptering, anonymisering og forfalskede identiteter. Det kan derfor være vanskelig å knytte bulklagring direkte opp mot konkrete personer og konkrete etterretningsmål. En slik utvelgelsesmåte kan også føre til mistenkeliggjøring av visse deler av befolkningen og i ytterste grad være diskriminerende.[413] Utvelgelse av visse geografiske områder kan medføre de samme problemene vedrørende

---

[412] *La Quadrature du Net* avsnitt 138).

[413] Generaladvokatens uttalelse av 15. januar 2020 i sak C-520/18 avsnitt 88).

diskriminering, og mistenkeliggjøring av befolkningsgrupper basert på bosted. Slike diskrimineringshensyn gjør seg ikke gjeldende ved bulklagring av offentlige tilgjengelige steder som flyplasser eller togstasjoner, og EU-domstolen har åpnet for at bulklagring kan avgrenses til slike offentlige tilgjengelige steder.[414]

Siden 2017 har Rådet i EU satt ned en arbeidsgruppe som skal jobbe med forslag til EU-lovgivning om personopplysningsvern på område for politi, påtalemyndighet- og etterretning.[415] Arbeidsgruppen har blant annet som formål å foreslå felleseuropeisk regelverk om bulklagring av metadata som er i tråd med EU-domstolens rettspraksis.[416]

Denne arbeidsgruppen har foreslått at lagring i metadata i bulk kan differensieres etter geografisk område eller spesielle persongrupper. I tillegg har arbeidsgruppen foreslått at differensiering også kan skje ved at kun metadata strengt nødvendig for etterretningsoperasjonen lagres, ved at metadataen psudonymiseres[417], ved at metadata lagres i en svært begrenset tidsperiode, ved at noen datakategorier ikke lagres eller at etableringen av et bulklagringsregime avhenger av den til enhver tid gjeldende trusselsituasjonen.[418]

I den rådgivende uttalelsen i sak C-520/18 uttalte generaladvokat Campos Sánchez-Bordona seg om hvilken regulering av målrettet bulklagring av metadata i medlemslandene han mener er mest i tråd med Charteret art. 7 og 8. Generaladvokaten mener at en løsning der visse kategorier av metadata begrenset til å gjelde metadata som er strengt nødvendig for nasjonal sikkerhet lagres midlertidig, er den løsningen som er mest i tråd med rettspraksis fra EU-domstolen.[419]

For å forhindre risikoen for misbruk ved lagring av store mengder metadata, mener jeg at en lagring av metadata knyttet opp mot konkrete trusselaktører er en regulering som i større grad

---

[414] *La Quadrature du Net* avsnitt 150).
[415] Working Party on Information Exchange and Data Protection (DAPIX). Se https://www.consilium.europa.eu/en/council-eu/preperatory-bodies/working-party-information-exchange-data-protection/# (Lastet ned 11.01.2021).
[416] Se Generaladvokatens uttalelse av 15. januar 2020 i sak C-520/18 avsnitt 78).
[417] Selektorer som knytter sammen metadata og en person erstattes med et alias. Ved psudonymisering, i motsetning til anonymisering, kan tilknytningen mellom lagret metadata og personen gjenskapes.
[418] Generaladvokatens uttalelse av 15. januar 2020 i sak C-520/18 avsnitt 92).
[419] Generaladvokatens uttalelse av 15. januar 2020 i sak C-520/18 avsnitt 93).

hensyntar både individets behov for personopplysningsvern og E-tjenestens behov for metadatalagring som etterretningsmetode.

EU-domstolen åpner for målrettet bulklagring som etterretningsmetode når det er saklig sammenheng mellom de som blir utsatt for lagring og behovet for lagring, så lenge ikke lagringen er generell og udifferensiert og rammer alle brukere av et ekomnett.[420]

Mitt forslag til regulering av målrettet bulklagring for etterretningsformål knytter sammen hjemmelen for bulklagring av metadata med en vurdering av medlemslandenes til enhver tid gjeldende trusselsituasjon. Igangsettelse av bulklagring av metadata foreslås besluttet av en domstol eller uavhengig administrativ myndighet på begjæring fra etterretningstjenesten. På denne måten kan brukerne av et ekomnett være sikre på at bulklagring for etterretningsformål kun skjer når det er strengt nødvendig av hensyn til nasjonal sikkerhet og at bulklagringen dermed er i tråd med Charteret art. 7 og 8.

Dersom for eksempel signaletterretningstjenesten i et medlemsland får et tips fra en samarbeidene tjeneste i et annet land eller gjennom andre innhentingsmetoder har konkrete holdepunkter for at et terrorangrep er under planlegging eller at en fremmed etterretningsoperasjon foregår, kan signaletterretningstjenesten henvende seg til domstolen eller det uavhengige administrative organet ansvarlig for bulklagring. Dersom denne domstolen er enig i at informasjonen utgjør et konkret holdepunkt for at nasjonal sikkerhet er i fare, kan domstolen autorisere bulklagring for en viss varighet og et visst omfang.

Dette kan belyses med et eksempel. Dersom de hemmelige tjenestene får et tips fra tollmyndighetene om at et firma har importert store mengder av en kjemisk substans som ofte brukes i produksjon av eksplosiver, og dersom de hemmelige tjenestene gjennom andre kilder samtidig har informasjon om at dette firmaet har kjøpt store mengder kunstgjødsel, foreligger det konkrete holdepunkter for en trusselsituasjon. Da kan tjenesten henvende seg til en domstol og be om å få iverksette et pålegg til ekomtilbydere til bulklagring og bulkaksess i for å kartlegge omfanget av mulige samarbeidene aktører. Domstolen kan da vurdere om de konkrete holdepunktene gir grunn til å autorisere bulklagring og bulkaksess knyttet til de berørte personene eller et begrenset geografisk område i nærhet av etterretningsmålet. Dersom denne innhentingen av metadata resulterer i at etterretningsmålet har omfattende kontakt med

---

[420] *La Quadrature du Net* avsnitt 150-151).

mange kjente etterretningsmål eller trusselaktører i store deler av landet, kan domstolen igjen samtykke til mer omfattende bulklagring og bulkaksess. Lagringstid og lagringsomfanget besluttes av domstolen eller den uavhengige administrative myndigheten i hvert enkelt tilfelle.

Ved at autorisasjonen av bulklagring og bulkaksess knytter seg til selve oppstarten av lagringen av metadata i bulk, og ikke etterfølgende søk i lagret metadata slik som den norske etterretningstjenesteloven legger opp til, vil forhåndskontrollen av bulklagringen i mye større grad utgjøre en reell kontroll. Det materielle vilkåret for bulklagring og bulkaksess må i tråd med EU-domstolens rettspraksis være at lagringen og aksessen er strengt nødvendig for en etterretningsoperasjon.

Etterretningstjenesteloven kapitel 7 og 8 legger opp til at Oslo tingrett skal godkjenne søk i lagret metadata knyttet til person- og modusselektorer. Små endringer i disse selektorene vil kunne føre til svært forskjellige søkeresultater. Ved at tingretten heller prøver om det foreligger konkrete holdepunkter for at lagring av metadata er strengt nødvendig for en etterretningsoperasjon, får domstolen en forhåndskontroll som i større grad ligner på forhåndsgodkjennelse av straffeprosessuelle tvangsmidler som kommunikasjonskontroll og dataavlesning i straffeprosessloven. Det fører også til at forhåndskontrollen blir en mindre fjern og ukjent kontroll for domstolen som skal autorisere lagringen og aksessen.

En slik regulering kan bli møtt med argumentet at dommerne i domstoler er generalistdommere som ikke har erfaring med å ta stilling til komplekse problemstillinger knyttet til trusselvurderinger og rikets sikkerhet. Dette er riktig, men på den andre siden er dommere i utgangspunktet ikke spesialister på noen livsområder, men er i stand til å ta stilling til om en handling er bevist utover enhver rimelig tvil i straffesaker og om noe har sannsynlighetsovervekt i sivile saker etter bevisføring. Ved bevisføring av etterretningstjenesten, vil også dommere i norske domstoler kunne ta stilling til om en trusselsituasjon er så alvorlig at bulklagring av metadata er rettmessig inngrep i den enkeltes privatliv.

9 Avsluttende refleksjoner

Etterretningstjenesteloven kapittel 7 og 8 er vedtatt av Stortinget, men regjeringen har valgt å ikke la kapitlene tre i kraft på ubestemt tid. Til tross for at regjeringen har utsatt ikrafttredelsen av etterretningstjenesteloven kapittel 7 og 8, og til tross for at EU-domstolen i realiteten har satt en stopper for generell og udifferensiert lagring av metadata i bulk når lagringen skjer av etterretningstjenestene selv, omtalte E-tjenestesjefen tilrettelagt innhenting som et av de viktigste verktøyene mot utenlandske trusler på NSMs sikkerhetskonferanse 11. mars 2021.[421] Hvorvidt uttalelsen betyr at regjeringen kommer til å la kapitlene tre i kraft eller om regjeringen vil komme tilbake til Stortinget med et nytt forslag er usikkert.

En av de fremtredende begrunnelsene for behovet for tilrettelagt innhenting er for å motvirke utenlandsk påvirkning av offentlig opinion og demokratiet.[422] Det fremstår som et paradoks at lovgivers resept mot utenlandsk påvirkning av fra statlige aktører i Russland og Kina kommer i form av omfattende statlig lagring av kommunikasjonsdata. Dette er en form for kontroll som kjennetegner Russland og Kina. Et skjold mot udemokratisk påvirkning bør ikke i seg selv være udemokratisk i formen.

I et liberalt demokrati er det inngrep i grunnleggende menneskerettigheter som må begrunnes, ikke fraværet av inngrepet. Selv om tilrettelagt innhenting er vedtatt i lovs form, må den etterfølgende utviklingen i tiden etter vedtakelsen føre til at lovgiver tar et skritt tilbake og igjen begrunner behovet for et slikt overvåkningssystem. EU-domstolens dommer fra oktober 2020 og de ventede storkammerdommene fra EMD bør avstedkomme en debatt om forholdsmessigheten av tilrettelagt innhenting og om behovet for metadatalagring. En slik offentlig og transparent debatt var det Lund-kommisjonen anbefalte for de hemmelige tjenestenes fremtid på slutten av 1990-tallet: "Et samfunn der befolkningens gjøren og laden overvåkes i minste detalj er ingen fjern teknologisk mulighet. I en slik tid er det fremfor noe viktig at ansvarlige politikere er villige til å håndtere forholdet mellom tjenestene og offentligheten med oppriktighet, uansett om spørsmålene måtte være ømtålige".[423]

---

[421] https://www.youtube.com/watch?v=Eid-fncaKEk&t=1190s (05.04.2021) (Ca. 19 minutter ut i avspillingen).
[422] Høringsnotatet side 193.
[423] DOK 15 (1995-1996) side 1130.

Referanseliste

Norske lover

Kongeriket Norges Grunnlov, Lov 17. mai 1814

Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven)

Lov 17. juli 1992 nr. 100 om barneverntjenester (barnevernloven)

Lov 27. november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven)

Lov 25. mars 1994 nr. 6 om granskningskommisjon for granskning av påstander ulovlig overvåkning av norske borgere

Lov 3. februar 1995 nr. 7 om kontroll med etterretnings- overvåkings- og sikkerhetstjeneste (EOS- kontrolloven)

Lov 4. august 1995 nr. 53 om politiet (politiloven)

Lov 20. mars 1998 nr. 11 om etterretningstjenesten (etterretningstjenesteloven)

Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven)

Lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven)

Lov 20. mai 2005 nr. 28 om straff (straffeloven)

Lov 17. juni 2005 nr. 90 om mekling og rettergang i sivile tvister (tvisteloven)

Lov 28. mai 2010 om behandling av personopplysninger i politiet og påtalemyndigheten (Politiregisterloven)

Lov 15. april 2011 nr. 11 om endringer i ekomloven og straffeprosessloven mv. (Lagringsloven)

Lov 17. juni 2016 nr. 54 (endringslov til straffeprosessloven mv. skjulte tvangsmidler)

Lov 16. juni 2017 nr. 59 om endringer i straffeprosessloven og politiloven (utlevering av informasjon fra PST til E-tjenesten)

Lov 1. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven)

Lov 5. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven)

Lov 19. juni 2020 nr. 77 om etterretningstjenesten (Etterretningstjenesteloven)

Norske forskrifter, instrukser og kongelige resolusjoner

Forskrift av 16. februar 2004 nr. 401 om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften)

Instruks av 19. august 2005 nr. (Instruks for politets sikkerhetstjeneste)

Instruks av 13. oktober 2006 nr. 1151 om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste (Samarbeidsinstruksen)

Kongelig resolusjon av 10. november 2020 om delt ikrafttredelse av Stortingets vedtak til lov om Etterretningstjenesten (etterretningstjenesteloven). Opphevelse av overgangsregler om behandling av personopplysninger og av kongelig resolusjon 31. august 2001.

Lovforarbeider og offentlige utredninger

NOU 2012: 2 Utenfor og innenfor- Norges avtale med EU

Innst. 186 S (2013-2014) Innstilling fra kontroll- og konstitusjonskomiteen om grunnlovsforslag fra Per-Kristian Foss, Martin Kolberg, Marit Nybakk, Jette F. Christensen, Anders Anundsen, Hallgeir H Langeland, Per Olaf Lundteigen, Geir Jørgen Bekkevold og Trine Skei Grande om grunnlovfesting av sivile og politiske menneskerettigheter, med unntak av romertall X og romertall XXIV.

NOU 2015:13 Digital sårbarhet-sikkert samfunn

Digitalt grenseforsvar (DGF) Lysne II-utvalgets utredning til forsvarsdepartementet

Prop. 56 L S (2017-2018) Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen

Prop. 80 L (2019-2020) Lov om etterretningstjenesten

Prop. 1 S Tillegg 1 (2020–2021) Statsbudsjettet 2021

Andre stortingsvedtak og stortingsdokumenter

Dokument nr. 15 (1995-1996) Rapport til Stortinget fra kommisjonen som ble oppnevnt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere ("Lund-rapporten").

DOK. nr. 16 (2011-2012) Rapport fra Menneskerettighetsutvalget om menneskerettigheter i Grunnloven

Innst. 164 S (2016-2017), Vedtak 466. Anmodningsvedtak om revidert etterretningstjenestelov

DOK 7:2 (2015-2016) Særskilt melding til Stortinget fra Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-utvalget).

Høyesterettsavgjørelser

Rt. 2005 s. 883

HR-2016-296 A

Internasjonale konvensjoner

Europarådets konvensjon av 4. november 1950 om beskyttelse av menneskerettighetene og de grunnleggende friheter (Den europeiske menneskerettighetskonvensjonen eller EMK)

Vienna Convention on the Law of Treaties, Wien, 23 mai 1969

Convention for the Protection of Individuals with regard to the Automatic Prosessing for Personal Data av 28. januar 1981 nr. 108.

Protocol No. 15 amending the Convention on the Protection of Human Rights and Fundamental Freedoms.

De forente nasjoners internasjonale konvensjon 16. desember 1966 om sivile og politiske rettigheter

FNs erklæring om menneskerettigheter av 10. desember 1948.

Avgjørelser fra EMD

Golder mot Storbritannia	*Golder mot Storbritannia* [P], ECHR:1975:0221JUD000445170
Handyside mot Storbritannia	*Handyside mot Storbritannia* [P], ECHR:1976:1207JUD000549372
Klass mfl. mot Tyskland	*Klass mfl. mot Tyskland* [J], ECHR:1978:0906JUD000502971
Tyrer mot Storbritannia	*Tyrer mot Storbritannia* [J], ECHR:1978:0425JUD000585672
Sporrong og Lönnroth mot Sverige	*Sporrong og Lönnroth mot Sverige* [J] ECHR:1982:0923JUD000715175
Malone mot Storbritannia	*Malone mot Storbritannia* [P], ECHR:1984:0802JUD000869179
Huvig mot Frankrike	*Huvig mot Frankrike* [J], ECHR:1990:0424JUD001110584
Rotaru mot Romania	*Rotaru mot Romania* [GC], ECHR:2000:0504JUD002834195
Amann mot Sveits	*Amann mot Sveits* [GC], ECHR:2000:0216JUD002779895
Peck mot Storbritannia	*Peck mot Storbritannia* [J], ECHR:2003:0128JUD004464798
Segersted-Wiberg mot Sverige	*Segersted-Wiberg mot Sverige* [J], ECHR:2006:0606JUD006233200
Weber og Saravia mot Tyskland	*Weber og Saravia mot Tyskland* [J], ECHR:2006:0629DEC005493400
S. and Marper mot Storbritannia	*S. and Marper mot Storbritannia* [GC], ECHR:2008:1204JUD003056204
Kennedy mot Storbritannia	*Kennedy mot Storbritannia* [J], ECHR:2010:0518JUD002683905

P. og S. mot Polen	*P. og S. mot Polen [*J], ECHR:2012:1030JUD005737508
M. og M. mot Storbritannia	*M.M. mot Storbritannia* [J], ECHR:2012:1113JUD002402907
Yefimenko mot Russland	*Yefimenko mot Russland* [J], ECHR:2013:0212JUD000015204
Roman Zakharov mot Russland	*Roman Zakharov mot Russland* [GC], ECHR:2015:1204JUD004714306
Szabó og Vissy	*Szabó og Vissy mot Ungarn* [J], ECHR:2016:0112JUD003713814
A.-M.V. mot Finland	*A.-M.V. mot Finland* ECHR:2017:0323JUD005325113
Centrum för rättvisa	*Centrum för rättvisa mot Sverige* [J], ECHR:2018:0619JUD003525208
Big Brothers Watch	*Big Brothers Watch mot Storbritannia* [J], ECHR:2018:0913JUD005817013

Avgjørelser fra EU-domstolen

Schecke og Eifert	Dom av 9. november 2010 [GC], *Volker und Markus Schecke GbR og Hartmut Eifer,* C-92/09 og C-93/09, EU:C:2010:662
Nexans France SAS	Dom av 14. november 2012 [C5] *Nexans France SAS og Nexans France SA,* T-135/09, EU:T:2012:596
Digital Rights	Dom av 8. april 2014 [GC], *Digital Rights Ireland Ltd og Kärtner Landesregierung mfl.,* C-293/12 og C-594/12, EU:C:2014:238
Deckmyn og Vrijheidsfonds VZW	Dom av 3. september 2014 [GC], *Johan Deckmyn and Vrijheidsfonds VZW*, C-201/13, EU:C:2014:2132

Adhésion de l'Union à la CEDH	Dom av 18. desember 2014 [GC], *Adhésion de l'Union à la CEDH*, C-2/13, EU:C:2014:2454
Hedqvist	Dom av 22. oktober 2015 [C5], *Skatteverket mot David Hedqvist*, C-264/14, EU:C:2015:718
Tele 2 and Watson	Dom av 21. desember 2016 [GC], *Tele2 Sverige AB og Tom Watson mfl.,*C-203/15 og C-698/15, EU:C:2016:970
Schrems II	Dom av 16. juli 2020 [GC], *Maximillian Schrems*, C-311/18, EU: ECLI:2020:559
Privacy International	Dom av 6. oktober 2020 [GC], *Privacy International, C-623/17,* EU:C:2020:790
La Quadrature du Net	Dom av 6. oktober 2020, *La Quadrature du Net,French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net,* C-511/18, C-512/18 og C-520/18, EU:C:2020:791
Prokuratuur	Dom av 2.mars 2021 [GC], *Prokuratuur,* C-746/18, EU:C:2021:152

Uttalelser fra EU-domstolens generaladvokater

Generaladvokat Campos Sánches Bordonas uttalelse i sak C-511/18 og C512/18 *La Quadrature du Net*

Generaladvokat Campos Sánches Bordonas uttalelse i sak C-520/18, *Ordre des barreaux francophones et germanophone*

Generaladvokat Campos Sánches Bordonas uttalelse C-623/17 *Privacy International*

EU- og EØS rettsakter

Avtale om Det europeiske økonomiske samarbeidsområde.

Traktat om Den Europeiske Union

EU-domstolens vedtekter

Traktat om Den Europeiske Unions Virkemåte

EU Charter of Fundamental Rights.

Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning).

Europaparlament- og rådsdirektiv 2006/24/ EF av 15. mars 2006 om lagring av data som fremkommer ved bruk av offentlig elektronisk kommunikasjon, samt endring i europaparlaments- og rådsdirektiv 2002/58/EF.

Europaparlaments- og rådsdirektiv 2002/58/EF av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon (direktivet om personvern og elektronisk kommunikasjon),

Directive (EU) 2016/680 of the European Parliament and of the Council of Europe of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

Beslutning fra EØS-komiteen nr. 80/2003 av 20. juni 2003.

Avgjørelser fra EFTA-domstolen

Rådgivende uttalelse i sak E-9/97 Erla María Sveinbjörnsdóttir mot Island

Juridisk litteratur

Aal, Jørgen "Rettsstat og menneskerettigheter"

Bernal, Paul, "Data Gatehering, surveillance and human rights: recasting the debate" i *Journal of Cyber Policy*, 1: 2 side 243-264

Bobek, Michael, "The Court of Justice of the European Union" i Damian Chalmers og Anthony Arnull (red.) *The Oxford Handbook of European Union Law*, Oxford University press, 2015.

Busch, Tor-Aksel «Noen utviklingstrekk i norsk kriminalpolitikk basert på 40 år i påtalemyndigheten», Tidsskrift for strafferett 2018/4, Juridika

De Hert P., Gutwirth S. (2009) "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action", I Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (red) *Reinventing Data Protection*?. DOI: https://doi.org/10.1007/978-1-4020-9498-9_1

Fause, Anett Beatrix Osnes «Kravet til legalitet, nødvendighet og proporsjonalitet når det utøves polisiær eller påtalemessig myndighet som griper inn i vernet etter EMK art. 8 nr. 1», Tidsskrift for strafferett 2014/1, Juridika

Fenger, Niels og Morten Broberg, *Præjudicielle forelæggelser for EF-domstolen,* Jurist- og Økonomforbundets Forlag 2008.

Fredriksen, Halvar Haukeland, "Betydningen av EUs pakt om grunnleggende rettigheter for EØS- retten", *Jussens venner* 06/2013.

Fredriksen, Halvard Haukeland og Gjermund Mathisen, "EU-rett som norsk rettskilde″ i *Juridisk metode og tenkemåte* Alf Petter Høgberg og Øyrehagen Sunde (red.), Universitetsforlaget, 2019, s. 386-420.

Fredriksen, Halvard Haukeland og Gjermund Mathisen, *EØS-rett*, 2. utgave, Fagbokforlaget 2018.

Graver, Hans Petter, ″Vanlig juridisk metode? Om rettsdogmatikken som juridisk sjanger" *Tidsskrift for Rettsvitenskap,* vol. 121, 2/2008, s. 149 –178.

Hale-Ross, Simon, *The Investigatory Powers Act 2016 The human rights conformist, Terrorism and State Surveillance of Communications*, Routledge 2019.

Harbo, Tor Inge "The Function of the Proportionality Principle in EU Law", i *European law journal: review of European law in context*, 2010-03, Vol.16 (2), p.158-185 side 159.

Harris, David, Collin Warbrick, M. O'Boyle *Law of the European Convention on Human Rights*, 3. Utgave, Oxford University Press, 2014.

Huijbers, Leonie M, " The European Court of Human Rights' procedural approach in the age of subsidiarity" i Cambridge International Law Journal, Vol. 6 No. 2, pp. 177–201.

Karnell, Ester Herlin, "Reflection Note: EU Data Protection Rules and the Lack of Compliance In Sweden" i *Nordic Journal of European Law* Vol. 3 No. 2 (2020)

Kjølbro, Jon Fridrik, *Den Europæiske menneskerettigheds konventionen- for praktikere,* 4. utg., Jurist- og Økonomforbundets Forlag, 2017.

Kokott, Juliane og Christop Sobotta, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR" i *International Data Privacy law*, 2013, vol. 3 no. 4 side 223

Kuner, Christopher, Fred Cate, Orla Lynskey, Christopher Millard, Nora Ni Loideain og Dan Svantesson, "An unstoppable force and an immoveable object? EU data protection law and national security", i *International Data Privacy Law,* 2018, Vol. 8, No. 1

Lynskey, Orla, "Deconstructing Data Protection", i *International & Comparative Law Quartely*, Cambridge University Press 2014.

Mayer, Jonathan, Patrick Mutchler og John C. Mitchell, "Evaluating the privacy properties of telephone metadata", *Proceedings of the National Academy of Sciences of the United States of America*, 113(20), 5536-5541. DOI: https://doi.org/10.1073/pnas.1508081113

Peers, Steve og Sacha Prechal, *Scope and Interpretation of Rights and Priciples, The EU Charter of Fundamental Rights: A commentary,* Bloomsbury publishing, 2014.

Poscher, Ralf, "The Right To Data Protection- A No-Right Thesis" i Russell A. Miller (red.) *Privacy And Power- A transatlantic Dialogue in the Shadow of the NSA- Affair*, Cambridge University Press, 2017.

Sejersted, Fredrik, Finn Arnesen, Finn Rognstad Ole-Andreas Rognstad, Sten Foyn, Olav Kolstad, *EØS-rett*, 3. utgave, Universitetsforlaget, 2011.

Skoghøy, Jens Edvin A. "Nasjonal skjønnsmargin etter EMK" i, *Lov og rett* 2011,4, årgang 4, side 189-190

Sloot, Bart van der og Eleni Kosta, "Big Brother Watch and Others v UK: Lessons from the Latest Strasbourg Ruling on Bulk Surveillance," i *European Data Protection Law Review* (EDPL) 5, no. 2 (2019)

Solheim, Stig Harald "Rettsanvendelsesprosessen på EMK-rettens område" i Alf Petter Høgberg (red.) og Jørn Øyrehagen Sunde (red.), *Juridisk metode og tenkemåte, Universitetsforlaget*, 2019 s. 361, Juridika

Vogiatzoglou, Plixavra. "Centrum for Rattvisa v Sweden: Bulk Interception of Communications by Intelligence Services in Sweden Does Not Violate the Right to

Privacy." *European Data Protection Law Review* (EDPL), vol. 4, no. 4, 2018, p. 563-567. HeinOnline.

Utenlandske rettskilder

Lag 2008:717

Lagen (2003:389) om elektronisk kommunikasjon (LEK)

Lagen om försvarsunderrättelsesverksamhet (2000:130)

Lagen om signalspaning i fôrsvarsunderrättelsesverksamhet (2008:717)

Tysk dom, BverfG, 1 BvR 209/83. Dom av 15. desember 1983. Tilgjengelig på http.//www.servat.unibe.ch/dfr/bv065001.html

Andre kilder

Written observations by The Kingdom of Norway av 14.02.2018 til EU-domstolen i sak C-623/17 Privacy International inntatt som vedlegg 1 til avhandlingen.

Orwell, George *1984,* Gyldendal 1950.

https://naob.no/ordbok/newspeak (03.03.2021)

https://www.nrk.no/urix/dansk-etterretning-skal-ha-samarbeidet-med-nsa-1.15138231 (29.08.2020)

Etterretningstjenestens nettsider: https://forsvaret.no/organisasjon/etterretningstjenesten (01.07.2020)

https://snl.no/de_hemmelige_tjenester (22.09.2020).

https://nsm.no/om-oss/dette-er-nsm/ (22.09.2020).

https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Fokus2021-web.pdf/_/attachment/inline/b9d52b53-0abe-4d1c-9c51-bf95796560bf:8dd66029b7efb38aab37d13e8b387d2e6ed0bd05/Fokus2021-web.pdf (09.02.2021)

https://www.regjeringen.no/contentassets/556459ec77bd448f828af034dd573e11/horingsnotat---forslag-til-ny-lov-om-etterretningstjenesten.pdf (17.09.2020)

https://www.nix.no/ (01.10.2020)

https://nrkbeta.no/2019/02/14/slik-kan-den-nye-etterretningsloven-pavirke-deg/ (13.09.2020)

https://snl.no/domene_-_IT (01.10.2020).

https://nrkbeta.no/2019/02/14/slik-kan-den-nye-etterretningsloven-pavirke-deg/ (01.10.2020).

https://www.cloudflare.com/learning/network-layer/internet-protocol/ (13.09.2020).

https://www.live.infrapedia.com (21.09.2020).

https://snl.no/internettprotokoll (01.10.2020)

Datatilsynets høringssvar av 06.02.2019, tilgjengelig på: https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/?uid=e0b87829-2c74-4f2c-8066-c75801bcd0d5 (15.03.2021)

https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest (14.09.2020)

Uttalelse 5/2019 fra Det europeiske Personvernrådet (EDPB), tilgjengelig på: https://edpb.europa.eu/our-work-tools/our- documents/styrelsens-yttrande-art-64/opinion-52019-interplay-between-eprivacy_en (15.03.2021)

Digitalt grenseforsvar (DGF) Lysne II-utvalgets utredning til forsvarsdepartementet. Tilgjengelig: https://www.regjeringen.no/globalassets/departementene/fd/dokumenter/lysne-ii-utvalgets-rapport-2016.pdf (15.03.2021)

Working Party on Information Exchange and Data Protection (DAPIX). Se https://www.consilium.europa.eu/en/council-eu/preperatory-bodies/working-party-information- exchange-data-protection/# (11.01.2021)

Tilbyderoversikt fra NKOM, tilgjengelig: https://www.nkom.no/files/ekomstat/Tilbyderoversikt.pdf (22.02.2021)

JPCIPB. 2016. Written Evidence to the Joint Parliamentary Committee on the Investigatory Powers Bill. Tilgjengelig: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/d raft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26854.html (22.02.2021)

Rapport fra 20. oktober 2017 fra European Union Agency for fundamental rights Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU Volume II. Field perscpectives and legal update. Tilgjengelig: https://fra.europa.eu/sites/defaul/files/fra_uploads/fra- 2017-surveillance-intelligence-services-vol-2_en.pdf (08.01.2021).

https://www.aftenposten.no/verden/i/vAl14j/dansk-etterretning-drev-ulovlig-overvaaking-av-dansker (15.03.2021)

EUs hjemmesider: https://europa.eu/european-union/about-eu/eu-in-brief_en (25.03.2021).

Publication office of the European Union, "How the European Union Works", DOI:10.2775/11255.

https://snl.no/Europarådet#-Venezia-kommisjonen (30.03.2021)

https://www.youtube.com/watch?v=Eid-fncaKEk&t=1190s (05.04.2021) (Ca. 19 minutter ut i avspillingen).

Datatilsynets høringsuttalelse 18.01.2017 til Forsvarsdepartementet. Tilgjengelig her: https://www.regjeringen.no/contentassets/84a90462cf9b4aebb310d97052083d26/horingssvar-med-merknader-datatilsynet-digitalt-grenseforsvar.pdf?uid=Datatilsynet

Høringsvar til Lysne II utvalgets rapport om digitalt grenseforsvar. Tilgjengelig her: https://www.regjeringen.no/no/dokumenter/horing-av-rapport-avgitt-av-lysne-ii-utvalget-om-digitalt-grenseforsvar/id2513635/?expand=horingssvar&lastvisited=b6c6e5c6-167a-421f-97d6-6f032afba031

EMDs nettsider: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/213 (30.04.21)