E-tjenestens elektronisk bulkinnsamling som lovlig etterretning

Vil E-tjenestens bulkinnsamling eller «bulkaksess» foreslått i DGF-forslaget være uforenlig med Grunnloven § 102?

Kandidatnummer: 81

Antall ord:12061

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

01.06.2018

Innholdsfortegnelse

1 Introduksjon, tema og problemstilling

1.1 Introduksjon

I denne avhandlingen skal det fokuseres på problemstillinger knyttet til elektronisk personvern og statlige inngrep i borgerens personvernrettigheter i etterretningssammenheng. Hovedfokuset blir rettet mot det nye statlige forslaget for å utvide Etterretningstjenestens (E-tjenesten) kapasitet med et nytt verktøy og hvordan det vil utfordre de grunnlovfestede personvernrettighetene som eksisterer i norsk rett.

Avhandlingen skal først kort presentere tema og problemstillingen for avhandlingen, vise hva det nye tiltaket går ut på og redegjøre for rettskilder som er relevante for rettsområdet som det nye tiltaket berører. Deretter skal avhandlingen argumentere for hvorfor det er relevant å diskutere gjeldende norske personvernregler i etterretningssammenheng og hvorfor det nye tiltaket vil bli omfattet av de gjeldende personvernrettighetene. Videre vil avhandlingen diskutere rettsvilkår som er stilt av de relevante rettskildene til tiltak som gjør inngrep i personvernsrettighetene og hvordan det nye tiltaket forholder seg til disse vilkårene.

1.2 Tema og Problemstilling

1.2.1 Tema

Moderne kommunikasjonsmidler er instrumentale i den teknologiske utviklingen det moderne samfunnet opplever. I de siste årene har særlig internett fått en sentral posisjon, og statistikker fra SSB[1] viser at omtrent 90% av befolkningen i Norge bruker internett, nettbaserte medier eller tjenester daglig. På grunn av dette har internett fått en stadig større betydning for

[1] Statistisk Sentralbyrå, Norsk mediebarometer, https://www.ssb.no/kultur-og-fritid/statistikker/medie/aar (Hentet 31/05/2018, sist oppdatert 19/04/2018)

bedrifter, media og politiske virksomheter. Dette forklarer hvorfor integreringen av statlige institusjoner og organer inn i en digital verden har blitt en prioritet for staten i de siste årene.[2]

Den uheldige siden ved denne utviklingen er at det blir stadig mindre av et annet viktig gode – personvern. Omtrent alle aktiviteter på internett etterlater spor etter seg, noe som, kombinert med den voksende popularitetenav internett-baserte tjenester, fører til at enorme mengder personlig informasjon passerer gjennom digitale kanaler daglig. Naturligvis har statlige organer stor interesse i å ha tilgang til denne store informasjonsskyen.

Det er gode grunner for at staten skal ha slik tilgang. De nye kommunikasjonsmidlene gjør det enklere for kriminelle grupper å planlegge og samordne lovstridig aktivitet. Samtidig kan sårbarhetene i den elektroniske infrastrukturen misbrukes til å utføre stadig mer sofistikerte angrep som blir stadig mer ødeleggende ettersom flere essensielle tjenester, også viktige statlige organer, blir en del av den store digitale infrastrukturen. Det er i samfunnets interesse at det skal finnes et effektivt forsvar som kan redusere og motvirke disse truslene, og i Norge har det lenge eksistert organer som skal ta seg av dette. Et av disse organene er E-tjenesten.

E-tjenesten er landets nasjonale – sivile og militære – og sektorovergripende strategiske utelandsetterretningstjeneste som har som formål å fremskaffe informasjon om og varsle trusler mot Norge og norske interesser, understøtte viktige politiske beslutningsprosesser med relevant informasjon vedrørende fokus for norsk utenriks-, sikkerhets- og forsvarspolitikk og støtte forsvarets operasjoner hjemme og ute i verden.[3] I dag innhenter E-tjenesten store mengder informasjon som transporteres i luftgrensesnittet, som for eksempel over satellitt, eller opplysninger som er tilgjengelige i åpne kilder, som for eksempel sosiale medier.[4] Mesteparten av elektronisk kommunikasjon skjer likevel gjennom fiberoptiske kabler som går inn og ut av landegrensen, noe som E-tjenesten ikke har tilgang til i dag.

I forsøk på å utvide E-tjenestens etterretningskapasitet har forsvarsdepartementet i brev av 24. februar 2016 oppnevnt et utvalg med mandat om å utrede sentrale problemstillinger knyttet til E-tjenestens tilgang til elektronisk informasjon som kommuniseres i fiberoptiske kabler inn og ut av Norge. Olav Lysne ble valgt som leder av det som nå heter Lysne II-utvalget. Resultatet av deres arbeid ble et forslag med tittelen «Digitalt Grenseforsvar» (DGF).

[2] St. Meld. 27 (2015-2016) Digital Agenda for Norge.
[3] Lysne II – utvalget 26.08.16: DGF s. 13
[4] Lysne II – utvalget 26.08.16: DGF s. 29

I utredningen ble DGF definert slik:

«*E-tjenestens målrettede innhenting og analyse av utenlandsketterretningsrelevant informasjon, basert på aksess til elektronisk kommunikasjon som går inn og ut av Norge, i den hensikt å kartlegge og motvirke mulige ytre trusler mot rikets sikkerhet og selvstendighet og andre viktige nasjonale interesser*.»[5]

Med andre ord vil forslaget gi Etterretningstjenesten et nytt virkemiddel for å skaffe informasjon for sin virksomhet. Dette middelet er nytt for norsk rett og setter en ny standard for hvordan staten forholder seg til balansen mellom personvern og nasjonal sikkerhet.

Datainnsamlingsinngrep er ikke noe nytt og eksisterer i norsk rett på flere måter[6]. Bruken av dem er med rette svært begrenset. I noen tilfeller er bruk av datainnsamlingstiltak betinget av et mistankekrav eller et krav om et særlig definert mål. I andre tilfeller er denne typen inngrep begrenset i sitt tekniske omfang og kan kun skje etter en særlig godkjennelse fra en lovbestemt myndighet, som for eks. lov. 22.05 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven) § 216o (dataavlesning). Disse begrensningene ble ansett for å være nødvendige for at slik inngripende myndighetsutøvelse ikke utfordrer personvernhensyn mer enn det var nødvendig. DGF-forslaget utfordrer disse etablerte begrensningene ved å foreslå flere tiltak hvor digital informasjon blir lagret på en generell basis uten at noen spesifikke mål er angitt og uten at det er påkrevd noe eksplisitt mistankekrav. I tillegg har den teknologiske utviklingen ført til at det blir omtrent ingen tekniske begrensninger som kan redusere effektiviteten av digitale datainnsamlingstiltak, slik som tilfellet er med de eksisterende lignende inngrep. Med andre ord har det blitt mye enklere og billigere å overvåke andre. Det naturlige spørsmålet blir da: hvor går den egentlige grensen? Temaet for denne avhandlingen er derfor digital overvåkning med fokus på grensene for statlig digital overvåkning av norske borgere.

[5] Lysne II – utvalget 26.08.16: DGF s. 10
[6] Se for eks. lov. 22.05 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven) kap. 16.

1.2.2 Tekniske begreper

Digital overvåkning er et omfattende tema og tiltaket som er diskutert i avhandlingen er teknisk komplisert. Derfor skal avhandlingen redegjøre for de viktigste begrep som er relevante for problemstillingen og forklare akkurat hvilket aspekt ved DGF som blir behandlet.

Bulkinnsamling (Bulkaksess)[7] - virksomhet hvor etterretningstjenester innsamler store mengder informasjon i form av metadata før de eventuelt søker etter informasjon som er relevant for utenlandsetterretningsformål i den store datamengden med bruk av mer målrettede midler.

Metadata – Data som beskriver annen data eller som inneholder ekstra informasjon knyttet til data. Dette kan for eksempel være data som beskriver typen eller formatet på innholdet, eller ekstra informasjon knyttet til innholdet, som for eksempel navn på forfatter/avsender, størrelse eller mottaker. I forhold til DGF vil lagring av metadata være begrenset til den type metadata som ikke avslører innholdet i dataene, og som ikke avslører handlinger foretatt av en bruker på nettsteder eller sosiale medier som for eksempel informasjon om hvilke søk brukeren har utført. [8]

Trafikkdata - elektroniske opplysninger som viser hvor, hvordan, fra hvem og når informasjon ble sendt. Har likheter med metadata men som regel inneholder ikke informasjon som temaet for en e-post eller brukernavn på en internettjeneste.

Innholdsdata – Data som ikke er metadata – for eksempel innholdet i en sms, epost, facebook-melding og lignende. [9]

[7] Lysne II – utvalget 26.08.16: DGF s. 10
[8] Sitat fra vedlegg 4 til Lysne II – utvalget 26.08.16: DGF s. 88
[9] Sitat fra vedlegg 4 til Lysne II – utvalget 26.08.16: DGF s. 88

Overskuddsinformasjon – i forslaget ble overskuddsinformasjon definert som «informasjon som ligger utenfor E-tjenestens ansvarsområde, men som E-tjenesten likevel kommer i besittelse av som følge av dens virksomhet rettet mot forhold innenfor ansvarsområdet».[10]

1.2.3 Problemstillingen

DGF-forslaget presenterer flere tiltak som går ut på innsamling og lagring av elektronisk informasjon. Blant de forskjellige tiltakene er det to som er mest relevant for temaet - bulkinnsamling av metadata og målrettet innsamling av innholdsdata. Denne avhandlingen skal fokusere på problemstillinger knyttet til E-tjenestens bulkinnsamling av metadata. E-tjenestens målrettet tilgang til innholdsdata skal kun nevnes når det har betydning for bulkinnsamlingen.

Videre er det mange aspekter ved bulkinnsamling av metadata som kan diskuteres i juridisk perspektiv. Spørsmål om innsamling av informasjon, lagring av denne og spørsmål om tilgang til og bruk av denne informasjonen må vurderes forskjellig fordi det er ulike innvendinger, hensyn og problemer som oppstår i hver type situasjon. Denne avhandlingen fokuserer seg primært til selve innsamlingen av informasjonen rettet mot norske borgere fra statens side og personvernspørsmål som gjør seg gjeldende for denne handlingen.

Andre aspekter vedrørende DGF vil likevel i varierende grad analyseres så lenge de har innvirkning på innsamlingsaspektet. For eksempel er lagringstiden og lagringsmåten til informasjonen ikke i seg selv en del av innsamlingshandlingen, men den måten informasjonen er lagret og eventuelt brukt gir innsamlingshandlingen forskjellig rettslig karakter.

Basert på denne avgrensningen kan hovedproblemstillingen for denne avhandlingen formuleres slik:

Vil E-tjenestens bulkinnsamling eller «bulkaksess» foreslått i DGF-forslaget være uforenlig med Grunnloven § 102?

[10] Lysne II – utvalget 26.08.16: DGF s 60, fotnote 94

2 Bulkinnsamlingen og Metode

I dette kapittelet skal jeg presentere de viktigste rettskildene som er brukt for å besvare avhandlingens problemstilling. Etterretningstjenestens overvåkning er et tema som ikke er særlig diskutert i jussen, noe som skaper flere utfordringer i analysen av lovligheten til Etterretningstjenestens foreslåtte bulkaksesskapasitet. Det åpenbare er at det er ingen ferdig og nøyaktig lovregulering av bulkinnsamlingstiltaket som kan analyseres og settes i forhold til Grunnloven § 102. Analysen må bygges utelukkende på et forslag til lovregulering, som er unøyaktig og presenterer kun de veiledende retningslinjene og prinsippene eventuelle lovbestemmelser kan bygges på. Mangel på analogiske tiltak i Norge utelukker også relevant rettspraksis knyttet til lovreguleringen av bulkaksess i nasjonale rettskilder.

2.1 Rettsområdet og Rettskildebruk

2.1.1 Grunnloven og internasjonale menneskerettigheter

Hovedproblemstillingen for avhandlingen skal diskuteres med utgangspunkt i Grunnloven § 102, og andre supplerende rettskilder som forarbeider og juridisk litteratur knyttet til denne bestemmelsen. DGF-forslaget påpeker at bulkinnsamlingen vil kreve ny lovregulering[11], men ingen lovregulering kan gå i direkte strid med Grunnloven § 102 i kraft av lex superior-prinsippet. Derfor er denne bestemmelsen det naturlige utgangspunktet for vurderingen av grenser for digital overvåkning av norske borgere i norsk rett.

Den gjeldende versjonen av Grunnloven § 102 er relativt ny og det er få andre nasjonale rettskilder som tar opp spørsmålet om hvordan Grunnloven § 102 skal tolkes i forhold til omfattende overvåkningstiltak. Blant relevant nasjonal rettspraksis er det Rt. 2014 s. 1105, som handler om bruk av overskuddsmateriale som var igjen etter etterforskning med bruk av kommunikasjonskontroll. Spørsmålet var om overskuddet kunne brukes som bevis i en ny sak. Høyesterett avklarer i denne saken hvordan bruk og lagring av personlige opplysninger skal skje i samsvar med Grunnloven § 102. Det er også andre saker som gir generell avklaring

[11] Lysne II – utvalget 26.08.16: DGF s. 60

om bestemmelsens innhold, men for å finne praksis i forhold til omfattende datainnsamlingstiltak må en foreløpig gå til internasjonal rett. Grunnloven § 102 må tolkes i samsvar med den korresponderende bestemmelsen i Den Europeiske Menneskerettskonvensjon[12] (EMK), nemlig EMK art. 8 og Den Europeiske Menneskerettsdomstolens (EMD) rettspraksis vedrørende den.[13] Et lignende interesseområde er regulert i SP[14] artikkel 17 som for det meste samsvarer[15] med bestemmelsen i EMK art. 8.

EMK art. 8 gir vern til fire grunnleggende rettigheter – privatlivet, familielivet, hjemmet og korrespondansen. Det er ikke praktisk å skille mellom de forskjellige rettighetene i elektronisk overvåkningssammenheng fordi de fleste elektroniske datalagringstiltak vil i varierende grad gjøre inngrep i flere av disse rettighetene, noe som er illustrert av EMDs avgjørelser som blir behandlet i avhandlingen.

Det er mange saker fra EMD som kommer til å bli nevnt i avhandlingen men det er særlig tre som handler om tiltak som ligner på bulkinnsamlingen som er foreslått i DGF-forslaget.

I Malone mot Storbritannia[16] tar EMD stilling til en klage over hemmelig overvåkning fra politiet som hadde myndighet til å innhente informasjon om telefonisk kommunikasjon, som for eksempel telefonnummer til samtalepartneren. EMD har konstatert et brudd på EMK art. 8. Det samme skjedde i Liberty og andre mot Storbritannia[17], som gjaldt en klage knyttet til et strategisk overvåkningstiltak. Dette tiltaket har mye til felles med bulkinnsamlingen beskrevet i DGF-forslaget fordi det britiske tiltaket omfattet alt av elektronisk kommunikasjon som krysset grensen til Storbritannia. Også i dette tilfellet har EMD konstatert brudd på EMK art. 8. Hovedbegrunnelsene for konklusjonen er hovedsakelig de samme for begge sakene. Det motsatte skjedde i Weber and Saravia mot Tyskland[18]. I denne saken har det tyske tiltaket (kjent som G10) blitt prøvd mot EMK art. 8 men, til forskjell av de siste to sakene, så gikk konklusjonen i favør av Tyskland.

---

[12] Jf. lov 21.05.1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven).
[13] Se bl. annet. Rt. 2014 s. 1105, Rt. 2015 s. 81 og Aall, Jørgen, *Rettsstat og menneskerettigheter*, 4. utgave, Bergen 2015, s. 214.

[14] Den internasjonale konvensjonen om sivile og politiske rettigheter med protokoller
[15] Se. Rt. 2015 s.81 avsnitt 60.
[16] EMD 02.08.1984 (saksnummer 8691/79)
[17] EMD 01.07.2008 (saksnummer 58243/00)
[18] EMD. 29.06.2006 (saksnummer 54934/00)

Alle sakene ovenfor handler om omfattende overvåkningstiltak. To av de inneholder bulkaksesselement som er sammenlignbar med bulkaksesstiltaket i DGF-forslaget. Analyse av EMDs argumentasjon mellom disse sakene kan vise hvordan kravene i EMK art. 8 og, som følge, Grunnloven § 102 stiller seg til omfattende overvåkningstiltak. Videre må det understrekes at overvåkningstiltaket i Weber and Saravia mot Tyskland har klare likheter med tiltaket i forslaget. Den første likheten ligger i teknisk gjennomføring. I likhet med DGF, inneholder tiltaket både et målrettet datainnsamlingstiltak og et bulkinnsamlingstiltak. Det er også likheter i formålet til overvåkningen, nemlig å beskytte nasjonale interesser fra alvorlige trusler uten at det foreligger konkret mistanke om slike trusler. En viktig forskjell er at DGF innebærer at E-tjenesten får tilgang til informasjon som går gjennom fiberoptiske kabler over grensen til Norge, mens det tyske tiltaket omfatter trådløs telefonkommunikasjon. Derfor kan EMDs argumentasjon vedrørende nødvendighet og proporsjonalitet i forhold til G10 også være nyttig for vurderingen om bulkaksesstiltaket i DGF vil stride mot EMK 8.

2.1.2 E-Loven, EOS-Kontrolloven og E-Instruksen

DGF-forslaget gjelder omtrent utelukkende Etterretningstjenesten og deres etterretningskapasitet. I dag er E-tjenestens overordnede virksomhet og oppgaver regulert i E-loven.[19] Loven gir regjeringen omfattende reguleringshjemmel både når det kommer til den administrative organiseringen av etterretningstjenesten som et organ og på områder som gjelder de oppgavene som Etterretningstjenesten jobber med, jf. lovens § 2 siste ledd og § 3 siste ledd. Reglene i Instruksen om Etterretningstjenesten (E-instruksen)[20] utdyper de generelle bestemmelsene i loven med mer konkrete regler.

Det er flere bestemmelser i E-loven som er relevante i forhold til det foreslåtte bulkaksesstiltaket. Tiltak som er foreslått i DGF-forslaget kan oppfattes for å være i strid med begrensningene i E-lovens § 4. E-tjenestens virksomhet er primært rettet mot utlandet og fremmede parter og håndtering av om informasjon vedrørende utenlandske forhold angår norske interesser, jf. E-loven § 3 første ledd. E-lovens § 4 første ledd oppstiller en generell regel for forholdet mellom E-tjenesten og norske fysiske og juridiske personer som sier at E-

[19] Lov 20. mars 1998 nr. 11 om Etterretningstjenesten.
[20] Instruksen om Etterretningstjenesten gitt ved kgl.res. 31. august 2001

tjenesten skal ikke på «norsk territorium overvåke eller på annen måte innhente informasjon om norske fysiske eller juridiske personer». Forarbeidene[21] peker på at dette forbudet var inntatt for å først og fremst understreke at E-tjenestens arbeid var rettet mot trusler som kommer utenfra. Videre i andre ledd er det inntatt en begrensning til E-tjenestens adgang til å oppbevare informasjon som gjelder norske fysiske eller juridiske personer. Den grunnleggende regel er at oppbevaringen kan kun finne sted dersom det er i samsvar med formål gitt i E-lovens § 3. Etter gjeldende rett og med gjeldende kapasitet vil E-tjenestens virksomhet i utgangspunktet ikke gjøre inngrep inn i rettssfæren til norske borgere. Hvordan bulkaksesskapasiteten kommer til å utfordre denne begrensningen kommer til å bli et tema videre i avhandlingen.

En annen side vedrørende E-tjenestens virksomhet som er relevant for problemstillingen er behandlingen av overskuddsinformasjon, særlig E-tjenestens deling av overskuddsinformasjon med andre statlige myndigheter. Reglene for dette finnes i E-instruksen § 5, som gir generell tilgang til å dele overskuddsinformasjon som ikke kan lagres av E-tjenesten til den rette offentlig myndighet. Etter gjeldende rett kan dette samarbeidet fortsette dersom E-tjenesten får utvidet etterretningskapasitet i form av bulkaksess. Avhandlingen vil ta opp hvordan forslaget stiller seg til denne eventuelle muligheten og hva det har å si for lovligheten av bulkaksesstiltaket.

EOS-kontrolloven (kontrolloven)[22] var laget med formålet om å gi Stortinget et utvalg med kapasitet til å kontrollere etterretnings, overvåkings – og sikkerhetstjeneste som utføres av den offentlige forvaltning eller under styring av eller på oppdrag av denne (EOS-utvalget) jf. kontrolloven § 1. EOS-utvalget skal ifølge kontrolloven § 2 (1) punkt 1-3 «klarlegge om og forebygge at noens rettigheter krenkes, herunder påse at det ikke nyttes mer inngripende midler enn det som er nødvendig etter forholdene, og at tjenestene respekterer menneskerettighetene, påse at virksomheten ikke utilbørlig skader samfunnets interesser og påse at virksomheten holdes innen rammen av lov, administrative eller militære direktiver og ulovfestet rett.»

DGF er foreslått som et nytt verktøy for E-tjenesten, noe som betyr at dersom E-tjenesten får DGF-kapasitet, kommer etterretningsvirksomheten knyttet til DGF også være underlagt EOS-

[21] Ot.prp. nr. 50 s. 10
[22] Lov 3. april 1995 nr. 7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-kontrolloven)

utvalgets kontroll med gjeldende lovgivning. Hvordan dette faktum påvirker lovligheten av bulkaksesstiltaket kommer også til å bli et tema i avhandlingen.

Til sist må det nevntes at i dag er lagring av data, elektroniske opplysninger og sikring av personvern på internett regulert av Datatilsynets kontroll etter personopplysningsloven[23].[24] E-tjenesten er likevel unntatt fra lovens melde- og konsesjonsplikt og Datatilsynets tilgang og kontroll med personopplysningene, jf. personopplysningsloven § 44 første til tredje ledd, jf. personvernforskriften § 1-2. [25] Dette ansvaret ligger i stedet på EOS-utvalget, jf. avsnittet ovenfor.[26]

2.1.3 EU og Datalagringsdirektivet

Datalagringsdirektivet[27] (DLD) er et EU-direktiv som ble vedtatt i 2006 og kom i kraft 2007-2009. Direktivet skulle fungere som et påbud for tele- og internett tilbydere om å lagre elektronisk trafikkdata som skal senere brukes av medlemsstatenes politi og sikkerhetsmyndigheter. I Norge ble direktivet vedtatt av Stortinget som følge av EØS-samarbeidet den 4. april 2011, men ble aldri implementert på grunn av flere utsettelser.

EU-domstolen konkluderte 8. april 2014 [28] at DLD er ugyldig. Domstolen har uttalt at direktivet strider med EU-charteret [29] artikkel 7 og 8 om retten til privat liv og personvern. Det var i tillegg fastsatt at direktivet gikk lenger enn unntaksadgangen artikkel 52 åpnet for. Eventuelt førte dette til at arbeidet med å implementere direktivet i Norge ble stanset.

Norge er ikke medlem av EU, noe som betyr at DLD ikke kunne anvendes direkte i Norge. Det betyr også at Norge ikke er direkte bundet av EU-charteret. Likevel er personvernreglene i EU-charteret sammenlignbare med reglene i EMK og Grunnloven § 102. Derfor kan avgjørelser rundt DLD ha betydning for problemstillingen, ettersom DLD er en av de mest omfattende datalagringstiltak som har til nå blitt introdusert og brukt i mange land med

[23] Lov 14.04.2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).
[24] Se NOU: 2009:1 Individ og integritet s. 246-247

[25] Jf. forskrift om behandling av personopplysninger (personopplysningsforskriften) § 1-2 første ledd.
[26] Lysne II – utvalget 26.08.16: DGF s. 17
[27] EU-direktiv 2006/24/EF
[28] Digital Rights Ireland Ltd. Sak C-293/12
[29] EU Charter of fundamental rights of the European Union, 2012/C 326/02

rettssystemer som er sammenlignbare med Norge. I forslaget er det også skrevet at DLD-dommen er relevant for DGF fordi den «gir uttrykk for gjeldende europeiske standarder for personvern og håndtering av personvernopplysninger.» [30] Rettspraksis relevant til DLD kan da belyse hvordan bulkaksesstiltaket i DGF-forslaget ville blitt vurdert i forhold til Grunnloven § 102.

Selv om DLD ble underkjent i Europa og kommer ikke til å bli implementert Norge, så betyr ikke det at Norge har skrapt alle planer om å implementere et tiltak som dette. I en utredning[31] «Datalagring og menneskerettighetene» (2015) avgitt til Justisdepartementet og Samferdselsdepartementet er det vurdert om det er mulig å implementere et lignende tiltak som kommer til å tilfredsstille både nasjonale og internasjonale krav til privatliv. I utgangspunktet er det vurdert om det er mulig å rette de feilene som den Europeiske domstolen har poengtert. Noen av disse vurderingene kan også være nyttige for avhandlingen fordi de viser hvordan staten vil løse (eller likevel akseptere) de manglene som EU-domstolen påpekte i DLD-dommen og hvordan de samme løsningene kan bli brukt på forhold knyttet til bulkinnsamlingen presentert i DGF-forslaget.

2.2 DGF som overvåkningsmekanisme

Etterretningstjenesten har som formål å beskytte norske interesser ved å skaffe informasjon i forhold til fremmede makter og trusler. I utredningen[32] er det nevnt at DGF er et nytt verktøy for å ivareta dette formålet. Dette virkemiddelet er begrunnet med det skiftende trusselbildet, hvor elektroniske trusler øker i antall, omfang og kompleksitet.

Som argument for utvidelsen av E-tjenestens kapasitet peker forslaget[33] blant annet på E-tjenestens begrensede mulighet til å få innsikt i kommunikasjonen mellom internasjonale terrororganisasjoner og ukjente personer i Norge og at norske myndigheter i dag har minimal

[30] Lysne II – utvalget 26.08.16: DGF s. 62
[31] Hans Petter Graver og Henning Harborg, En utredning avgitt til Justisdepartementet og Samferdselsdepartementet 1. oktober 2015 – (UTRDJ-2015-1)
[32] Lysne II – utvalget 26.08.16: DGF s. 5
[33] Lysne II – utvalget 26.08.16: DGF s. 28

mulighet til å avdekke at andre stater driver spionasje mot norske offentlige og private virksomheter ved hjelp av digitale midler.

I utgangspunktet faller dette under de lovbestemte formål med Etterretningstjenestens virksomhet etter E-loven. Likevel vil det ikke være uproblematisk å utvide Etterretningstjenestens kapasitet med et bulkinnsamlingstiltak. Det er både tekniske og rettslige grunner for dette. Det skal derfor forklares hvordan virksomheten som i utgangspunktet ikke har som formål å berøre interessene til de norske borgere vil likevel gjøre det på grunn av det tekniske omfanget med bulkaksess.

2.2.1 Bulkaksess og overvåkningens omfang

Mesteparten av kommunikasjon som går ut og inn i Norge går i fiberoptiske kabler.[34] Det er her det første problemet ved tiltaket oppstår, fordi innførselen av DGF innebærer at E-tjenesten får tilgang til den digitale kommunikasjonen som går gjennom disse fiberoptiske kablene, både den utgående og inngående. Isolert sett fremstår dette som innenfor E-tjenestens formål, fordi informasjonstilførselen blir begrenset i det at kommunikasjonen må først krysse grensen før den blir fanget opp av bulkaksesstiltaket, noe som betyr at kommunikasjonen mellom norske borgere vil i utgangspunktet ikke være omfattet av noen tiltak som er foreslått i DGF-forslaget. Da vil bulkaksess-tiltaket ikke utfordre formålsbegrensningene i E-lovens §§ 3 og 4.

Men i realiteten går mye av dagens elektroniske kommunikasjon i Norge gjennom utlandet og utenlandske servere. De aller fleste nettsider og elektroniske tjenester som blir brukt, som for eks. Facebook, Google og de fleste E-post tjenester, har de fleste av sine servere i utlandet. Dette betyr at mye elektronisk kommunikasjon som skjer mellom to norske borgere går gjennom de fiberoptiske kablene som tiltaket omfatter, selv om både senderen og mottakeren er norske fysiske eller juridiske personer som oppholder seg på norsk territorium, jf. E-loven § 4.

[34] Lysne II – utvalget 26.08.16: DGF s. 29

Ifølge vedtaket er det ikke praktisk mulig[35] å filtrere data slik at bare den informasjonen som er relevant for Etterretningstjenestens oppgaver blir tatt opp. Som følge av dette vil Etterretningstjenesten også ha tilgang til mye private opplysninger om kommunikasjonen til norske borgere, uansett om de oppholder seg i Norge eller ikke, så lenge kommunikasjonen krysser landets grenser gjennom de forannevnte fiberoptiske kablene. I praksis vil tiltaket da omfatte de fleste, om ikke alle, norske innbyggere. Dette utfordrer begrensningen i e-lovens § 4 første ledd.

Det kommer også fram at det teknologiske utstyret som gjør DGF mulig kan brukes til masseovervåkning av norske borgere [36] , selv om dette ikke er formålet med tiltaket. Lagringstiden til informasjonen er også relativt lang. Metadata vil bli lagret i opptil 18 måneder. Innholdsdata vil bli lagret «i så lang tid som anses nødvendig for å løse etterretningsoppdraget til E-tjenesten og maksimalt i 18 måneder.»[37] Overvåkningskapasiteten av DGF er bedre forstått hvis den er sammenlignet med et annet overvåkningstiltak, som i denne avhandlingen blir DLD. Selv om DLD aldri ble implementert i Norge, har direktivet vært et relativt stort diskusjonstema, fordi eventuell implementering var planlagt som del av EØS-samarbeidet. I tillegg har omfanget til DLD blitt vurdert av EU-domstolen flere ganger. DLD, og avgjørelser rundt dette direktivet, kan derfor bli brukt for å få et komparativt perspektiv.

Datalagringsdirektivet skulle fungere som et påbud for tele- og internett tilbydere om å lagre opplysninger om trafikkdata, lokaliseringsdata og abonnementsdata som fremkommer ved bruk av telefoni, mobiltelefoni, bredbåndstelefoni, e-post og internettaksess. [38] Det som blir lagret er data om hvem som kommuniserte med hvem, når kommunikasjonene fant sted, hvor kommunikasjonen skjedde og hvilken form ble benyttet. Dette er noe som i stor grad faller inn under definisjonen av «metadata» i DGF-forslaget. Innholdsdata skal ikke lagres i medhold av direktivet.[39] Data skulle lagres i minst 6 måneder og opptil 2 år fra kommunikasjonsdatoen.[40] Et viktig moment er at Direktivet overlater nasjonale myndigheter mye av detaljreguleringen. Reguleringen av lovhjemmelen, håndteringen, prosessuelle krav er overlatt til nasjonale myndighetene, noe som i utgangspunktet er forståelig fordi det handler

[35] Lysne II – utvalget 26.08.16: DGF s. 5
[36] Lysne II – utvalget 26.08.16: DGF s. 51
[37] Lysne II – utvalget 26.08.16: DGF s. 55
[38] Innst. 275 L (2010-2011) 1.2 (13/3/2018)
[39]EU-direktiv 2006/24/EF Artikkel 5.
[40] EU-direktiv 2006/24/EF Artikkel 6.

om et EU-direktiv som må implementeres og tilpasses rettssystemer som ikke er nødvendigvis like på alle områder.

DLD har mye likheter med bulkaksess-delen av DGF både i omfanget og gjennomføringsmåten. På noen områder går DGF enda lenger i hvor mye informasjon den vil gjøre tilgjengelig for staten, ved å tillate innhenting av innholdsdata basert på analyse av metadata. Når EU-domstolens konklusjon var at DLD åpnet for overvåkning som var i strid med proporsjonalitetsprinsippet, blir det overordnede spørsmålet om bulkaksess i DGF kan gjennomføres på en måte som ikke strider mot de grunnleggende prinsippene i norsk rett.

3 Bulkaksess og Lovlig Etterretning

3.1 Grunnloven § 102

DGF er presentert som en kombinasjon av flere tiltak som fungerer på forskjellige måter – bulkaksesstiltaket er kun en av flere mekanismer som er foreslått. Lignende tiltak har ikke vært innført i Norge før, og det er ikke opplagt om et tiltak som dette vil i det hele tatt være innenfor det som Grunnloven § 102 er ment til å regulere. I tillegg er det ikke opplagt at Grunnloven § 102 er relevant i forhold til Etterretningstjenestens virksomhet.

Analysen må derfor ta utgangspunkt i anvendelsesområdet til Grunnloven § 102 for å se om særlig bulkinnsamlingen av metadata er innenfor bestemmelsens anvendelsesområde.

3.1.1 Bestemmelsens anvendelsesområde

Grunnloven § 102 lyder:

«Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller.

Statens myndigheter skal sikre et vern om den personlige integritet.»

Spørsmålet er så om hvilke interesser er beskyttet og om bulkinnsamlingen av metadata vil i utgangspunktet true disse interessene. I følge Høyesterett i Rt. 2015 s. 93 har uttrykket «privatliv» ingen uttømmende definisjon og at basert på praksis fra EMD skal «… privatliv «omfatte menneskets fysiske og psykiske integritet, enkeltes identitet og personlig autonomi.»[41] Selv om innsamling av personlig informasjon kan true beskyttelsen av denne interessen er det klart at et tiltak som kontinuerlig samler inn informasjon om kommunikasjon vil lettere omfattes av ordlyden i «kommunikasjon» i bestemmelsen. Metadata er likevel ikke det som man vanligvis ser på som kommunikasjon i seg selv, fordi det er en form for digital adresse, med avsender, mottaker, osv. Vil Grunnloven § 102 omfatte innsamling av metadata?

[41] Rt. 2015 s. 93 avsnitt 58.

Spørsmålet må besvares med utgangspunkt i ordlyden av bestemmelsen. Uttrykket «kommunikasjon» blir vanligvis brukt for å beskrive selve handlingen, hvor en part deler informasjon med en annen, blant annet med bruk av en tekstmelding, telefonsamtale, et bilde eller video. «Kommunikasjon» er også brukt for å beskrive innholdet i en telefonsamtale eller tekstmelding. Dette er bekreftet i forarbeidene[42], hvor det står at uttrykket «kommunikasjon» ble bevisst valgt i stedet for «korrespondanse» som er brukt i EMK art. 8 første ledd for å omfatte moderne kommunikasjonsmetoder. Videre legger forarbeidene til grunn at innholdet av bestemmelsen slik som den er «… skal leses som at systematisk innhenting, oppbevaring og bruk av opplysninger om andres personlige forhold bare kan finne sted i henhold til lov, benyttes i henhold til lov eller ved informert samtykke og slettes når formålet ikke lenger er til stede». [43] Dette taler for at metadata slik som den er definert i DGF derfor er innenfor anvendelsesområdet til Grunnloven § 102.

EU-domstolens avgjørelse over DLD kan støtte opp mot dette. Informasjonen som DLD omfattet var hvem som kommuniserte med hvem, når kommunikasjonen fant sted, hvor kommunikasjonen skjedde og hvilken form ble benyttet.[44] Dette, som nevnt ovenfor, er hovedsakelig innenfor definisjonen av «metadata» som bulkinnsamlingen vil omfatte ifølge forslaget. Ordlyden i EU-charteret artikkel 7 og Grunnloven § 102 er sammenfallende og det er tvilsomt at det kan være store tolkningsforskjeller mellom disse bestemmelsene. Resultatet av DLD-dommen viser da at det er ikke nødvendig at den informasjonen som blir lagret har innholdet av kommunikasjonen for å være omfattet av kommunikasjonsvernet.[45]

Avgjørelser i EMD peker i samme retning. I Malone mot Storbritannia [46] sier EMD at informasjon om tidspunkt og lengde på telefonsamtaler og hvilke telefonnummer man har ringt til og fra, må regnes som et «integrert element» av telekommunikasjon og at politiets bruk av denne må regnes som et inngrep i rettighetene gitt av EMK art. 8. Det samme gjelder tilsvarende informasjon om bruk av E-post og internett, jf. Copland mot Storbritannia[47]. Ettersom Grunnloven § 102 må tolkes i lys EMD sin praksis i forhold til EMK art. 8, må dette

[42] Dok. 16-2011-2012 s. 178. (Rapport om Menneskerettighetsutvalget om menneskerettigheter i Grunnloven)
[43] Innst. 186 S (2013-2014) s. 27
[44] EU-direktiv 2006/24/EF Artikkel 5.
[45] Se Ingvild Bruce, «Datalagringsdirektivet – en menneskerettskrenkelse eller -forpliktelse?» *LOV OG RETT,* vol. 49, s. 1–2, 2010 (s. 9)
[46] EMD 02.08.1984 (saksnummer 8691/79) se avnistt 84 om «metering».
[47] EMD. 03.04.2007 (saksnummer 62617/00), avsnitt 41-43

være et sterkt argument for at bulkinnsamling av metadata er et inngrep omfattet av kommunikasjonsvernet i Grunnloven § 102.

En kan også se på dette fra en vinkel hvor kvaliteten til informasjonen i det som er kjent som «metadata» ikke er avgjørende. I Weber and Saravia mot Tyskland[48] var det konstatert at det ikke er kvaliteten til den informasjonen som blir innsamlet og lagret som er avgjørende i vurderingen om kommunikasjonsvernet er krenket. Selve eksistensen av et tiltak som samler inn personlig informasjon, også metadata, uten brukerens samtykke kan være et inngrep i kommunikasjonsvernet etter EMK art. 8. [49]Dermed må Grunnloven § 102 kunne anvendes ovenfor en bulkaksess tiltak som samler inn metadata så lenge denne kan inneholde opplysninger av personlig karakter.

Dette er også et argument for hvorfor Grunnloven § 102 vil være relevant for etterretningstjenestens virksomhet ovenfor utlandet i denne sammenheng. Selv om formålet med bulkinnsamlingen ikke er rettet direkte mot norske borgere og det er lite sannsynlig at deres personlige opplysninger kommer til å bli brukt av E-tjenesten, så vil bulkinnsamlingen uansett være et inngrep ovenfor dem fordi bulkaksesstiltaket kommer til å samle inn og lagre deres personlige informasjon uten deres samtykke. Dette er hovedbegrunnelsen for hvorfor Lysne II-utvalget tar utgangspunkt i at bulkinnsamlingen er innenfor anvendelsesområdet til Grunnloven § 102[50] og EMK art. 8. Selv om EMK i utgangspunktet ikke er til hinder for at E-tjenesten kan drive utenlandsk etterretning, så må virksomheten holdes innenfor konvensjonens ramme.[51]

Konklusjonen blir da at bulkinnsamlingen av metadata i DGF-forslaget er regulert av Grunnloven § 102.

---

[48] EMD. 29.06.2006 (saksnummer 54934/00), avsnitt 78.
[49] Jørgen Aall, *Rettsstat og menneskerettigheter*, 4. utgave, Bergen 2015, s. 226
[50] Lysne II – utvalget 26.08.16: DGF s. 39
[51] Se Ragnar Line Auglend, og Henry John Mæland, *Politirett*, 3. utgave, Oslo 2016 s. 396 og Erik Møse, «Forholdet mellom visse sider ved de hemmelige tjenester og menneskerettighetskonvensjonene», vedlegg 2 i Dok. nr.15 (1995-1996) s. 595-609.

3.1.2 Hva er "lovlig etterretning"?

Det er nå avklart at et tiltak som samler inn metadata i bulk er innenfor anvendelsesområdet til Grunnloven § 102. Det neste spørsmålet blir da om hvordan dette vil påvirke tiltaket. Bestemmelsen verner retten til «respekt for sitt privatliv» og «kommunikasjon», men hva ligger i dette kravet?

I Rt. 2014 s. 1105 referer Høyesterett til Innst. 186 S (2013-2014) side 27, og legger til grunn at Grunnloven § 102 «skal leses som at systematisk innhenting, oppbevaring og bruk av opplysninger om andres personlige forhold bare kan finne sted i henhold til lov, benyttes i henhold til lov eller informert samtykke og slettes når formålet ikke lenger er til stede». Videre føyer Høyesterett til at «hvorvidt en lov som griper inn i privat- og familielivet, hjemmet, kommunikasjonen eller den personlige integritet, er forenlig med § 102, også beror på om loven ivaretar et legitimt formål og er forholdsmessig».

Dette viser først og fremst at det kan gjøres inngrep i retten etter Grunnloven § 102 til tross for at det ikke kommer klart ut av lovteksten. Annen rettspraksis[52] støtter opp mot dette og viser til unntaket i EMK artikkel 8[53] andre ledd som fastslår uttrykkelig at offentlige myndigheter har en viss margin for inngrep så lenge de holder seg innenfor bestemmelsens betingelser. Dette synspunktet er også lagt til grunn i Innst. 186 (2013-2014) på s. 27, hvor det står at «respekt for» skal forstås som at «lovlig etterretning ikke er utelukket».

Problemstillingen i avhandlingen vil da avhenge av spørsmålet om bulkaksess tiltaket, slik som den er beskrevet i DGF-forslaget, kan holde seg innenfor den marginen som Grunnloven § 102 tillater.

EMK art. 8 andre ledd lyder:

«Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge

[52] Bl. annet. Rt. 2014 s. 1105, Rt. 2015 s. 81.
[53] Dok. 16-2011-2012 s. 175. (Rapport om Menneskerettighetsutvalget om menneskerettigheter i Grunnloven)

uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.»

I følge rettspraksis[54] fra EMD stiller EMK art. 8 andre ledd tre hovedvilkår for at statlige datainnsamlingstiltak aksepteres som konvensjonelle. Det første er at tiltaket skal ha hjemmel i nasjonal rett, jf. «… i samsvar med loven». De neste to vilkårene er at tiltaket må ha et legitimt formål og være forholdsmessig, jf. «… nødvendig i demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet …».

Dette er i samsvar med Høyesteretts uttalelse i Rt. 2014 s. 1105 og disse vilkår må da gjelde for inngrep i rettighetene etter Grunnloven § 102.

Lovligheten til bulkinnsamlingen i DGF-forslaget vil da være avhengig av hvorvidt bulkinnsamlingen oppfyller hvert enkelt krav. Det rettslige innholdet av disse kravene og hvorvidt bulkinnsamlingen vil oppfylle de skal være det neste temaet i avhandlingen.

3.1.3 Lovkravet

Lovkravet er det første av de tre kravene som må oppfylles for at bulkinnsamlingen skal anses som «lovlig etterretning». I følge Grunnloven § 113 må myndighetens inngrep ovenfor den enkelte ha grunnlag i lov, og bulkinnsamlingen, som vist tidligere, kommer til å være et inngrep i rettighetene til mange. En klar lovhjemmel vil bidra til at enhver kan forutberegne deres rettslige stilling, et hensyn som gjør seg særlig gjeldende når en gjør inngrep i en grunnlovfestet menneskerettighet. Videre stiller Grunnloven § 102, jf. EMK art. 8 andre ledd, et lovkrav for alle inngrep i kommunikasjonsvernet jf. Rt. 2014 s. 1105 og EMD i Weber og Saravia mot Tyskland [55]og Malone mot Stobritannia[56].

Grunnloven § 102 må modifisere det generelle lovkravet for å sikre «respekt» for de rettighetene bestemmelsen skal verne. Dette har først og fremst betydning i forhold til kvaliteten av lovhjemmelen. Jo mer tyngende inngrepet er – jo større krav er det til kvaliteten av lovhjemmelen, noe som kommer tilstrekkelig klart ut av rettspraksis[57]. Lovhjemmelen må

[54] Se blant annet. EMD 02.08.1984 (saksnummer 8691/79)
[55] EMD. 29.06.2006 (saksnummer 54934/00)
[56] EMD 02.08.1984 (saksnummer 8691/79)
[57] Jf. Rt. 1995 s. 530 (Fjordlaksdommen)

være tilstrekkelig klar for at den enkelte kan forholde seg til den og forutberegne sin rettslige stilling.[58] Dette betyr at lite inngripende maktutøvelse fra statens side kan være hjemlet i en generell bestemmelse, mens mer inngripende maktutøvelse trenger klarere regler om inngrepet og vilkåret for å foreta det. Hjemmelskravet avhenger av omfanget og styrken av inngrepet noe som betyr at man må først vurdere hvor sterk inngrepet vil være i lovens forstand. Det er flere sentrale nyanser i vurderingen av styrken av inngrepet ifølge Høyesterett i Rt. 1995 s. 530. Lovhjemmelskravet må nyanseres ut ifra «hvilket område en befinner seg på, arten av inngrepet, hvordan det rammer og hvor tyngende det er overfor den som rammes».

3.1.4 Det relative lovkravet

DGF-forslagets bulkinnsamling vil være et inngrep i en grunnlovfestet menneskerettighet, noe som i utgangspunktet må tale for et strengt lovhjemmelskrav. Inngrep som går ut på innsamling av personlige opplysninger er ikke nytt i norsk rett og har som regel nokså omfattende lovhjemmel.[59] Forskjellen ved andre former for innsamling er at de som regel går ut på lagring av innholdsdata og er målrettede. Spørsmålet blir da hvilke hensyn og momenter som gjelder særlig i tilfellet med bulkaksesstiltaket presentert i DGF-forslaget.

Hvis man ser på kvaliteten til opplysninger lagret med bruk av bulkaksess så viser det seg at metadata i små mengder inneholder lite personlig informasjon. Det er ikke like inngripende å kunne se hvor brevet kommer fra i forhold til å kunne se hva som er skrevet. Men situasjonen kan forandre seg dersom en får tilgang til veldig mye metadata samtidig. Selv om metadata i utgangspunktet ikke gir mange personlige opplysninger i hvert enkelt tilfelle, så kan innsamling av metadata i bulk bli svært inngripende. Analyse av mange typer metadata kan gi et like klart, om ikke klarere bilde av oppførselen til et individ. I forhold til dette har EU-domstolen konkludert at metadata som var lagret i medhold av DLD:

«…taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried

[58] Jf. EMD 02.08.1984 (saksnummer 8691/79) avsnitt. 78-80.
[59] Se for eks. lov. 22.05 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven) kap. 16 a

out, the social relationships of those persons and the social environments frequented by them». [60]

I sin rapport «The Right to Privacy in the Digital Age» har FNs høykommissær et lignende standpunkt :

«The aggregation of information commonly referred to as "metadata" may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication».[61]

På grunn av dette kan det konkluderes med at når mange typer metadata er kombinert kan en få like mange, om ikke mer, personlige opplysninger uten at det er i det hele tatt nødvendig å gå inn på innholdet av kommunikasjonen. Men betyr dette at bulkinnsamling av metadata er like inngripende som innsamling av innholdsdata?

I dag er digital kommunikasjon, særlig med bruk av internett, preget av at brukeren må velge å dele noe personlig informasjon som en del av selve kommunikasjonsprosessen. De fleste brukere gjør dette frivillig, og mye av den personlige informasjonen som er utgitt frivillig for å få tilgang til en tjeneste eller ønsket informasjon er nettopp metadata. Siden metadata er så vanlig så kan tilgang til den fremstå som mindre inngripende. I denne situasjonen er det likevel brukeren selv som tar et mer eller mindre bevisst valg om å dele deres informasjon. Derfor kan ikke det faktum at deling av metadata er en normal del av kommunikasjonsprosessen ha betydning i forhold til inngrepets styrke. Brukeren har rett til å kunne informert velge å dele noen opplysninger med tilbyderen av kommunikasjonstjenesten som del av kommunikasjonsprosessen uten at staten får innsyn i dem, noe som EMD også mener i Malone mot Storbritannia i forhold til informasjon om samtalelengden og brukshyppighet som telefonselskaper lagrer for å kreve riktig betaling.[62]

I tillegg forutsetter forslaget at store mengder metadata kommer til å bli akkumulert over en lang tidsperiode og det er ingen tvil om at etterretningstjenesten kommer til å ha både tekniske muligheter og faglig kunnskap til å kunne behandle metadata slik at den samlede informasjonsverdien av den blir tilnærmet informasjonsverdien av innholdsdata. Med andre ord får etterretningstjenesten en reell mulighet til å kunne overvåke de fleste norske

[60] Digital Rights Ireland Ltd. Sak C-293/12, avsnitt 27
[61] «The Right to Privacy in the Digital Age» 2014; A-HRC-27-37_en (avsnitt 19)
[62] EMD 02.08.1984 (saksnummer 8691/79) se avnistt 84 om «metering».

innbyggere og med høy grad av presisjon konstruere deres handlingsmønstre både på internett og andre situasjoner. [63] Dette betyr at bulkinnsamlingen kan bli et verktøy som gir like mye eller mer personlig informasjon som andre eksisterende målrettede overvåkningstiltak, som for eksempel kommunikasjonskontroll[64].

På den andre siden så er ikke bulkaksesstiltaket ment for å brukes mot norske borgere. E-tjenesten kommer ikke til å behandle metadataen til norske innbyggere dersom det ikke faller under formålet med deres etterretningsvirksomhet mot utlandet. Det betyr at E-tjenesten i utgangspunktet ikke kommer til å sette sammen metadata for å få ut detaljerte opplysninger av norske fysiske eller juridiske personer. Siden opplysningene som ikke faller under formålet med E-tjenestens virksomhet kommer til å være fragmenterte, så taler det for at bulkaksesskapasiteten ikke kommer til å utgjøre et stort inngrep i rettighetene i Grunnloven § 102. Likevel vil selve bulkinnsamlingen åpne opp for et stort potensial for misbruk som må tas med i vurderingen av inngrepets styrke. Det at mesteparten av E-tjenestens virksomhet holdes hemmelig må også tas med i vurderingen, ettersom denne hemmeligheten kommer til å gjøre det vanskelig for de fleste å beskytte sine rettigheter etter Grunnloven § 102 i misbrukstilfeller.

For å hindre at det samles inn mer informasjon enn det som skal, kan filtreringsmekanismer brukes for å redusere hvor mye informasjon som blir samlet inn og lagret. Det er åpenbart at et tiltak som samler inn mindre informasjon er også et mindre inngrep. I forslaget[65]er automatisk filtrering omtalt som lite praktisk på grunn av teknologiske begrensninger på den ene siden, og sterk redusering av etterretningsmessige verdi av DGF på den andre. Ettersom det er ikke noen garantier for at irrelevant informasjon blir filtrert har ikke dette kontrollaspektet mye verdi som et argument for inngrepets styrke.

Med dette kan det konkluderes med at bulkaksesstiltaket som DGF foreslår må regnes for å være et sterkt inngrep i kommunikasjonsvernet Grunnloven § 102 oppstiller og det bør da stilles særlig strenge krav til lovhjemmel for denne typen myndighetsutøvelse.

Spørsmålet blir da om hva lovhjemmelen må faktisk omfatte for at et inngripende tiltak som dette oppfyller lovkravet i Grunnloven § 102.

[63] Lysne II – utvalget 26.08.16: DGF s. 61
[64] Jf. Lov 22.05 1981 nr. 25 om rettergangsmåten i straffesaker (Straffeprosessloven) Kap. 16 a.
[65] Lysne II – utvalget 26.08.16: DGF s. 50 og 70

3.1.5 Lovkravet i internasjonal rett

Andre land har hatt mer erfaring med store datainnsamlingstiltak enn Norge, og internasjonal rett kan bedre vise til hva lovhjemmelen til denne typen tiltak må faktisk omfatte for å ikke være rettsstridig.

I Digital Rights Ireland (DLD-dommen) [66] var lovgrunnlaget for DLD prøvd mot lovkravet stilt av EU-charter art. 7 og 8. Det er ikke sikkert at krav til lovgivningen stilt av EU-charteret samsvarer fullstendig med den som gjelder i norsk rett, men vurderingskriteriene som EU-domstolen bruker i denne saken er omtrent de samme som Høyesterett bruker i Rt. 2014 s. 1105:

«*Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data*».[67]

EU-domstolen stiller strenge krav til hjemmel som regulerer omfanget og bruk av tiltaket, det vil si at lovgivningen må sette klare regler om hvordan tiltaket kan bli brukt og hvem det kan bli brukt på. Domstolen mener at lovgivningen til DLD må ha regler som gir borgeren tilstrekkelig garanti for beskyttelse av deres personlige opplysninger fra misbruk. Til slutt skal lovgivningen begrense inngrepet til det som er strengt nødvendig, noe som ifølge EU-domstolen kan bli oppnådd ved å stille presiseringskrav til lovgivningen når det gjelder omstendighetene som betinger bruken av det aktuelle inngrepet. Hvordan har lovhjemmelskravet i forhold til EU-charterets regler påvirket EU-domstolens vurdering?

I forhold til hvor klar og presis lovgivningen til DLD er sier EU-domstolen:

«*In this respect, it must be noted, first, that Directive 2006/24 covers, in a generalised manner, all persons and all means of electronic communication as well as all traffic data*

[66] Digital Rights Ireland Ltd. Sak C-293/12
[67] Digital Rights Ireland Ltd. Sak C-293/12, avsnitt 54

without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime»[68]

Domstolen refererer til direktivets artikkel 1, hvor det er skrevet at data skal være tilgjengelig «for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law»[69].

Direktivet overlater den nærmere definisjonen av alvorlig kriminalitet til medlemstatenes nasjonale rett. Vilkåret for bruk av lagrede informasjonen avhenger da av hvor klart vilkåret er definert i det nasjonale regelverket til den individuelle medlemsstaten – direktivet i seg selv gir ingen objektive kriterier, noe som EU-domstolen bemerker i DLD-saken:

«…Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law» [70]

Videre kritiserer EU-domstolen at direktivets artikkel 4 ikke angir prosessuelle garantier som begrenser statenes tilgang til den lagrede informasjonen kun til situasjoner hvor formålet er å bekjempelse og etterforskning av alvorlig kriminalitet, og overlater den nærmere reguleringen av dette til medlemsstatene ved generell henvisning til proporsjonalitetsprinsippet og nødvendighetskravet.[71] EU-domstolen presiserer at for å oppfylle minimumskravene måtte DLD angi presist hvilke kriminelle handlinger som kan begrunne inngrepet, oppstille klarere regler om hvem som kan bli rammet av overvåkningen og angi regler om behandlingen av informasjonen, som for eks. bruk og oppbevaring av personopplysningene lagret av direktivet.

I Malone mot Storbritannia sier domstolen at kvalitetskravet stilt til lovhjemmelen innebærer at lovhjemmelen må være «compatible with the rule of law» eller i samsvar med rettsstatsprinsippet.[72] På den andre siden sier EMD at kravet til forutberegnelighet ikke i seg

[68] Digital Rights Ireland Ltd. Sak C-293/12, avsnitt 57
[69] Directive 200/24/RC artikkel 1
[70] Digital Rights Ireland Ltd. Sak C-293/12, avsnitt 60
[71] Digital Rights Ireland Ltd. Sak C-293/12, avsnitt 61
[72] EMD 02.08.1984 (saksnummer 8691/79), avsnitt 67

selv betyr at borgeren må kunne forutberegne akkurat når myndighetene kan overvåke hans kommunikasjon men kun angi betingelser for når statens blir bemyndiget til å bruke hemmelig overvåkning.[73]

Dette er bekreftet i Weber og Saravia mot Storbritannia.[74] I denne saken konkluderer EMD at det tyske overvåkningstiltaket oppfyller lovkravet i forhold til EMK art. 8 fordi loven avgrenser hvem som bli rammet av tiltaket, avklarer hvor lenge overvåkningen kan skje for hvert tilfelle, angitt reglene for deling av informasjon med andre statlige organer og regler for hvor lenge informasjonen kan bli lagret og prosedyrene for sletting av slik informasjon. Til slutt har EMD konkludert at lovhjemmelen for overvåkningstiltaket oppstiller de nødvendige sikkerhetsventilene mot misbruk av det strategiske overvåkningstiltaket.[75]

Ut av dette kan det konkluderes at for å oppfylle lovkravet i Grunnloven §102 må loven som hjemler bulkinnsamlingen angi hvilke handlinger som betinger E-tjenestens bruk av informasjonen som var hentet med bruk av bulkaksess, oppstille regler for lagring og sletting av informasjonen samt for hvilke formål denne informasjonen kan brukes og regler om deling av denne informasjonen med andre statlige myndigheter.

Spørsmålet blir da om Lysne II-utvalgets forslag til lovregulering oppfyller disse minimumskravene.

3.1.6 Forslagets lovtiltak

I forslaget presenterer utvalget et forslag for ny lovregulering [76] som skal lovfeste noen prinsipper som gjelder allerede i dag, og vil gi lovhjemmel for noen særlige krav og begrensninger som skal gjelde for DGF.

Det skal lovfestes at dataen som lagres av E-tjenesten skal minimeres i størst mulig utstrekning og slettes når informasjonen ikke lenger har etterretningsmessig verdi. Dette gir uttrykk for det generelle «minste inngrep-prinsippet» og er i samsvar med hva Høyesterett mener i Rt. 2014 s. 1105, nemlig at informasjonen skal «slettes når formålet ikke lenger er til

[73] EMD 02.08.1984 (saksnummer 8691/79), avsnitt 67
[74] EMD. 29.06.2006 (saksnummer 54934/00), avsnitt 93
[75] EMD. 29.06.2006 (saksnummer 54934/00), se avsnitt 93 – 102.
[76] Lysne II – utvalget 26.08.16: DGF kapittel 9.4. s. 60-62.

stede» og kravet om at lovhjemmelen må angi regler for når informasjonen skal slettes nevnt av EMD i Weber og Saravia mot Tyskland. Det neste prinsippet som skal lovfestes vil sikre at DGF kun benyttes dersom andre og mindre inngripende innhentingstiltak ikke antas for å kunne fremskaffe den samme informasjonen. Lovfesting av dette vil være en klar begrensning for bruken av bulkinnsamlingen. Videre poengterer utvalget at lovreguleringen av DGF må omfatte E-tjenestens rammer, bruk og lagring av DGF-fremskaffet informasjon. Dette er i samsvar med innvendingene som EU-domstolen fremmer i DLD -saken i forhold til direktivets manglende lovgivning og EMDs rettspraksis vedrørende lovkravet. Når det kommer til tilgjengeligheten av lovreguleringen mener utvalget at reguleringen ikke skal overlates som et internt regelverk hos tjenesten, men «så langt som mulig være offentlig kjent for å styrke tilliten i E-tjenestens virksomhet». Videre foreslår utvalget å stille kvalifiserende vilkår som betinger tilgangen til datatrafikken med et grunnleggende vilkår om at tilgangen gjelder forhold som det er rimelig grunn til å undersøke om at det berører de formål «-tjenesten skal ivareta etter E-lovens §§ 1 og 3», noe som vil bidra til å oppfylle kravet om regler for når og for hvilke formål informasjonen skal brukes i Weber og Saravia mot Tyskland. Til sist skal lovreguleringen utvides til å omfatte regler om E-tjenestens samarbeid med andre myndigheter og deling av informasjon som er innhentet med bruk av bulkaksesstiltaket.

Oppsummert så foreslår utvalget strenge krav til lovhjemmelens klarhet, og det vil være omfattende reguleringer som stiller krav til både hvor lenge informasjonen kan lagres og regulering av E-tjenestens tilgang til informasjonen. Dersom disse kravene etterleves, vil bulkinnsamlingen ha relativt omfattende detaljregulering, som i utgangspunktet vil oppfylle alle forannevnte krav i EMDs rettspraksis vedrørende lovkravet i EMK. art. 8. Denne typen detaljregulering vil sørge for at bulkinnsamlingen oppfyller lovhjemmelskravet i Grunnloven § 102 så lenge den endelige lovtekst følger de foreslåtte retningslinjene.

3.1.7 Formålsmessigheten av lovlig etterretning

Det neste kravet stilt av Grunnloven § 102, jf. EMK art. 8 andre ledd er kravet om at tiltaket skal ha et legitimt formål.

Grunnloven § 102 viser ikke til noen formålskrav for å gjøre inngrep i kommunikasjonsvernet i lovteksten, men dette kravet må innfortolkes i bestemmelsen som del av kravet til «respekt», jf. Rt. 2014 s. 1105 der Høyesterett påpeker at Grunnloven § 102 skal tolkes slik at informasjonen må «slettes når formålet ikke lenger er til stede». Dette betyr at det statlige inngrep må i utgangspunktet ha legitimt formål for å være lovlig etter Grunnloven § 102. Hvilke formål begrunner inngrep i rettighetene etter § 102?

I lys av EMK art. 8 andre ledd kan det kun gjøres inngrep i retten til privatliv og kommunikasjonsvernet når det er «nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter.» Definisjonen EMK art. 8 andre er nokså omfattende. Nasjonal sikkerhet er et hensyn som er uttrykkelig nevnt i EMK art. 8 andre ledd og er i utgangspunktet legitim. Bulkaksess, på linje med andre tiltak i DGF-systemet har som formål å sikre nasjonal selvstendighet og suverenitet og om å kunne effektivt møte nasjonale sikkerhetsutfordringene som Norge møter og kommer til å møte i fremtiden. Dette er i utgangspunktet legitime formål.

EMD prøver som regel ikke de nasjonale domstolenes vurdering av formålsmessigheten av tiltaket og slutter seg til de nasjonale domstolenes vurdering.[77] Det er også lite aktuelt at domstolene skal sette lovgivers vurdering av dette kravet utenom tilfeller der staten åpenbart bruker tiltaket for et helt annet formål enn det som var forutsetningen. [78]

Formålskravet inneholder også et krav om at inngrepet må være egnet til å oppnå de formål som den er ment for å fremme. Ettersom bulkaksesstiltaket ikke er implementert er det ingen

[77] Se for eks. EMD 02.08.1984 (saksnummer 8691/79), EMD. 29.06.2006 (saksnummer 54934/00), avsnitt 104.
[78] Se Arnfinn, Bårdsen, «Grunnloven, overvåking og domstolenes rolle» 21. april 2017, 3 Høyesteretts nettsider 2017 nr. 4 s. 21. (s. 11)

statistikk eller annen data som kan brukes som bevis for effektiviteten av DGF, men som nevnt ovenfor, var andre bulkaksess tiltak som DLD [79]og det tyske overvåkningstiltaket G10 [80] sett som formålstjenlige av de respektive domstolene.

Konklusjonen må da bli at bulkaksesstiltaket i DGF oppfyller formålskravene i Grunnloven § 102.

3.1.8 Forholdsmessigheten av lovlig etterretning

I DLD-dommen [81] fastslår EU-domstolen at DLD er formålstjenlig, og at formålet om å bekjempe alvorlig kriminalitet er valid og i utgangspunktet tillater inngrep i rettighetene gitt av EU-charteret art.7 og 8. Likevel mente EU-domstolen at formålsmessighet i seg selv ikke er nok for et slikt inngrep. Inngrepet må også være proporsjonal i forhold til den retten som den beskytter. Dette kravet er særlig problematisk i forhold til veldig omfattende datainnsamlingsinngrep. For eksempel var det uforholdsmessigheten av direktivet som var den primære grunnen for underkjennelsen av DLD.[82]

Som nevnt ovenfor, inneholder Grunnloven § 102 også et forholdsmessighetskrav. Den siste delproblemstilling i avhandlingen vil derfor omhandle dette forholdsmessighetskravet og om bulkaksess foreslått av DGF-forslaget vil være forholdsmessig. Inngrepet må være «nødvendig» i et demokratisk samfunn, noe som er i utgangspunktet et nokså relativt vilkår. Hvilke krav ligger det da i denne betingelsen og hvordan står de i forhold til bulkaksess?

Grunnloven § 102 oppstiller ifølge Høyesterett en alminnelig forholdsmessighetsbegrensning for inngrep, jf. Rt. 2014 s. 1105 hvor Høyesterett sier at kravet om at personlig informasjon slettes når formålet ikke er lenger til stedet er «nettopp en konsekvens av den alminnelige forholdsmessighetsbegrensningen som gjelder også for lovhjemlede og saklig begrunnede inngrep i rettighetene og frihetene fastsatt i Grunnlovens menneskerettsbestemmelser». [83] Høyesterett fastslår videre i at forholdsmessighetskravet gjelder den rene lagringen av materialet uavhengig av den senere bruken og referer til Menneskerettsdomstolens avgjørelser

[79] Digital Rights Ireland Ltd. Sak C-293/12, avsnitt 44
[80] EMD. 29.06.2006 (saksnummer 54934/00), avsnitt 106.
[81] Digital Rights Ireland Ltd. Sak C-293/12, avsnitt 41-44
[82] Digital Rights Ireland Ltd. Sak C-293/12, avsnitt 69
[83] Rt. 2014 s. 1105, avsnitt 28

i Leander mot Sverige[84], Amann mot Sveits [85]og S., Marper mot Storbritannia[86] og forarbeider til bestemmelsen som tar lignende standpunkt.[87] Dette viser at forholdsmessighetskravet innebærer at et inngrep som går ut på samling av personlige opplysninger må kun gå så langt som det er nødvendig for å oppnå formålet med det.

I HR-2016-2554-P (Holship), som gjaldt en boikott, foretar Høyesterett en vurdering om inngrepet i organisasjonsfrihet er «nødvendig i et demokratisk samfunn» eller «for å beskytte andres rettigheter og friheter» jf. EMK art. 11. Høyesterett sier da at dette vilkåret beror på en «sammensatt proporsjonalitetsvurdering».[88] I denne dommen velger Høyesterett å sette «rett til boikott» mot retten til fri etablering stilt av EØS-avtalen artikkel 31, og spør om «det inngrep i en eventuell rett til boikott som etableringsretten representerer er proporsjonalt.» Dette viser en viktig side ved vurderingen av forpliktelser i forhold til EMK. Staten kan også være forpliktet til å innføre tiltak som beskytter andre rettigheter. EMK forplikter staten å beskytte borgerne fra krenkelser av deres sikkerhet, jf. EMK art 5, og i den moderne verden kan digitale angrep være like ødeleggende som fysiske. På grunn av dette kan staten også være forpliktet til å sikre den elektroniske infrastrukturen, og denne interessen kan komme i konflikt med rettighetene etter Grunnloven § 102 og EMK art. 8. Det bør da være en margin som tillater staten å oppfylle denne plikten uten å innskrenke andre konvensjonelle rettigheter.

EMDs praksis[89] har vist at statene har en nokså vid skjønnsmargin i vurderingen av forholdsmessigheten til inngrep, noe som er forklart med at det er som regel statlige myndigheter som har bedre forståelse over de truslene som er mest aktuelle og midlene som kan brukes for å motvirke de. Likevel overlater ikke EMD hele forholdsmessighetsvurderingen til statene. Forholdsmessighetsvurderingen, som nevnt tidligere, innebærer hvor nødvendig tiltaket er i forhold til formålet som skal fremmes og at tiltaket ikke skal gå lenger enn strengt nødvendig. Når EMD tar stilling til spørsmålet om et overvåkningstiltak oppfyller forholdsmessighetskravet, vil EMD som regel se på lovhjemmelen og vurdere om lovhjemmelen, kombinert med andre instrukser for rutiner, begrenser overvåkningstiltaket til det som er absolutt nødvendig for å oppnå det formålet som

[84] EMD 26.03.1987 (saksnummer 9248/81)
[85] EMD 16.2.2000 (saksnummer 27798/95)
[86] EMD 04.12.2008 (saksnummer 30562/04 og 30566/04)
[87] Prop. 147 L (2012-2013), s. 95
[88] Se HR-2016-2554-P (Holship), avsnitt 52.
[89]Se for eks. EMD 06.09.1979 (saksnummer 5029/71), EMD. 26.03.1987 (saksnummer 9248/81) og EMD 02.08.1984 (saksnummer 8691/79)

staten bruker for å begrunne tiltaket og om lovhjemmelen har de nødvendige sikkerhetsventiler mot misbruk. Dette viser at både formålskravet og lovkravet er tett knyttet til forholdsmessighetskravet.

I Weber og Saravia mot Tyskland sier EMD:

«*The Court reiterates that, when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, it has consistently recognised that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law*».[90]

Kravet om at inngrepet må begrenses til det som er strengt nødvendig fremkommer også i Dragojevic mot Kroatia:

«*This in particular bears significance as to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, since the Court has held that powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are strictly necessary for safeguarding democratic institutions (see Kennedy, cited above, § 153). In assessing the existence and extent of such necessity the Contracting States enjoy a certain margin of appreciation, but this margin is subject to European supervision. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society". In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded*».[91]

[90] EMD 29.06.2006 (saksnummer. 54934/00), avsnitt 106
[91] EMD 15.01.2015 (saksnummer 68955/11), avsnitt 84

Dette viser at forholdsmessighetskravet er avhengig av hvorvidt lovkravet er oppfylt. Samtidig vil en omfattende reguleringshjemmel som oppstiller klarere vilkår og begrensninger bidra til at tiltaket fremstår som mer forholdsmessig. Dette gjelder begrensninger både i forhold til hva som blir lagret, hvor lenge og i hvilke situasjoner den informasjonen kan bli brukt. Dersom loven er så upresis at staten kan stå fritt i tolkningen av den er risikoen for misbruk mye større. Dette momentet var avgjørende for hvorfor EMD i Weber og Saravia mot Tyskland [92] vurderte det strategiske overvåkningstiltaket for å være forholdsmessig når det britiske tiltaket i Malone mot Storbritannia var dømt for å være uforholdsmessig selv om tiltaket i Malone mot Storbritannia var mindre omfattende fra et teknisk perspektiv. I tillegg var det upresis lovregulering og mangel på nødvendig rettslig avgrensning som var blant de viktigste grunnene for hvorfor DLD ble underkjent av EU-domstolen.

Med dette kan det konkluderes med at forholdsmessighetsvurderingen av bulkaksesstiltaket i DGF-forslaget må ta utgangspunkt i hvordan bulkaksess er begrenset av lovhjemmelen for å redusere datainnsamlingen til kun det som er nødvendig for å oppnå formålet med tiltaket og hvilke garantier som eksisterer som gjør misbruk av bulkaksesskapasiteten og formålsglidning mindre sannsynlig.

Lysne II-utvalget [93] forutsetter at DGF vil være primært fokusert på håndtering av cybertrusler og elektroniske angrep, samt potensielle terrortrusler på norsk jord. Utvalget konkluderer i forslaget med at DGF vil være et «mektig verktøy» for E-tjenesten. Samtidig er det i forslaget konkludert at DGF er «potensielt svært inngripende, og skadepotensialet er stort dersom det ikke legges tydelige føringer på hvordan det skal benyttes, og det ikke underlegges et sterkt kontrollregime som sørger for at det ikke blir misbrukt». Utvalget vil derfor innføre flere mekanismer som skal hjelpe å begrense tiltakets omfang til et nivå som kan regnes til å være forholdsmessig til de formål DGF er ment til å ivareta. Disse tiltak kan deles i to typer – tiltak som begrenser overvåkingens omfang og kontrolltiltak som sikrer at de lovfestede begrensningene blir etterlevd i praksis.

[92] EMD 29.06.2006 (saksnummer. 54934/00), avsnitt. 85-102
[93] Lysne II – utvalget 26.08.16: DGF s. 62

3.2 Kontroll med bulkaksess

3.2.1 Formålsbegrensning

Den første kontrollmekanismen dokumentet foreslår kommer i form av en formålsbegrensning. Forslaget konkluderer at DGF-installasjonen vil ikke kun være av nytte for utenlandsetterretning, men også «vil kunne være et svært kraftfullt virkemiddel også for nasjonale myndigheter som har ansvar for innenlandske forhold.» Forslaget forutsetter klart at DGF må kun brukes for utenlandsetterretningsformål, og vil derfor sikre dette med forskjellig mekanismer som skal hindre at det skjer formålsglidning.

Denne typen formålsbegrensning har størst betydning for bruk av informasjonen som blir lagret, ikke for selve lagringen. Formålsbegrensning kan ikke i seg selv hindre at informasjonen som ikke er relevant for utenlandsetterretningsformål blir lagret. Sensitiv informasjon, inkludert kommunikasjonen til personer hvor det er behov for særlig fortrolighet, kan ikke med dagens teknologi filtreres på noen praktisk akseptabel måte.[94] Bulkinnsamlingen forutsetter at mye irrelevant metadata vil bli lagret til tross for formålsbegrensningen. Denne utfordringen vil Lysne II-utvalget løse ved lovtiltak som skal sikre at overskuddsinformasjon som E-tjenesten innhenter med bruk av DGF skal slettes og med dette ta vekk muligheten for at denne informasjonen skal kunne deles med andre myndigheter, noe som er tillatt ifølge gjeldende lovgivning, jf. instruks om etterretningstjenesten § 5. Utvalget mener at denne behandlingen av overskuddsinformasjon skal lovfestes for å hindre formålsglidning og for å skape tillit hos publikum til at DGF ikke misbrukes og kun brukes for de formål som den er ment for. Denne begrensningen skal være streng og det er uttrykkelig poengtert at dersom E-tjenesten tilfeldigvis får informasjon om at en person har begått et drap eller andre alvorlige kriminelle handlinger, så vil slik informasjon bli slettet uten videre oppfølging.[95] Denne type lovregulering vil i teorien bidra til at kravet om at inngrepet som overvåkningstiltaket innebærer begrenses til kun hva som er strengt

[94] Lysne II – utvalget 26.08.16: DGF s. 50
[95] Lysne II – utvalget 26.08.16: DGF s. 60

nødvendig for de formål som tiltaket er ment å fremme, nemlig styrking av nasjonal sikkerhet mot ytre trusler jf. EMK art. 8 (2).

Mye metadata knyttet til norske borgere vil likevel falle inn under utenlandsetterretningsformål som E-tjenestens virksomhet knytter seg til og det blir problematisk dersom denne informasjonen kan brukes mot norske borgere for formål som strider med det opprinnelige formålet for E-tjenestens bulkaksess. Utvalget foreslår at det bør fastsettes i lov at DGF-innhentet informasjon ikke under noen omstendighet kan bli brukt som bevis mot tiltalte i straffesaker for å videre bevare tilliten til at DGFs formålsbegrensninger blir overholdt. [96] Dette vil da også gjelde opplysningene som man kan få fra systematisk behandling av metadata, selv om informasjonen opprinnelig faller inn under etterretningstjenestens formål. På den måten vil bulkaksesstiltaket bli mye mer forholdsmessig, fordi informasjonen vil i utgangspunktet ikke kunne brukes direkte mot norske borgere.

Forslaget nevner likevel at selv om slik informasjon ikke skal kunne brukes som bevis i straffesaker, så utelukker ikke utvalget muligheten for at informasjon som «ikke er å anse som overskuddsinformasjon kan deles med PST – herunder gjennom Felles kontraterrorsenter (FKTS) – på vanlig måte, som kan bruke informasjonen som inngangsverdi for egen metodebruk/etterforskning basert på PSTs hjemmelsgrunnlag.» [97]Utvalget avklarer ikke hva som menes med «inngangsverdi», men det er klart at ved å tillatte denne muligheten går utvalget imot det opprinnelige målet om å hindre formålsglidning og imot prinsippet om å ikke kunne bruke E-tjenestens bulkaksessopplysninger som bevis i straffesaker mot norske borgere. Selv om andre myndigheter ikke skal kunne bruke informasjon innhentet som følge av bulkaksess så utelukker ikke forslaget at andre myndigheter kan utnytte den store informasjonstilførselen som bulkaksess vil skape for E-tjenesten.

Det er for tidlig å si hvordan dette vil påvirke tiltakets forholdsmessighet og hva slags egentlige verdi DGF kommer eventuelt til å ha for andre myndigheter dersom det foreslåtte tiltaket blir gjennomført. Det er likevel klart at det kommer til å være vanskeligere å begrunne bruken av E-tjenestens bulkaksesskapasitet dersom det er brukt for å gi andre relevante

[96] Lysne II – utvalget 26.08.16: DGF s. 61
[97] Lysne II – utvalget 26.08.16: DGF s. 61

statsmyndigheter «tips» om hvor eventuell etterforskning bør gjennomføres og på den måten vesentlig effektivisere arbeidet til disse myndighetene.

I tillegg vil ikke utvalget tilrå at det oppstilles særlige regler til vern av kommunikasjonen av yrkesutøvere med streng taushetsplikt[98], som for eksempel advokater og psykologer, selv om mangelen av slik særskilt beskyttelse var en av de innvendingene EU-domstolen hadde mot DLD[99]. Grunnen til det er nemlig at dagens filtreringsteknologi ikke kan garantere at en slik begrensning blir etterlevd. Dette faktum kombinert med uklarheten rundt behandlingen av informasjon som kan deles med andre myndigheter vil være et argument mot forholdsmessigheten av tiltaket, ettersom grensene for E-tjenestens bruk av informasjon som er anskaffet som følge av bulkaksesskapasiteten ikke er tilstrekkelig klare og det fremkommer ikke klart at bulkinnsamlingen begrenser seg kun til hva som er nødvendig for å tjene det opprinnelige formålet.

3.2.2 Kontrollorganer

I følge forslaget skal det opprettes en domstol som skal sørge for at DGF-kapasiteten skal brukes etter formålet. DGF-domstolen skal primært sørge for forhåndsgodkjenninger, noe som gjør den til den kontrollmekanismen som kommer tidligst til uttrykk, bortsett fra den generelle formålsbegrensningen. Utvalget foreslår at hovedreglene for den nye domstolskontrollen skal bli en del av E-loven og det skal gjelde «beviskrav» for nødvendigheten av søket i datalageret og kontroll om at tillatelse ikke vil være uforholdsmessig inngripende. Med dette forslaget tar utvalget inspirasjon fra politilovens regler om PSTs adgang til å bruke tvangsmidler i forebyggende sammenheng, jf. politilovens kapittel III A. Forslaget nevner også at det skal være mulig å få tilgang til informasjonen uten å avvente domstolens avgjørelse, i likhet med politiloven § 17d (3) med etterfølgende domstolskontroll.

Denne kontrollmekanismen kan være inspirert av den tyske forfatningsdomstolens dom [100] i en sak om den tyske gjennomføringen av DLD og dens forenelighet med den tyske

[98] Lysne II – utvalget 26.08.16: DGF s. 62
[99] Digital Rights Ireland Ltd. Sak C-293/12, se avsnitt 58.
[100] BVerfG, Judgment of the First Senate of 02 March 2010 - 1 BvR 256/08 (avsnitt 237)

grunnloven. Blant de krav som allerede har blitt diskutert var det et krav om at dataen skal kun kunne overleveres til den rette myndigheten etter en rettslig avgjørelse. Slik prøving vil ha en positiv effekt på forholdsmessigheten av tiltaket fordi den vil bidra til å redusere faren for at personopplysningene som er innhentet med bruk av bulkaksesstiltaket misbrukes og vil generelt redusere den mengden informasjon som E-tjenesten kan disponere over.

Videre foreslår Lysne II-utvalget et forvaltningsorgan som skal holde «tilnærmet kontinuerlig og uavhengig kontroll – i nær sanntid» knyttet til implementering av DGF-systemet. Det er ikke mye detaljinformasjon som kan trekkes ut av forslaget om hvordan deres virksomhet skal organiseres. Blant annet mener utvalget at dette organet ikke skal ha myndighet til å stanse virksomheten knyttet til DGF eller offentlig kritisere E-tjenesten for brudd på regelverket for DGF. Dette organet skal likevel kunne rapportere eventuelle avvik fra regelverket til EOS-utvalget som skal vurdere oppfølgingstiltak i tråd med deres fullmakter.

Lov om kontroll med etterretnings-, overvåkings/ og sikkerhetstjeneste (EOS – kontrolloven) gir regler for EOS-utvalgets organisering og virksomhet. I følge kontrolloven § 2 er formålet med EOS-utvalget å forebygge at noens rettigheter krenkes som følge av E-tjenestens virksomhet og sørge for at den holder seg innenfor den marginen som menneskerettighetene åpner for. Utvalget fører som regel etterfølgende kontroll, jf. kontrolloven § 2 (3) og det er klart at dersom DGF er innført som et nytt virkemiddel for E-tjenesten så skal EOS-utvalget føre etterfølgende kontroll over bruken av bulkaksess og søket i metadatalageret, noe som er nevnt i forslaget. Det påpekes at EOS-utvalget bør også tillegges ytterligere ressurser for å ivareta sitt kontrollansvar.

Et slik omfattende kontrollregime vil utvilsomt bidra til at bulkaksess holder seg innenfor forholdsmessighetsmarginen. Det er nettopp det effektive kontrollregimet som loven oppstilte for det tyske strategiske overvåkningstiltaket G10 som var grunnen for at EMD dømte i favør av staten i Weber og Saravia mot Tyskland.[101]

[101] EMD 29.06.2006 (saksnummer. 54934/00)

4 Konklusjon

Utvidelsen av E-tjenestens kapasitet med et tiltak som vil lagre metadata som går i fiberkablene over landets grense vil i utgangspunktet innebære et sterkt inngrep i retten til respekt for enhvers privatliv og kommunikasjon, jf. Grunnloven § 102. Det er likevel gode grunner for hvorfor dette tiltaket må eksistere i det moderne samfunn. Når digitale trusler blir større og mer skadelige er det nødvendig for at forsvarsmekanismene også blir mer sofistikerte og omfattende.

Bulkaksesstiltaket i DGF må ha tilstrekkelig lovhjemmel for å kunne være forenlig med Grunnloven § 102, noe som Lysne II-utvalget vil sikre ved å innføre en ny omfattende lovregulering som skal styre alle de viktigste sidene ved bulkaksesskapasiteten. Dersom de forslagene blir praktisk etterlevd, vil bulkaksesskapasiteten oppfylle lovkravet i Grunnloven § 102. Bulkaksesskapasiteten er også begrunnet med legitime formål og retter seg mot reelle trusler som eksisterer allerede i dag, noe som oppfyller formålskravet i Grunnloven § 102. Det er likevel et åpent spørsmål om Grunnloven § 102 i det hele tatt tillater at personlige opplysningene blir innsamlet i bulk, men som rettspraksis viser – så er det som regel staten som styrer hvor vidt de legitime truslene som staten står ovenfor begrunner så omfattende inngrep i de grunnleggende menneskerettighetene. Det er nemlig folkesuverenitetsprinsippet som skal sikre at staten fører politikk som er mest lønnsom for statsborgerne. Internasjonal rett viser likevel at til og med vidtgående strategisk datalagring kan bli akseptert dersom systemene som skal føre overvåkningen er begrenset av effektive kontrollmekanismer. Dersom loven er klar og presis, har legitimt formål og har de nødvendige sikkerhetsventiler vil de fleste moderne datalagringstiltak være innenfor marginen til EMK art. 8 og som følge Grunnloven § 102. Ettersom E-tjenestens bulkaksesskapasiteten skal i utgangspunktet ikke være brukt mot overvåkning av norske borgere, og dersom de kontrollmekanismene som er foreslått skal effektivt sørge for at denne formålsbegrensningen blir etterlevd i praksis, vil bulkaksessen foreslått i DGF være forholdsmessig i forhold til retten i Grunnloven § 102. Som konklusjon er det sannsynlig at tilstrekkelig lovregulering og kontroll kan føre til at E-tjenestens bulkinnsamling eller «bulkaksess» til metadata foreslått i DGF vil være forenlig med Grunnlovens § 102.

Menneskerettighetene er likevel ikke statiske, noe som gjelder særlig for retten til respekt for privatliv og kommunikasjon i EMK art. 8. Den teknologiske utviklingen fører til at personvernet kommer stadig under flere trusler, noe som kan begrunne ytterligere beskyttelser av denne retten ved å ytterlig stramme vilkårene for innføring av statlige datalagringstiltak. Det er flere saker som nå står under forberedelse i EMD som kan videre avklare den gjeldende internasjonale standarden for personvern.[102] Grensene for statlig digital overvåkning er et åpent spørsmål og vil fortsette å være det i nærmeste fremtid.

[102] Se for eks. Big Brother Watch og andre mot Storbritannia EMD. 4.08.2013 (saksnummer 58170/13)

Litteraturliste

Litteratur:

Aall, Jørgen, *Rettsstat og menneskerettigheter*, 4. utgave. (Bergen: Fagbokforlaget, 2015)

Line Auglend, Ragnar og John Mæland, Henry, *Politirett*, 3. utgave (Oslo: Gyldendal Norsk Forlag, 2016)

Artikler:

Arnfinn, Bårdsen, «Grunnloven, overvåking og domstolenes rolle» 21. april 2017, 3 Høyesteretts nettsider 2017 nr. 4 s. 21.

Bruce, Ingvild, «Datalagringsdirektivet – en menneskerettskrenkelse eller -forpliktelse?» *LO OG RETT*, vol. 49, s.1–2, 2010

Forarbeider og andre publikasjoner fra det offentlige:

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

Dok. 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»))

FN rapport «The Right to Privacy in the Digital Age» 2014.

Innst. 275 L (2010-2011)

Møse, Erik, «Forholdet mellom visse sider ved de hemmelige tjenester og menneskerettighetskonvensjonene», vedlegg 2 i Dok. nr.15 (1995-1996) s. 595-609.

NOU: 2009:1 Individ og integritet

Petter Graver, Hans og Harborg, Henning, En utredning avgitt til Justisdepartementet og Samferdselsdepartementet «Datalagring og Menneskerettighetene» 1. oktober 2015 – (UTRDJ-2015-1)

Prop. 147 L (2012-2013)

St. Meld. 27 (2015-2016) «Digital Agenda for Norge»

Utredning avgitt av Lysne II-utvalget 26. august 2016 om digitalt grenseforsvar (DGF).

Dommer:

HR-2016-2554-P (Holship)

Rt. 2014 s. 1105

Rt. 2015. s. 81

Rt. 2015 s. 93

Avgjørelser I EMD:

Amann mot Sveits, EMD 16.2.2000 (saksnummer 27798/95)

Big Brother Watch og andre mot Storbritannia, EMD. 4.08.2013 (saksnummer 58170/13)

Copland mot Storbritannia, EMD. 03.04.2007 (saksnummer 62617/00)

Dragojevic mot Kroatia, EMD 15.01.2015 (saksnummer 68955/11)

Leander mot Sverige, EMD 26.03.1987 (saksnummer 9248/81)

Liberty og andre mot Storbritannia; EMD 01.07.2008 (saksnummer 58243/00)

Maloen mot Storbritannia, EMD 02.08.1984 (saksnummer 8691/79)

S., Marper mot Storbritannia, EMD 04.12.2008 (saksnummer 30562/04 og 30566/04)

Weber og Saravia mot Tyskland, EMD 29.06.2006 (saksnummer. 54934/00)

Andre avgjørelser:

BVerfG, Judgment of the First Senate of 02 March 2010 - 1 BvR 256/08

EF-domstolen, Digital Rights Ireland Ltd. Sak C-293/12

Nasjonale lover, forskrifter og instrukser:

Instruksen om Etterretningstjenesten gitt ved kgl.res. 31. august 2001

Forskrift av 15. desember 2000 nr. 1265 om behandling av personopplysninger (personopplysningsforskriften).

Lov 14.04.2000 nr. 31 om behandling av personopplysninger (personopplysningsloven)

Lov 20. mars 1998 nr. 11 om Etterretningstjenesten.

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

Lov 3. april 1995 nr. 7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-kontrolloven)
Lov. 22 mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven)

Internasjonale lover og konvensjoner:

Den Europeiske Menneskerettskonvensjon

Den internasjonale konvensjonen om sivile og politiske rettigheter med protokoller.

EU Charter of fundamental rights of the European Union, 2012/C 326/02

EU-direktiv 2006/24/EF «Datalagringsdirektivet»

Andre kilder:

Statistisk Sentralbyrå, Norsk mediebarometer, https://www.ssb.no/kultur-og-fritid/statistikker/medie/aar (Hentet 31/05/2018, sist oppdatert 19/04/2018)