Bacheloroppgave

ADM650 Jus og administrasjon

Digitalt grenseforsvar- Norges svar på masseovervåkning?

Sofie Hoff Jensen og Karoline Strand Kormeset

Totalt antall sider inkludert forsiden: 32

Molde, 22.05.17

Høgskolen i Molde
Vitenskapelig høgskole i logistikk

Obligatorisk egenerklæring/gruppeerklæring

Den enkelte student er selv ansvarlig for å sette seg inn i hva som er lovlige hjelpemidler, retningslinjer for bruk av disse og regler om kildebruk. Erklæringen skal bevisstgjøre studentene på deres ansvar og hvilke konsekvenser fusk kan medføre. Manglende erklæring fritar ikke studentene fra sitt ansvar.

Du/dere fyller ut erklæringen ved å klikke i ruten til høyre for den enkelte del 1-6:		
1.	**Jeg/vi erklærer herved at min/vår besvarelse er mitt/vårt eget arbeid, og at jeg/vi ikke har brukt andre kilder eller har mottatt annen hjelp enn det som er nevnt i besvarelsen.**	☒
2.	**Jeg/vi erklærer videre at denne besvarelsen:** • ikke har vært brukt til annen eksamen ved annen avdeling/universitet/høgskole innenlands eller utenlands. • ikke refererer til andres arbeid uten at det er oppgitt. • ikke refererer til eget tidligere arbeid uten at det er oppgitt. • har alle referansene oppgitt i litteraturlisten. • ikke er en kopi, duplikat eller avskrift av andres arbeid eller besvarelse.	☒
3.	**Jeg/vi er kjent med at brudd på ovennevnte er å betrakte som fusk og kan medføre annullering av eksamen og utestengelse fra universiteter og høgskoler i Norge, jf. Universitets- og høgskoleloven §§4-7 og 4-8 og Forskrift om eksamen §§14 og 15.**	☒
4.	**Jeg/vi er kjent med at alle innleverte oppgaver kan bli plagiatkontrollert i Ephorus, se Retningslinjer for elektronisk innlevering og publisering av studiepoenggivende studentoppgaver**	☒
5.	**Jeg/vi er kjent med at høgskolen vil behandle alle saker hvor det forligger mistanke om fusk etter høgskolens retningslinjer for behandling av saker om fusk**	☒
6.	**Jeg/vi har satt oss inn i regler og retningslinjer i bruk av kilder og referanser på biblioteket sine nettsider**	☒

Publiseringsavtale

Studiepoeng: 15

Veileder: Odd Anders Bøyum- Folkeseth

Fullmakt til elektronisk publisering av oppgaven

Forfatter(ne) har opphavsrett til oppgaven. Det betyr blant annet enerett til å gjøre verket tilgjengelig for allmennheten (Åndsverkloven. §2).
Alle oppgaver som fyller kriteriene vil bli registrert og publisert i Brage HiM med forfatter(ne)s godkjennelse.
Oppgaver som er unntatt offentlighet eller båndlagt vil ikke bli publisert.

Jeg/vi gir herved Høgskolen i Molde en vederlagsfri rett til å gjøre oppgaven tilgjengelig for elektronisk publisering:	☒**ja**	☐**nei**
Er oppgaven båndlagt (konfidensiell)?	☐**ja**	☒**nei**
(Båndleggingsavtale må fylles ut)		
- Hvis ja:		
Kan oppgaven publiseres når båndleggingsperioden er over?	☐**ja**	☐**nei**
Er oppgaven unntatt offentlighet?	☐**ja**	☒**nei**
(inneholder taushetsbelagt informasjon. Jfr. Offl. §13/Fvl. §13)		

Dato: 22.05.17

Antall ord: 7838

Forord

Denne oppgaven er skrevet i forbindelse med det tredje og siste året vårt på Jus og administrasjon ved Høgskolen i Molde. Arbeidet med denne oppgaven har vært krevende til tider, men svært interessant og lærerik. Temaet er veldig aktuelt i forhold til det dagsaktuelle nyhetsbilde, og vi føler oppgaven belyser et samfunnsdilemma som mange kanskje ikke er så klare over.

Vi ønsker å rette en stor takk til veilederen vår, Odd Anders Bøyum-Folkeseth for konstruktive tilbakemeldinger, inspirasjon og gode råd som har hjulpet oss mye i forbindelse med skriveprosessen. Vi vil også takke våre nærmeste for støtte og motivasjon.

Sammendrag

Samfunnet vi lever i har de siste årene opplevd en digitalisering på mange plan. Nettbaserte kommunikasjonsplattformer og andre digitale tjenester har blitt en stor del av hverdagen til mange. Den digitale globaliseringen gjør at vi har mulighet til å kommunisere med mennesker fra hele verden. Men den medfører også at vi er mer sårbare for trusler som reiser over landegrenser. Dette kan være terrortrusler eller cybertrusler som søker å utfordre den nasjonale sikkerheten til ulike land i verden.
26. august 2016 kom Lysne II-utvalgets med en anbefaling om innføring av et digitalt grenseforsvar i Norge. Det digitale grenseforsvaret er et system skal hjelpe etterretningstjenesten å ivareta sitt samfunnsoppdrag ved innsamling, filtrering og lagring av datatrafikk. I denne oppgaven stiller vi spørsmålstegn ved lovligheten ved en eventuell innføring av et digitalt grenseforsvar, i forhold til menneskerettighetene og personvern i lys av den europeiske menneskerettighetskonvensjonen artikkel 8. Vi vil prøve å belyse personvernets stilling i et så omfattende system.
Avslutningsvis ser vi på funn som peker på at systemet har både fordeler og ulemper, og se på hvilke av dem som veier tyngst.

Innhold

1.0 Innledning

I kjølevannet av terrorangrepene mot USA 11.september 2011 ble det klart at noe måtte gjøres for å best mulig forebygge fremtidige terrorhandlinger. Allerede 28.september samme år holdt FNs sikkerhetsråd møte, og vedtok resolusjonen 1373. Resolusjonen oppfordrer stater og nasjoner til å stå sammen om kampen mot terror og å opprettholde internasjonal fred og sikkerhet (Regjeringen, 2002)

I den vestlige verden har tiårene etter terrorangrepene i USA ført til en endring i fokuset på sikkerhetstiltak og samfunnsvern. Frykten for gjentakelse har ført til et ønske om skjerpet sikkerhet i det offentlige rom. 22. juli 2011 ble Norge rammet av to grusomme terrorangrep, mot regjeringskvartalet og Utøya. Dette ble symbolet på et skille i norsk historie, Norge før og Norge etter 22.juli. I etterkant av 22.juli 2011 har sikkerhetsfokuset i Norge blitt strammere.
Gjennom digitaliseringen av samfunnet har det dukket opp nye former for terrorhandlinger. Digitale trusler og cyberangrep har den siste tiden preget nyhetsbilde. For å verne samfunnet mot slike angrep i det digitale rom, kreves det sikkerhetstiltak. Spørsmålet om samfunnssikkerhet og sårbarhet blir stadig diskutert. Og spørsmålet om hvor grensen for overvåking går, og hva vi er villig til å ofre av frihet for å verne samfunnet, er uklar og vanskelig å sette.

2.0 Tema og problemstilling

2.1 Tema

Allerede før vi startet prosessen med å skrive denne oppgaven, var vi klar på at sikkerhet var et tema vi ville ta for oss. Vi synes at lovgivningen som skal sikre menneskers rettigheter er både spennende og svært viktig i forhold til spørsmålet om overvåkning i samfunnet. Derfor valgte vi å skrive en juridisk basert oppgave med fokus på menneskerettigheter og personvern.

Med stadig nyheter om terrorangrep rundt om i verden, ble vi først enige å ta for oss sikkerhetstiltak i forbindelse med avverging av terrorangrep, men vi snudde fort da vi kom

over Lysne II-utvalgets anbefaling fra 26.august 2016 om innføring av et digitalt grenseforsvar i Norge.

De siste årene har utviklingen av teknologiske løsninger skutt i været. Stadig flere arenaer i samfunnet blir digitalisert og nettbasert. Vi deler svært mange opplysninger om oss selv på sosiale medier og andre nettbaserte kontoer. Dette gjør at vi blir svært sårbare for hackerangrep, identitetstyveri og misbruk av personlige opplysninger, ikke bare innad i landet men også fra andre nasjoner. Etterretningen har på lik linje med samfunnet, digitalisert seg og inntatt den digitale plattform. Samfunnet står overfor nye trusler og sikkerhetsbekymringer, som krever at gamle metoder erstattes med nye for å best mulig ivareta rikets sikkerhet.

Parallelt med denne utviklingen kreves det sikkerhetsrammer for å værne om befolkningens rettigheter og sikkerhet. Vi mener det er viktig at sikkerhetstiltak ikke overskrider fundamentale rettigheter i form av menneskerettigheter, derfor settes det dagsaktuelle trusselbildet i sammenheng med i hvor stor grad et digitalt grenseforsvar kan strekke seg før det er for inngripende. Vi så at det i etterkant av rapporten ble en samfunnsdebatt om innføringen av et slikt digitalt grenseforsvar. En rekke kjente institusjoner og organisasjoner som Datatilsynet, ICJ- Norge og Norges nasjonale institusjon for menneskerettigheter mener at det digitale grenseforsvaret (slik det er presentert i rapporten) er i strid med personvernet, da spesielt EMK art.8. Vi ønsker å se om dette stemmer, da vi og andre er opptatt av personvernet vårt, og hva en eventuell implementering av digitalt grenseforsvar vil bety for personvernet.

2.2 Problemstilling

Vi har valg følgende problemstilling:

"Bryter en eventuell implementering av et digitalt grenseforsvar med EMK art.8?"

Problemstillingen vår er vid og krever derfor en avgrensning. Vi har derfor valgt å ta for oss de to mest inngripende delene av det digitale grenseforsvaret; Innsamlingsprosessen av data og lagringen. Selv om vi har valgt å ta for oss kun to deler av det digitale grenseforsvaret, er det begrenset med tid og ressurser til å gå skikkelig i dybden på disse delene av systemet. Drøftelsen tar derfor utgangspunkt i de mest åpenbare problemstillingene ved en eventuell implementering av et digitalt grenseforsvar. For å svare best mulig på problemstillingen vil vi drøfte innsamling og lagring med hvert enkelt

av vilkårene i EMK art.8 og dele opp drøftelsen i fire deler, hvor vi tar for oss de ulike vilkårene: inngripelse, legalitet, nødvendighet og formål.

3.0 Juridisk Metode

Ved at vi forsøker å se på betydningen av EMK art.8 ved en eventuell implementering av DGF, vil juridisk metode være det aktuelle verktøyet for å belyse dette. Vi presiserer nedenfor at juridisk metode også brukes på tolkning av lover, men det vi presenterer er juridisk metode som brukes på tolkning av traktater.

I den juridiske metoden er formålet med tolkning av traktater å bestemme partenes gjensidige plikter og rettigheter ut fra den aktuelle traktaten/konvensjonen. Tradisjonelt sett har det vært tre teorier som forteller hvordan traktater skal tolkes. Den objektive tolkningsteorien legger vekt på traktatens ordlyd. Den subjektive tolkningsteorien fokuserer på at partenes vilje må finnes, selv om det går på bekostning av ordlyden. Den teleologiske tolkningsteoriens fokus er at traktatens formål først må bestemmes, og at en tolkning overenstemmelse med dette formålet velges. Sentralt for tolkning av traktater er Wien konvensjonen om traktatretten av 23. mai 1969. Denne konvensjonen uttrykker i stor grad folkerettslig sedvanerett, og gir plikter og rettigheter mellom land som skal inngå/ har inngått traktater. I Wien konvensjonen artikkel 31 (1) fastsettes det at traktater skal tolkes i «god tro». Dette har forbindelse med «pacta sunt servanda», den grunnleggende regelen om at avtaler skal holdes, som også henviser til «god tro». Dette innebærer en lojalitetsplikt mellom partene. Videre skal en traktat tolkes i samsvar med «the ordinary meaning» av ordlyden, jf. art. 31 (1), som direkte oversatt betyr at man skal tolke ordene etter den vanlige betydningen av ordene. Det må også tas hensyn til konteksten og formålet til konvensjonen (Ruud og Ulfstein 2011).

Avgjørelser fra Den europeiske menneskerettighetsdomstol (heretter EMD) og den tidligere Kommisjonen vil være viktig, både som veiledning for tolkningsmetoden og for den materielle tolkningen av konvensjonens rettigheter og plikter. *Golder mot Storbritannia* fra 1975 viser til at tolkningen av konvensjonens bestemmelser vil kunne bruke de generelle bestemmelsene om traktattolkning i Wienkonvensjonens art. 31-33. Annen praksis fra EMD er at konvensjonens rettigheter og friheter må ses i sammenheng med konvensjonens overordnede formål, slik at disse blir effektive og ikke teoretiske. EMDs praksis viser også til at konvensjonen må tolkes ut fra gjeldende samfunnsformål og hensynet til effektivitetsprinsippet (Fause, 2014)

Generelle tolkningsregler

Den europeiske menneskerettighetskonvensjonen (heretter omtalt som EMK) art. 8 nr.2 angir de vilkår som må være oppfylt for at et inngripende tiltak skal kunne anses som konvensjonsmessig. Det står derimot ikke videre klart hvilke spesifikke tiltak som kan tillates, i hvilke situasjoner tiltaket kan iverksettes eller hvilken inngreps grad som kan aksepteres innenfor konvensjonens ramme. De ulike kravene og deres rammer må derfor klarlegges ved tolkning. Konvensjonen i seg selv forteller lite om hvordan bestemmelsene skal tolkes. Her legges det imidlertid vekt på konvensjonens fortale som sier at konvensjonen skal sikre en universell og effektiv anerkjennelse av konvensjonens rettigheter og friheter. Utgangspunktet vil derfor være at det må legges til grunn en naturlig, språklig forståelse av den aktuelle bestemmelsen ved tolkning. (Fause, 2014)

3.1 Kildekritikk

Det er viktig å stille krav og ha et kritisk blikk på de kildene vi velger, slik at vi vet at empirien vi samler inn, gir oss de svarene vi ser etter. Et kritisk blikk på kildene vil være viktig da feil eller ufullstendig informasjon kan forekomme. Et kravet er at empirien er reliabel, som vil si at den er troverdig og pålitelig. Pålitelighet og troverdighet handler om at innhåldet må være til å stole på. Det vil derfor være viktig at kildene vi bruker er tatt fra troverdige utgivere, slik at oppgaven vil være så troverdig og pålitelig som mulig (Jacobsen 2015).

De kildene vi bruker gjør at det er viktig at vi er så objektive som mulig når vi skal forstå innholdet og bruke dette til å belyse problemstillingen. De fleste av kildene våre er offentlige, men kommer fra flere ulike aktører /institusjoner som alle har ulike oppgaver og roller i samfunnet, og i debatten om et digitalt grenseforsvar. At det er offentlige kilder, og ikke private kilder, gjør de ikke mindre pålitelige. Det stilles, som nevnt over, et større krav til at vi klarer å holde oss selvstendige og objektive til det vi bruker, slik at vi på best mulig måte klarer å svare på det vi spør etter i problemstillingen.

4.0 Bakgrunn og fakta

4.1 Den Europeiske menneskerettighetskonvensjonen

Den Europeiske Menneskerettighetskonvensjonen har som mål å sikre at rettighetene den inneholder blir universelt og effektivt anerkjent og etterlevd (Menneskerettsloven 1953). Den europeiske Menneskerettighetskonvensjonen (heretter omtalt som EMK) ble vedtatt av Europarådet 4.november 1950, og trådte i kraft 3. september 1953. Norge ratifiserte konvensjonen 15.januar 1952 (Møse, 2002).

EMK er en slags videreutvikling av FNs verdenserklæring. Verdenserklæringen kan tolkes som en oversikt over menneskerettigheter, og omhandler både politiske, økonomiske, kulturelle, sosiale og sivile rettigheter (Ruud, 2014) Den viktigste forskjellen mellom EMK og FNs verdenserklæring er at EMK hovedsakelig omhandler sivile og politiske rettigheter, mens verdenserklæringen også tar for seg økonomiske, sosiale og kulturelle rettigheter. En annen vesentlig forskjell er at EMK også opprettet en domstol (Den Europeiske menneskerettighetsdomstol) som kan vedta bindende vedtak.
Begrepet «menneskerettigheter» er ikke entydig og kan være vanskelig å definere, men enkelt forstått er det fundamentale rettigheter som gjelder alle mennesker, der disse rettighetene skal sikre enkeltindividenes frihet, verdier og grunnleggende krav som sammen danner et grunnlag for rettferdighet og fred i verden. Det er viktig å påpeke at menneskerettighetene ikke kan bli fratatt noen i et internt rettssystem, og er med på å verne enkeltindividet mot overgrep fra myndighetene/staten. Oppsummert er det rettigheter for individet uansett retts- eller samfunnssystem (Møse, 2002)

Forholdet mellom EMK og norsk lov

Gjennom menneskerettsloven av 21.mai 1999 nr.30 ble EMK gjort til en del av norsk rett. Denne loven fastsetter i §2 at konvensjonen, med protokoller, skal gjelde som norsk lov. Om det oppstår motstrid går det frem av §3 i menneskerettsloven at bestemmelsene i konvensjonen skal gå foran bestemmelser i annen lovgivning. Menneskerettsloven er med på å styrke menneskerettigheters stilling og gir rettslig grunnlag for anvendelsen av slike bestemmelser i norsk rett (Elgesem, 2003).

4.2 Definisjon/forklaring

I denne oppgaven vil vi bruke flere begreper som er viktig å ha rett forståelse av, for å unngå feiltolkning eller andre misforståelser. Vi skal derfor gi en kort forklaring på følgende sentrale begreper i denne oppgaven.

4.2.1 E-tjenesten

Etterretningstjenesten er Norges militære og sivile utenlandsetterretningstjeneste, og jobber i hovedsak med overordnede politiske prioriteringer og tar oppdrag fra hele myndighetssystemet. E-tjenestens tre hovedoppgaver er for det første å understøtte norske myndigheter med informasjon og vurderinger om utenriks-, sikkerhets- og forsvarspolitiske forhold, for det andre å fremskaffe informasjon og varsle om forhold som kan true Norge og norske interesser, og for det tredje støtte forsvarets operasjoner (Forsvaret 2017)

4.2.2 Sikkerhetstiltak

Sikkerhetstiltak er handlinger som blir utført for å sikre seg mot, hindre eller begrense fremtidige uønskede handlinger/hendelser.
Ordet sikkerhetstiltak generelt kan brukes i flere sammenhenger og omfatter mye i store og små situasjoner. Sikkerhetstiltak kan deles inn i tre kategorier: Fysiske, tekniske og administrative tiltak. I denne sammenhengen er sikkerhetstiltak, i form av tiltak, som vil hindre/begrense terrorplanlegging eller utførelsen av terrorhandlinger (Søvik 2012).

4.2.3 Terror/terrorhandlinger

Ordet terror er latin og betyr «å skremme» eller «å skremme hele byen». Terrorister er de som utfører terror. Ordet terror brukes ikke om alle kamphandlinger og krigssituasjoner, kun for situasjoner der uskyldige blir drept bare for å skremme.
Man kan forstå terrorhandlinger på to måter. Den første er terrorhandlinger som blir utført av personer med sykdomsforklaringer. Den andre er terrorhandlinger som blir gjort av politiske og religiøse begrunnelser (Forsvaret 2015).

4.2.4 Digitale trusler

Digitale trusler kan både være komplekse dataangrep og kommunikasjon mellom terrorister som planlegger aksjoner i Norge (Regjeringen, 2017)

4.2.5 Nedkjølingseffekten

Nedkjølingseffekten vil i denne sammenhengen defineres som at vi endrer oppførsel dersom vi er klar over at vi blir overvåket. Vi lar for eksempel være å søke på visse ting eller besøke enkelte nettsider fordi vi frykter at opplysninger om oss vil bli etterlatt og medføre negative konsekvenser. Nedkjølingseffekten fører til press på ytringsfriheten (Laumann, 2016)

4.2.6 Metadata

Metadata kalles ofte for "data om data". Metadata kan sammenlignes med det man finner utenpå en konvolutt. Dette vil omfatte avsender og mottakers navn og adresse. I den digitale verden ser man at metadata vil inneholde informasjon som e-postadresser, IP-adresser, data, tidssone og avsender og mottakers navn i en digital interaksjon (som for eksempel e-post) (Datatilsynet, 2014:46-47).

4.2.7 Innholdsdata

Innholdsdata skiller seg fra metadata, ved at det her er snakk om innholdet i en e-post eller samtale. Informasjonen man får fra innholdsdata vil derfor være hva man har snakket om i en telefonsamtale eller hva man har skrevet til mottakeren av en e-post (Lysne II- utvalget 2016).

4.2.8 Selektor

Selektor er en identifikator for en bruker på en kommunikasjonstejeneste eller søkealgoritme. Dette kan være et telefonnummer, e-postadresser eller brukernavn på en gitt tjeneste (Lysne II-utvalget 2016)

5.0 Lysne II-utvalgets digitale grenseforsvar

Lysne II-utvalget ble oppnevnt i 24. februar 2016 med oppgave om å utrede sentrale problemstillinger knyttet til Etterretningstjenestens mulige tilgang til elektronisk informasjon som kommuniseres i fiberoptiske kabler inn og ut av Norge. 26. august. 2016 la Lysne II-utvalget frem anbefalingen om et digitalt grenseforsvar. (Lysne II utvalget ,2016)

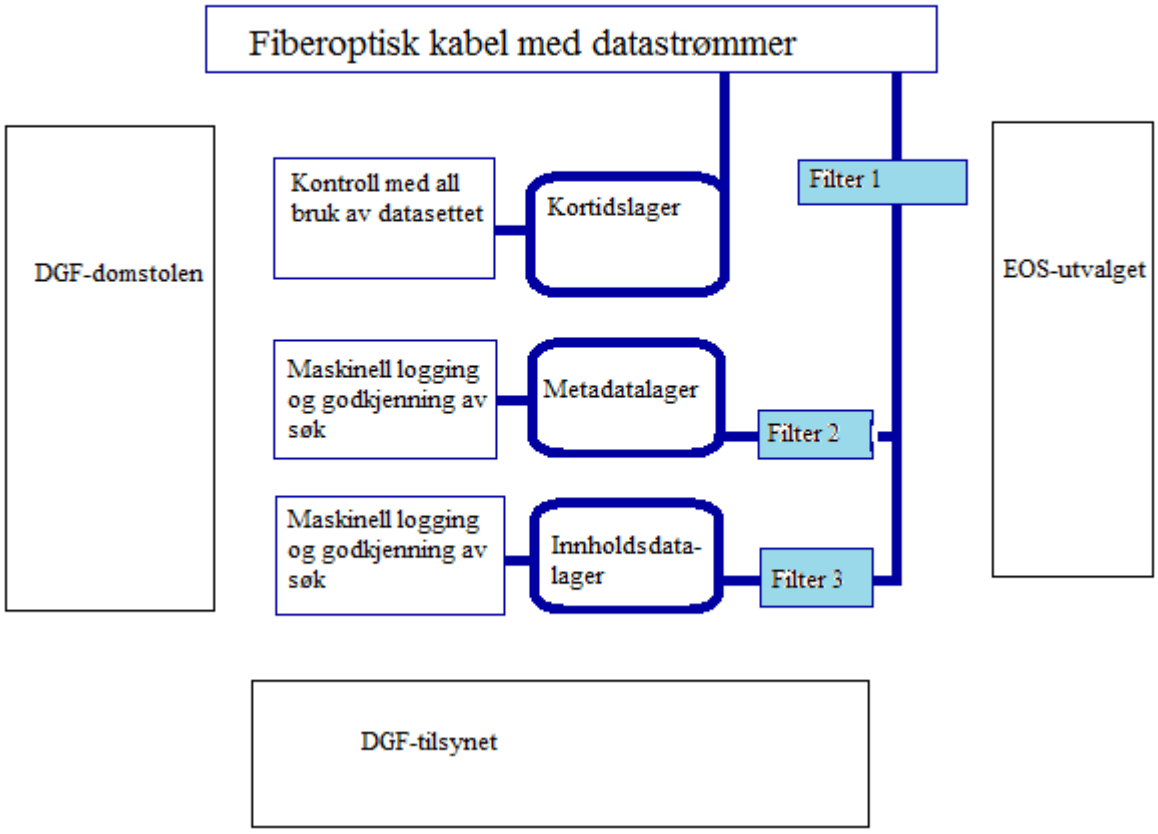
Digitalt grenseforsvar (DGF) kan defineres som E- tjenestens innhenting og analyse av informasjon fra utlandet, som er etterretningsrelevant. Informasjonen vil være basert på å gi en utvidet mulighet til E-tjenestens aksess til elektronisk kommunikasjon som krysser Norges landegrense. Hensikten med tjenesten er å eksaminere og avverge eventuelle ytre trusler som truer landets selvstendighet, nasjonale interesser og rikets sikkerhet (Lysne II utvalget ,2016).

Digitalt grenseforsvar er et juridisk, teknologisk og etterretningsfaglig konsept. At begrepet «grense» benyttes er fordi det vil skape en digital landegrense mellom norske og utenlandske/ytre trusler og kommunikasjonsaktører. Formålet med DGF er å kartlegge og motvirke spionasje, cyberangrep og terrorplanlegging gjennom innhenting av informasjon i transportfasen (Forsvaret, 2017) Lysne II-utvalget hevder at digitalt grenseforsvar vil være nødvendig for at E-tjenesten fortsatt skal ivareta sitt samfunnsoppdrag.

Omfanget av informasjon som i dag er teknologisk er enormt. Denne store mengden med elektronisk informasjonen og kommunikasjonsstrømmer som samles i fiberkablene er blant annet informasjon fra globale tjenesteleverandører som Skype, iMessage eller skytjenester, samt SMS, e-post og facebookmeldinger som blir brukt/sendt inn og ut av Norge.

Lysne II- utvalget beskriver i rapporten et mulig digitalt grenseforsvar som et system som skal samle inn all informasjonen som går gjennom fiberkabelene, filtrer ut og lagre det som er etterretningsrelevant og deretter slette alt som ikke er av interesse. Det digitale grenseforsvaret er svært inngripende og krever derfor strenge retningslinjer og kontrollorganer. Systemet er basert på tre kontrollmekanismer som skal bidra til sikkerheten og troverdigheten til det digitale grenseforvaret. Prinsippene som formålsavgrensing, minimalisering, autorisasjon og kontroll skal prege prosessen.

5.1 Prosess



Figur 1. Vår fremstilling av overordnet beskrivelse av DGF.

Det digitale grenseforsvaret (heretter omtalt som DGF) er kort fortalt en database som e-tjenesten ønsker å bruke til å søke og lete etter digitale trusler eller følge opp sikkerhetsbekymringer. Denne databasen vil bestå av tre ulike datalager som inneholder forskjellige typer data. Siden prosessen er svært inngripende, kreves det strenge sikkerhetsrammer rundt prosessen fra informasjonen blir samlet inn til den skal behandles. Kontroll av hvordan DGF skal benyttes vil bestå av tre hovedelementer:

1.DGF-domstol som forhåndsgodkjenner bevegelser og søk i lagrene.

2. DGF-tilsyn fører tilsyn med at virksomheten drives i henhold til lov, avgjørelsene fra DGF-domstolen og E-tjenestens sine interne retningslinjer.

3. EOS-utvalget driver etterhåndskontroll av de hemmelige tjenestene den dag i dag. De vil motta rapporter fra DGF-tilsynet og ha oversikt over hvordan e-tjenesten bruker DGF.

5.1.1 Innsamling/filtrering

Alle datastrømmer som går via de fiberoptiske kablene vil bli samlet opp (ufiltrert) i et korttidslager. Innsamlingen vil foregå i korte tidsintervaller som vil inneholde både metadata og innholdsdata. Denne informasjonen må ikke lagres lenger enn 14 dager. Korttidslageret vil måtte behandles av mennesker, men med strenge retningslinjer. Lageret vil ikke bli brukt til annet enn å studere optimalisering av neste fase- Filtreringen. Korttidslageret er et viktig mellomlager for å opprettholde kvaliteten på filtrene som skal filtrere informasjonen videre (Lysne II-utvalget, 2016)

Filtreringen av data vil bestå av tre ulike filtre som har forskjellige oppgaver. Det første filteret vil redusere mengden med innhentet data, ved å filtrere bort den kommunikasjonsstrømmen som åpenbart er utenfor interesseområdet. Deretter vil det andre filteret filtrere bort all innholdsdata, og filtrere ut metadata til metadatalageret.

5.1.2 Datalagring

Metadatalageret inneholder den mest betydningsfulle informasjonen for e-tjenesten. Søk i dette lageret må være forhåndsgodkjent av DGF-domstolen. Alle søk som blir gjort i metadatalageret må gjøres av en DGF-operatør og går gjennom en sluse basert på to punkter. Først må søket loggføres slik at søket kan føres tilsyn med, deretter vil det bli gjort en maskinell sjekk på om søket er tillatt og hjemlet i lov. Alle søk som bli gjort må inneholde én av to punkter:

1. Den bør identifisere konkrete individer som det er lov å gjøre søk på (avgjørelsen vil åpne for søk på alle personselektorer tilknyttet dette individet), eller

2. den bør identifisere et handlingsmønster som det er lov å gjøre søk på (modusselektorer)

Søkene som blir gjort vil enten identifisere konkrete individer og åpne for søk på alle personer tilknyttet individet (personselektor), eller så identifiserer søket et handlingsmønster (individselektor) (Lysne II-utvalget)

Det tredje filteret skal slippe gjennom innholdsdata fra kommunikasjonsstrømmer knyttet til objekter som er godkjent av DGF-domstolen, og lagre det i innholdsdatalageret. Innholdsdatalageret er med andre ord det mest uproblematiske lageret, fordi det bare vil inneholde godkjent data fra DGF-domstolen.

6.0 Europeiske menneskerettighetskonvensjonen art. 8

I sin helhet lyder den europeiske menneskerettighetsdomstolen art. 8 som følger (norsk oversettelse):

> *1. Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.*
>
> *2. 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 uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.* (Menneskerettsloven, 1999)

Formålet med EMK art. 8 er å beskytte borgerens rett til respekt for privatliv, familieliv, hjem og korrespondanse. Ved at artikkelen ligger i konvensjonens kapittel om beskyttelse av menneskerettigheter og grunnleggende friheter, forteller det oss at dette er en viktig og grunnleggende rett. Artikkelen er delt i to deler, hvor det i første ledd slår fast hva som skal beskyttes. Videre klargjør det andre leddet at det kan gjøres inngrep i beskyttelsen, så lenge de vilkår som stilles blir oppfylt. De tre vilkårene som nevnes er: i samsvar med lov, legitimt formål og nødvendig for et demokratisk samfunn. Eller i andre ord krav om legalitet, proporsjonalitet og nødvendighet. (Thyve, 2010)

I vår oppgave vil det være relevant å gå nærmere inn på hva som legges i begrepene privatliv og korrespondanse, og hva som blir sett på som inngripende.

6.1 Privatliv og korrespondanse EMK art. 8 første ledd

Den europeiske menneskerettighetsdomstolen (heretter EMD) har gjennom en rekke avgjørelser kommet frem til at «privatliv» er vanskelig å gi en klar avgrenset definisjon på. Ordlyden i seg selv vil innebære flere deler av den private sfære. Gjennom tidligere dommer har EMD lagt vekt på at art. 8 skal beskytte både moralsk og fysisk integritet. Videre skal det beskytte den sfæren hvor borgerne har mulighet til å søke utvikling av sosiale nettverk og personlighet. «Privatliv» skal ikke begrenses til en såkalt indre sirkel, den vil også omfatte andre former for kommunikasjon, som for eksempel profesjonelle relasjoner og relasjoner man har på arbeidsplassen (Thyve, 2010).

Om man ser på ordlyden til korrespondanse, kan dette omfatte så mangt. Basert på tidligere rettspraksis vil dette omfatte alt av telefonsamtaler, brev, e-post og lignende form for kommunikasjon. For å belyse dette, har vi valgt å bruke Malone- dommen. Denne er aktuell for vår problemstilling da den i all hovedsak omhandler uthenting av "data obtained from metering". Etter vår tolkning vil dette også omfatte lagring av data (metadata) som vil falle under det vide omfanget av begrepet korrespondanse. Den viser altså til at metering- informasjon (metadata) beskyttes av EMK art.8. Med det menes hvem man kommuniserer med, hvilke nummer man har ringt, når man har ring og annen informasjon som omhandler kommunikasjonen.I dagens internettbaserte samfunn vil det være naturlig at dette videreutvikles til også å omfatte IP- adresser, DNS data og posisjonsdata mm (Thyve, 2010).

Spesielt relevant for vår oppgave er dette avsnittet (§ 84) fra Den europeiske menneskerettighetsdomstolen 1984, Malone v. Storbritannia:

> *"The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Article 8 (art. 8). The records of metering contain information, in particular the numbers dialed, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the concent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8 (art. 8)".*

6.1.1 Hva er inngripende?

Basert på ordlyden i artikkel 8 er det en handling (eller unnlatelse) som må komme i strid med bestemmelsen, for å være et inngrep. Dette kan for eksempel være formell myndighetsutøvelse i form av vedtakelser av lover eller reell myndighetsutøvelse av politi/forvaltning. Rettspraksis viser også til at det ikke er nødvendig med faktiske handlinger for at et inngrep skal foreligge (Thyve, 2010).

6.2 Vilkår i EMK art.8 andre ledd

6.2.1 I samsvar med lov (legalitetskravet)

Etter Menneskerettighetsdomstolens rettspraksis er et inngrep i overensstemmelse med loven om det er basert på en bestemmelse i en nasjonal lov. Dette gjelder ikke bare krav om nasjonal lov, men også et kvalitetskrav til de gitte lovreglene. Det stilles visse kriterier for at dette skal være oppfylt. Lovene må være tilgjengelig, virkningen må være forholdsvis forutsigbar og de må være forståelige for borgerne (Europarådet, 2014)

6.2.2 Nødvendig i et demokratisk samfunn

Etter ordlyden og følgende rettspraksis må det ses på om et inngrep er nødvendig i et demokratisk samfunn. Dette fremstilles som en forutsetning for at et inngrep skal kunne skje, og retten vil her se på om tiltaket faktisk er nødvendig. Rettspraksis legger her til grunn for en proposjonalitetsvurdering. Her legges det vekt på om de positive konsekvensene vil være veie opp mot eventuelle ulemper og om det finnes mindre inngripende tiltak som medfører de samme positive konsekvensene. En proporsjonalitetsvurdering går ut på at statens fordeler av inngrepet må være større enn individenes ulemper. Etter rettspraksis har statene her et relativt stort rom for skjønn, men domstolen vil gripe inn om den ser at inngrep er ikke-nødvendige, ikke- proporsjonale eller når andre eller mindre inngrep kunne ha blitt iverksatt istedenfor (Fause, 2014)

6.2.3 Legitimt formål

I dette vilkåret ligger det krav om at inngrepet må fremme visse angitte formål. Det går frem av rettspraksis at staten må følge et legitimt mål for at det skal være et berettiget inngrep. Listen over mål er relativt langt, og utfyllende. Det nevnes krav som *"hensyn til den nasjonale sikkerheten, offentlig trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter"*. De aller fleste inngrep fra staten vil forsøke å oppnå et av målene over (Thyve, 2010).

7.0 Drøftelse

7.1 Respekt for sitt privatliv og korrespondanse

Slik det digitale grenseforsvaret beskrives i Lysne rapporten vil E-tjenesten ha innsyn i datastrømmene som krysser den norske landegrensen, og samle inn utenlandsk data. Vi stiller oss kritisk til beskrivelsen av innsamlingsprosessen og lagringen i Lysne II-utvalget. Innledningsvis vil vi se på om innsamling og lagring faktisk utgjør en personverns inngripelse etter EMK art.8 1.ledd.

7.1.1 Innsamling

E-tjenestens sentrale etterrettningsskilde er innhenting av informasjon i transportfasen (Forsvaret, 2017) E-tjenesten hevder at de mest avanserte truslene i det digitale rom ikke kan avdekkes med dagens metoder (Forsvaret, 2017) Informasjonen som før var papirbasert, er i dag digital og befinner seg i datastrømmer i fiberkabler. Problemet er at svært mye av den informasjonen ligger utenfor e-tjenestens samfunnsoppdrag. Basert på beskrivelsen oppfatter vi at innsamlingen hovedsakelig vil bestå at nordmenns daglige bruk at kommunikasjonstjenester i større grad enn det Lysne II-utvalget hevder. Disse dataene gir oss kunnskap om våre tanker, relasjoner og i stor grad hvordan vi lever livene våre.

Nordmenn har rett til respekt for sitt privatliv og sin kommunikasjon jf. EMK art.8 punkt 1. Kommunikasjon mellom mennesker i dag blir i stor grad uttrykk skriftlig. Gjennom de ulike sosiale mediene og kommunikasjonsplattformene deles det daglig mye privat og sensitiv informasjon som ikke bør komme på avveie. Svært mange av de store nettjenestene bruker ikke Norge som transittland, da de blir drevet av utenlandske aktører (Datatilsynet, 2017) De store tjenestene som Facebook, Google og Skype har base i større land enn Norge og bruker altså ikke lille Norge som transittland. Det vil med andre ord si at all kommunikasjon som blir gjort av nordmenn via mange utenlandske nettjenester vil gå via kablene og bli samlet inn. Det gjelder også kommunikasjonen mellom to nordmenn som begge befinner seg i Norge.

Å foreta en innsamling, som ikke er basert på mistanke, av datatrafikken og kommunikasjonen til Norges befolkning vil på flere måter være inngripende på nordmenns krav til respekt for sin kommunikasjon. Selv om store deler av informasjonen vil bli slettet

og aldri lest av fysiske personer, vil det likevel være oppbevart i en base som ikke er hundre prosent sikker for misbruk eller andre formålsglidninger. Det er vanskelig å garantere at det digitale grenseforsvaret ikke vil bli utsatt for en formålsglidning en gang i fremtiden, ved en eventuell implementering. Etterretningstjenesten som er landets utenlandsetterretning vil, slik vi ser det, sitte med informasjon om Norges befolkning. Dette er et paradoks som er verdt å merke seg.

7.1.2 Lagring

Lysne II- utvalget (2016) beskriver i rapporten at det største hinderet når det kommer til lagring vil være metadatalageret. Kort fortalt vil dette lageret inneholde metadata fra utvalgte protokoller til utvalgte kommunikasjonstjenester. Metadata som ikke går under E-tjenestens samfunnsoppdrag, vil så lang som mulig filtreres i Filter 1 og 2.

Som nevnt tidligere fremgår det av konvensjonsteksten til EMK art.8 at det skal foreligge en rett til respekt for korrespondanse. Jf. Malone dommen (se punkt 6.1) ser vi at EMD ser på trafikkdata som en sentral del av kommunikasjon og derfor en del av korrespondanse som skal beskyttes etter første ledd. Derfor vil uthenting, overvåkning og/eller lagring av lignende data bli betegnet som et inngrep i rettighetene etter første ledd. Basert på EMDs praksis og i tråd med generelle utvidende prinsipper om tolkning, kan «data obtained by metering» sies å ha sammenheng med IP-adresser, pålogging tidspunkt og andre data som vil falle under det som lagres av metadata i DGF-systemet. Basert på informasjonen vi får gjennom rapporten, vil det være liten tvil om at det som lagres i metadatalageret går innenfor beskyttelsesområdet i bestemmelsen. Vi mener derfor at det her er på det rene at metadatalagring slik det er presentert i rapporten, vil være et brudd på beskyttelsesområdet i første ledd av bestemmelsen.

Et annet moment som vil tale for at det er inngripende data som lagres, er at metadata ofte kan være like avslørende som innholdet i kommunikasjonen. «*Metadata avslører ikke innholdet i en samtale, men kan vise at du ringte gynekologen din, pratet i 23 minutter og like etter ringte en abortklinikk*» (Datatilsynet 2014:48). Ved at metadata kan være så avslørende, er det etter vår mening liten tvil om at det vil være inngripende i personvernet at slike data skal lagres i et så omfattende system som DGF.

Videre står det lite om hvilke typer metadata som skal lagres, og hvor stor mengde metadata som vil bli lagret i et slikt system. Som Datatilsynet (2017) skriver i sin

høringsuttalelse, vil det derfor være vanskelig å få et helhetlig og klart bilde av lagring og omfanget av lagring i et mulig DGF system.

7.2 Legalitet

7.2.1 Innsamling

I saken Rotaru mot Romania fastslo EMD at ved mangel på forutsigbarhet vil det føre til brudd på art. 8. Romanias lovgivning tillot innsamling, registrering og arkivering av opplysninger som var av betydning for rikets sikkerhet i hemmelige arkiver uten å fastsette betingelser for utøvelse av disse aktivitetene. Bakgrunnen for at domstolen kom frem til at det var brudd på EMK art. 8 var for det første at den rumenske lovgivningen ikke definerte hvilken type informasjon som kunne behandles. For det andre var det heller ikke definert hvilke mennesker som kunne bli utsatt for overvåking. For det tredje var det heller ikke sagt noe om hvilke forutsetninger som måtte ligge til grunn for en slik overvåking eller hvilken prosedyre som skulle følges (Europarådet, 2014)

Sammenlignet med Rotaru mot Romania er det digitale grenseforsvaret klarere på betingelsene. I det digitale grenseforsvaret blir definisjonen på informasjonen som skal behandles beskrevet som utenlandske digitale trusler mot Norge, men innsamlingen er svært lite spesifikk, er svært generell og har likhetstrekk med Rotaru mot Romania. Vi ser at rapporten ikke gir oss klart svar på hvilke mennesker som vil bli overvåket.

7.2.2 Lagring

I EMK art. 8 andre ledd legges det frem et krav om lov for å kunne gjøre en lovlig inngripelse. Her ligger det krav om kvalitet, tilgjengelighet og at loven skal være presis nok slik at borgerne skal være i stand til å forutse sin rettsposisjon. Siden det er E-tjenesten som vil få ansvaret for DGF, vil det slik vi tolker det, være Etterretningstjenesteloven av 1998 (heretter forkortet til E-loven) med instrukser, som vil være den gjeldende loven. Etter E-lovens §4 (2) heter det at E-tjenesten bare kan samle inn og lagre informasjon som gjelder fysiske eller juridiske personer dersom informasjonen har direkte tilknytning til ivaretakelsen av tjenestens oppgaver, eller er direkte knyttet til en slik persons arbeid eller oppdrag for tjenesten. Problemet med dette knyttet opp mot DGF, vil være at det her vil bli

lagret informasjon om fysiske personer som ikke har direkte tilknytning til ivaretakelsen av tjenestens oppgave. Slik det presenteres i rapporten, vil enkeltindivids kommunikasjon bli en del av lagringen, og dette vil derfor gå imot det som blir sett på som E-tjenestens oppgave basert på formålet til DGF. På den andre siden kan man se at det vil være vanskelig i et så omfattende system som DGF å sile ut denne informasjonen, og at det derfor vil kunne være nødvendig å sitte med denne informasjonen om enkeltindivid, slik at man har større mulighet til å oppdage nye trusler.

Videre er det relevant å se på regelverket for lagringstid. Det går frem av rapporten at E-tjenesten ikke skal lagre personopplysninger lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. Vi får her vite at nødvendighets/relevans vurderingen baserer seg på en etterretningsfaglig vurdering som vil variere fra fag- og saksområde. Disse vurderingene bestemmes av E-tjenestens interne regelverk (Lysne II-utvalget 2016). Om vi ser på kravene som stilles til lovverk etter EMK art. 8 andre ledd, vil dette by på noen utfordringer. For det første er ikke dette tilgjengengelig for alle, da det ligger internt i E-tjenesten. For det andre vil det på grunn av manglende tilgjengelighet være vanskelig for personer å vite hvilke rettigheter de har når det kommer til lagringstiden av opplysninger som angår dem. For det tredje vil det kanskje for mange virke urimelig at lagringstiden er på hele 18 måneder.

7.3 Nødvendighet i et demokratisk samfunn

7.3.1 Innsamling

Det norske samfunnet vi lever i er i stor grad basert på tillit. Tilliten i landet er basert politisk stabilitet og et velfungerende rettssystem (Nygaard, 2011) Demokratiet er avhengig av at befolkningen har tillit til myndighetene for å være velfungerende. En konstant overvåkning av datatrafikk i den grad den er fremstilt i rapporten, kan få negative konsekvenser i forbindelse med demokratiet og nedkjølingseffekten vi er vitne til. Et mistillitsforhold til myndighetene er ikke en ønsket samfunnsutvikling. Nedkjølingseffekten har negative følger for privatlivet og ytringsfriheten i Norge. At man tenker seg om to ganger, eller unnlater å søke på enkelte ord i usikkerhet for at opplysningene kan bli brukt mot dem ved senere anledninger, er en uønsket utvikling og legger et uønsket press på ytringsfriheten. I datatilsynet sin rapport fra 2014 viser de til at

hele 16% av befolkningen gjør nettopp dette (Datatilsynet, 2014) Vi mener det derfor er grunn til å anta at dersom DGF blir innført kommer disse tallene til å øke.

I henhold EMK art.8 nr 2 er det grunn til å stille spørsmål om det er nødvendig med et så inngripende system basert på nasjonens fremtidige sikkerhet, eller om det er uforholdsmessig inngripende. Tele2 dommen fra 21.desember 2016 konkluderte EU-domstolen med at masselagring og generell innsamling av personlig informasjon og kommunikasjon opplysninger strider mot menneskerettighetene. Domstolen påpekte også at det må være en sammenheng med trusselbilde og informasjonsinnsamlingen. På bakgrunn av dette oppfatter vi det nødvendig å stille spørsmål til E-tjenestens målrettethet og det dagsaktuelle trusselbilde i sammenheng med innsamlingen og lagringen.

Trusselbildet har i senere tid endret seg mye da mengden cybertrusler mot Norge og norske interesser har økt i omfang. For å skape en oversikt over det dagsaktuelle trusselbilde viser vi til at PST nevner i sin årlige trusselvurdering fra 2017 at "datanettverksopperasjoner vil være en integret del av de ulike etteretningsopperasjonene mot mål i Norge". Deretter hevder E-tjenesten i sin årlige trusselvurdering (Fokus) at Russland og Kina utgjør en alvorlig trussel mot digitale system i Norge. Blant annet hevder de at Russland har over lengre tid gjort forsøk på å hacke seg inn i norske styresmakters datasystem, og driver aktivt med manipulering av sosiale medier. Videre hevder de at Russland står bak flere digitale trusler som sjikane og trusler via SMS/oppringninger og digital sabotasje. (Forsvaret, 2017) Dessuten bruker terrornettverk aktivt sosiale medier og andre datatjenester i Norge for rekruttering og planlegging av angrep.

E-tjenesten viser til trusler som de mener er sannsynlig at vil bli gjennomført i 2017. Vi ser her at både mengden og kompleksiteten av digitale angrep har økt betraktelig de siste årene. Gjennom det digitale rom og det teknologibaserte samfunnet, vil vi påstå at det er relativt enkelt å formidle det som oppfattes som digitale trusler mot konkrete mål og mennesker. Gjennom datainnsamlingen vil trolig e-tjenesten sitte med svært mange former for mistenksom kommunikasjon som faller inn under begrepet "digital trussel". Vi stiller oss spørsmålet om alle trusler vil bli behandlet på samme premisser, eller om det vil foregå et vilkårlig utvalg.

Rapporten gir uttrykk for at kjente aktører og kjente modus er utgangspunktet for søkene de vil foreta i metadatalageret. Den gir ikke noe klart svar på hvordan de vil gå frem for å

oppdage trusler med ukjent opphav. Vi stiller spørsmål til Lysne II-utvalgets beskrivelse av selve behandlingen av det de oppfatter som trusler. Dersom søkeprosessen kun vil omfatte spesifikke trusler de allerede kjent med, hvordan vil de oppdage nye trusler og terrornettverk?

Vi mener at rapporten ikke gir en tilstrekkelig forklaring på denne problemstillingen.

Basert på opplysningene vi nevnte over, er det grunn til å tro at andelen digitale trusler har nådd en høyde som krever nye sikkerhetstiltak. Likevel avveier vi at forslaget om et digitalt grenseforsvar lener seg på en begrunnelse som trolig er gradert. Å legge frem så drastiske og omfattende tiltak, opplever vi at krever en bedre begrunnelse. Å gi norges befolkning innsikt i det reelle trusselbilde basert på konsise opplysninger, vil trolig gi en bedre forståelse for behovet for et digitalt grenseforsvar. På den andre siden har vi forståelse for at å gi for mye informasjon om trusselbilde kan få motsatt effekt og skape uro.

I rapporten er et digitalt grenseforsvar således begrunnet med at "eldre etterretningskapasiteter må fases ut og erstattes med nye". Det er forståelig i sammenheng med digitaliseringen av Norge, men gir oss ikke innsikt eller forståelse for trusselbildet. Uten en mer konkret forklaring på hvorfor det er nødvendig med et digitalt grenseforsvar, er begrunnelsen svært tynn og gir oss ikke inntrykk av at generell innsamling av personlig informasjon og kommunikasjon er nødvendig for rikets sikkerhet.

7.3.2 Lagring

I forhold til lagring vil det her være nødvendig med en proporsjonalitetsvurdering. EU-domstolen hevdet videre i Tele2-dommen at masselagring bare kan være lovlig dersom den er målrettet. Gjennom hele prosessen fra innsamling til behandlingen av data, ser vi at målet er å oppdage aktuelle trusler og avverge angrep mot Norge og norske interesser. Men i startfasen av lagringen er det lite målrettethet. De lagrer i første omgang alt av innsamlet informasjon i korttidslageret, for deretter å filtrere bort det de i etterkant ser er ute av interesseområdet. Dersom e-tjenesten her var ute etter en spesiell aktør, eller spesifikke grupper eller personer, mener vi at det ville foreligget rimelig grad av målrettethet. Men vi oppfatter at lagringen er basert på leting etter uspesifikke trusler, og søkingen kanskje deretter vil foregå i blinde.

Videre vil det være aktuelt å se på om mengden data som ligger i et slikt lager er nødvendig. Ved at det er snakk om all informasjon som går mellom fiberkabler inn og ut av Norge, vil det være en stor mengde med data som ligger i lageret. Selv om dette skal filtreres i de ulike filtrene (se punkt 5.2.1) har Lysne II- utvalget (2016) sagt at det vil være urealistisk, teknisk og ressursmessig krevende å klare en fullstendig filtrering av det som ligger utenfor e-tjenestens samfunnsoppdrag. Videre vil det kunne være uforholdsmessig for borgerne å vite at informasjon om de ligger i et slikt lager.

7.4 Formål

Et viktig prinsipp er at personopplysninger ikke kan samles inn eller lagres uten et bestemt formål. Formålet med DGF beskrives i rapporten som "formålet med informasjonsinnhentingen er besluttningsstøtte for myndighetene, og ikke straffeforfølging, og tjenesten er avgrenset mot overvåkning av nordmenn i Norge". Formålsbeskrivelsen av DGF, slik vi oppfatter det, er svært generelt. Den gir oss ikke kunnskap om i hvilken seksjon besluttningsstøtten vil finne sted, eller om det vil omfatte de fleste situasjoner der beslutninger skal tas.

Prinsippet om at det må foreligge et bestemt formål, er sentralt i forbindelse med lovligheten av søkeprosessen i det digitale grenseforsvaret. Vi stiller spørsmål ved effektiviteten i henhold til effektivitetskravet i utøvende rettspraksis. Sikkerhetsrammene rundt det digitale grenseforsvaret er i høyeste grad nødvendig, men vi ser at en forhåndsgodkjenning av en egen domstol kan være tidkrevende dersom denne domstolen vil fungere på mange måter som den norske domstolen. Hvordan forhåndsgodkjenningen skal fungere er svakt forklart i rapporten, men vi legger til grunn at det vil bli krevende å opprettholde effektivitetskravet i samsvar med sikkerheten rundt.

Vi opplever at formålet med DGF slik det først beskrives, ikke samsvarer med forklaringen på prosessen i selve rapporten. Derfor mener vi at formålet til det digitale grenseforsvaret er upresist.

8.0 Avslutning

På bakgrunn av problemstillingene vi har tatt for oss i oppgaven, mener vi at Lysne II-utvalgets utgreiing om et digitalt grenseforsvar er for lite utfyllende til å være betryggende. Dette begrunner vi med at det burde formuleres en bedre begrunnelse for hvorfor vi trenger et system som DGF. Basert på det dagsaktuelle trusselbildet og den informasjonen om eventuelle trusler vi evner å finne, er ikke disse faktorene en tilstrekkelig begrunnelse for innføring av et digitalt grenseforsvar. Trusselnivået, vi er klare over, veier ikke tyngre enn respekten til privatliv i henhold til EMK art. 8 andre ledd.

Det digitale grenseforsvaret er såpass inngripende i forhold til personvern og respekten til kommunikasjon, at det etter vår mening ikke kan innføres slik det fremstilles i rapporten.

Vi ser også at et slikt system vanskelig kan reverseres om det først blir implementert, og at man ikke kan forutse hvilke konsekvenser dette vil ha for ytringsfriheten, demokratiet og personvernet i Norge.

Gjennom analysen vi har gjort føler vi at vi har belyst problemstillingen, både med fordeler og ulemper for en eventuell implementering av et digitalt grenseforsvar. Det vi har sett er at det i forhold til EMK art.8 vil kunne ses på som nødvendig, spesielt med tanke på de nylige hackeangrepene. Men vi har derimot valgt å legge vekt på hvor inngripende et slikt system vil kunne være på personvernet, og har derfor kommet frem til at en eventuell implementering av DGF vil bryte med personvernet etter EMK art.8.

9.0 Referanseliste

Datatilsynet. 2014. *Personvern. Tilstander og trender 2014*.

https://www.datatilsynet.no/globalassets/global/04_planer_rapporter/persovern_tilstandogtrender_2014.pdf Lest 05.04.17

Europarådet, 2014. *Håndbog om europæisk databeskyttelseslovgivning.*

http://www.echr.coe.int/Documents/Handbook_data_protection_DAN.PDF Lest 10.04.17

Elgesem, Frode. 2003. *Tolkning av EMK- Menneskerettsdomstolens metode. Tidsskrift om lov og rett* 42, (4-5): 203-230

https://www.idunn.no/lor/2003/04-05/tolking_av_emk_-_menneskerettsdomstolens_metode_1

Etterretningstjenesteloven. *Lov om etterretningstjenesten av 20.mars 1998 nr.11*
https://lovdata.no/dokument/NL/lov/1998-03-20-11?q=Etterretningstjeneste loven

Fause, Anett Beatrix Osnes. 2014. *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* 14, (1): 46-60

https://www.idunn.no/tidsskrift_for_strafferett/2014/01/kravet_til_legalitet_noedvendighet_og_proporsjonalitet_naar_

Forsvaret.no, 2017. Digitalt grenseforsvar https://forsvaret.no/etjenesten/dgf Lest 27.03.17

Forsvaret.no, 2017. Fokus 2017 https://forsvaret.no/fokus Lest 16.03.17

Forsvaret.no .2015 (Oppdatert 28.juni. 2016). *Hva er terror?*
https://forsvaret.no/tjeneste/familier/barn-ungdom/hva-er-terror Lest 14.03.17

Jacobsen, Dag Ingvar. 2015. *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode*. 3. utgave. Cappelen Damm Akademisk

Laumann, Kari 2016. Nedkjølingseffekten indikerer at ytringsfriheten er under press etter Snowden https://www.personvernbloggen.no/tag/nedkjolingseffekt/ Lest 05.04.17

Lysne II- utvalget. 2016. *Digitalt Grenseforsvar (DGF).*

https://www.regjeringen.no/globalassets/departementene/fd/dokumenter/lysne-ii-utvalgets-rapport-2016.pdf Lest 27.03.17

Malone v. The United Kingdom.The European Court of Human Rights, Strasbourg, 1984

http://hudoc.echr.coe.int/eng#{"display":["0"],"languageisocode":["ENG"],"appno":["8691/79"],"documentcollectionid2":["CHAMBER"],"itemid":["001-57533"

Menneskerettsloven, 1999. *Lov om styrking av menneskerettighetenes stilling i norsk rett*.

https://lovdata.no/dokument/NL/lov/1999-05-21-30/KAPITTEL_2#KAPITTEL_2 Lest 20.03.17

Møse, Erik. 2002. *Menneskerettigheter.* 1. utgave. Cappelen Akademisk.

Nygaard, Lars. 2012. *Tillit skaper velferdsstaten- ikke omvendt.* http://forskning.no/sosiologi/2012/03/tillit-skaper-velferdsstaten-ikke-omvendt Lest 25.04.17

Pst.no 2017. Trusselvurdering 2017 http://www.pst.no/media/82444/PST_Trusselvurd-2017.pdf Lest 16.03.17

Regjeringen.no, 2002. FNs sikkerhetsråds resolusjon. https://www.regjeringen.no/no/dokumenter/fns-sikkerhetsrads-resolusjon-1373/id107760/ Lest 02.03.17

Regjeringen. 2005. *Den europeiske menneskerettighetskonvensjonen (EMK)*. https://www.regjeringen.no/no/dokumenter/den-europeiske-menneskerettighetskonvens/id88366/ Lest 10.03.17

Regjeringen.no, 2017 Høringsuttalelse- Raport avgitt av Lysne II-utvalget om digitalt grenseforsvar, https://www.regjeringen.no/contentassets/84a90462cf9b4aebb310d97052083d26/horingssvar-med-merknader-datatilsynet-digitalt-grenseforsvar.pdf. Lest 22.03.17

Ruud, Morten og Ulfstein, Geir. 2011. *Innføring i folkerett*. 4. utgave. Universitetsforlaget.

Søvik, Vegard Floor. 2012 (Oppdatert 04.03.17). *Sikkerhetstiltak- en introduksjon.* http://ndla.no/nb/node/89104?fag=52291 Lest 10.03.17

Tele2 Sverige AB v. Post-och telestyrelsen, Sweden. Court of Justice of the European Union, Luxembourg, 21 December 2016. https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-12/cp160145en.pdf Lest 09.03.17

Thyve, Ulrik F.2010. *EMK artikkel 8.* http://lex-superior.blogspot.no/2010/04/datalagringsdirektivet.html Lest 30.03.17