Universitetet
i Stavanger

Noen våker over deg

En studie av hvordan digitalt grenseforsvar kan true samfunnssikkerheten

Masteroppgave i Samfunnssikkerhet

Universitetet i Stavanger

Våren 2019

Secilie Schelbred

Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Master i samfunnssikkerhet	Vårsemesteret, 2019 Åpen
Forfatter: Secilie Schelbred	..... Secilie S. ..... (signatur forfatter)
Fagansvarlig: Odd Einar Falnes Olsen	
Tittel på masteroppgaven: Noen våker over deg - En studie av hvordan digitalt grenseforsvar kan true samfunnssikkerheten Engelsk tittel: Someone is watching over you - A study of how digital border defense can threaten societal safety	
Studiepoeng: 30	
Emneord: Samfunnssikkerhet, digitalt grenseforsvar, overvåking, demokrati, personvern, rettssikkerhet, tillitt, kommunikasjonsvern, etterretningstjenesten, risikostyring, IKT	Sidetall: 78 + vedlegg/annet: 90 Stavanger, 14.06.2019

Forord

Denne masteroppgaven representerer avslutningen på utdanningen innen samfunnssikkerhet ved Universitetet i Stavanger. Studietiden har vært lærerik med mange spennende utfordringer. Gjennom de siste årene har det vokst frem en personlig interesse for temaet overvåking. Jeg fulgte blant annet debatten om Datalagringsdirektivet, og finner spenningsforholdet mellom sikkerhet og personvern interessant. Da utredningen og den politiske behandlingen av det digitale grenseforsvaret startet, var dette et felt jeg ønsket å studere nærmere. I den forbindelse er jeg veldig takknemlig for at universitetet har gitt meg mulighet til å gjøre nettopp dette. Prosessen har vært lang og tung, og det føles godt å endelig være i mål med et produkt som forhåpentligvis har noe å bidra med i diskusjonen om overvåking og samfunnssikkerhet.

Jeg vil takke veilederen min Odd Einar Olsen for konstruktive og ærlige tilbakemeldinger som har hjulpet meg videre på veien. Takk til mine nærmeste medstudenter som har vært helt uunnværlige gjennom studietiden, dere vet hvem dere er. Jeg vil også takke familien min som har støttet meg gjennom studietiden. Marianne Thorbjørnsen, takk for at du har holdt motet mitt oppe og for at du er den du er. Hani Elsayed, you are my everything!

Hyggelig lesning!

Istanbul, Juni 2019.

Secilie Schelbred

Sammendrag

Denne masteroppgaven i samfunnssikkerhet er gjennomført ved det teknisk-naturvitenskapelige fakultetet ved Universitetet i Stavanger. Oppgaven er knyttet til tema om overvåking og samfunnssikkerhet, og studerer det digitale grenseforsvaret (DGF) som for øyeblikket er under politisk behandling. Det digitale grenseforsvaret er en innretning som åpner for at Etterretningstjenesten (E-tjenesten) skal gis tilgang til å overvåke all informasjon om kommunikasjon som krysser landegrensen gjennom fiberoptiske kabler. Oppgavens hovedmål og problemstilling er å undersøke hvordan det digitale grenseforsvaret kan true samfunnssikkerheten. Ifølge Samfunnssikkerhetsinstruksen (2017) handler samfunnssikkerhet om evnen samfunnet har til å beskytte liv og helse gjennom å håndtere trusler mot grunnleggende verdier og funksjoner. Videre blir problemstillingen understøttet av tre forskningsspørsmål. Det første forskningsspørsmålet handler om hva som kan overvåkes gjennom DGF. Dette retter seg mot omfanget og hva som potensielt kan overvåkes gjennom DGF. Det neste forskningsspørsmålet undersøker hvilke kontrollmekanismer som er tenkt implementert i DGF-systemet. Dette handler om systemets oppbygging hvor blant annet datalagrene, filtrering av informasjon og ulike tilsyns- og kontrolltiltak undersøkes. Det siste forskningsspørsmålet ser nærmere på hvilke samfunnsfunksjoner og verdier som kan påvirkes ved etablering av DGF. Her knyttes DGF opp mot definisjonen av samfunnssikkerhet gjennom vurdering av hvordan samfunnsfunksjoner og kritisk infrastruktur kan påvirkes. DGF blir deretter knyttet opp mot grunnleggende samfunnsverdier, hvor prinsipper om personvern, rettssikkerhet, og tillitt står sentralt.

Oppgavens metode bygger på et kvalitativt litteraturstudie hvor det empiriske grunnlaget tar utgangspunkt i den offentlige utredningen om DGF som er gitt av Lysne II-utvalgets rapport (2016). Denne rapporten er sentral for studien i og med at den fremlegger generell informasjon og drøfter sentrale forslag og problemstillinger knyttet til en eventuell etablering av DGF.

Resultatene fra studien viser at overvåkingskapasiteten, faren for utilsiktet eller uautorisert tilgang til DGF-systemet, samt den potensielle påvirkningen av grunnleggende samfunnsverdier er utfordringer som reises gjennom DGF. Overvåking blir ofte oppfattet for å

være noe som bidrar til å ivareta samfunnssikkerheten. Studien viser imidlertid at DGF i seg selv kan bidra til å skape nye sårbarheter i samfunnet. DGF vil fange opp betydelige mengder informasjon om kommunikasjon som krysser landegrensen. Dermed vil sikkerheten rundt og beskyttelsen av selve dataene og DGF-systemet være viktig, fordi store mengder sensitiv informasjon vil befinne seg i systemet. Utfordringen ligger i at det til tross for høy sikkerhet og flere kontrollmekanismer vil kunne være fare for angrep eller misbruk av systemet. Videre viser studien at selv om DGF-systemet og E-tjenestens oppdrag er rettet mot utlandet, vil norske borgere i stor grad berøres. Dermed vil DGF kunne påvirke og utfordre samfunnets grunnleggende verdier som personvern, rettssikkerhet og tillitt. Studien viser at DGF vil ha et betydelig overvåkingspotensiale, men at effekten samtidig kan reduseres ved at det finnes relativt enkle løsninger for å unngå å fanges opp av systemet. Dette vil også kunne bety at trusselaktører kan skjule seg, mens vanlige borgere som ikke iverksetter tiltak for å skjule kommunikasjonen sin vil fanges opp av systemet.

Konklusjonen tilsier at DGF kan være en trussel overfor samfunnssikkerheten. Til tross for at DGF er et tiltak som skal bidra til et tryggere samfunn, kan det samtidig true samfunnssikkerheten ved å utfordre flere av prinsippene og verdiene som vårt demokratiske samfunn er bygget på. DGF vil imidlertid ikke anses for å være en innretning som truer samfunnssikkerheten gjennom å direkte være til fare for borgernes liv og helse. Videre kan det synes å mangle et risikostyringsperspektiv på hvordan DGF skal kunne reguleres i etterkant med tanke på hvilke forutsetninger som ligger til grunn for å eventuelt skulle endre eller avvikle systemet. Konklusjonen stiller spørsmål ved hvorvidt en innretning med betydelig overvåkingskapasitet vil kunne forsvares og være forenelig overfor andre samfunnshensyn dersom systemet potensielt sett har svekket effektivitet. Det gjenstår likevel å se hvordan samfunnet og borgerne eventuelt vil påvirkes gjennom en etablering av DGF. Studien tilsier at sentrale spørsmål og utfordringer knyttet til DGF bør utredes ytterligere før en eventuell implementering iverksettes. Risikoen blir på mange måter et spørsmål om hva samfunnet er villig til å akseptere, enten det skjer gjennom etablering av DGF eller ikke.

Innholdsfortegnelse

1. Introduksjon 1
1.1 Tema og problemstilling 3
1.1.1 Forskningsspørsmål 4
1.2 Avgrensninger 4
1.3 Struktur 6
2. Bakgrunn 7
3. Teori 10
3.1 Samfunnssikkerhet 10
3.1.1 Statens sikkerhetsansvar 10
3.1.2 Rikets sikkerhet og nasjonale interesser 11
3.1.3 Samfunnssikkerhet og IKT 12
3.1.4 Viktige samfunnsfunksjoner og kritisk infrastruktur 13
3.2 Risikostyring 14
3.3. Overvåking 16
4. Metode 18
4.1 Kvalitativt litteraturstudie 18
4.2 Datagrunnlag 20
4.3 Validitet og reliabilitet 20
4.3.1 Validitet 21
4.3.2 Reliabilitet 22
4.3.3 Kildebruk 22
4.4 Styrker og svakheter ved metoden 24
5. Empiri 27
5.1 Etterretningstjenesten 27
5.1.1 Styring og kontroll av E-tjenesten 27
5.1.2 E-tjenestens arbeid 28
5.1.3 Vilkår for informasjonsinnhenting 29
5.2 Digitalt grenseforsvar 30
5.2.1 Formålet med DGF 31
5.3 Hva kan overvåkes gjennom DGF? 32
5.3.1 Kryptering 33
5.4 Hvilke kontrollmekanismer er tenkt implementert ved etablering av DGF? 34
5.4.1 Kontrollmekanismer i DGF-systemet 35
5.5 Hvilke samfunnsfunksjoner og verdier kan påvirkes ved etablering av DGF? 38

5.5.1 Samfunnsfunksjoner 39
5.5.2 Grunnleggende samfunnsverdier 40
6. Analyse 44
6.1 Hva kan overvåkes gjennom DGF? 44
6.1.1 Masseovervåking? 46
6.1.2 Ulike typer data 48
6.1.3 Kryptering 49
6.2 Hvilke kontrollmekanismer er tenkt implementert ved etablering av DGF? 50
6.2.1 Datalager 51
6.2.2 Filter 55
6.2.3 Andre momenter og tidligere eksempler 56
6.3 Hvilke samfunnsfunksjoner og verdier kan påvirkes ved etablering av DGF? 59
6.3.1 Samfunnsfunksjoner 59
6.3.2 Grunnleggende samfunnsverdier 61
7. Konklusjon 73
7.1 Oppsummering av konklusjon 76
8. Videre forskning 78
Litteraturliste 79
Figurer 83

1. Introduksjon

På verdensbasis ligger Norge i topp når det gjelder bruk av informasjons- og kommunikasjonsteknologi (IKT), og er å regne som et av de mest digitaliserte land i verden. Digitaliseringen har gjennom nyere tid ført til gjennomgripende samfunnsmessige endringer, og i dag finnes IKT overalt, fra telefonen og postkassen til bilen og hvitevarene. De fleste private hjem og arbeidsplasser berøres av den teknologiske utviklingen, i tillegg til at viktige samfunnsfunksjoner og kritisk infrastruktur digitaliseres. Samfunnet blir stadig mer avhengig av IKT og internettbaserte løsninger eller tjenester. Digitaliseringen har også revolusjonert måten mennesker kommuniserer på, hvor blant annet mobiltelefoner og sosiale medier er blitt en del av hverdagen (NOU 2015:13: 15, 18).

Den teknologiske utviklingen bringer imidlertid noen utfordringer med seg, og digitalisering har ført til store endringer i risiko- og sårbarhetsbildet. Hvordan disse risikoene og sårbarhetene imøtekommes, vil få betydning for hvordan samfunnet vil se ut i fremtiden. For å ivareta de grunnleggende verdiene bak rettsstaten og demokratiet kreves det en forsvarlig håndtering av de ulike risiko- og sårbarhetsutfordringene. Samtidig vil de grunnleggende verdiene utfordres i møte med nettopp digitaliseringen og de mulighetene den medbringer, som for eksempel gjennom overvåking (NOU 2015:13: 15, 18). Dette er også tema som myndighetene legger stort fokus på. I 2017 kom for eksempel den første stortingsmeldingen som utelukkende omhandler digital sikkerhet, og hvordan IKT påvirker samfunnet gjennom komplekse grenseoverskridende utfordringer som går på tvers av land, sektorer og virksomheter (Regjeringen.no, 2019: 24, Meld. St. 38, 2016-2017). Stortingsmeldingen om «Digital agenda for Norge» tar for seg regjeringens digitaliseringspolitikk og viser til aspekter knyttet til både personvern og digital sikkerhet (Meld. St. 27, 2015-2016).

Mulighetene som finnes i overvåkingsteknologien er enorm, og dag er det for eksempel mulig å spore enkeltpersoners bevegelsesmønster ved å kople mobilbruk opp mot ulike dataregistre. Her kan det blant annet hentes ut informasjon om hvor vi har vært og hvem vi har kontakt med, noe som ikke var like enkelt for noen år tilbake (Engen, Kruke, Lindøe, Olsen, Olsen & Pettersen, 2016, 383-384). Debatten om overvåking aktualiseres på mange måter gjennom den politiske behandlingen av digitalt grenseforsvar (DGF) som nå foregår. Lysne II-utvalgets rapport (2016) behandler spørsmål og problemstillinger knyttet til innføring av DGF i Norge.

I 2016 sendte Forsvarsdepartementet Lysne II-utvalgets rapport (2016) om DGF på høring. Godt over hundre høringssvar ble gitt, blant annet av PST, Datatilsynet og Justis- og beredskapsdepartementet (Regjeringen.no2, 2016). Gjennom samfunnsdebatten stilles ofte overvåking i et slags motsetningsforhold til personvernet. På den ene siden står personvernet som en viktig verdi i samfunnet, på samme måte som for eksempel ytringsfriheten og rettssikkerheten. På den andre siden står overvåking som kan oppfattes som en trussel mot personvernet, men også som et viktig verktøy både i samfunnsstyringen og for bekjempelse av kriminalitet (Newth, 2014: 7-9, 12).

Behovet for DGF formidles av Etterretningstjenesten (E-tjenesten) som etterspør informasjonstilgang tilknyttet digitale data. Moderne kommunikasjonssignaler går ikke lenger gjennom radio og satellitt, men via digitale data som transporteres gjennom fiberoptiske kabler. Det meste av den digitale trafikken inn og ut av Norge går gjennom det fiberoptiske kabelnettverket, og det er i denne informasjonsstrømmen E-tjenesten ønsker tilgang. Det vil være sentrale spørsmål og overveielser knyttet til balansegangen mellom det sikkerhets- og etterretningsmessige behovet og aktuelle personvernsaspekter i vurderingen av DGF (Regjeringen.no, 2019). Både Lysne II-utvalget (2016) og rapporten «Et felles løft» (2015) konkluderer med anbefaling om å innføre DGF (Regjeringen.no, 2017).

Et sentralt aspekt ved samfunnssikkerhet er nettopp forebygging og håndtering av uønskede hendelser. Arbeidet med forbedringer av samfunnssikkerheten har ofte en tendens til å dreie seg om å avverge hendelser og forhindre at lignende hendelser skal skje igjen. I etterkant av store og alvorlige hendelser er oppmerksomheten ofte rettet mot de katastrofale konsekvensene, samtidig som det politisk presset for å gjøre noe øker. I kjølvannet av slike hendelser, som for eksempel terrorangrep, heves gjerne toleransen overfor innføring av nye tiltak som kan bidra til å forhindre at noe lignende skal gjenta seg. Dette kan gjerne dreie seg om tiltak som bidrar til å øke sikkerheten på kort sikt, men som på lang sikt kan svekke samfunnssikkerhetens fundament (Engen et al., 2016, 392). Boken «fra terror til overvåking» (Hausken, Yazdani & Haagensen, 2014) kan for eksempel illustrere noen aspekter om hva som foregikk i etterkant av terrorangrepet som rammet Norge 22. juli.

DGF og overvåking fremstår som viktige verktøy som skal bidra til å styrke samfunnssikkerheten. Myndighetene ønsker å innføre DGF nettopp for å gjøre Norge tryggere og beskytte norske interesser. Med dette som utgangspunkt vil det være interessant å snu om på tankesettet og studere om DGF kan true samfunnssikkerheten på noen måte.

1.1 Tema og problemstilling

Teamet for denne avhandlingen handler om overvåking og samfunnssikkerhet. Fokuset er rettet mot DGF som overvåkingsverktøy, og hvordan dette kan påvirke samfunnssikkerheten. Utgangspunktet for studien baserer seg på Lysne II-utvalgets rapport (2016) som utreder DGF og tar stilling til ulike spørsmål og demokratiske hensyn i forbindelse med å gi E-tjenesten tilgang til den digitale kommunikasjonen som krysser grensen i de fiberoptiske kablene. Videre tar studien utgangspunkt i sikkerhetsinstruksens definisjon av samfunnssikkerhet hvor sentrale begreper som samfunnsfunksjoner, kritisk infrastruktur, vern og håndtering av trusler, samt ivaretakelse og beskyttelse av borgernes liv og helse står sentralt. Generelt sett anses ofte overvåking som et verktøy som bidrar til å ivareta samfunnssikkerheten. Blant annet fordi det kan gi myndighetene mulighet til å detektere og avverge uønskede hendelser som for eksempel kriminalitet, terror, eller andre angrep som truer samfunnssikkerheten. På den andre siden kan det imidlertid stilles spørsmål om overvåking i seg selv kan bidra til å true samfunnssikkerheten. Dette danner grunnlaget for oppgavens problemstilling som er:

Hvordan kan digitalt grenseforsvar true samfunnssikkerheten?

Denne problemstillingen er valgt fordi den gjerne har et litt annerledes utgangspunkt enn hva overvåkingsdiskursen vanligvis har. Jeg er av en oppfatning av at overvåking ofte blir ansett for å ivareta og forbedre samfunnssikkerheten. Tanken bak den valgte problemformuleringen er derfor at den kan bidra til å belyse viktige sider i debatten om overvåking og samfunnssikkerhet ut fra en slags motsatt betraktning. Studiens aktualitet ligger i samfunnsutviklingen hvor teknologi og digitalisering bidrar til endringer som får betydning utover hvordan hver enkelt av oss påvirkes. DGF berører oss alle, og vil av den grunn også kunne sies å være av samfunnsmessig betydning. Oppgaven er ikke å svare på hvorvidt en innføring av DGF vil være riktig eller galt. Hensikten med studien er å drøfte ulike hensyn og

spørsmål knyttet til DGF ut fra et samfunnssikkerhetsfaglig ståsted, og da med tanke på hvordan samfunnssikkerheten kan trues gjennom overvåking i lys av DGF. Formålet er å bidra til den offentlige debatt vedrørende DGF og overvåking generelt, samt gi innsikt i hvordan dette henger sammen med og kan true samfunnssikkerheten.

1.1.1 Forskningsspørsmål

For å kunne svare på problemstillingen, er det vurdert som hensiktsmessig å utarbeide noen forskningsspørsmål. Forskningsspørsmålene er utarbeidet på en slik måte at de både hver for seg, og ikke minst samlet sett, kan bidra til å belyse studiens problemstilling. Spørsmålene er som følgende:

- *Hva kan overvåkes gjennom DGF?*
- *Hvilke kontrollmekanismer er tenkt implementert ved etablering av DGF?*
- *Hvilke samfunnsfunksjoner og verdier kan påvirkes ved etablering av DGF?*

De tre forskningsspørsmålene legger føringer for studiens retning, og utgjør grunnlaget som brukes for å svare på problemstillingen. Spørsmålene anses for å dekke ulike aktuelle sider ved DGF som i neste omgang er relevante også overfor samfunnssikkerhetsfeltet.

1.2 Avgrensninger

Denne studien handler om hvordan DGF kan true samfunnssikkerheten. Arbeidet tar ikke sikte på å studere fordeler eller ulemper knyttet til DGF. Gjennom besvarelsen av de ulike forskningsspørsmålene vil det likevel kunne sies at fordeler og ulemper ved DGF omtales. Årsaken til dette er knyttet til at spørsmålene og problemstillingen er utformet på en slik måte at det vil være naturlig å diskutere ulike sider ved DGF. Formålet er imidlertid ikke å gi noe korrekt svar eller avveininger for eller mot etableringen av DGF. Videre er studien begrenset ved at den ikke går i dybden på ulike juridiske spørsmål ved innføring av DGF. Rettssikkerhet er for eksempel et aspekt som omtales og er relevant i forbindelse med overvåking, men studien tar ikke sikte på å gi grundige innføringer i juridiske forhold knyttet til lovverket. Denne avgrensingen er gjort dels på grunn av begrensninger i omfang, men også fordi juridiske forhold oppfattes som et stort tema som krever et annet utgangspunkt og en egen problemstilling.

En annen avgrensning ved studien er at den ikke tar for seg andre lands erfaring fra lignende overvåkingssystemer og hvordan dette eventuelt kan ha påvirket samfunnssikkerheten der. Årsaken er at jeg ønsker å undersøke DGF i forhold til det norske samfunnet. Et komparativt studie ville også kunne blitt veldig annerledes i forhold til hva som er hensikten og bakgrunnen for denne studien. Videre vil det ikke være fokus på ulike kostnadseffektive momenter ved innføring og drift av DGF. Det samfunnsøkonomiske regnestykket vil på mange måter også kunne være aktuelt i forhold til å vurdere DGF, og da spesielt med tanke på om det finnes andre alternativer. I tillegg kan samfunnsøkonomiske perspektiv bidra med en viktig dimensjon i debatten om DGF. Et slikt utgangspunkt vil imidlertid falle inn under andre premisser og dermed fordre en annen problemstilling slik jeg ser det.

Fagfeltet innen samfunnssikkerhet er ganske omfattende, og favner bredt i samfunnet. I den forbindelse er det ansett som fruktbart å avgrense aspekter ved samfunnssikkerhet til å gjelde de ulike forhold knyttet til selve definisjonen av begrepet. Definisjonen av begrepet er hentet fra Samfunnssikkerhetsinstruksen (2017) som anses for å inkludere de mest elementære momentene som inngår i begrepet, samt at den også kan sies å være i overensstemmelse med fagfeltets forklaringer av begrepet.

Det er også blitt gjort en avgrensning i forhold til at det ikke gjøres vesentlig forskjell på begrepene metadata og stordata. I Lysne II-utvalgets rapport (2016) beskrives et skille mellom begrepene, hvor metadata viser til store mengder data om beskriver andre data, mens stordata viser til så store datasett at det er nødvendig å benytte maskinelle analyser og algoritmer for å finne meningsfull informasjon og mønstre (Lysne II-utvalget, 2016: 25-26). Videre i Lysne II-utvalgets rapport (2016) anvendes begrepet metadata, samtidig som automatisert og maskinell filtrering og programmering skal være en del av DGF-systemets tekniske utforming. Videre kan det antas at de store mengdene metadata som samles inn også kan grense til å være innenfor definisjonen av hva stordata er. Datatilsynet (2017) peker på at omfanget av metadatalageret som foreslås i DGF-systemet er noe uklart. Det vises ikke til den totale mengden av metadata som vil lagres i systemet (Datatilsynet, 2017: 10) og av den grunn kan det tolkes slik at DGF også kan sies å inneholde stordata. Det viktigste skillet for denne studien er imidlertid forskjellen mellom metadata og innholdsdata. Av den grunn er det ikke

gjort noe videre skille på hvorvidt dataene i DGF-systemet vil anses for å være metadata eller stordata. Begrepet som brukes for studien er derfor metadata som vurderes som dekkende i denne sammenheng.

1.3 Struktur

Første del av studien tar for seg innledning, tema og problemstilling. Her beskrives også de ulike avgrensingene som er foretatt. Kapittel 2 presenterer bakgrunnen for DGF og gir et innblikk i hvilken kontekst studien befinner seg i. I Kapittel 3 beskrives det teoretiske fundamentet som studien baserer seg på. Her vektlegges momenter knyttet til statens sikkerhetsansvar, samfunnssikkerhet, og kort om utviklingen innen informasjons- og kommunikasjonsteknologi (IKT). Videre presenteres teoretiske aspekter knyttet til risikostyring, samt det teoretiske grunnlaget for begrepet overvåking slik det forstås og anvendes i forbindelse med denne studien. I kapittel 4 gjøres det rede for studiens metode gjennom å forklare hva som er gjort og hvordan studien er utført. Her begrunnes og redegjøres det blant annet for valg av metode, studiens datagrunnlag, validitet og reliabilitet, samt ulike styrker og svakheter ved den metodiske fremgangsmåten.

Kapittel 5 presenterer studiens empiriske funn. Her gis det først generell informasjon knyttet til E-tjenesten og deres arbeid, samt styring og vilkår angående deres informasjonsinnhenting. I tillegg gis en beskrivelse av hovedelementene ved DGF og hva som er formålet. Deretter starter presentasjonen av de empiriske funnene knyttet til forskningsspørsmålene. Først forklares det hva som kan overvåkes gjennom DGF. Deretter presenteres de ulike kontrollmekanismene som er tenkt implementert i DGF-systemet. Her fokuseres det blant annet på mekanismer som er knyttet til datalager og filter. Tilslutt presenteres funnene knyttet til forskningsspørsmålet om hvilke samfunnsfunksjoner og verdier som kan påvirkes ved etablering av DGF. Samfunnsfunksjonene ses i sammenheng med kritisk infrastruktur og de ulike kriteriene som avgjør kritikaliteten. Videre er verdiene personvern, rettssikkerhet og tillitt sentrale i å forklare hvordan DGF kan påvirke samfunnsverdiene. I kapittel 6 analyseres de ulike forskningsspørsmålene med utgangspunkt i det teoretiske grunnlaget og empiriske materialet for studien. Her drøftes de empiriske funnene sammen med teoretiske momenter for å gi svar på forskningsspørsmålene. Tilslutt, i kapittel 7, vil det gis et endelig svar på problemstillingen om hvordan DGF kan true samfunnssikkerheten.

2. Bakgrunn

I USA 11. september 2001 rammet terrorangrepet (heretter 9/11) som i ettertid kom til å endre den generelle oppfatningen om trusselbildet i verden. I Norge og mange andre land har dette bidratt til å sette fokus på faren for nye terrorangrep, krig og politisk ustabilitet (Aven, Boyesen, Njå, Olsen & Sandve, 2004: 23). Manglende beskyttelse blir ofte et fokus i etterkant av terrorangrep. Myndighetenes svar vil ofte være mer overvåking av befolkningen, for å kunne avverge eller være forberedt på det neste angrepet (Hausken, 2014: 33). Etter 9/11 ble det erklært krig mot terror, og det ble fremsatt et valg som stod mellom sikkerhet eller frihet. Idealet om garantert sikkerhet ble brukt for å rettferdiggjøre innføringen av en rekke tiltak, som blant annet dreide seg om mer omfattende overvåking (Lyon, 2003: 40). For Norge sin del ble det i etterkant av 9/11 gjennomført en rekke «terrorpakker» for å øke sikkerheten (Lysne II-utvalget, 2016: 67).

Vi kan også gå tilbake til 1996, da Lund-kommisjonen la frem en rapport om de hemmelige tjenestene i Norge. Rapporten kritiserte etterkrigstidens etterretningsarbeid som var preget av trusselen fra Sovjetunionen og faren for atomkrig. I sikkerhetens navn var individets rett til beskyttelse mot overgrep fra staten blitt nedprioritert. Den påfølgende politiske behandlingen samt Stortingets høring av rapporten, medførte store kontroverser. Blant annet førte det til at den daværende justisministeren måtte gå av, og personer som mistenkte at de ble overvåket fikk tilgang til «mappen sin» (Engen et al., 2016: 30). Lund-rapporten om de hemmelige tjenestene fikk senere noe av skylden for at gjerningspersonen som sto bak terrorangrepet 22. juli 2011 ikke ble oppdaget og stoppet i tide. Den daværende PST-sjefen hevdet blant annet at en mer velutrustet etterretningstjeneste kunne ha oppdaget og avverget angrepet. Lund-rapporten ble fremstilt som en av hovedårsakene til etterretningstjenestens «beskjedne» tilstand, fordi den hadde skapt frykt for å gjøre feil i sikkerhetsarbeidet (Engen et al., 2016: 30-31).

I 2013 kom de såkalte Snowden-avsløringene som, gjennom dokumentlekkasjer til media, viste en omfattende global masseovervåking. Avsløringene viste til det amerikanske National Security Agency (NSA) og deres hittil hemmelige og massive overvåking av vanlige borgere og deres private informasjon. I tillegg viste avsløringene hvordan myndigheter, selskaper og organisasjoner, som for eksempel Microsoft og andre hverdagslige kilder som Facebook,

Twitter, Google, og GPS signaler fra smarttelefoner, var innblandet eller ble brukt i overvåkingen som fant sted også utenfor de amerikanske grensene (Lyon, 2015: 1-4). I etterkant av avsløringene ble det også iverksatt gransking i regi av EU om elektronisk masseovervåkning av europeiske borgere. For Norge sin del dreide dette seg om problemstillinger knyttet til hvorvidt andre stater fikk tilgang til norske borgeres kommunikasjon, og da særlig gjennom den svenske overvåkingsloven som gir Försvarets radioanstalt (FRA) tilgang til store mengder datatrafikk som krysser den svenske riksgrensen. Det meste av datatrafikken mellom Norge og utlandet går via Sverige, som dermed kan overvåke den norske kommunikasjonen (Sveinbjørnsson, 2013).

I kjølvannet av blant annet 9/11 og terrorangrepene i London og Madrid, ble EU's datalagringsdirektiv (DLD) utviklet, som en del av arbeidet med terrorforebygging (Hausken, Yazdani & Haagensen, 2014: 110). Deklarasjonen om DLD fremhevet et behov for kollektive virkemidler for å bekjempe terror, og foreslo opprettelsen av et felles europeisk lovverk for lagring av elektronisk kommunikasjonsdata (Prop. 49 L (2010-2011: 11). Intensjonen bak DLD var å gi justismyndighetene verktøy for å avdekke, etterforske og straffeforfølge alvorlig kriminalitet (EU direktiv 2006/24/EF, 2006). I Norge ble direktivet vedtatt av Stortinget i 2011, men ble senere kjent ugyldig av EU-domstolen fordi det sto i strid med grunnleggende menneskerettigheter (Thon, 2014: 110-111). Behandlingen av DLD skapte stor politisk debatt her hjemme i Norge om temaer knyttet til spesielt overvåking, menneskerettigheter og kriminalitetsbekjempelse.

På mange måter har debatten omkring overvåking igjen blusset opp ettersom den politiske behandlingen om etablering av det norske DGF foregår for fullt. På mange måter kan DGF sies å være en slags etterkommer av DLD, hvor E-tjenesten nå søker tilgang til å overvåke all datatrafikk som krysser norskegrensen gjennom fiberkabler. Et interessant moment i forhold til forgjengeren DLD, var at dette ikke ville innebære lagring av kommunikasjonsinnhold (EU direktiv 2006/24/EF (2006): Artikkel 1 og 5) slik DGF ønsker å åpne for. I sin tid ble imidlertid DLD kjent ugyldig og strid med menneskerettighetene. Med dette utgangspunktet er det interessant å følge diskusjonen rundt DGF som tilsynelatende legger til rette for et større og bredere overvåkingspotensiale enn hva DLD tilsynelatende gjorde i sin tid.

Debatten om overvåking belyser hvordan det kan være en balansekunst å skulle ivareta de ulike, og i mange tilfeller motstridene, hensynene knyttet til samfunnssikkerhet. I følge David Lyon (2015) vil overvåking bidra til å begrense eller påvirke mulighetene og evnene til å kunne leve fritt i et demokratisk samfunn. Frykt for terrorisme kan imidlertid synes å øke aksepten overfor overvåking i samfunnet (Hammerlin, 2009: 71). Overvåking bidrar til å reise viktige politiske og etiske spørsmål. Og det er viktig å vite om selve overvåkingen, hva det er, hvem som praktiserer den, hvorfor, og hvilken påvirkning det har overfor måten vi lever på (Lyon, 2015: VIII).

3. Teori

I dette kapittelet presenteres studiens teoretiske forankring som er knyttet til overordnede tema om samfunnssikkerhet, risikostyring og overvåking.

3.1 Samfunnssikkerhet

Samfunnssikkerhet er et relativt nytt begrep som har utviklet røtter til både sosiale, politiske, økonomiske, kulturelle, organisatoriske og teknologiske aspekter. Begrepet sammensatt og grensene mellom de ulike elementene som inngår i begrepet er flytende og kan være vanskelige å avgrense (Engen et al., 2016: 53-54). Hvordan man ser på samfunnssikkerhet vil kunne variere alt etter for eksempel ståsted, arbeid eller faglig bakgrunn. I Norge er samfunnssikkerhet relevant for utforming av viktige samfunnsinstitusjoner, og er samtidig en sentral del av politiske beslutninger og prioriteringer (Engen et al., 2016: 25-27).

Samfunnssikkerhet vil i denne studien defineres som «samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare» (Samfunnssikkerhetsinstruksen, 2017). Hensynet til samfunnssikkerheten vil i mange tilfeller kunne virke styrende på politiske prioriteringer, samt bidra til å påvirke sentrale utviklingstrekk i samfunnet. Samfunnssikkerhetsbegrepet vil ofte rettes mot faktorer og trusler som på en eller annen måte kan føre til skade i samfunnet (Engen et al., 2016: 27). Selve hendelsene kan ha sitt opphav i naturlige faktorer, eller utløses gjennom tekniske eller menneskelig feil. I tillegg kan også hendelsene være et resultat av bevisste handlinger (Samfunnssikkerhetsinstruksen, 2017).

3.1.1 Statens sikkerhetsansvar

Mye av grunnlaget for en statsdannelse ligger i statens selvstendighet og evne til indre og ytre forsvar. På den måten inkluderes sikkerhetsbegrepet som en del av selve statens essens og er knyttet til både økonomisk vekst og kulturell utvikling. Dannelsen eller formuleringen av staters selvkontroll og definisjon for maktutøvelse inngår som en del av forståelsen av sikkerhetsbegrepet som videre har lagt flere premisser for samfunnssikkerhetsbegrepet. Særlig etter første verdenskrig har det nasjonale interessebegrepet vokst frem og blir i dag ofte brukt

som grunnlag for staters ekstraordinære sikkerhetstiltak. Et sentralt spørsmål har vært hvordan en stat kan øke sin egen sikkerhet uten at dette oppfattes som en trussel av andre. I den internasjonale politikken kan dette generere strukturelle sikkerhetsdilemmaer hvor trusselen på sikt eskaleres. På denne måten henger både statens ansvar og nasjonale interesser sammen med samfunnssikkerhetsbegrepet. Noe som blant annet kan illustreres gjennom konseptet og grunntanken bak totalforsvaret (Engen et al., 2016: 33). Totalforsvaret beskrives som alle de ulike sivile og militære tiltakene og ressursene som kan mobiliseres for å ivareta den nasjonale sikkerheten og forsvaret av landet (NOU 2006:6, 2006: 37).

Nasjonal Sikkerhetsmyndighet (NSM) opererer med fire ulike nivåer av sikkerhet. Det øverste nivået viser til statssikkerheten som handler om å ivareta statens eksistens, suverenitet og integritet gjennom beskyttelse av verdier som er sentrale for rikets sikkerhet og nasjonale interesser. Det neste underliggende nivået er samfunnssikkerheten som handler om ivaretakelse av borgernes liv, helse og trygghet. Dette handler også om å sikre sentrale samfunnsfunksjoner, kritisk infrastruktur, og andre samfunnsmessige interesser mot skade. Det tredje nivået viser til virksomheter i både offentlig og privat sektor hvor det foreligger behov for beskyttelse av drift og egne interesser. Det fjerde nivået omhandler enkeltindividet som også har behov for beskyttelse. De fire nivåene vil gjennom det digitale samfunnet ha mer eller mindre gjensidig avhengighet. For eksempel vil individers handlinger og adferd gjennom kommunikasjon over Internett ha betydning for både egen sikkerhet, men også samfunnssikkerheten (Nasjonal Sikkerhetsmyndighet, 2015: 9-10).

3.1.2 Rikets sikkerhet og nasjonale interesser

Rikets sikkerhet henger sammen med sikkerhetspolitiske forhold som blant annet er knyttet til nasjonal handlefrihet og territoriell integritet. I tillegg er begrepet aktuelt i forbindelse med scenarier som krig, sikkerhetspolitiske kriser og terrorisme. Nasjonale interesser kan også sies å være en del av begrepet rikets sikkerhet. Nasjonale interesser handler blant annet om forholdet til andre stater, samt ulike interesser knyttet til for eksempel infrastruktur, forsyning, kommunikasjon, helse eller samfunnsøkonomiske forhold. Dermed vil kritisk infrastruktur og kritiske samfunnsfunksjoner falle inn under begrepet nasjonale interesser. Sammen vil rikets sikkerhet og nasjonale interesser utgjøre samfunnets totale sikkerhetsinteresser. Hvilke

sikkerhetsinteresser dette er snakk om vil til enhver tid variere alt etter hvilke utfordringer Norge står overfor (NOU 2006:6, 2006: 34-35)

3.1.3 Samfunnssikkerhet og IKT

I utgangspunktet vil teknologier være sosiale, kulturelle og politiske produkt som formes gjennom måten de brukes på (Sejersted, 2002: 159). Norge har i større grad blitt avhengig av elektroniske kommunikasjonstjenester (ekomtjenester) for å opprettholde viktige funksjoner i samfunnet. Derav har sikringen av den fysiske og kritiske infrastrukturen som ivaretar de ulike samfunnsfunksjonene blitt en viktig prioritet for myndighetene (Nasjonal Kommunikasjonsmyndighet, 2015: 59, 61).

IKT- utviklingen har bidratt til å kople sammen det nasjonale og internasjonale samfunnet, hvor informasjons- og beslutningsprosesser er blitt raskere og mer effektive (Aven et al., 2004: 21). Teknologiske systemer har systemiske trekk som handler om hvordan systemets ulike deler samhandler og påvirker hverandre. Beskrivelser av denne dynamikken kan videre bidra til å forklare utviklingen av sårbarheter og uønskede hendelser. Ulike teorier kan vise til ulike organisatoriske eller samfunnsmessige begrensninger til å forutse eller arbeide med risiko og sikkerhet i teknologiske systemer (Engen et al., 2016: 150). IKT representerer ulike teknologier som i dag finnes omtrent overalt og som dermed har et stort og bredt nedslagsfelt (Sejersted, 2002: 160).

I teorien om risikosamfunnet fokuseres det på interaksjonen mellom komplisert teknologi, komplekse organisasjoner og individuelle handlinger. Samspillet mellom de ulike komponentene foregår i omgivelser som stadig endrer seg, samtidig som koplingene mellom dem kan være relativt tette og kompliserte. Samfunnet er også blitt mer avhengig av tilgang til IKT-tjenester både i forhold til produksjon og andre samfunnsaktiviteter. Utviklingen har bidratt til betydelig mer effektivitet, men på samme tid skapes det også nye sårbarheter i samfunnet. Kompleksiteten og dynamikken i samfunnet gjør at det blant annet kan være vanskelig å styre sikkerheten. I tillegg til at innvirkningen og konsekvensene være omfattende når det først går galt (Aven et al., 2004: 21-22).

3.1.4 Viktige samfunnsfunksjoner og kritisk infrastruktur

Opprettholdelse av samfunnets kritiske funksjoner er viktig for å ivareta samfunnssikkerheten (Samfunnssikkerhetsinstruksen, 2017). De kritiske funksjonene ivaretas gjennom kritisk infrastruktur. Den kritiske infrastrukturen vil være de ulike anlegg og systemer som anses som helt nødvendige for å opprettholde samfunnets kritiske funksjoner. Videre skal de kritiske funksjonene ivareta samfunnets grunnleggende behov, samt befolkningens trygghetsfølelse (NOU 2006:6, 2016: 32). De ulike samfunnsfunksjonene deles inn i tre ulike kategorier basert på hvordan de bidrar til å ivareta borgernes sikkerhet og trygghet. Den første handler om styringsevne og suverenitet hvor kriseledelse og forsvar inngår som sentrale funksjoner. Den neste handler om befolkningens sikkerhet som ivaretas gjennom ulike funksjoner i form av lov og orden, helse og omsorg, redningstjenestene, IKT-sikkerhet og natur og miljø. Den siste kategorien viser til samfunnets funksjonalitet gjennom forsyningsevne, vann og avløp, finansielle tjenester, kraftforsyning, elektroniske kommunikasjonstjenester, transportsektoren og satellittbaserte tjenester (DSB, 2016: 8-9).

Samfunnet er avhengig av funksjonaliteten til bestemte funksjoner for å kunne fungere, og viktige samfunnsfunksjoner kan forstås som selve bærebjelkene i samfunnet. På mange måter interagerer de ulike funksjonene med hverandre, hvorpå noen bestemte funksjoner sørger for at et stort antall andre funksjoner fungerer. En av disse funksjonene er IKT-systemene som mange andre samfunnsfunksjoner er avhengig av for å kunne fungere. Kraftforsyningen, banker, trafikksystemer, og redningstjenestene er eksempler på noen funksjoner som er avhengige av ulike IKT-systemer. IKT blir på mange måter et bindeledd mellom ulike samfunnsfunksjoner, og sørger for kommunikasjon og informasjonsutveksling mellom både mennesker og maskiner. Svikt i IKT- systemer kan føre til at et betydelig antall andre funksjoner også svikter eller får problemer med å fungere. I tillegg til at det kan oppstå feil i systemene, vil de også kunne være attraktive angrepsmål. Angrep kan komme fra kriminelle eller andre aktører med den hensikt å stjele, manipulere eller ødelegge dataene eller selve systemene. Slike ondsinnede handlinger vil potensielt sett kunne lamme viktige samfunnsfunksjoner via datasystemene (Aven et al., 2004: 23-24).

3.1.4.1 Samfunnsverdier

Ivaretakelse av sikkerheten og fokus på de ulike sårbarhetene knyttet til digitaliseringen og IKT-avhengigheten i samfunnet, er viktige faktorer for å opprettholde grunnleggende rettsstatlige og demokratiske verdier. I arbeidet med å redusere sårbarhetene og styrke samfunnssikkerheten, må de ulike tiltakene vurderes opp mot verdiene som ligger til grunn for det velfungerende demokratiske samfunnet. De ulike verdiene som samfunnet hviler på kommer blant annet til uttrykk gjennom både den nasjonale og internasjonale lovgivningen. I tillegg er det norske rettssystemet er basert på ulike rettsstatsprinsipper, hensyn til demokratiet og menneskerettigheter. Dette dreier seg blant annet om prinsipper eller verdier som rettssikkerhet, ytringsfrihet og personvernsprinsipper. De ulike verdiene bidrar til å regulere både fordelingen mellom statsmaktene i form av maktfordelingsprinsippet, samt forholdet mellom myndighetene og befolkningen (NOU 2015:13, 2015: 25).

3.2 Risikostyring

Det finnes ulike definisjoner av risiko, og det er vanlig å skille mellom et realistisk og konstruktivistisk perspektiv. Det realistiske perspektivet ser på risiko som et produkt av sannsynlighet og konsekvens, og bruker gjerne matematiske beregninger for å estimere risiko. Det konstruktivistiske synet handler om hvordan fremtiden tolkes og hvordan risiko forstås og oppleves. Her vil risiko kunne være noe som konstrueres i samspill mellom individer, grupper, organisasjoner eller institusjoner (Engen et al., 2016: 78-79).

Felles for de ulike synene på risiko er at risiko handler om noe som kan skje, og viser til forholdet mellom mulige handlinger og valgte handlinger (Engen et al., 2016: 79). Dermed handler risiko også om usikkerhet. Aven og Renn (2010) knytter risiko opp mot usikkerhet om og alvorligheten av hendelser, samt konsekvensene av en aktivitet i forhold til noe mennesker verdsetter (Aven & Renn, 2010: 3). Usikkerhet blir dermed et uttrykk for om hendelser blir realisert, hva som blir konsekvensene, og hvor alvorlig det er. Alvorlighetsgraden handler om hendelsens intensitet, utbredelse og omfang. Alvorligheten kan knyttes til forverring eller tap av noe mennesker verdsetter, eller det kan utrykkes kvantitativt gjennom for eksempel antall dødsfall eller økonomisk tap. Vurderingen av risiko

kan også være avhengig av hvilke verdier, holdninger og erfaringer som legges til grunn, samt alle de ulike usikkerhetsaspektene som gjør seg gjeldende. Risikostyring vil dreie seg om å beskrive og systematisere ulike aktiviteter og risikoforhold. Ved å beskrive risiko kan det lettere la seg gjøre å beregne eller vurdere risikoen med tanke på hvordan den eventuelt bør håndteres. Risikostyring handler dermed om hvordan samfunnssikkerhet forstås, og hvordan det er ønskelig at samfunnet organiseres (Engen et al., 2016: 79-82).

Et samfunn som på en eller annen måte konfronteres med trusler fra planlagte og ondsinnede handlinger vil ofte kunne tilrettelegge for politiske beslutninger som ville vært kontroversielle eller vanskelige å få gjennomslag for under normale omstendigheter. Slike trusler vil derfor i stor grad aktualisere politiske, etiske og manipulerende dimensjoner (Engen et al., 2016: 28). Ved å omdefinere et politisk problem til å handle om folks sikkerhet, kan det fort bli vanskelig å argumentere imot. Spørsmål knyttet til sikkerhet og risiko har dermed potensielt stor påvirkningskraft i samfunnet og politisk sett (Engen et al., 2016: 38-39).

I dagens samfunn blir mer informasjon og elektroniske spor etterlatt, samtidig som det etableres omfattende dataarkiver. Dette kan bidra til å legge potensiale for et såkalt overvåkingssamfunn. Spørsmålene videre blir således hvorvidt det finnes adekvate garantier eller muligheter for å styre de ulike kontrollmekanismene som overvåkingen representerer. Mer kompliserte og effektive kontrollteknologier vil gi større muligheter til de som representerer eller styrer systemet og strukturene som samfunnet inngår i. Representanter av systemet kan for eksempel være offentlige myndigheter eller ulike arbeidsgivere. Videre bidrar dette til å aktualisere spørsmålet om hvem som skal vokte vokterne. I forholdet mellom myndighetene og individet ligger en grunnleggende forutsetning for demokratiet. Hvorvidt myndighetene representerer individene og fellesskapet eller fremstår som en motpart med egeninteresser, vil utgjøre en demokratisk variabel med tanke på hvorvidt myndighetene oppfattes som en beskytter eller kontrollinstans. Dette er elementer som er sentrale med tanke på tillitten til det offentlige, samt stabiliteten i samfunnet (Sejersted, 2002: 167, 169-170).

3.3. Overvåking

Det engelske ordet for overvåking, *surveillance*, stammer fra det franske ordet *surveiller*, som direkte kan oversettes til *watch over* (Lyon, 2007: 14) eller *våke over* som dermed blir *overvåking* på norsk. I denne sammenheng vil det å våke over noen kunne relateres til et ønske om å beskytte eller skape trygghet. Ved å introdusere en eller annen form for overvåkingsteknologi for å uttrykke dette, skapes det samtidig et dilemma for når denne form for beskyttelse beveger seg over til å bli en uakseptabel form for kontroll (Lyon, 2007, 13-14). Selve fenomenet overvåking kan enkelt forklares som observasjoner som utføres for å innhente informasjon. Ved denne definisjonen vil overvåking favne om et bredt spekter av ulike metoder innenfor ulike fagfelt (Hausken, Yazdani & Haagensen, 2014: 16-17). Dette kan blant annet dreie seg om disipliner innen sosiologi, geografi, politisk vitenskap, økonomi og rettsvitenskap. De ulike overvåkingsmetodene er i dag stort sett teknologibasert (Lyon, 2007: 20-23), og overvåking er på mange måter en del av menneskets verden. Parallelt med overvåkingen reises samtidig en rekke viktige verdi- og samfunnsspørsmål som blant annet fordrer at det foretas etiske overveielser med tanke på blant annet overvåkingens utførelse, metode og formål (Lyon, 2007: 12, 14).

For at informasjonsinnhenting skal kunne karakteriseres som overvåking, vil det gjerne forutsette en relativt systematisk fremgangsmåte. I tillegg innebærer det en viss varighet og et relativt stort omfang. Sporadisk, tilfeldig og kortvarig informasjonsinnhenting vil derfor ikke falle inn under definisjonen av overvåking slik begrepet forstås i denne sammenheng (Schartum, 2010: 22). Definisjonen innebærer at overvåking følger bestemte protokoller og metoder, samt at den er tilsiktet (Lyon, 2007: 14). Det er derimot ikke et krav at informasjonen som innhentes blir brukt. Dermed vil overvåking også dreie seg om informasjon som lagres for å eventuelt kunne hentes frem ved behov (Shartum, 2010: 22). Videre karakteriseres overvåkingsbegrepet som en systematisk oppmerksomhet med fokus på informasjon eller personlige detaljer hvor hensikten er å styre, påvirke, kontrollere eller beskytte (Lyon, 2007: 14).

I denne oppgaven vil overvåkingsbegrepet forstås som innsamling av informasjon med formål om å forebygge eller verne samfunnet mot trusler som kriminalitet, terror eller andre former for angrep (Bing, 2010: 5) som for eksempel trusler gjennom spionasje og utenlandsk

etterretning. Videre vil overvåkingsbegrepet være knyttet til den lovlige overvåkingen som utføres av statlige organer med siktemål om å styrke den nasjonale sikkerheten (Bing, 2010: 5-6) og derav samfunnssikkerheten. Den statlige overvåkingen forstås som et fenomen som representerer ulike former for makt og kontroll, i tillegg til å være forbundet med beskyttelse og vern av samfunnet.

4. Metode

Formålet med denne avhandlingen har vært å undersøke hvordan DGF kan true samfunnssikkerheten. For å kunne svare på denne problemstillingen ble det i tillegg utviklet tre forskningsspørsmål som tar for seg DGF-systemets overvåkingskapasitet, kontrollmekanismene i systemet, og hvilke samfunnsverdier som kan påvirkes ved etablering av DGF. I det følgende kapittelet gjøres det rede for valg av metodisk fremgangsmåte, studiens datagrunnlag, reliabilitet og validitet, samt styrker og svakheter ved metoden.

4.1 Kvalitativt litteraturstudie

Det er vurdert som hensiktsmessig å bruke en kvalitativ fremgangsmåte for å kunne svare på oppgavens problemstilling om hvordan DGF kan true samfunnssikkerheten. Hensikten med studien er å kunne danne en forståelse av hva DGF innebærer og hvordan det kan påvirke samfunnet. I følge Aase og Fossaskåret (2014) handler kvalitativ metode om å studere fenomeners innhold og egenskaper for å kunne danne dypere forståelse og innsikt. En kvantitativ metode som vil være opptatt av utbredelse, mengde og omfang (Aase & Fossaskåret, 2014: 13) er derfor ikke vurdert som hensiktsmessig i denne sammenheng. Oppgavens formål er å si noe om *hvordan* DGF kan utgjøre en trussel mot samfunnssikkerheten, ikke hvor stort omfanget eller trusselen mot samfunnssikkerheten eventuelt er. Halvorsen (2008) forklarer videre at metode viser til de ulike verktøy som brukes for å studere virkeligheten på en systematisk måte gjennom informasjonsinnhenting og innsamling av data. Utgangspunktet for hvilke metoder som er egnet ligger i de spørsmål eller den problemstilling som skal besvares (Halvorsen, 2008: 20-21). Litteraturstudie ble valgt på bakgrunn av at det kan være utfordrende å innhente egne primærdata for å svare på den aktuelle problemstillingen (Jacobsen, 2015: 171). Problemstillingens karakter gjorde det hensiktsmessig å kunne foreta datainnsamling, tolkning og analyse av dataene parallelt. Dette er også noe som ifølge Halvorsen (2008) kjennetegnes av et kvalitativt studie som preges av et mer fleksibelt opplegg.

På noen områder kan det argumenteres for at studien også inneholder enkelte kvantitative elementer ved at den blant annet beskriver utbredelsen og omfanget av DGF, da særlig med tanke på overvåkingskapasiteten i systemet. Selv om hensikten med avhandlingen ikke er å

kvantifisere, så kan disse dataene si noe om utbredelsen og omfanget av DGF og trusselen det kan utgjøre for samfunnssikkerheten. På den måten vil de kvantitative dataene fungere som et supplement til de kvalitative dataene. Halvorsen (2008) peker på at en kombinasjon av kvalitativ og kvantitativ metode kan bidra til metodetriangulering, og dermed styrke studiens reliabilitet og validitet. Samtidig er ikke studiens fundament basert på kvantitativ metode, men de kvantitative elementene inkluderes for å kunne si noe kvalitativt om hvordan DGF kan true samfunnssikkerheten.

Videre ble litteraturstudie vurdert som en fordel fordi det allerede foreligger en offentlig utredningsrapport om DGF, samt at det foregår en politisk behandling hvor forslaget om å etablere DGF er sendt ut på høring. Høringsfristen var i januar 2017, og de ulike tilbakemeldingene er offentlig tilgjengelige. Fordelen med litteraturstudie er i denne sammenheng knyttet til at det kan være vanskelig å skulle utføre intervjuer eller ta i bruk andre metoder hvor tilgang på informanter eller informasjon kan være begrenset. Denne vurderingen baserer seg på at aktuelle informanter i for denne studien, som for eksempel E-tjenesten, Forsvarsdepartementet, regjeringen eller Stortinget, kan være utilgjengelige eller utfordrende å komme i kontakt og utføre intervjuer med. I tillegg er de ulike aktuelle kildene representert gjennom de offentlige rapportene og utredningene som brukes i studien. Dokumentene ble derfor vurdert som informative med tanke på at de kan argumenteres for å dekke de ulike aktuelle aktørenes synspunkter eller bidrag i den politiske behandlingen av DGF. I tillegg kan det argumenteres for at dokumentene har informativt innhold og detaljerte beskrivelser av DGF med tanke på at de også skal fungere som et politisk beslutningsgrunnlag i DGF-saken.

Det kvalitative litteraturstudiet hadde en induktiv tilnærming, hvor hensikten var å danne en helhetsforståelse av fenomenet som studeres. Den induktive fremgangsmåten innebærer også at fenomenet studeres uten klare forutsetninger og hypoteser. Det vil si at studiet har en relativt åpen tilnærming i å forstå virkeligheten eller det fenomenet som studeres, hvor hensikten er å danne en forståelse av de ulike aspektene ved fenomenet (Halvorsen, 2008: 128-129).

4.2 Datagrunnlag

Det ble vurdert som hensiktsmessig å ta utgangspunkt i hovedutredningen om DGF som er gitt av Lysne II-utvalget (2016). Denne vurderingen baserer seg på at den nevnte rapporten er sentral med tanke på at den fremlegger forslag om hvordan DGF anbefales å etableres. I tillegg er rapporten utformet med hensyn til at viktige problemstillinger skal kunne diskuteres i det offentlige rom. DGF faller inn under de hemmelige tjenestene og er under pågående politisk behandling, noe som kan indikere utfordringer for å få tilgang til nok datamateriale og ferdigbehandlet informasjon. Lysne II-utvalgets rapport (2016) er derfor en sentral kilde i denne oppgaven, fordi den utgjør selve forslaget til hvordan DGF eventuelt skal innrettes i Norge. Den inneholder også bakgrunnen for de ulike vurderingene og anbefalingene som blir skissert, gjennom at den diskuterer ulike problemstillinger som DGF aktualiserer. Videre er et utvalg av de tilhørende høringsuttalelsene angående grenseforsvaret brukt som kilder til hvordan innretningen kan påvirke samfunnet og derved også samfunnssikkerheten.

Grunnlaget for studiens analyse er med dette basert på ulike sekundære prosess- og forskningsdata gjennom institusjonelle- og offentlige kilder. Prosessdata viser til en type sekundærdata som dannes gjennom den løpende samfunnsaktiviteten i form av for eksempel forvaltningsdokumenter, stortingsdokumenter eller annen ubearbeidet informasjon via aviser og stortingsdebatter (Halvorsen, 2008: 114-115). Utvalget er formålsorientert og basert på tilgjengelighet, hvorpå relevante offentlige utredninger, faglitteratur, og tidligere forskning er en del av datagrunnlaget for avhandlingen (Jacobsen, 2015: 194-195).

4.3 Validitet og reliabilitet

Metoden som anvendes kan få betydning for analysen og resultatenes validitet og reliabilitet. (Halvorsen, 2008: 72). Denne studien er basert på et kvalitativt litteraturstudie hvor ulike dokumenter og rapporter utgjør fundamentet som oppgavens analyser hviler på. Derfor har det vært viktig å finne frem til, og plukke ut den litteratur og de dokumenter som oppfattes som både pålitelige og sentrale for å kunne svare på problemstillingen.

4.3.1 Validitet

Validitet viser til gyldighet, og handler om i hvilken grad dataene som brukes er relevante for å gi svar på problemstillingen. Validiteten for denne studien vil være et resultat av subjektive vurderinger og argumentasjon for hvorfor dataene bidrar til å svare på problemstillingen (Halvorsen, 2008: 67, 72). Dette vil grovt sett dreie seg om hvorvidt overvåking kan sies å utgjøre en trussel mot samfunnssikkerheten. Validiteten gjør seg også gjeldende i lys av forskningsspørsmålene, og hvordan disse er relevante og kan bidra til å svare på problemstillingen. Forskningsspørsmålene handler om hva som kan overvåkes gjennom DGF-systemet, kontrollmekanismene som er tenkt implementert, samt aktuelle samfunnsfunksjoner og verdier som berøres ved etablering av DGF. Spørsmålet om validitet handler således om de ulike forskningsspørsmålene er egnet til å gi relevante indikatorer på trusler mot samfunnssikkerheten. Det argumenteres for at overvåkingskapasiteten, kontrollmekanismene, og de ulike funksjonene og verdiene vil kunne ha betydning for samfunnssikkerheten, fordi det berører viktige elementer av fundamentet som samfunnssikkerhet hviler på ut fra den begrepsdefinisjonen som er gitt i teorikapittelet.

Et sentralt moment for validiteten i denne studien hviler dermed på innholdsvaliditeten eller den definisjonsmessige validiteten. Dette handler om hvorvidt det er samsvar mellom begrepene som brukes i det teoretiske og videre i det empiriske datamaterialet. Grunnlaget for denne validiteten henger sammen med den teoretiske operasjonaliseringen som er foretatt, samt den argumentasjonen som ligger til grunn for de ulike vurderinger og valg som er gjort for å besvare problemstillingen (Halvorsen, 2008: 67-68). For eksempel vil dette handle om hvor godt egnet overvåkingskapasiteten i DGF er til å gi et valid uttrykk for om DGF kan true samfunnssikkerheten. Ifølge Halvorsen (2008) vil den interne validiteten kunne ivaretas gjennom troverdig og saklig argumentasjon, samt gjennom samsvar mellom problemstilling, teori og analyse (67-70).

Gjennom forskningsopplegget i dette kvalitative studiet kan det være vanskelig å ivareta den eksterne validiteten i form av statistisk generaliserbarhet. I denne sammenhengen vil det være mer fornuftig å vise til en empirisk generaliserbarhet, hvor resultatene av studien kan ha en overførbarhet til andre tilsvarende miljø eller saker. Formålet er primært å bidra med kunnskap som går i dybden på det bestemte temaet, men samtidig kan resultatene også ha en

overføringsverdi gjennom kunnskapsformidling som kan være relevant i andre sammenhenger (Halvorsen, 2008: 154, 164-165). For eksempel kan studien være overførbar til lignende saker som for eksempel omhandler overvåking, eller bidra med kunnskap som kan være relevant innen samfunnssikkerhetsfeltet.

4.3.2 Reliabilitet

Reliabilitet dreier seg om hvorvidt analysens resultater er troverdige og bekreftbare. Høy reliabilitet er en forutsetning for å sikre høy validitet. Reliabiliteten for studien er knyttet til den tilnærmingen, tolkningen og analysen som foretas. Troverdigheten sikres gjennom en bevissthet om at også personlige verdier kan påvirke prosessen (Halvorsen, 2008: 68, 72). Det betyr at egne personlige holdninger omkring DGF, overvåking og samfunnssikkerhet kan påvirke utformingen av oppgaven og analysenes resultater. Videre kan dette ha betydning for hvilken informasjon som vektlegges og hva som eventuelt utelates. Det er forsøkt å holde et relativt nøytralt forhold til DGF, og jeg har vært oppmerksom på egne holdninger og synspunkt gjennom hele prosessen. Egne personlige holdninger overfor DGF er ambivalente og vil derfor i utgangspunktet ikke dreie i en bestemt retning i form av hvorvidt DGF er ønskelig eller ikke. Samtidig kan det påstås at problemstillingens vinkling legger føringer for hva som vektlegges i analysen. I og med at det fokuseres på hvordan DGF kan true samfunnssikkerheten, vil gjerne oppmerksomheten kunne sies å rettes mot negative implikasjoner ved DGF. Dette inntrykket kan gjerne forsterkes i og med at det i liten grad gjøres vurderinger av hvordan DGF eventuelt kan styrke samfunnssikkerheten. Selv om avhandlingen ikke har til hensikt å tale for eller imot DGF, vil problemstillingen med dette kunne fremstå som noe forutinntatt. Derfor anses det som desto viktigere å poengtere avhandlingens formål, samt å utføre analysen og databehandlingen på nøytralt grunnlag. Reliabiliteten kan dermed sikres ved å redegjøre for hvordan problemstillingen kan virke førende for analysen, samt gjennom å være oppmerksom på dette gjennom analyseprosessen.

4.3.3 Kildebruk

Videre er det forsøkt å sikre gyldighet og troverdighet ved å anvende pålitelige kilder. Informasjonen og litteraturen som brukes er enten hentet gjennom offentlige dokumenter eller utgitt av anerkjente forfattere og bokforlag. For å finne frem til relevant informasjon er det benyttet søkefunksjoner på UiS-bibliotekets-, regjeringens-, og stortingets nettsider, samt

gjennomgang av aktuelle artikler som er publisert i ulike aviser. Selv om kildene vurderes som relativt pålitelige, vil sekundærkilder ifølge Halvorsen (2008) kunne være preget hvordan disse dataene ble utformet i utgangspunktet. Dermed har det vært viktig å vurdere kildene både med tanke på opphav og i forhold til hvilken sammenheng eller arena de ulike kildebidragene opprinnelig var ment for.

Den teoretiske delen har tatt utgangspunkt i faglitteratur knyttet til samfunnssikkerhet, samt offentlige utredninger som omhandler samfunnssikkerhetsaspekter i tilknytning til overvåking. Faglitteraturen er først vurdert ut fra relevans for problemstillingen, og deretter med tanke på troverdighet gjennom å vurdere forlag og eventuelt forfatterens bakgrunn og kompetanse. Dette bidrar til å underbygge studiens kredibilitet og faglige forankring.

Den empiriske delen har tatt utgangspunkt i offentlig tilgjengelige dokumenter knyttet til DGF. Et sentralt spørsmål i den forbindelse var hvorvidt all aktuell informasjon om DGF faktisk er offentlig tilgjengelig eller om det også foreligger gradert informasjon som kunne vært aktuell. Ifølge forsvarsminister Ine Eriksen Søreide (se Regjeringen.no1, 2016) har utredningen av DGF og den påfølgende høringen bevisst blitt utformet for å kunne offentliggjøres i sin helhet. Samtidig kan det stilles spørsmål om det finnes eventuelle begrensninger ved selve utredningen i og med at den ble utformet nettopp med tanke på at den skulle ut i offentligheten. Dermed kan det tenkes at det finnes tema eller informasjon som ikke er inkludert i utredningen fordi det berører gradert materiale eller informasjon som er unntatt offentligheten. Det fremkommer av Lysne II-utvalgets rapport (2016) at deler av DGF-systemet er hemmelig og dermed ikke har vært mulig å gjøre rede for i den offentlige debatten. Dette dreier seg blant annet om E-tjenestens kapasiteter, eksempelvis innen feltet kryptering, som i forbindelse med denne avhandlingen kunne vært aktuell eller av betydning for analysen. Søreide (se Regjeringen.no1, 2016) peker på at utredningens offentliggjøring har vært et viktig element for å fordre en bred og offentlig debatt om DGF for å danne et legitimt og solid vurderingsgrunnlag for en eventuell innføring a DGF. Med dette kan det argumenteres for at utredningen om DGF er troverdig og relevant litteratur for å belyse DGF og gi innsikt i studiens problemstilling. Ut fra den foreliggende offentlige informasjonen om DGF som er anvendt i studien, knyttet opp mot de teoretiske perspektivene om samfunnssikkerhet, forsøkes det å svare på problemstillingen om hvordan DGF kan true samfunnssikkerheten.

Videre er samtlige forfattere og utgivere vurdert med tanke på akademisk faglighet, for å sikre troverdighet. Nettsidene som benyttes er for det meste hentet fra regjeringen og offentlige utregninger som er publisert på nett. Avisartikler vil ikke nødvendigvis ha samme krav til akademisk forankring, og av den grunn er ikke avisartikler benyttet i særlig grad. De ulike avisartiklene som er lest i forbindelse med denne studien har derfor blitt brukt som utgangspunkt for å finne relevant offentlig informasjon. Det vil si at det offentlige materialet som avisartiklene eventuelt er basert på er brukt i stedet for selve avisartikkelen. De utvalgte avisartiklene som eventuelt brukes er vurdert med tanke på omdømme og kredibilitet, slik som for eksempel Aftenposten som kan anses for å være et velrenommert og seriøst mediehus.

4.4 Styrker og svakheter ved metoden

Ved kvalitativ forskning kan det gjerne sies at forskeren selv bidrar til å produsere data gjennom utvelgelse, fortolkning og analyse av ulike data. På den måten kan det hevdes at man som forsker ikke kan forholde seg helt nøytral eller utenforstående til det fenomenet det forskes på. Det vil som oftest, bevisst eller ubevist, foretas prioriteringer og vurderinger av forskeren som i neste omgang kan sies å være en form for produksjon av data. Hva som inkluderes i forskningen eller hvordan noe blir tolket er dermed også en del av forskningen. Forskeren bør være klar over sin egen rolle i forskningen, og samtidig være oppmerksom på de bevisste valgene som tas gjennom forskningsprosessen (Aase & Fossaskåret, 2014: 36-40). Samtidig kan det hevdes at en av fordelene ved litteraturstudie, er at dataene er utarbeidet uten noen form for innvirkning fra forskeren selv. Likevel kan det være flere aspekter ved forskerrollen som gjør seg gjeldende i denne studien. For det første kan egne holdninger knyttet til DGF og overvåking ha innvirkning på studiens retning og hva som inkluderes eller ekskluderes av informasjon. I den forbindelse kan det være relevant å nevne at min interesse knyttet til DGF og overvåking er generell og ikke forutinntatt av bestemte holdninger hverken for eller imot. Personlig har jeg ingen formening om DGF bør innføres eller ikke, og tenker at dette kan være et relativt nøytralt utgangspunkt for å studere et slikt tveegget tema.

For det andre kan det være verdt å nevne at studiens formål ikke er rettet mot å gi argumenter for eller mot, men snarere studere DGF opp mot samfunnssikkerhetsaspekter. Hvilke aspekter ved samfunnssikkerhet som inkluderes i studien kan derimot avhenge av hvordan jeg som forsker har forstått og tolket både samfunnssikkerhet og DGF, både som fenomen og begrep. Ved å fokusere på hvordan DGF kan true samfunnssikkerheten, vil gjerne analysen kunne sies å være forutinntatt i den forstand at det fokuseres på negative eller problematiske sider ved DGF. Derfor er det viktig å påpeke at formålet med avhandlingen ikke er å vurdere fordeler og ulemper ved DGF, men undersøke hvordan DGF kan true samfunnssikkerheten. En svakhet med litteraturstudiet slik det fremkommer i denne avhandlingen kan derfor være at det mangler klare «motstemmer», eller argumenter og forskning, som eventuelt kan si noe om hvordan DGF kan virke positivt inn på samfunnssikkerheten. Dette har ikke vært fokus for denne studien, som dermed kan fremstå som noe ensidig. Samtidig er det begrunnet og forklart hvorfor studiet er organisert på denne måten, slik at det fremstår som klart overfor leseren hva som er formålet med avhandlingen.

En av styrkene ved bruk av kvalitativt metode er fleksibiliteten i undersøkelsesopplegget, hvor datainnsamlingen og analysen kan foregå parallelt (Halvorsen, 2008: 131). Dette bidro til at aktuelle dokumenter som dukket opp underveis kunne inkluderes og brukes i analysen. I tillegg la dette opp til at analysen kunne foregå kontinuerlig og samtidig som det ble arbeidet med teoretiske aspekter og empiriske funn. Samtidig kan et slikt opplegg ifølge Jacobsen (2015) føre til utfordringer knyttet til å begrense og avslutte undersøkelsen, fordi det stadig dukker opp ny og relevant informasjon. Dette viste seg spesielt i forhold til overvåkingstemaet generelt, hvor det finnes betydelige mengder spennende og aktuell informasjon. Likevel var fokuset rettet mot DGF som er et relativt nytt fenomen i Norsk sammenheng, og derfor har begrenset med forskning som konkret retter seg mot en slik innretning. Tilgang på relevant informasjon, som var en forutsetning for å kunne gjennomføre denne studien, var også noe som ble vurdert tidlig i prosjektet. Spesielt med tanke på om relevant og avgjørende informasjon angående DGF var offentlig tilgjengelig. Etter gjennomgang av Lysne II-utvalgets rapport (2016), samt regjeringens informasjon tilknyttet DGF, ble prosjektet betraktet som gjennomførbart.

En utfordring ved utformingen av oppgaven var å ta avgrensende beslutninger, og da spesielt knyttet til den empiriske og analytiske delen som handler om hvilke samfunnsfunksjoner og

verdier som kan påvirkes gjennom DGF. Utfordringen ligger blant annet i at det er mange verdier og flere av de ulike menneskerettighetene som kan være relevante, og ikke minst spennende, å drøfte i forbindelse med temaet overvåking og DGF. Likevel var det nødvendig å gjøre noen avgrensninger og fokusere på de momentene som ble ansett for å ha størst relevans for å besvare oppgavens forskningsspørsmål og problemstilling. De ulike verdiene og samfunnsfunksjonene som er vektlagt i oppgaven er personvern, rettssikkerhet og tillitt. I tillegg koples andre momenter inn, slik som for eksempel ytringsfrihet og retten til privatliv. De tre hovedmomentene ble valgt ut på bakgrunn av at de står som sentrale prinsipper i beskrivelsen av det norske demokratiet, samt at de i særlig grad kan sies å påvirkes gjennom de ulike aspektene som overvåking representerer. Det argumenteres også for at personvern, rettssikkerhet og tillitt kan knyttes opp mot samfunnssikkerheten. På bakgrunn av dette ble avgrensingen vurdert som hensiktsmessig både med tanke på oppgavens begrensinger i forhold til omfang, samt at de vurderes som dekkende for å kunne gi innsikt og svar på problemstillingen.

5. Empiri

I dette kapittelet presenteres studiens empiriske funn. Først vil det gis noen generelle forklaringer knyttet til E-tjenesten, for å blant annet kunne sette DGF i kontekst. Innledningsvis vil det også gis en presentasjon av DGF, hva det er, og hva som er formålet. Deretter vil det empiriske materialet knyttet til de tre forskningsspørsmålene legges frem. Først ut er spørsmålet knyttet til hva som kan overvåkes gjennom DGF, og deretter hvilke kontrollmekanismer som er tenkt implementert i systemet. Tilslutt presenteres funn knyttet til hvilke samfunnsfunksjoner og verdier som kan påvirkes gjennom DGF.

5.1 Etterretningstjenesten

E-tjenesten er Norges eneste sivile og militære etterretningstjeneste rettet mot utlandet. Det fremste samfunnsansvaret til E-tjenesten er å innhente informasjon knyttet til fremmede stater, organisasjoner eller individer som har relevans ovenfor norske interesser. E-tjenestens oppdrag går ut på å varsle om trusler mot Norge og norske interesser. Hva som blir definert som nasjonale interesser vil variere i tråd med trusselbildet og de ulike sikkerhetsutfordringene Norge står overfor til enhver tid. Fokuset retter seg mot utenlandsk aktivitet, hvorpå informasjon brukes for å understøtte utenriks-, sikkerhets- og forsvarspolitisk beslutningstaking. Formålet er derved å bistå myndighetene i politiske beslutningsprosesser. Videre skal E-tjenesten støtte Forsvarets operasjoner både hjemme i Norge og i utlandet. (Lysne II-utvalget, 2016: 5-15).

5.1.1 Styring og kontroll av E-tjenesten

Det er forsvarsministeren som har det parlamentariske og konstitusjonelle ansvaret for E-tjenestens virksomhet. Forsvarsministeren kan utøve direkte kontroll og styring av E-tjenesten, eller gå via Forsvarssjefen. Videre har forsvarsdepartementet en styringsfunksjon overfor E-tjenesten gjennom det årlige prioriteringsdokumentet. (Lysne II-utvalget, 2016: 18). E-loven regulerer E-tjenestens virksomhet og dens ulike oppgaver. Loven viser til de grunnleggende prinsipper og grenser som virksomheten må forholde seg til. Regjeringen har mulighet til å styre visse sider ved E-tjenestens arbeid i henhold til lovverket. Videre blir

loven utdypet gjennom den såkalte E-instruksen. E-tjenesten har gjennom reguleringer i E-instruksen en såkalt forleggelsesplikt overfor Forsvarsdepartementet. Denne tar blant annet for seg ulike etterretningsoperasjoner, iverksetting av nye tiltak eller kapasiteter, samt samarbeidsavtaler med andre utenlandske tjenester og organisasjoner. Forleggelsesplikten innebærer at disse sakene er underlagt politisk kontroll (Lysne II-utvalget, 2016: 14, 18).

Det er etablert flere ordninger for kontroll og styring av E-tjenesten som skal bidra til å sikre Stortinget, regjeringen og Riksrevisjonen innsikt i virksomheten. Stortingets kontrollutvalg for etterretnings- overvåkings- og sikkerhetstjeneste (EOS-utvalget) er det parlamentariske kontrollorganet som skal sørge for at E-tjenestens virksomhet overholder de fastlagte rammene. EOS-utvalget har åtte stortingsutnevnte medlemmer som rapporterer til Stortinget gjennom årsmeldinger eller ved behov. E-tjenesten har også egne interne kontrollfunksjoner og reguleringstiltak som skal sikre lovlig drift av virksomheten. Blant annet er det etablert et system for avviksrapportering som også blir lagt frem for EOS-utvalget. Videre orienteres Stortinget gjennom en såkalt «årlig orientering for Stortingets president» hvor Utenriks- og forsvarskomiteens leder og nestleder, samt riksrevisoren deltar. I tillegg blir E-tjenestens budsjetter, planer, personellrammer og regnskap gjennomgått og kontrollert av Koordineringsutvalget for Etterretningstjenesten (K-utvalget) (Lysne II-utvalget, 2016: 18-19).

5.1.2 E-tjenestens arbeid

Etterretning viser til ulike åpne eller fordekte metoder for systematisk innhenting og prosessering av informasjon rettet mot utlandet. Etterretningsvirksomhet har som formål å bidra til å skape forståelse og redusere usikkerhet. Aktiviteten og etterretningstjenestens arbeid skal foregå i henhold til statens legale rammer. E-tjenesten har hatt en økende etterspørsel etter etterretningsinformasjon- og vurderinger. Det har også vært en økende andel oppdragsgivere som søker kunnskap gjennom unik informasjon som i utgangspunktet er skjult. E-tjenestens aktualitet ligger i at Norge har fått en mer aktiv utenrikspolitikk som bidrar til å synliggjøre Norge i det globale bildet (Lysne II-utvalget, 2016: 13-14).

Alt arbeid som e-tjenesten foretar seg i forbindelse med innhenting og behandling av informasjon skal være formålsavgrenset. E-tjenestens oppgaver vil styres gjennom forsvarsdepartementets årlige prioriteringsdokument, samt gjennom det såkalte RFI-systemet (Request For Information) som ved behov vil kunne gi fortløpende oppdrag. Det vil si at det er de politiske myndighetene som legger føringer for hva som skal prioriteres, og på den måten vil ikke E-tjenesten drive etterretning på sine egne vegner (Lysne II-utvalget, 2016: 15).

E-tjenestens oppdrag går ikke ut på å drive straffeforfølgning og overvåking av nordmenn i Norge. Samtidig kan E-tjenesten behandle informasjon om fysiske eller juridiske norske personer dersom det er relevant og formålstjenlig. Dette til tross for at E-tjenesten ikke har lov til å drive fordekt innhenting av informasjon angående norske personer på norsk territorium. Denne begrensningen er knyttet til arbeidsfordelingen mellom E-tjenesten og politiet, for å skape klare skiller mellom hvor de ulike tjenestene opererer. Grensene mellom E-tjenesten og Politiets sikkerhetstjeneste (PST) sitt arbeid kan derimot fremstå som mer uklar, og reguleres blant annet gjennom e-instruksen. I henhold til e-instruksen kan E-tjenesten, etter godkjenning fra PST, drive informasjonsinnhenting om norske fysiske eller juridiske personer. Slike tilfeller vil være knyttet til fremmed etterretningsvirksomhet som foregår i Norge og som utøves av norske personer. E-tjenestens faste praksis er å begrense den fordekte informasjonsinnhentingen i Norge til å gjelde i de tilfeller hvor det foregår fremmed etterretning som utøves på vegne av en fremmed makt. Denne praksisen henger sammen med at PST oppfatter det som sin oppgave å skulle drive etterretning mot utenlandske borgere i Norge. I tillegg til at tjenestenes virksomhet og ansvarsområder vil overlappe dersom både PST og E-tjenesten arbeider parallelt (Lysne II-utvalget, 2016: 5, 14-16).

5.1.3 Vilkår for informasjonsinnhenting

Etterretningstjenesten har fire ulike rangerte vilkår for innhenting av informasjon. Det første vilkåret er knyttet til et formål om målutvikling og er selve fundamentet for all etterretningsvirksomhet. Målutviklingsformålet handler om å drive bred etterretning som innebærer å lete etter ukjent informasjon som kan være av interesse. Dette kan gå ut på å finne nye trusselaktører eller innhente mer informasjon om aktuelle mål som allerede er kjent. Den eneste terskelen for å starte målutvikling, er at det må foreligge et legitimt etterretningsbehov

som er i tråd med E-tjenestens oppdrag. Selve arbeidsmetoden er vanligvis basert på historiske data gjennom ulike inngangsparameter. Et eksempel på et inngangsparameter kan være avsløringen av en terrorist og oppnøsting av ulike tilknyttede linker som telefonnummer, eposter, nettverk eller andre ledetråder (Lysne II-utvalget, 2016: 19-20).

Det neste vilkåret for informasjonsinnhentingen dreier seg om at det skal være en rimelig grunn til å undersøke. Etter at målutviklingen for eksempel har pekt ut et antatt interesseområde, vil terskelen for å hente ut informasjon være noe høyere. Det skal foreligge rimelig grunn til å undersøke nærmere om målet kan generere relevant informasjon for utenlandsetterretningen. Det skal for eksempel være objektive og etterprøvbare argumenter for å starte innsamling av data om en bestemt person (Lysne II-utvalget, 2016: 20).

Andre potensielle vilkår vil kunne være såkalt «skjellig grunn til mistanke» eller «bevist utover enhver rimelig tvil» for å kunne innhente informasjon. I og med at E-tjenesten ofte arbeider på grunnlag av usikker informasjon, vil ikke disse to vilkårene være aktuelle for deres etterretningsvirksomhet. Grunnen til dette ligger i at det vil være vanskelig for E-tjenesten å løse sine oppgaver dersom det stilles for høye krav til vilkårene eller «bevisføringen» for å drive etterretningen (Lysne II-utvalget, 2016: 20).

5.2 Digitalt grenseforsvar

Digitalt grenseforsvar (DGF) forstås som en innretning eller virksomhet som vil kunne gi E-tjenesten innsyn og tilgang til digitale datastrømmer som krysser norskegrensen gjennom land- eller sjøbaserte fiberoptiske kabler. Informasjonen som innhentes og analyseres skal være relevant for utenlandsetterretningen, hvor hensikten er kartlegging og bekjempelse av ytre trusler mot rikets sikkerhet, selvstendighet og nasjonale interesser (Lysne II-utvalget, 2016: 5, 10)

5.2.1 Formålet med DGF

Det er flere utviklingstrekk som aktualiserer DGF som et etterretningsmessig virkemiddel. For det første vises det til et endret trusselbilde, hvor cybertrusler mot Norge øker både i mengde og kompleksitet. I tillegg er det økt trussel fra internasjonal terrorisme hvor terrorvirksomhet i økende grad koordineres gjennom nettbaserte kanaler på tvers av landegrenser. Videre har teknologiutviklingen dreiet, hvor tradisjonelle kommunikasjonskanaler har blitt erstattet med nye kanaler som går via Internett. Det overordnede formålet med DGF er å sikre E-tjenesten tilgang til relevant etterretningsinformasjon i takt med den teknologiske utviklingen. E-tjenesten behøver tilgang til kommunikasjonskanaler hvor relevant informasjon genereres, for å imøtekomme sikkerhetspolitiske hensyn gjennom kartlegging, varsling og motvirkning av alvorlige trusler (Lysne II-utvalget, 2016: 5, 10).

Ved å inkludere forsvarsbegrepet i DGF vises det til at innretningen skal fungere som et førstelinjeforsvar, hvor det innhentes kunnskap og informasjon om de mest prekære trusler, for å kunne motvirke at de eventuelt materialiseres (Lysne II-utvalget, 2016: 10). Trusselbildet er komplekst og under stadig endring. De alvorligste trusler mot rikets sikkerhet og selvstendighet er nærmest utelukkende knyttet til utlandet og utenlandske forbindelser. Ulike trusselaktører kommuniserer over landegrenser, og har gjennom utvikling av avanserte IKT-verktøy fått evne til å ramme norske interesser på nye måter. Trusselaktørene anvender elektroniske kommunikasjonskanaler til blant annet formidling eller rapportering om oppdrag og planer, samt rekruttering, radikalisering og innhenting av informasjon om aktuelle mål. I tillegg antas det at ytre trusler slik som cyberangrep, digital spionasje, terror og spredning av masseødeleggelsesvåpen vil intensiveres i tiden fremover. I den forbindelse vil det være avgjørende for norske myndigheter å ha kunnskap om den informasjonen som strømmer gjennom det globale kommunikasjonsnettet. Det argumenteres for at DGF vil kunne være et viktig verktøy for å bedre etterretningskapasiteten og effektivisere myndighetenes responsevne (Lysne II-utvalget, 2016: 11).

5.3 Hva kan overvåkes gjennom DGF?

Det skilles gjerne mellom to typer metoder for overvåking innen etterretningsfeltet. Den ene kalles for «HUMINT» som dreier seg om menneskelig etterretning (human intelligence), mens den andre kalles for «SIGINT» som viser til signaletterretning (signal intelligence). Det digitaliserte samfunnet har ført til at SIGINT-basert overvåking er blitt en mer aktuell og relevant metode. SIGINT er mindre ressurskrevende enn HUMINT, og kan overvåke og tappe informasjon fra fiberoptiske kabler som for eksempel internettaktivitet, mobilbruk, og kommunikasjon gjennom e-post. Dette legger til rette for en bred overvåking hvor kvantitet og tilgang på data ikke lenger er en utfordring. Datamaskiner kan settes til å utføre grovarbeidet gjennom prosessering av enorme mengder data, for å søke etter koplinger og sammenhenger (Hammerlin, 2014: 75-76). På mange måter har mulighetene i bruken av metadata bidratt til endringer for hvordan etterretningsarbeidet foregår. Fremgangsmåten for informasjonskartlegging handler ikke lenger om å ta utgangspunkt i mistenkelige personer som deretter kartlegges gjennom ulike etterretningsmetoder som for eksempel telefonavlytting. I dag kan de enorme mengdene data som samles inn brukes til å finne mønster eller korrelasjoner som i neste omgang kan avdekke mistenkelige forhold (Datatilsynet, 2013: 23). Den stadige utviklingen av IKT bidrar på flere måter til å øke mulighetene for overvåking. I tillegg er overvåking gjennom IKT-baserte metoder ofte å foretrekke da maskinell og automatisert innsamling av data er relativt effektiv, samt mindre tid- og ressurskrevende enn andre metoder som for eksempel spaning (Schartum, 2010: 21).

Innsamling av data gjennom DGF vil foregå etter såkalt bulk-innhenting eller bulk-aksess. Det vil si at E-tjenesten samler inn eller gis tilgang til store mengder data (metadata) før de kan påbegynne målrettet arbeidet for å selektere og hente ut relevant informasjon fra den større datamengden. Dette innebærer at den totale datamengden som samles inn også vil inneholde betydelige menger med informasjon som ikke er relevant for formålet knyttet til utenlandsetterretningen. I neste omgang skal E-tjenesten kunne hente ut selve innholdet i kommunikasjonen som krysser grensen gjennom de fiberoptiske kablene. Innhentingen av innholdet vil derimot ikke foregå i bulk, men etter målrettet arbeid. Samtidig vil det kunne samles inn metadata innenfor bestemte kommunikasjonslinker som velges ut. Dermed innebærer dette også innsamling av store mengder informasjon om kommunikasjon som er irrelevant for E-tjenesten (Lysne II-utvalget, 2016: 10). Ifølge Søreide (2017) flyter omtrent 99 prosent av all kommunikasjon inn og ut av Norge gjennom de fiberoptiske kablene.

Kommunikasjonsbegrepet viser til kommunikasjon som overføres gjennom et signalsystem via nett og tjenester. Det omfatter kommunikasjon som foregår mellom to eller flere parter, samt ensidig kommunikasjon som for eksempel overføring av lyd, tekst, bilder eller andre data. Argumentet for innsamling av ensidig kommunikasjon henger sammen med faren for cyberangrep som ikke er avhengig av gjensidig kommunikasjon mellom to eller flere parter. DGF vil ikke gjelde for innhenting av lagrede data, som for eksempel data som lagres i skyen. (Lysne II-utvalget, 2016: 10).

Norske borgere vil etterlate seg store mengder digitale spor og informasjon som vil fanges opp av DGF-systemet. Norge blir i liten grad brukt som transittland for kommunikasjon. Det vil si at mesteparten av kommunikasjonen som krysser landegrensen i de fiberoptiske kablene vil ha minst en avsender eller mottaker i Norge. Informasjon som vil krysse landegrensen og dermed omfattes av DGF-systemet, vil dreie seg om telefonsamtaler, meldinger og e-poster som konkret sendes mellom Norge og utlandet. I tillegg vil svært mye av det man foretar seg på nettet krysse landegrensen, blant annet fordi de fleste nettjenester er eid og drevet av utenlandske aktører. Dette vil for eksempel dreie seg om de vanligste søketjenester og sosiale media. Videre vil flere av kommunikasjonstjenestene være utformet på en slik måte at informasjon om kommunikasjonen mellom to parter som begge befinner seg i Norge, kan gå ut og inn via de fiberoptiske kablene som krysser landegrensen. Dette vil blant annet dreie seg om bruk av e-post tjenester som har servere i utlandet, mobiltelefoni dersom en av partene benytter et annet abonnement enn Telenor sitt mobilnett, eller andre kommunikasjonstjenester som for eksempel Skype, WhatsApp eller Instagram for å nevne noen (Lysne II-utvalget, 2016: 48, 61).

5.3.1 Kryptering

Kryptering er en grunnleggende sikkerhetsfunksjon som legger til rette for å sikre informasjonens konfidensialitet. Flere lands etterretnings- og overvåkingstjenester gir uttrykk for økt tilgjengelighet og bruk av krypterte tjenester. I kjølvannet av Snowden-avsløringene er det blitt større oppmerksomhet knyttet til overvåkingsmulighetene ved bruk av IKT. Dette har ført til at mange som har et ønske eller behov for å skjule sin informasjon nå gjør det, fordi de er klar over at de kan bli sett (Lysne II-utvalget, 2016: 26-27). Et sentralt dilemma i

diskusjonen mellom kommunikasjonsvern og kriminalitetshensyn ligger i mulighetene for kryptering. Krypterte kommunikasjonstjenester vil på den ene siden ivareta hensynet til kommunikasjonsvernet, men på den andre siden kunne tilrettelegge for at kriminelle kan holde kommunikasjonen sin skjult (Nasjonal Kommunikasjonsmyndighet, 2015: 67).

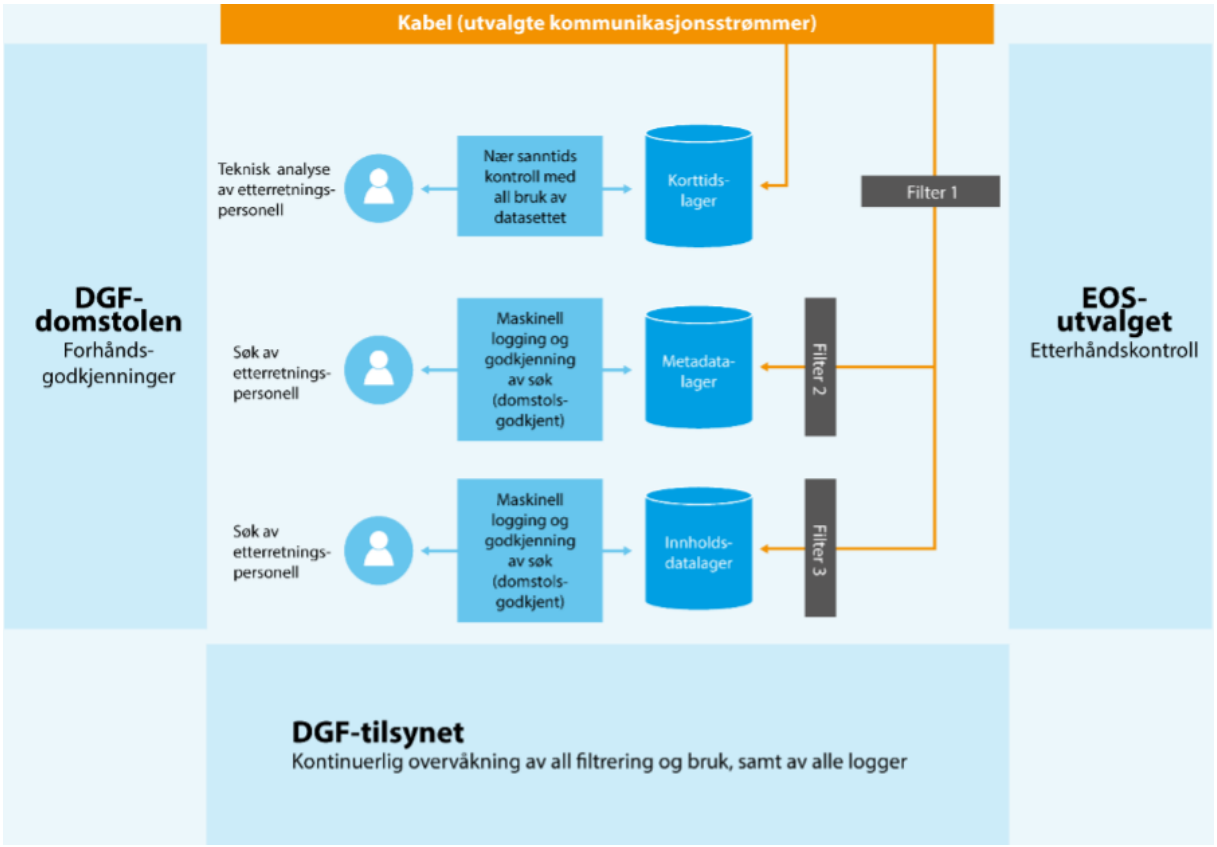
Det antas at bruken av kryptering, og sterk kryptering, vil øke i fremtiden som følge av utviklingen innen sikkerhetsteknologien. Graden av kryptering kan gjerne deles inn i to kategorier. Den første dreier seg om krypteringsmekanismer som man er klar over kan dekrypteres gjennom kjente og tilgjengelige metoder. Den andre viser til krypteringsmekanismer som det ikke finnes offentlig kjente metoder for å dekryptere. En eventuell forsering av slik kryptert informasjon vil kunne la seg gjøre ved bruk av krypteringsnøkler, eller ved å bruke datamaskiner for å forsøke å knekke koder.

5.4 Hvilke kontrollmekanismer er tenkt implementert ved etablering av DGF?

Gjennom et teknologisk vern kan det legges til rette for at overvåkingen kontrolleres gjennom å implementere IKT-løsninger for monitorering og automatisering av overvåkingsvirksomheten. Dette kan bidra til å øke tillitten til at overvåkingen foregår i henhold til de ulike lover og regler som er fastsatt. Monitoreringen vil for eksempel kunne foregå ved at kontroll- og tilsynsorganer gis tilgang til logger eller registreringer som gjøres i det elektroniske informasjonssystemet. På denne måten vil kontrollorganet kunne monitorere og bli varslet om bruken av overvåkingssystemet (Schartum, 2010: 32) som i dette tilfellet anvendes av E-tjenesten. Det teknologiske vernet gjennom automatisering viser til selve programmeringen av datasystemet. Det vil si at overvåkingssystemet vil følge de ulike fastsatte regler gjennom implementere begrensninger og regler. Systembegrensningene kan blant annet dreie seg om ulike muligheter for tilgang, og eventuelt videreformidling av informasjon. Det teknologiske vernet handler dermed om å bruke IKT for å kontrollere overvåkingsvirksomheten, samt å konstruere datasystemet med elektroniske begrensninger (Schartum, 2010: 32-33).

5.4.1 Kontrollmekanismer i DGF-systemet

Ulike problemstillinger knyttet til etableringen av DGF fordrer at det bør implementeres visse begrensninger ved systemet, og det er særlig to typer teknologiske begrensninger som er aktuelle. Den ene dreier seg om et filter som vil kunne begrense hvilke data som blir lagret. Den andre begrensningen er rettet mot hvordan og hvem som kan benytte dataene som lagres (Lysne II-utvalget, 2016: 50). Nedenfor følger en overordnet figur som viser hvordan datainnhenting og kontroll av DGF innretningen er tenkt gjennomført i henhold til Lysne II-utvalgets rapport (2016).



Figur 1: *Overordnet beskrivelse av DGF. Fra Lysne II-utvalgets rapport 2016, s. 53.*

Selve kontrollen av DGF vil foregå gjennom tre ulike mekanismer. Den første dreier seg om en DGF-domstol som skal kunne forhåndsgodkjenne enkelte bestemmelser over hva det kan gjøres søk på i metadatalageret, og hvilke innholdsdata som kan hentes ut. I tillegg skal domstolen kunne behandle prøving for enkeltsaker som faller utenfor forhåndsgodkjenningen,

og kontrollere at tilgang til data er i henhold til de fastsatte vilkår eller «beviskrav» (Lysne II-utvalget, 2016: 52, 57).

Den neste kontrollmekanismen handler om tilsyn med DGF. Dette vil innebære at de ulike elementene ved DGF som ikke faller inn under forhåndsgodkjenningen skal være under et kontinuerlig tilsyn som har tilgang til og fullt innsyn i DGF-systemet. Blant annet skal tilsynet motta informasjon om alle søk som foretas i DGF-systemet, hvilke filter og søkekriterier som benyttes, samt de ulike avgjørelsene tatt av DGF-domstolen. Tilsynet skal rapportere til EOS-utvalget, Forsvarsdepartementet og Samferdselsdepartementet, og i tillegg legge frem eventuelle avvik til EOS-utvalget. Tilsynet skal også kontrollere at datasikkerheten er så høy som teknologisk og praktisk mulig (Lysne II-utvalget, 2016: 52, 59).

Den siste kontrollmekanismen handler om EOS-utvalgets ansvar for å drive etterhåndskontroll ved bruken og E-tjenestens utøvelse av DGF. Dette skal foregå ved at utvalget mottar tilsynsrapporter, samt at de følger Forsvarsdepartementets styring av E-tjenesten. EOS-utvalget skal ha ubegrenset innsynsrett i DGF-systemet, og i tillegg ha et rapporteringsansvar overfor Stortinget (Lysne II-utvalget, 2016: 52, 59).

5.4.1.1 Datalager

Videre viser modellen (Figur 1) de ulike komponentene som inngår i DGF-systemet. Fra fiberkablene hentes det inn data som legges inn i korttidslageret. Her vil ufiltrert metadata og innholdsdata lagres i en to-ukers periode, for å kunne drive teknisk vedlikehold av de ulike filtrene som er i systemet. Dette lageret skal ikke benyttes til søk for etterretningsformål, men anses som helt sentral for å kunne oppdatere og sikre kvaliteten på filter 1 og 2. Kortidslageret bør reguleres gjennom sterke begrensninger, da både maskiner og mennesker vil måtte drive behandling av lageret. Det anbefales at kun et fåtall mennesker skal få tilgang til å operere i korttidslageret, hvorpå DGF-tilsynet skal kunne drive kontinuerlig kontroll for å etterse at retningslinjene følges. Videre skal EOS-utvalget kontinuerlig orienteres om eventuelle filteroppdateringer, samt hvordan korttidslageret blir benyttet (Lysne II-utvalget, 2016: 53-55).

I det neste lageret vil filtrert metadata fra utvalgte kommunikasjonsstrømmer bli lagret. I metadatalageret vil det kunne innhentes informasjon i tråd med de ulike forhåndsgodkjente parameterne, eller gjøres søk knyttet til personer etter godkjenning fra DGF-domstolen. Metadatalageret anses for å ville inneholde den største delen av systemets etterretningsmessige verdi. Her vil metadata foreslås å lagres med en begrensning på 18 måneder, for å kunne drive effektiv retrospektiv analyse av trafikkdataene. Samtidig er dette lageret utfordrende med tanke på at det vil være vanskelig å filtrere ut all den informasjon om kommunikasjon som ikke skal være der og som ikke dekkes av E-tjenestens formål. Derfor foreslås strenge kontroll- og tilsynsmekanismer, samt regulering eller begrensning av søk. Tanken er at det skal kunne føres maskinell godkjenning og logging for søk. Dersom etterretningspersonell skal gjøre søk i lageret vil det gå gjennom en sluse. Denne slusen skal loggføre både søket og resultatet av søket, for at det skal kunne være mulig å drive tilsyn. Videre skal slusen kunne foreta en maskinell kontroll av om søket er i overensstemmelse med lovverk, retningslinjer og i tråd med eventuelle rettsavgjørelser. De ulike rettsavgjørelsene må derfor oversettes til maskinelt definerte søkeprivilegier, og dersom søket ikke godkjennes vil det bli avvist. Søkeprivilegiene kan for eksempel dreie seg om konkrete personer eller visse handlingsmønster som det er lov å søke på. Søk etter handlingsmønster vil være aktuelt i forbindelse med målutvikling, og kan dreie seg om søk etter både kjente eller ukjente personer og handlingsmønster. Et kriteriet som foreslås er at minst én av disse må være kjent. Det vil si at det for eksempel kan søkes etter ukjente personer gjennom et kjent handlingsmønster, eller omvendt. Dette kan eksempelvis dreie seg om kjent utenlandsk etterretningspersonell, eller ulike typer kommunikasjonsformer som terrorister er kjent for å bruke (Lysne II-utvalget, 2016: 53-56).

I innholdsdatalageret oppbevares fullstendige datastrømmer om kommunikasjon etter godkjenning fra DGF-domstolen. Det innebærer at også innholdsdata skal lagres her. Kontrollering av søk som foretas er mest relevant for metadatalageret, og vil ikke være like relevant for hverken innholdsdatalageret eller korttidslageret. Det vil si at søkekriterier i innholdsdata- eller korttidslageret ikke behøver å være hjemlet i en rettsavgjørelse, men kontrolleres i henhold til de interne retningslinjene. Innholdsdatalageret anses for å være minst problematisk i lys av personvern- og menneskerettighetshensyn, fordi det kun vil inneholde kommunikasjonsstrømmer som er domstolgodkjent. DGF-tilsynet skal ha innsyn i rettsavgjørelsene og utformingen av filteret for å kunne kontrollere at lageret ikke inneholder

noe annet enn det som er godkjent. I tillegg skal tilsynet ha tilgang til søkeloggen, og rapportere til EOS-utvalget om bruken av lageret. Innholdsdata vil kun bli lagret så lenge det anses som nødvendig for å løse E-tjenestens oppgaver (Lysne II-utvalget, 2016: 53, 55, 57).

5.4.1.2 Filter

De ulike datalagrene vil være tilknyttet ulike filter som skal bidra til å regulere hvilke data som plukkes opp fra fiberkablene og lagres i DGF-systemet. Modellen overfor (Figur 1) viser at systemet er tiltenkt tre ulike filtre. Filter 1 skal redusere mengden data som kommer inn i systemet ved å velge ut hvilke kabler eller kommunikasjonsstrømmer eller -tjenester som til enhver tid blir fokusert på. Samtidig skal dette filteret luke ut all datatrafikk som enkelt vil kunne gjenkjennes for å være utenfor E-tjenestens oppdrag. En slik form for negativ filtrering vil derimot kunne innebære at nyutviklede kommunikasjonsformer vil slippe gjennom filteret. Filter 2 skal regulere dataene som kommer inn i metadatalageret. Her skal alt av innholdsdata, og så mye som mulig av metadata som ikke er relevant for E-tjenestens oppdrag, filtreres bort. Det vil ikke være teknisk reelt å kunne filtrere bort all irrelevant metadata, og metadatalageret vil derfor inneholde store mengder informasjon som ligger utenfor E-tjenestens virkeområde. En årsak til dette ligger i at det vil være utfordrende å definere eksakt hva som faller innenfor eller utenfor etterretningsoppdraget. For eksempel vil informasjon som i utgangspunktet ikke anses for å være relevant, kunne vise seg å være det i etterkant. I tillegg vil det være vanskelig å filtrere bort all kommunikasjon som foregår mellom fysisk norske personer. Filter 3 er knyttet til innholdsdatalageret og skal sørge for at det kun slippes gjennom innholdsdata som er godkjent av DGF-domstolen. Dette vil dreie seg om innholdsdata fra kommunikasjonsstrømmer knyttet til indikatorer eller personer som det er gitt lov til å søke etter. Denne typen filtrering vil kunne gjennomføres med god presisjon (Lysne II-utvalget, 2016: 53-54).

5.5 Hvilke samfunnsfunksjoner og verdier kan påvirkes ved etablering av DGF?

Globalt sett har Norge en svært høy grad av digitalisering i både privat og offentlig sektor (Lysne II-utvalget, 2016: 5-15), og den globale trafikken gjennom Internett vokser eksepsjonelt. Internett utgjør en grunnleggende samfunnsressurs som kan tilby vekst og

innovasjonsmuligheter innenfor de fleste samfunnsområder (Nasjonal Kommunikasjonsmyndighet, 2015: 39). Samfunnets digitalisering bidrar til å skape økt IKT-avhengighet for de ulike virksomhetene som understøtter grunnleggende nasjonale funksjoner (NOU 2016:19, 2016: 20). IKT-baserte teknologier har gjerne generelle bruksområder, men det er ikke teknologien i seg selv som begrenser mulighetene, men brukerne av teknologien. Gjennom kreative og alternative metoder kan teknologi brukes på helt andre måter enn det som egentlig er formålet (Engen et al., 2016, 384).

5.5.1 Samfunnsfunksjoner

Samfunnssikkerheten vil på mange måter påvirkes av de ulike sentrale infrastrukturene som ivaretar samfunnets kritiske funksjoner. I et samfunnssikkerhetsperspektiv vil dette handle om å sikre samfunnets grunnleggende behov og borgernes trygghetsfølelse (Samfunnssikkerhetsinstruksen, 2017, NOU 2006:6, 2016: 32). For å identifisere hva som anses for å være samfunnets kritiske infrastrukturer og samfunnsfunksjoner er det utarbeidet noen retningslinjer. Retningslinjene skal bidra til å belyse hvilke kritiske infrastrukturer som er nødvendige for å kunne opprettholde samfunnets funksjoner som ivaretar de grunnleggende behovene. Retningslinjene viser til tre overordnede kriterier som handler om avhengighet, alternativer, og tette koplinger. Avhengigheten viser til hvorvidt en bestemt infrastruktur har flere underliggende infrastrukturer som er avhengig av funksjonaliteten til den bestemte infrastrukturen. Jo flere infrastrukturer som er avhengig av den bestemte infrastrukturen, dess mer kritisk vil den anses for å være. Alternativer handler om hvorvidt det eksisterer andre alternative infrastrukturer som kan ivareta funksjonaliteten. Dersom det er få eller ingen alternativer, vil infrastrukturen anses for å være kritisk. Tett kopling viser til hvordan infrastrukturen er koplet sammen eller fungerer som et helhetlig system. Er systemet tett koplet vil svikt eller forstyrrelser på ett område føre til konsekvenser for systemet i sin helhet (NOU 2006:6, 2016: 32-33).

DGF vil kunne sies å falle inn under kategorien som handler om styringsevne og suverenitet. Ifølge Lysne II-utvalgets rapport (2016) kan DGF anses for å være en del av totalforsvaret, hvor DGF blir en slags form for førstelinjeforsvar. Forsvaret beskrives som en av de sentrale samfunnsfunksjonene som skal bidra til å ivareta styringsevnen og suvereniteten (NOU 2006:6, 2016: 32). På den måten kan DGF oppfattes som en infrastruktur som skal bidra til å ivareta samfunnsfunksjonen som forsvaret har.

5.5.2 Grunnleggende samfunnsverdier

Et av de primære formålene til en liberal rettsstat er å sørge for friest mulig handlingsrom for livsutfoldelse og selvbestemmelse for individet. På mange måter kan dette handlingsrommet innskrenkes av hensyn til vernet av samfunnet, hvor borgerne og samfunnets interesser også har behov for beskyttelse (Hammerlin, 2009: I). Metodene som blir brukt av myndighetene for å beskytte samfunnet kan føre til inngrep i befolkningens grunnleggende rettigheter. Spesielt vil dette dreie seg om retten til privatliv, personvern og kontroll over egne opplysninger. Myndighetenes tiltak vil ikke utelukkende ramme personer som er mistenkt eller som har begått noe straffbart, men også berøre utenforstående eller befolkningen generelt. Spørsmålet videre er knyttet til om befolkningens rettssikkerhet blir ivaretatt på en tilfredsstillende måte i tilknytning til myndighetenes bruk av ulike metoder for kontroll og samfunnsvern. I et samfunn som er basert på menneskeverd og demokrati, er det en forutsetning at personvernet og rettssikkerheten blir ivaretatt. Et slikt samfunn vi imidlertid også forutsette at borgernes sikkerhet ivaretas og at de beskyttes mot kriminalitet. På den måten vil graden av personvern og rettssikkerhet til enhver tid måtte måles opp mot myndighetenes tiltak og begrunnelsen for bruken av dem (Bruce & Haugland, 2010: 62-63).

5.5.2.1 Menneskerettigheter

De internasjonale menneskerettighetene fastslår at hvert enkelt menneske har visse grunnleggende rettigheter og friheter. De ulike rettighetene og frihetene skal bidra til at mennesker kan utvikle seg fritt og selvstendig, for å dernest kunne bidra positivt i samfunnet. Bakgrunnen for utviklingen av de ulike rettighetene kommer fra andre verdenskrig hvor menneskers integritet og verdighet ble utsatt for alvorlige krenkelser. Dermed har også menneskerettighetene en bakenforliggende tanke om å kunne bidra til å hindre nye konflikter og samfunnskollaps (NOU 2015:13, 2015: 26, FN-sambandet, 2018). Ansvaret for menneskerettighetene er fordelt slik at forpliktelsene hviler på staten, mens individene er rettighetshaverne. For eksempel vil retten til liv bety både at staten ikke skal ta liv, samt at den skal legge til rette for å ivareta borgernes liv gjennom å etablere politi, helsevesen, og rettsinstanser (NOU 2015:13, 2015: 26).

Menneskerettighetserklæringen består av tretti artikler som tar for seg ulike rettigheter som ethvert menneske besitter (FN-sambandet, 2018). I tillegg til de internasjonale menneskerettighetene finnes også den europeiske menneskerettighetskonvensjonen (EMK) som skal verne om menneskets rettigheter og grunnleggende friheter (Council of Europe, 2010). Flere av de ulike menneskerettighetene som beskrives vil kunne sies å være aktuelle i forbindelse med overvåking og DGF. De mest sentrale er gjerne retten til privatliv, ytringsfrihet, eller rettsstatlige prinsipper som at man skal være betraktet som uskyldig til det motsatte er bevist.

5.5.2.2 Personvern

E-tjenesten er ikke underlagt personopplysningsloven, men har en egen særlovgivning hvor EOS-utvalget fører tilsyn (Datatilsynet, 2013: 23). Samtidig kan det hevdes at personvern og vern om personopplysninger er viktige bærebjelker i et demokratisk samfunn, og derfor ikke kan tilsidesettes i diskusjonen om E-tjenestens overvåking i forbindelse med DGF-behandlingen. Ifølge Bruce og Haugland (2010) er personvernet knyttet opp til menneskers behov for en privat sfære som er fri for innblanding fra utenforstående. Personvernet dreier seg ikke bare om å være i fred, men også om personopplysningsvern som handler om å ha kontroll over opplysninger om seg selv. Videre er personvernet knyttet til begrepet personlig integritet, som handler om retten til selvbestemmelse over egen kropp, eiendom og tanke (Bruce & Haugland, 2010: 63-64).

I forbindelse med personvernets stilling i både norsk og europeisk sammenheng er det utledet flere ulike prinsipper som skal bidra til å beskytte og ivareta personvernet. For det første skal all behandling av personopplysninger måtte være hjemlet i lov. Videre tilsier prinsippet om formålsbegrensning at innsamling av personopplysninger være regulert gjennom spesifikke formål og kun brukes i henhold til de bestemte formålene. Prinsippet om dataminimering viser til at personopplysningene skal også være adekvate, relevante og begrenset til det som er nødvendig for formålet med innsamlingen. Behandling av opplysninger som ikke dekkes, eller som anses for å være uriktige, i forhold til formålet må slettes eller korrigeres. Det er også et prinsipp om lagringsbegrensning som sier at lagringen ikke skal foregå slik at personer kan identifiseres i lengre perioder utover det som er nødvendig. Prinsippet om integritet og konfidensialitet viser til at det skal være tilstrekkelig sikkerhet for

personopplysningene. Det vil si at det skal etableres tiltak for å hindre uautorisert eller utilsiktet tilgang, samt beskyttelse mot tap, videreformidling eller skade (Bruce & Haugland, 2010: 68-69, Europarådskonvensjonen, 2016, kapittel II artikkel 5 bokstav a-f).

5.5.2.3 Kommunikasjonsvern

Kommunikasjonsvern handler om å sikre at brukeres kommunikasjon holdes privat. Dette er et vern som tradisjonelt sett har stått sterkt i Norge, og som er hjemlet i den ordinære lovgivningen, samt i Grunnlovens § 102. I tillegg er kommunikasjonsvernet sikret gjennom EUs lovverk og EMK. Kommunikasjonsvernet er en viktig forutsetning for å sikre tillitten til de ulike kommunikasjonstjenestene. Dermed blir kommunikasjonsvernet også viktig overfor demokratiske verdier som ytringsfrihet og forsamlingsfriheten. Motsatsen ligger i hensyn til kriminalitetsbekjempelse og etterretningsarbeid, som fordrer at kommunikasjonsvernet har visse begrensninger (Nasjonal Kommunikasjonsmyndighet, 2015: 66-67). Spørsmål knyttet til hvordan kommunikasjon foregår eller kan foregå, er viktig i den forstand kommunikasjon mellom mennesker er samfunnskonstituerende. På samme måte som små samfunn kan virke mer demokratiske fordi kommunikasjonen er enklere, så kan ITK og kommunikasjonsmulighetene mellom mennesker argumenteres for å være demokratiserende i store samfunn (Sejersted, 2002: 171).

5.5.2.4 Rettssikkerhet

Rettssikkerhet som begrep har ikke en entydig og presis definisjon, men handler i stor grad om individets rett til beskyttelse mot vilkårlighet og overgrep fra myndighetene. Videre omfavner rettssikkerhetsbegrepet verdier som likhet, rettferdighet og mulighet til å forutberegne sin rettsstilling. I tilknytning til overvåking vil prinsippet om forutberegnelighet dreie seg om at vilkårene og rammene for overvåkingen skal være kjent slik at enhver kan innrette seg etter forholdene. Dette innebærer også at vernet mot vilkårlighet og overgrep, ikke er ensbetydende med vern mot inngrep. I et demokratisk samfunn vil det kunne være legitime begrunnelser og behov for inngrep i enkeltpersoners private eller rettslige sfære. Forutsetningen er at inngrepet skal foregå i henhold til de rettslige rammene, slik at borgerne skal kunne forutse og innrette seg mot inngrepet (Bruce & Haugland, 2010: 71).

5.5.2.5 Tillitt

Tillitt er en viktig faktor som henger sammen med samfunnssikkerheten og som bidrar til å skape et robust samfunn (Engen et al., 2016: 49). Betydningen av tillitt har fått økende oppmerksomhet i samfunnsvitenskapen. Tillitt blir blant annet ansett for å være et viktig grunnlag og «lim» i samfunnet, som bidrar til å skape demokratisk stabilitet. Uten tillitt vil samfunnet falle sammen, og på den måten blir tillitt en viktig faktor eller verdi for myndighetene (Hammerlin, 2014: 63-64). Dersom samfunnstillitten er lav vil befolkningen unngå de institusjoner eller virksomheter den ikke har tillitt til, eller finne egne løsninger. I tillegg vil det ofte være slik at dess mindre kunnskap det er om trusler og risikoer, dess mer forutsetter det at de ulike aktørene med ansvaret for sikkerheten har tillitt. Usikkerhet kan reduseres gjennom ny kunnskap, mens tillitt kan gjøre usikkerheten mer akseptabel (Engen et al., 2016: 49).

Selve begrepet tillitt kan forklares som at noen stoler på noen med hensyn til noe. Det vil si at tillitt består av noen som gir tillit, noen som får tillit, og hva denne tillitten er knyttet til. Videre kan tillittsrelasjonen svekkes eller styrkes ut fra hvordan tillitten blir forvaltet, for eksempel om den som mottar tillitt faktisk er til å stole på. Tillitsrelasjoner på makronivå handler blant annet om relasjonen mellom borger og myndighet. Her kan tillitsrelasjonen påvirkes på tre ulike måter. For det første kan myndighetenes tillitt til borgerne påvirkes. Myndighetene har monopol på legitim bruk av makt, men har samtidig, gjennom demokratiske og rettsstatlige prinsipper, begrensede muligheter for å kontrollere og overvåke borgerne. Dermed vil myndighetene måtte utvise tillitt til borgerne i form av at det vises respekt overfor de ulike lover og regler som er etablert. For det andre kan borgernes tillitt til myndighetene påvirkes. Myndighetenes evne til å beskytte samfunnet og borgerne mot indre og ytre trusler, er et av premissene som ligger til grunn for dens legitime maktmonopol. Dermed vil borgerne måtte ha tillitt til at myndighetene kan beskytte og sikre samfunnet. Den siste relasjonen handler om borgernes gjensidige tillitt til hverandre. Idealet for et liberalt demokrati er at den politiske maktkampen skal foregå augmentativt gjennom politisk meningsbrytning. Det skal være rom for ulike politiske ideer, synspunkter og ideologier i samfunnet. Noe som fordrer gjensidig tillitt mellom borgerne om å forholde seg til demokratiets politiske spilleregler (Hammerlin, 2014: 72-75).

6. Analyse

I det følgende kapittelet knyttes det empiriske og teoretiske grunnlaget sammen til en analyse og diskusjon som bidrar til å gi svar på de tre forskningsspørsmålene. Dette skal danne grunnlaget for å kunne svare på oppgavens problemstilling om hvordan DGF kan true samfunnssikkerheten. Først vil spørsmålet om hva som kan overvåkes gjennom DGF besvares. Her vil fokuset være på ulike problemstillinger knyttet til overvåking gjennom DGF, samt utfordringer som reises gjennom krypteringsmuligheter. I det neste avsnittet vil ulike momenter knyttet til kontrollmekanismene som er tenkt implementert i DGF-systemet analyseres. Det vil også gis noen tidligere eksempler fra E-tjenestens virksomhet hvor det har oppstått eller blitt gjort feilvurderinger. Tilslutt vil analysen rette seg mot hvilke samfunnsfunksjoner og verdier som kan berøres av DGF. Her vil DGF først fokuseres på knyttet til samfunnsfunksjoner og kritisk infrastruktur i lys av den teoretiske definisjonen av samfunnssikkerhet. Videre analyseres DGF opp mot de ulike grunnleggende samfunnsverdiene som blant annet tar for seg aspekter knyttet til personvern, rettssikkerhet og tillitt.

6.1 Hva kan overvåkes gjennom DGF?

De ulike overvåkingsmetodene vil skille seg fra hverandre med tanke på hvor inngripende de er. Samtidig vil gjerne overvåking som utføres i regi av staten ha det største potensialet for utøving av myndighet og kontroll. Dette aktualiserer diskusjoner om overvåkingens omfang og formålstjenlighet, samt balansegangen mellom hva som er tilstrekkelig og hvor grensen går for hva som er for mye overvåking (Schartum, 2010: 21). Med tanke på at 99 prosent av all kommunikasjon krysser grensen via de fiberoptiske kalene (Søreide, 2017, Etterretningstjenesten, 2016: 1), vil overvåkingspotensialet til DGF-systemet tilsynelatende være enormt. DGF vil også innebære innsamling og overvåking av nærmest alle typer kommunikasjon (Datatilsynet, 2017: 10).

Potensielt sett vil det være store menger informasjon som vil kunne overvåkes gjennom fiberkablene som krysser landegrensen. Det er flere årsaker til at det vil være problematisk å gi E-tjenesten tilgang til all denne datatrafikken. For det første vil kun en liten del av datatrafikken være relevant i henhold til E-tjenestens oppdrag. For det andre vil prinsippet om

forholdsmessighet i juridisk forstand utfordres dersom E-tjenestens tilgang ikke reguleres godt nok. Vurdering av forholdsmessighet, i forhold til hvilke data E-tjenesten skal kunne få tilgang til, vil også kunne angi hvorvidt innretningen er i henhold til Grunnloven, personlovgivningen og de internasjonale menneskerettighetene. For det tredje vil DGF være avhengig av at offentligheten har tillitt til at det ikke drives masseovervåking av norske borgere (Lysne II-utvalget, 2016: 50)

En annen sentral problemstilling handler om bredden av overvåkingen. Det vil si hvor omfattende og presis overvåkingsvirksomheten er. Her kan det gjerne skilles mellom overvåking av bestemte personer eller grupper, og overvåking av en udefinert personkrets. Ved å overvåke bestemte personer eller grupper legges det opp til en relativt presis strategi som kan fokusere på for eksempel kriminelle miljøer eller terrororganisasjoner. Overvåking av en udefinert personkrets derimot, vil innebære at det registreres informasjon om alle personer som for eksempel utfører visse handlinger eller beveger seg innenfor bestemte områder. Dette kan eksempelvis dreie seg om overvåking av alle som bruker telekommunikasjon. Dermed vil dette representere overvåking av en ubestemt personkrets og anses for å være en upresis metode, fordi de fleste brukere av telekommunikasjon ikke er terrorister eller tunge kriminelle. En slik upresis overvåkingsstrategi vil i utgangspunktet kunne sies å være uforholdsmessig, og vil ofte kunne oppfattes som en uakseptabel form for overvåking av alminnelige samfunnsgrupper. Dersom det kreves at overvåkingen skal være tilsiktet, begrunnet og relativt presis, vil ikke masseovervåking av udefinerte personkretser kunne sies å være akseptabelt. En mulig løsning for å kunne foreta masseovervåking av udefinerte personkretser, vil muligens kunne være å rette overvåkingen mot bestemte personprofiler eller karakteristikker for å redusere overvåkingen. Samtidig vil en selektiv overvåkingsstrategi som dette trolig bli betraktet som svært diskriminerende (Schartum, 2010: 27).

Overvåkingen gjennom DGF kan i utgangspunktet betraktes som en upresis metode hvor all informasjon om kommunikasjon som passerer grensen i fiberkablene blir omfattet. I følge Datatilsynet (2017) sin høringsuttalelse anses DGF for å være et svært omfattende og inngripende verktøy hvor E-tjenesten vil besitte betydelig mengder informasjon om kommunikasjon til egne borgere (Datatilsynet, 2017: 2). Videre kan kategorisering eller de

ulike programmeringene som implementeres i systemet, for å finne personer av interesse, potensielt sett være diskriminerende. I følge Richards (2013) vil slik sortering eller kategorisering kunne være skadelig, spesielt med tanke på rettslige prinsipper som blant annet hviler på rettferdighet. Han viser til kommersielle eksempler hvor store mengder data fra Internett anvendes for å skape avanserte profiler som viser folks interesser, rutiner, og kjøpevaner. De ulike profilene kan dernest sorteres og kategoriseres slik at profilene mottar ulike muligheter eller tilbud basert på hvilken kategori de faller innunder. På samme måte som kommersielle selskap kan benytte data til å skape kjøpsprofiler for effektiv markedsføring, kan myndighetene benytte data til å kategorisere borgerne basert på for eksempel risiko for kriminalitet. Diskrimineringen blir en utfordring idet den genererer forskjeller basert på eksempelvis velstand, etnisitet, kjønn eller geografi. Et eksempel kan være at bestemte personprofiler gjennomgår mindre eller kortere sikkerhetskontroll på flyplassen, mens andre personprofiler blir grundigere sjekket. Eksempelet viser at muligheten for å kunne behandle personer forskjellig vil kunne utfordre både sivile rettigheter og rettslige prinsipper om rettferdighet (Richards, 2013: 1956-1957). Det er ikke dermed sagt at DGF vil kunne føre til at borgere behandles forskjellig. Kanskje spesielt fordi DGF i utgangspunktet er rettet mot utlandet og ikke fysiske og juridiske norske personer. Samtidig er det viktig å være klar over den potensielle diskrimineringen som DGF-systemet utgjør i form av den programmering og behandling av data som foretas. Spesielt med tanke på hva eller hvilke kriterier som legger føringer for hvilken informasjon som kan hentes ut for videre analyser.

Lysne II-utvalgets rapport (2016) kan også fremstå som noe uklar med tanke på om data ved bruk av skytjenester vil fanges opp i systemet. Rapporten skriver at DGF ikke vil gjelde for data som lagres, for eksempel gjennom bruk av skytjenester. Samtidig fremkommer det at data som genereres ved bruk av skytjenester for backup av telefon, eller gjennom tjenester som gir brukeren tilgang til bilder og filer på flere maskiner vil kunne føre til at informasjon om kommunikasjon vil kunne krysse landegrensen (Lysne II-utvalgets rapport, 2016: 10, 48).

6.1.1 Masseovervåking?

I Lysne II-utvalgets rapport (2016) argumenteres det for at E-tjenesten har behov for å kunne samle inn og behandle rådata for å kunne løse sine etterretningsoppgaver. Samtidig innebærer dette at det samles inn store mengder informasjon som faller utenfor E-tjenestens interessefelt.

Blant annet kan dette dreie seg om innsamling av data knyttet til norske personer. E-tjenestens lagring av slike data har vært vanlig praksis over lengre tid (Lysne II-utvalget, 2016: 16). Samtidig skal det være høy terskel for å vurdere noe som en trussel mot rikets sikkerhet og vitale nasjonale interesser (NOU 2006:6, 2006: 35). Dermed kan det også stilles spørsmål ved formålstjenligheten til DGF og den potensielle masseovervåkingen det representerer, i den forstand trusler mot nasjonen og nasjonale interesser dreier seg om noen få tilfeller. Et spørsmål som kan stilles i den forbindelse, er hvorvidt den høye terskelen for å vurdere noe som en trussel not rikets sikkerhet og nasjonale interesser, rettferdiggjør overvåking som også vil fange opp store mengder informasjon om kommunikasjon som ikke er relevant for E-tjenestens etterretningsformål. Dette kan også sies å handle om proporsjonalitet mellom inngrepet og formålet. Datatilsynet (2017) viser til at E-tjenestens interesseområde og formål favner svært bredt, og derav vil DGF i tråd med loven potensielt sett ha et stort bruksområde.

Etterretningstjenesten (2016) påpeker at over 99% av all informasjon i dag transporteres gjennom fiberoptiske kabler og at det derfor er essensielt for E-tjenesten med tilgang til informasjonen der den opptrer for å i det hele tatt kunne løse sine samfunnsoppdrag. Det blir imidlertid hevdet at lagring av metadata, for å kunne finne den etterretningsrelevante informasjonen, ikke har noe med masseovervåking å gjøre (Etterretningstjenesten, 2016: 1, 2). Dette vil imidlertid kunne sies å være et definisjonsspørsmål som henger sammen med hvor man setter grensen for at informasjonsinnhenting kan kalles overvåking, og hvor mye informasjon dette er snakk om før det kan kalles masseovervåking. Ifølge Datatilsynet (2017) vil mange oppfatte informasjonsinnhenting som overvåking idet informasjonen blir brukt til vurderinger av mennesker eller som grunnlag for ulike analyser. Den forutgående masseinnsamlingen av informasjon vil med dette ikke anses som overvåking. Datatilsynet på sin side mener at innsamling av personopplysninger er et inngrep i seg selv (Datatilsynet, 2017: 6). Definisjonen av begrepet overvåking som er gitt i denne avhandlingen tilsier at overvåking dreier seg om systematiske fremgangsmåter hvor informasjonsinnhentingen har en vis varighet og er av et relativt stort omfang. Det er heller ikke ansett som et krav at informasjonen som hentes inn vil bli brukt, slik at selve lagringen av informasjon også vil være å anse som overvåking (Shartum, 2010: 22). I og med at DGF innebærer innsamling av store mengder data, samt betydelige menger informasjon om norske borgere, vil DGF kunne argumenteres for å være masseovervåking. Dette vil også kunne sies å være i tråd med de definisjonsmessige kriteriene for hva overvåking innebærer.

6.1.2 Ulike typer data

I noen tilfeller kan det være vanskelig å skille mellom hva som er metadata og hva som er innholdsdata. Årsaken til dette er at metadata kan inneholde informasjon som mer eller mindre kan sies å beskrive deler av selve innholdet. Et eksempel kan være en epost som inneholder metadata om avsender, mottaker og tidspunkt. I tillegg vil ofte eposter ha et felt for emne («subject»), som i mange tilfeller vil kunne gi indikasjoner på innholdet i eposten. Dermed vil metadata i noen tilfeller også inneholde elementer som kan anses for å være innholdsdata. Et annet eksempel kan være en web-adresse som i utgangspunktet vil defineres som metadata. Samtidig vil en web-adresse kunne være avslørende med tanke på innholdet i selve navnet på adressen. Eksempelvis kan adressen inneholde søkeord som er brukt i en søkemotor (Lysne II-utvalget, 2016: 54).

En annen sentral utfordring ved bruk av metadata er mulighetene for reidentifisering. Selv om dataene i utgangspunktet er anonyme så kan mengden og sammenstillingen av dataene, ved bruk av ulike teknikker, føre til at individer kan identifiseres (Datatilsynet, 2013: 8). Metadata kan på mange måter bli tillagt en verdi i seg selv. Denne verdien er knyttet til dataenes fremtidige muligheter og bruksområder. Dette kan i neste omgang påvirke virksomhetens motivasjon angående sletting av dataene, hvor virksomhetene vegrer seg for å slette data som kan ha et nyttepotensiale på et senere tidspunkt (Datatilsynet, 2013: 25). Det fremkommer også i Lysne II-rapporten (2016) at E-tjenesten har behov for å kunne lagre data over lengre tid for å kunne drive effektiv analyse av dataene, og eventuelt lagre visse data lengre enn lagringsfristen dersom etterretningsverdien av dataene skulle tilsi det (Lysne II-utvalget, 2016: 19). En utfordring som kan oppstå i dette tilfellet, kan knyttes til sorteringen av data med tanke på hva som skal beholdes og hva som skal slettes. Dersom det er vanskelig å skulle forutse viktigheten og de fremtidige bruksmulighetene av dataene, kan det tenkes at data som skulle vært slettet blir beholdt i tilfellet de kan bli nyttige senere.

Lysne II-utvalget utelukker ikke at det i fremtiden vil kunne bli mulig å få mer ut av datastrømmene enn det er i dag (Lysne II-utvalget, 2016: 67). Dette kan bety at verdien av å kunne analysere de ulike dataene som samles inn via DGF vil kunne generere mer informasjon og kunnskap. Samtidig kan det også bety at DGF kan bli mer utfordrende overfor aspektene knyttet til personvernet, og dermed oppfattes som mer inngripende.

6.1.3 Kryptering

Den økende krypteringstrenden har ført til en diskusjon om hvorvidt kryptering bør underlegges strengere kontroll, blant annet for å kunne ivareta statens behov for innsyn. Et totalt forbud mot kryptering vil trolig ramme ulike individer og virksomheter som har et legitimt behov for konfidensialitet og beskyttelse av sin kommunikasjon. Et aktuelt alternativ kan derfor være å etablere ulike bakdører for å få tilgang til den krypterte informasjonen. Trenden viser at E-tjenesten trolig må forholde seg til mer kryptering i fremtiden. Videre vil en slik trend særlig synliggjøre to effekter. For det første vil det kunne bli mer fokus over på transporten av informasjon, som dermed kan bidra til å konstruere innhold selv om dette er skult. For det andre vil informasjon som transporteres ikke nødvendigvis være kryptert i det den lagres. Det vil si at enheter som for eksempel mobiltelefoner, PC, eller andre nettverk og skytjenester, hvor informasjonen eller innholdet i den krypterte kommunikasjonen lagres, sannsynligvis vil bli svært ettertraktet å få tilgang til. Det pekes på at DGF vil kunne gi E-tjenesten mulighet til å overvåke trusler mot Norge gjennom trafikkdata, selv om kommunikasjonen i noen tilfeller er kryptert (Lysne II-utvalget, 2016: 27).

Eksakt informasjon og detaljer omkring hvordan E-tjenesten behandler kryptert kommunikasjon er svært sensitivt, men det påpekes at sterke krypteringsmekanismer er generelt utfordrende. Et betydelig antall ulike krypteringsmetoder vil trolig ikke la seg forsere, noe som betyr at DGF ikke vil tilby E-tjenesten tilgang til all informasjon som kommuniseres over grensen. I tillegg vil trolig nettoperatørene selv i økende grad kryptere trafikken som krysser landegrensen. Dette kalles gjerne for linkkryptering hvor hensikten er å sikre nettet. På den andre siden vil linkkryptering i utgangspunktet være problematisk i forhold til effekten av DGF (Lysne II-utvalget, 2016: 27, 49, 68). I den forbindelse skal teletilbyderne pålegges en tilretteleggingsplikt for å levere datastrøm uten linkkryptering (Datatilsynet, 2017: 12, Lysne II-utvalget, 2016: 68).

I Lysne II-utvalgets rapport (2016) bekrefter E-tjenesten at det vil være utfordringer knyttet til økende kryptering av kommunikasjon. Samtidig hevdes det at DGFs viktigste funksjoner, som blant annet handler om å detektere IP-adresser, i mindre grad vil utfordres av økende kryptering. I tillegg vil DGF sammen med E-tjenestens øvrige metoder eller kapasiteter kunne kompensere for noen av utfordringene ved krypteringen. E-tjenesten erfarer også at mye av

informasjonen fortsatt går ukryptert (Lysne II-utvalget, 2016: 77). Datatilsynet (2017) hevder derimot at det vil være relativt enkelt å kunne omgå DGF. For det første vil tilretteleggingsplikten om linkkryptering ikke omfatte ende-til-ende kryptering, slik at for eksempel ulike applikasjoner kan kryptere sine egne tjenester. For det andre finnes det teknologiske løsninger som kan anonymisere IP-adresser slik at også metadataene kan miste mye av nytteverdien. Eksempler på slike løsninger kan være VPN (Virtuelt Privat Nettverk) eller TOR (The Onion Router) som anonymiserer kommunikasjonen. Dermed vil DGF ramme vanlige borgere som ikke iverksetter tiltak for å beskytte kommunikasjonen, mens ulike trusselaktører som bevisst vil operere i skjul kan unngå å fanges opp i DGF-systemet (Datatilsynet, 2017: 2, 12).

Den antatte økningen i bruken av kryptering er positivt for å bidra til å hindre uvedkommende tilgang til informasjon. I tillegg kan kryptering bidra til å styrke til kommunikasjonsvernet- og friheten (Lysne II-utvalget, 2016: 68). På den andre siden kan det stilles spørsmålstegn ved nødvendigheten av DGF dersom effekten av systemet likevel vil kunne vise seg å være betydelig redusert gjennom både sluttbrukerkryptering og linkkryptering. DGF kan i seg selv også bidra til at bruken av kryptering øker, fordi overvåkingen kan skape et insentiv for folk til å skjule sin kommunikasjon. I tillegg til at spådommen tilsier at det trolig vil være mer kryptering i fremtiden, bør DGF-systemet vurderes opp mot den samfunnsmessige nytten og behovet for overvåkingen.

6.2 Hvilke kontrollmekanismer er tenkt implementert ved etablering av DGF?

De ulike kontrollmekanismene som inngår i DGF-systemet kan på flere områder gjerne kalles for et teknologisk vern. Særlig gjelder det den automatiserte og maskinelle kontrollen og tilgangen, hvor domstolens rettslige kjennelser er tenkt implementert i systemet. En forutsetning for det teknologiske vernet er at de ulike regler og rettskjennelser kan oversettes og uttrykkes gjennom programmeringsspråket i systemet (Schartum, 2010: 33).

6.2.1 Datalager

Det fremkommer av Lysne II-utvalgets rapport (2016) at det vil kunne foreligge risiko for misbruk av DGF. Misbruk kan for eksempel dreie seg om at folks e-poster, sms'er, internettrafikk, facebookmeldinger eller lignende, blir urettmessig eller ulovlig avlest og overvåket. Rapporten skriver at risikoen for misbruk må være usannsynlig og viser videre til de ulike vilkårene og kontrollmekanismene som skal kunne redusere faren for misbruk. (Lysne II-utvalget, 2016: 52).

De interne regler og kontrollmekanismer som er etablert i E-tjenestens virksomhet skal blant annet vurderes jevnlig. Formålet er å sørge for at regelverket er oppdatert og tilpasset den kontinuerlige teknologiske og operative utviklingen (Lysne II-utvalget, 2016: 16). Samtidig kan den dynamiske tilpasningen av interne kontrollmekanismer kan bidra til å skape et uoversiktlig nettverk av ulike regler og prosedyrer. Ved å stadig endre prosedyrer og regler, kan det tenkes at det blir mer krevende for kontrollmyndighetene å ha oversikt. Samtidig fremkommer det av Lysne II-utvalgets rapport (2016) at EOS-utvalget kun holdes informert om E-tjenestens rutiner og praksis for internkontroll så langt det lar seg gjøre for å dekke utvalgets kontrollbehov (Lysne II-utvalget, 2016: 19). Dermed kan det fremstå slik at tilsynsmulighetene overfor DGF-systemet og den interne bruken reduseres ved at tilsynsmyndighetene ikke har fullstendig innsikt eller

Det kommer frem i rapporten fra Lysne II-utvalget (2016) at E-tjenesten har ytret ønske om at bruken av korttidslageret skal kunne benyttes som et retrospektivt verktøy. Dette gjelder særlig i tilknytning til kontrete trusler eller i etterkant av hendelser hvor kortidslageret kan benyttes for etterretningsformål. Rapporten går derimot ikke inn for å anbefale en slik tillatelse for bruk av korttidslageret. For det første vil det innebære lagring av mer ufiltrert data enn det som er nødvendig. For det andre vil det kunne åpne for at de begrensninger som ellers er tenkt i DGF-systemet kan omgås (Lysne II-utvalget, 2016: 55). E-tjenestens ideelle ønske om bruken av korttidslageret viser at de ser potensiale i den informasjonen som vil lagres i korttidslageret. Noe som i neste omgang kan knyttes opp mot utfordringene knyttet til hva og hvilke data som blir slettet eller beholdt i datalagrene.

Ifølge Lysne II-utvalgets rapport (2016) vil en av kontrollmekanismene i DGF-systemet bestå av domstolsbehandling. Her diskuteres det hvorvidt det skal nedsettes en spesialdomstol hvor noen av personene som skal ta stilling til spørsmål knyttet til DGF skal ha etterretningsfaglig bakgrunn. Justis- og beredskapsdepartementet (2017) peker på at dette kan være positivt at domstolsavgjørelser også er basert på kunnskap om etterretningsfaget og trusselbildet. Samtidig pekes det på at en spesialdomstol vil kunne medføre risiko for at dommerne etterhvert identifiserer seg med E-tjenestens oppgaver og virkeområde (Justis- og beredskapsdepartementet, 2017: 4). Et spørsmål vil derfor kunne rette seg mot hvorvidt en domstol som også består av etterretningsfaglig personell vil kunne sies å være uavhengig eller nøytral i behandling av DGF-saker.

Lysne II-utvalget (2016) skriver videre at det i noen tilfeller vil kunne være behov for E-tjenesten å igangsette søk før DGF-domstolen har fattet en rettslig avgjørelse. Rapporten sier videre at en slik ordning bør kunne etableres, så lenge det stilles krav til sletting av søk dersom domstolen gir avslag på kjennelsen (Lysne II-utvalget, 2016: 58). En slik åpning i systemet kan føre til økt risiko for systemfeil i form av at det foretas søk som ikke er i overensstemmelse med det etablerte rammeverket forøvrig. Det kan argumenteres for at en slik ordning vil kunne fremstå som en demokratisk og lovmessig sårbarhet i form av at det utøves skjønn i vurderingen av hva det skal søkes etter i datalagrene. Justis- og beredskapsdepartementet (2017) peker på at problemstillinger knyttet til søk forutfor domstolsavgjørelser vil måtte avklares nærmere.

6.2.1.1 Datalager som kritisk infrastruktur

Ved å knytte DGF opp til samfunnssikkerhet, kan DGF-innretningen og datalagrene betraktes som en infrastruktur. Med tanke på at datalagrene i henhold til DGF vil inneholde enorme mengder data og personsensitiv informasjon, kan det argumenteres for at datalagrene kan betraktes som en kritisk infrastruktur i lys av systemets sensitivitet. Dette kan gjerne sies å sammenfalle med Lysne II-utvalgets rapport (2016) som viser til viktigheten av å beskytte dataene, som for eksempel mot uautorisert tilgang eller misbruk. Samtidig kommer det ikke tydelig frem hvordan datalagrene skal beskyttes mot risikoer utenfra. IKT utvikler seg raskt og kan samtidig føre til økt digital sårbarhet i form av blant annet cyber-angrep. Dermed kan DGF i seg selv utgjøre en sårbarhet dersom systemet blir et mål for hacking eller spionasje,

eller utsettes for cyber-angrep. I følge teorien knyttet til samfunnssikkerhet vil det være helt sentralt å beskytte kritisk infrastruktur for å bevare samfunnssikkerheten og viktige samfunnsfunksjoner. I Lysne-II utvalgets rapport (2016) kan det påstås at det er manglende forklaringer for hvordan DGF og datalagrene, som en kritisk komponent i seg selv, konkret skal ivaretas og beskyttes mot ytre risikoer. Rapporten argumenterer for at E-tjenesten består av et av Norges sterkeste ekspertisemiljø innen cybertrusler. I tillegg er det stort fokus på datasikkerhet og elektronisk sikkerhet, samt at tjenestens lokaler er godt fysisk skjermet. E-tjenestens evne og kompetanse til å ivareta sikkerheten rundt sine systemer beskrives som nærmest enestående i Norsk sammenheng. Sensitiviteten til DGF-systemet er en sentral årsak til at det blir lagt vekt på å etablere gode sikkerhets- og kontrollmekanismer, samt sørge for at datasikkerheten er så høy som mulig. Det er en viktig prioritet å redusere risikoen for at uvedkommende får tilgang til data eller utstyr. Samtidig blir det påpekt at det ikke vil være fullt ut mulig å sikre elektroniske systemer mot datainnbrudd (Lysne II-utvalget, 2016: 69). Dette er gjerne noe som også bør vurderes opp mot prinsippet om integritet og konfidensialitet som skal sikre personopplysninger mot uautorisert eller utilsiktet tilgang.

Det vil det være viktig å diskutere de ulike konsekvensene som kan oppstå, for å kunne være forberedt og klar over den samfunnsmessige påvirkningen. Det kan for eksempel dreie seg om alvorlighetsgraden av informasjonseksponering, borgernes tillitt til myndighetene, fremmede staters tilgang på betydelige mengder sensitiv informasjon, internt misbruk eller svikt i kontroll- og tilsynsfunksjonene. Med dette kan det argumenteres for at Lysne II-utvalgets rapport ikke uten videre kan basere sine konklusjoner på at DGF-systemet er tilnærmet sikkert. Det må tas høyde for at det kan oppstå svikt i systemet, og inkludere mulige risikoer og konsekvenser i sine utregninger. Datatilsynet (2017) peker på at informasjonen som samles inn gjennom DGF vil ha så stor nytteverdi for andre aktører innen justis- og sikkerhetsarbeid at en formålsutglidning nærmest må forventes. Dermed vil også DGF i seg selv bli mer inngripende enn det som i utgangspunktet var hensikten (Datatilsynet, 2017: 2).

6.2.1.2 DGF og risikostyring

Et annet moment er hvilke muligheter man har til å kontrollere eksistensen av DGF etter at systemet eventuelt har blitt implementert. Her menes det hvilke muligheter eller indikatorer som skal være gjeldende for å eventuelt stenge ned og avvikle DGF. I følge Engen et al.

(2016) vil regler for hvordan vurderingen av tiltakene fungerer og effekten av dem, bidra til å imøtekomme demokratiske hensyn. Tiltak som innføres for å styrke sikkerheten bør evalueres etter tre til fem år, og dersom det ikke kan vises til noen effekt bør det fjernes (Engen et al., 2016: 392). Lysne II-utvalgets rapport mener det bør tas høyde for at behovet for DGF kan endre seg i fremtiden, og foreslår at det utføres en evaluering av DGF etter fem år. Gjennom evalueringen skal det vurderes hvorvidt DGF skal videreføres med tanke på nødvendighet og forholdsmessighet på evalueringstidspunktet (Lysne II-utvalget, 2016: 67). En slik løsning kan bidra til flere fordeler i henhold til risikostyring. For det første vil en kontinuerlig evaluering av ethvert sikkerhetstiltak bidra til å skape innsikt og kunnskap om hva som fungerer eller hva som ikke fungerer. For det andre kan det bidra til en mer helhetlig oversikt og tydeligere ansvar for sikkerhetsarbeidet, fordi det kan redusere faren for at summen av ethvert sikkerhetstiltak blir nok ett skritt på veien mot et samfunn som ingen egentlig vil ha. (Engen et al., 2016: 392). Lysne II-utvalget (2016) peker også på at det er viktig å vurdere totaliteten av de ulike overvåkingstiltakene i samfunnet. Hver for seg kan ethvert tiltak gjerne ha god begrunnelse og intensjon, mens de samlet sett kan utgjøre en utfordring for personvernet. (Lysne II-utvalget, 2016: 67). For det tredje kan det bidra til å skape en kontinuerlig og levende debatt om hva et sikkert samfunn er, og hvordan det bør være (Engen et al., 2016: 393). En av utfordringene vil være om det eksisterer politisk vilje til å reversere DGF, som kan tolkes for å være et relativt omfattende sikkerhetstiltak. Et annet spørsmål vil dreie seg om hvilke bestemte indikatorer eller mål på effektivitet som skal være gjeldende for å vurdere videreføringen eller nedleggelsen av DGF. I tillegg kan evalueringen være problematisk å gjennomføre i offentligheten med tanke på at E-tjenestens virksomhet og arbeid er hemmelig, noe som kan føre til at det blir mindre åpenhet omkring hvordan effekten av DGF blir vurdert.

DGF kan forstås som relativt komplisert teknologi med tanke på systemet i seg selv, men også de ulike faktorene rundt, som for eksempel ulike lover og reguleringer. I tillegg kan det tolkes slik at DGF inngår i en kompleks organisasjon med samfunnsoppdrag som favner bredt, og i tillegg samarbeider og er tett knyttet til flere andre aktører og myndigheter. Dynamikken og kompleksiteten i samfunnet kan ifølge teorien om risikosamfunnet føre til at det blir vanskelig å styre sikkerheten, samt at konsekvensene kan være omfattende når noe først går galt. Ved å betrakte DGF i lys av risikosamfunnet kan det sies at konsekvensene av det oppstår eller gjøres feil i forbindelse med DGF-systemet kan være betydelige. Dette argumentet henger

blant annet sammen med hvordan DGF kan knyttes opp mot viktige samfunnsfunksjoner- og verdier. Videre tolkes det også slik at overvåkingskapasiteten og hva som blir gjenstand for overvåking gjennom DGF-systemet er så omfattende at konsekvensene derfor kan bli alvorlige. Spesielt sett i lys av at fremmede stater kan ha interesse av å tilegne seg tilgang til informasjonen i DGF-systemet.

En annen utfordring som skisseres er knyttet til en eventuell ikke-demokratisk maktovertakelse, hvor det foreslås at det skal implementeres destruerende mekanismer i systemet. Det går ut på at all informasjon skal kunne slettes samt at DGF-utstyret skal kunne ødelegges (Lysne II-utvalget, 2016: 69). Dette kan i utgangspunktet være et positivt sikkerhetstiltak for å kunne avverge at DGF gjøres tilgjengelig ved en eventuell ikke-demokratisk maktovertakelse. Utfordringen kan være knyttet til hvorvidt de destruerende mekanismene faktisk vil bli iverksatt. Det kan gjerne spekuleres i ulike årsaker til at iverksettingen ikke skjer, for eksempel vegring for å slette betydelige mengder med potensielt verdifull informasjon. Men poenget er at denne destrueringsmekanismen gjerne bør konkretiseres for å vise til hvordan dette vil fungere i praksis og under hvilke bestemmelser destrueringen iverksettes. Spesielt utfordrende vil det trolig være dersom det ikke er snakk om en tydelig ikke-demokratisk maktovertakelse, men en samfunnsutvikling som over tid dreier i en uønsket retning. Det kan også være snakk om fremtidige demokratisk valgte regjeringer som vil kunne endre, utvide eller anvende DGF på andre måter enn det som var tenkt i utgangspunktet. Datatilsynet (2017) peker også på at behovet for destrueringsmekanismer bidrar til å signalisere hvor alvorlig og hvilket maktmiddel DGF faktisk er.

6.2.2 Filter

De ulike filtrene i DGF-systemet er en kontrollmekanisme som skal bidra til å regulere og sortere dataene i DGF-systemet og hindre innsamling av informasjon som faller utenfor E-tjenestens virksomhetsområde (Lysne II-utvalget, 2016: 54) Datatilsynet (2017) peker imidlertid på at det ikke er mulig å filtrere all informasjon i systemet. Blant annet vil det ikke kunne foretas effektiv filtrering av kommunikasjon som foregår mellom personer som begge befinner seg i Norge. Metadatalageret vil derfor inneholde store mengder informasjon innenlandske forhold og norske personer i Norge. Det kan derfor stilles spørsmålstegn ved

hvorfor utenlandsetterretningen skal besitte slike store informasjonsdata om egne borgeres kommunikasjon (Datatilsynet, 2017: 5).

Datatilsynet (2017) peker videre på den negative filtreringen som foreslås i DGF-systemet. De stiller seg blant annet spørrende til hvorfor behovet for filtrering og lagring av informasjon i korttidslageret oppstår i utgangspunktet. Den negative filtreringen innebærer at det på forhånd spesifiseres hva som skal filtreres bort, og det er her korttidslageret skal anvendes for å kunne vedlikeholde og oppdatere filtrene. I kortidslageret vil imidlertid ikke informasjon om kommunikasjon som krysser landegrensen filtreres bort og på den måten vil dette lageret inneholde store mengder meta- og innholdsdata. Paradokset er at DGF-systemet legger opp til etablering av et lager som inneholder mer detaljerte opplysninger og informasjon enn det som forsøkes korrigert. Selv om korttidslageret skal inneholde korte tidsintervaller med informasjon, så vil lageret inneholde betydelige mengder ufiltrert informasjon om norske borgeres kommunikasjon. Konsekvensen av dette vil i så måte bety at all informasjon i prinsippet vil samles inn gjennom DGF-systemet. Det vil også bety at hver enkelt borger må ta utgangspunkt i at alt kan bli overvåket og sett av personell i E-tjenesten (Datatilsynet, 2017: 8-9).

6.2.3 Andre momenter og tidligere eksempler

Organisasjoner med høy sikkerhetskompetanse er ikke fritatt for at det kan forekomme eller gjøres feil. I 2010 ble ulike opplysninger om ansatte i Forsvaret og E-tjenesten gjort tilgjengelige for et betydelig antall personer ansatt i den offentlige forvaltningen. Eksempelet illustrerer at det alltid vil kunne finnes en risiko for at sikkerhetsrutiner kan svikte (Schartum, 2010: 35).

I 2014 ble EOS-utvalget varslet om at E-tjenesten hadde foretatt ulovlig overvåking av en norsk person som befant seg i Norge. Årsaken til avviket var at E-tjenestens systemer ikke hadde stoppet innsamlingen. Videre kritiserte EOS-utvalget samarbeidet og informasjonsflyten mellom E-tjenesten og PST i tilknytning til en annen sak der det var mistanke om at E-tjenesten drev fordekt informasjonsinnhenting om en norsk person i Norge.

Kritikken rettet seg blant annet mot at PST hadde varslet E-tjenesten om at den aktuelle personen hadde returnert til Norge, men at dette ikke umiddelbart hadde ført til at innsamlingen hadde opphørt (EOS-utvalget, 2015: 40-41). I følge en avisartikkel fra Aftenposten (Færaas, 30.04.2015) bekrefter EOS-utvalgets leder, Eldbjørg Løwer, at utvalget for første gang hadde avdekket slike lovbrudd. Dette var trolig knyttet til utvalgets enklere tilgang til å selv kunne undersøke hva E-tjenesten gjør. E-tjenesten selv understreker at oppdraget var lovlig da det ble innhentet informasjon utenlands, men at innhentingen ved en feil ikke ble avsluttet idet vedkommende returnerte til Norge. Feilen forklares som en uheldig menneskelig feil (Færaas, 30.04.2015). Eksemplene kan bidra til å illustrere hvordan det kan oppstå feil i systemet selv om det er etablert tilsynelatende gode rutiner og et styrende lovverk for å regulere virksomheten. Ved å dra eksemplene videre til DGF kan det tenkes at lignende feil kan skje også her. Det er etterretningspersonell som til syvende og sist skal behandle og gjøre vurderinger av informasjon som kan karakteriseres som svært sensitiv. Samtidig kan denne informasjonen mistolkes eller vurderes feilaktig, og dermed føre til ulovlig overvåking. At tilsynsmyndighetene oppdager avvik er bra, men avvikene er også en indikasjon på at noe som ikke skal skje har skjedd. Spørsmålet videre blir derfor hvorvidt samfunnet kan tolerere at det kan gjøres slike feil hvor E-tjenesten og deres etterretningspersonell får tilgang til og behandler sensitiv og privat informasjon på ulovlig grunnlag.

I et annet tilfelle ble det utført tilsyn av E-tjenestens arkiver i forbindelse med en klagesak. E-tjenesten meldte om at det ikke var funnet noen registreringer om klageren i deres arkiver eller registre. I EOS-utvalgets egne undersøkelser derimot, ble det registrert syv treff i E-tjenestens datasystemer. E-tjenesten beklaget hendelsen og forklarte at årsaken lå i rettighetene til etterretningspersonellet som utførte søkene. Personellet hadde ikke tilstrekkelige tilgangsrettigheter til de datamappene hvor dokumentene om klageren befant seg (EOS-utvalget, 2015: 41). Dette eksempelet viser at selv kontrollmekanismene kan ha svakheter. Det viser også at tilsynsmyndighetene fungerer som et kontrolltiltak ved at ulike avvik oppdages, men at det samtidig eksisterer hull som tilfeldigvis kan føre til at feil eller avvik ikke blir oppdaget. En annen bemerkelse som ble gjort i forbindelse med EOS-utvalgets årsmelding (2015) var E-tjenestens rutiner for sletting av informasjon som ikke lenger anses for å være relevant for virksomhetens formål og oppdrag. Det kom frem at det var etablert interne retningslinjer for sletting av informasjon i ulike informasjonssystemer, men at det samtidig var noe uklarhet knyttet til hvordan E-tjenesten konkret sikrer at de ikke behandler

informasjon og personopplysninger som ikke lenger er relevant eller nødvendig med tanke på formålet med behandlingen (EOS-utvalget, 2015: 40). Dette kan tyde på at det til tross for retningslinjer, lover og praksis for sletting, vil kunne avhenge av skjønnsvurderinger for hvorvidt informasjon anses for å være relevant eller ikke. I neste omgang kan det tenkes at det fører til urettmessig lagring av informasjon som for E-tjenesten blir vurdert som relevant. Det kan også hende at irrelevant informasjon lagres med tanke på at informasjonen blir vurdert som mulig aktuell på et senere tidspunkt. I forhold til DGF kan man møte på de samme utfordringene. I henhold til Lysne II-rapporten (2016) kommer det frem at det behøves lagring over en viss tid for å kunne danne et bilde av hva som faktisk er relevant informasjon eller ikke. Videre er rapporten tydelig på at de ulike lagrene i DGF systemet vil inneholde betydelige mengder data som hverken er relevant for formålet eller i tråd med lovverket som tilsier at E-tjenesten ikke kan drive overvåking eller innhenting av informasjon om norske juridiske eller fysiske personer.

De ulike eksemplene underbygger påstanden om at det alltid er en fare for at svikt eller feil kan oppstå. Schartum (2010) peker på at det ikke er mulig å helgardere seg, og at ingen overvåkingsmetoder vil kunne være fritatt fra potensielle sikkerhetssvikt. I et sårbarhetsperspektiv vil det derfor være viktig å ta stilling til de ulike vilkårene for å kunne innhente informasjon utover det som tåler å bli eksponert eller utsatt for illegitim overvåking. I tillegg vil et sentralt spørsmål knyttet til overvåking være hvordan den innsamlede informasjonen skal sikres (Schartum, 2010: 35). Dette innebærer at det ikke kan garanteres total beskyttelse og feilfri drift eller bruk av DGF-systemet, og de ulike usikkerhetsmomentene må tas i betraktning for å helhetlig kunne vurdere DGF opp mot samfunnssikkerheten. Spørsmålet blir om samfunnet eventuelt kan tåle materialiseringen av ulike risikoer knyttet til DGF. Enten det dreier seg om internt misbruk, sikkerhetssvikt, ytre risikoer, fremmed etterretning eller cyberangrep. Dette momentet er også knyttet til hvorvidt DGF vil representere en sårbarhet i seg selv dersom systemet fremstår som et attraktivt mål for angrep eller kontraspionasje.

6.3 Hvilke samfunnsfunksjoner og verdier kan påvirkes ved etablering av DGF?

I dette kapittelet analyseres ulike sentrale momenter knyttet til samfunnsfunksjoner, kritisk infrastruktur, og samfunnsverdier som personvern, rettssikkerhet og tillitt. Disse elementene oppfattes som særlig relevante knyttet til overvåking slik det fremkommer gjennom det teoretiske og empiriske utgangspunktet for studien.

6.3.1 Samfunnsfunksjoner

På mange måter kan ivaretakelsen av kritiske infrastrukturer og samfunnsfunksjoner anses for å være en viktig del av begrepene rikets sikkerhet og nasjonale interesser (NOU 2006:6, 2006: 35). I Lysne II-utvalgets rapport (2016) fremstilles DGF som et viktig verktøy som E-tjenesten skal kunne bruke nettopp for å ivareta rikets sikkerhet og interesser. Spørsmålet vil dermed kunne sies å være hvorvidt DGF er nødvendig og kan bidra til å ivareta hensyn til rikets sikkerhet og interesser. DGF kan anses som en infrastruktur som skal bidra til å ivareta samfunnsfunksjonen forsvar og sikkerhet, for å verne om borgernes trygghet. Ved å anse DGF som en infrastruktur kan kritikaliteten av DGF vurderes ut fra de ulike retningslinjene som handler om avhengighet, alternativer og tett kopling.

DGF vil i utgangspunktet ikke tolkes for å ha stor grad av avhengighet. Det vil si at andre infrastrukturer og samfunnsfunksjoner ikke er avhengig av DGF for å fungere. Et annet spørsmål vil kunne dreie seg om hvorvidt E-tjenesten er avhengig av DGF for å kunne utføre sine arbeidsoppgaver. E-tjenesten selv uttrykker i Lysne II-utvalgets rapport (2016) et behov for å kunne overvåke kommunikasjonen som krysser grensen i de fiberoptiske kablene for å kunne drive effektiv etterretning. I tillegg påpeker E-tjenesten at DGF vil kunne bidra til at Norge blir mindre avhengig av andre lands etterretning. Samtidig vil ikke E-tjenestens funksjonalitet i så stor grad avhenge av DGF at de mister evnen til å utføre sine oppdrag dersom DGF ikke etableres. E-tjenesten har også andre metoder og muligheter for å drive etterretning. Dette handler om den neste retningslinjen som viser til alternativer. Det fremkommer av Lysne II-utvalgets rapport (2016) at E-tjenesten har behov for DGF, samtidig som det påpekes at E-tjenesten har flere ulike etterretningsmetoder.

Dermed kan det tolkes slik at det finnes andre alternativer for DGF, men samtidig kommer det frem i Lysne II-utvalgets rapport (2016) at E-tjenesten ikke har tilsvarende metoder for å kunne overvåke kommunikasjon, og da spesielt gjennom bulk-aksess slik DGF vil legge opp til. Det finnes imidlertid andre overvåkingsverktøy som kan anvendes for å oppdage eller avverge cyberangrep. NOU 2015:13 (2015) peker blant annet på varslingssystem for digital infrastruktur (VDI), som er et eksempel på et system hvor sensorer plasseres ut i nettverket for å inspisere inn- og utgående datatrafikk. Sensorene fungerer som et slags antivirus, og kan enten operere passivt ved å detektere angrep, eller aktivt gjennom å forsøke å stoppe angrepet. Et annet alternativ for å oppdage og avverge cyberangrep kan være å opprette lokkeduer («honeypots»). Strategien går ut på å etablere falske ressurser som vil fremstå som attraktive for innbrytere, for deretter å følge med eller overvåke lokkeduene (NOU 2015:13, 2015: 38). Med dette kan det argumenteres for at kritikaliteten og nødvendigheten av DGF reduseres ved at det finnes andre alternativer for å detektere og avverge cyberangrep.

Den siste retningslinjen handler om koplingen i systemet. I følge NOU 2006:6 (2006) vil eksempler på tett koplede systemer være lufttrafikk og jernbane, hvorpå bortfall på et sted i systemet vil kunne få konsekvenser for systemet som helhet. Hvorvidt DGF vil vurderes som tett koplet vil avhenge av hvordan den tekniske innretningen ser ut. Aven et al. (2004) peker generelt på at integreringen og koplingen mellom de ulike IKT-systemene fører til at det blir vanskeligere å utvikle, teste og evaluere systemene isolert eller på lokalt nivå. Videre kan det for eksempel tenkes at feilvurderinger av domstolene, eller tekniske problemer med datafiltrene kan skape utfordringer for DGF-systemet i den forstand at det ikke fungerer slik det er tenkt. Videre vil alvorligheten av eventuelle feil eller bortfall av deler i systemet avhenge av konsekvensene. Dersom en feil fører til at det ikke blir innhentet informasjon fra fiberkablene over en viss tid, vil dette kunne tolkes for å være en alvorlig feil som truer funksjonaliteten i systemet. Men samtidig vil ikke konsekvensene tolkes for å være større enn at E-tjenesten mangler noe data i datalagrene. På den andre siden kan feil som fører til at det foretas ulovlig overvåking eller at data kommer på avveie, vurderes for å være alvorlig. Spesielt med tanke på lovreguleringene knyttet til overvåkingen, samt E-tjenestens behov for tillitt blant befolkningen for å i det hele tatt kunne drive overvåking gjennom DGF.

Datatilsynet (2017) peker på at det kan være en fare for at kommunikasjon kan bli tatt ut av sammenheng og dermed fremstå som mistenkelig. Dermed kan det tolkes slik at DGF-systemet skaper nye sårbarheter i samfunnet, ved at det foreligger en risiko for mistolking av informasjonen eller dataene. Spørsmålet vil være hva som eventuelt blir konsekvensene av at E-tjenesten agerer på noe som ikke er reelt, men basert på misforståelser eller mistolking av informasjon.

Som en samfunnsfunksjon kan det argumenteres for at DGF på den ene siden kan bidra til å ivareta borgernes trygghetsfølelse. DGF kan øke trygghetsfølelsen i form av systemets formål som handler om å beskytte samfunnet og verne om nasjonale interesser. På den andre siden kan DGF også utfordre trygghetsfølelsen, fordi systemet kan oppfattes som invaderende eller tolkes som et verktøy for myndighetenes behov for kontroll. Selv om DGF ikke skal være rettet mot fysiske eller juridiske norske personer, er Lysne II-utvalgets rapport (2016) tydelig på at store mengder data om norske borgere vil innhentes og lagres i systemet.

6.3.2 Grunnleggende samfunnsverdier

I et demokratisk samfunn vil ivaretakelse av rettsstatlige prinsipper og menneskerettigheter være viktige forutsetninger for å i det hele tatt kunne akseptere overvåking av borgerne. Et usikkerhetsmoment vil dermed kunne sies å være knyttet til fremtidige samfunnsendringer, hvor disse hensyn og garantier svikter eller ikke lenger er gjeldende. Økonomisk krise, terrortrussel, opptøyer og sosial uro kan være eksempler på situasjoner eller hendelser som kan påvirke samfunnet, enten de foregår i Norge eller andre steder i verden (Schartum, 2010: 34-35).

På mange måter kan det argumenteres for at informasjonssamfunnet selv har lagt til rette for at fremmede, og eventuelt fiendtlige, stater eller politiske grupperinger kan overvåke norske borgere (Schartum, 2010: 35). Spørsmålet i denne forbindelse vil dermed rette seg mot om dette kan fungere som legitime argumenter for å godta at norske myndigheter også skal kunne drive overvåking av norske borgere slik DGF mer eller mindre vil kunne legge opp til.

I tråd med demokratiske prinsipper kan dilemmaer knyttet til samfunnssikkerhet imøtekommes gjennom institusjonalisering av prosedyrer og regler for hvordan effekten av nye tiltak skal vurderes. Tiltak som implementeres for å styrke sikkerheten kan således evalueres etter en viss tid, for deretter å fatte beslutninger om å beholde eller forkaste tiltaket basert på effekten (Engen et al., 2016, 392). En utfordring med dette knyttet til DGF kan være tilgang og åpenhet i forhold til E-tjenestens arbeid. Det vil trolig være problematisk å vurdere effekten av DGF, fordi E-tjenestens arbeid og virksomhet er underlagt hemmelighetsklausuler. Det kan tenkes at effekten av DGF, i form av hvorvidt tiltaket fungerer som tiltenkt formålet, kan være vanskelig å vurdere gjennom åpne demokratiske prosesser. Dermed vil også den eventuelle innvirkningen som DGF kan ha overfor personvernet vanskelig måles eller debatteres offentlig. Demokratisk sett kan dette være en utfordring, fordi det rokker ved elementære demokratiske verdier som personvern, deltakelse, åpenhet og frihet. Verdier som også er en del av samfunnssikkerheten.

Det årlige prioriteringsdokumentet som Forsvarsdepartementet utgir, legger føringer for E-tjenestens arbeid og fokus. Dette dokumentet er gradert, og oppdateres gjennom kontinuerlig dialog (Lysne II-utvalget, 2016: 18). Dette er et interessant moment knyttet til E-tjenestens hemmelige arbeid, og vil potensielt sett stå i et slags motsetningsforhold overfor samfunnsverdier og demokratiske prinsipper som åpenhet og tillitt. Datatilsynet (2017) peker på at det er uklarheter om hva som skal være styrende for bruken eller begrensningene av DGF-systemet. Både E-loven og de årlige politisk bestemte etterretningsformålene tilsier at DGF-systemet vil kunne favne svært bredt (Datatilsynet, 2017: 16).

6.3.2.1 Personvern

Koplingen mellom personvern og overvåking vil på mange måter kunne sies å stå i et spenningsfelt til hverandre. På den ene siden står personvernet og en nærmest ukrenkelig rett til å selv kunne råde over egne personopplysninger. På den andre siden står myndighetenes behov for tilgang til mest mulig personopplysninger for å kunne beskytte samfunnet og enkeltindivider. I forhold til menneskerettighetene vil personvernet dreie seg om retten til et privatliv, mens myndighetenes beskyttelse- og sikkerhetsansvar kan handle om å ivareta retten til liv (NOU 2015:13, 2015: 28).

E-tjenestens virksomhet er tidkrevende, og forutsetter at oppbevaring og analyse av informasjon foregår i henhold til et langsiktig perspektiv. For å danne et bilde av normalsituasjonen kreves det en langvarig opparbeidelse av informasjon. Forståelsen av normalsituasjonen er vesentlig for å blant annet kunne identifisere avvik. DGF vil samtidig kunne representere en svært personverninngripende metode for overvåking (Lysne II-utvalget, 2016: 19, 52). Dermed kan DGF oppfattes som en kontrast til prinsippene om personvern. Fordi informasjonen som lagres ikke bare er hemmelig, men også lagres over veldig lang tid. Det fremkommer i tillegg av Lysne II-utvalgets rapport (2016) at det historisk sett er gitt prioritet til dokumentasjonshensyn, fremfor å slette informasjon som ikke er relevant. Videre er etterretningsvirksomheten mer informasjonsorientert enn den er personorientert. Det viktigste er å kunne innhente relevant informasjon for utenlandsetterretningen. Dette innebærer at det i utgangspunktet er irrelevant hvorvidt personer som det innhentes informasjon om har gjort noe straffbart eller ikke. Videre har etterretningsvirksomheten lav terskel for å bearbeide usikker informasjon i tråd med målutviklingsformålet (Lysne II-utvalget, 2016: 19-20).

Dette kan bety at E-tjenestens innsamling av metadata gjennom DGF står i et motsetningsforhold til prinsippene om både formålstjenlighet og personvern. Selv om E-tjenesten ikke nødvendigvis gis innsyn i all data, innebærer DGF lagring av betydelige mengder informasjon som i utgangspunktet ikke er relevant for etterretningsvirksomheten. I tillegg vil tidsperspektivet tilsi at dette vil kunne dreie seg om data som på sikt vil kunne hentes frem ved behov. Spesielt kritisk vil dette være dersom kontrollmekanismene overfor E-tjenesten har begrenset innsyn, og virksomhetens praksis reguleres gjennom egne behovsstyrte internkontroller og prosedyrer. Den interne virksomheten i E-tjenesten kan gjerne sørge for at E-tjenesten opererer innenfor de fastlagte lover og reguleringer, men det kan være problematisk dersom lovverket er uklart og åpner opp for tolkning, samt at kontrollmyndighetene ikke har en fullstendig oversikt eller tilgang til virksomheten. I tillegg peker Datatilsynet (2013) på utfordringene som innsamling av store mengder data representerer i forhold til dataminimering. Prinsippet om dataminimering handler om at det ikke skal samles inn mer data enn det som er nødvendig for å imøtekomme formålet. Således vil metadata kunne sies å være problematisk sett opp mot personvernprinsipper (Datatilsynet, 2013: 25).

6.3.2.2 Kommunikasjonsvern

Kommunikasjonsvernet handler om å verne om personers kommunikasjon og sørge for at den holdes privat. Ved inngrep i kommunikasjonsvernet skal det stilles strengere krav til dokumentasjon av behovet og effektiviteten av de aktuelle tiltakene som iverksettes med hensyn til kriminalitetsbekjempelse og etterretning. Nye tiltak som er inngripende overfor kommunikasjonsvernet, skal også vurderes med hensyn til mengden av de samlede tiltakene som berører kommunikasjonsvernet (Nasjonal Kommunikasjonsmyndighet, 2015: 69). Ved å tillate myndighetene lagring eller tilgang til kommunikasjonen mellom mennesker, vil dette kunne utgjøre et demokratisk problem i den forstand at det kan legge begrensninger på måten det kommuniseres på. Det fremstår gjerne i tillegg som uoversiktlig hvilken informasjon og i hvilke tilfeller denne informasjonen potensielt sett blir fanget opp av DGF-systemet. Det er tilsynelatende vanskelig og komplekst å ha en fullstendig oversikt over hvor informasjonen i fiberkablene til enhver tid «reiser» og dermed vanskelig å vite når kommunikasjon eventuelt krysser grensen eller ikke. I forlengelse av dette vises det til at store deler av den fiberoptiske kommunikasjonen krysser grensen via Sverige, hvor også kommunikasjon mellom norske fysiske eller juridiske personer foregår.

Det er viktig for myndighetene å ivareta befolkningens tillitt til Internett. Det er en forutsetning for utviklingen av Internett og internettbaserte tjenester at det leveres med fokus på stabilitet og sikkerhet. Samtidig skal det sikres at Internett består som en åpen og tilgjengelig arena for samfunnsøkonomisk vekst og sosial utvikling. En utfordring på dette området er at det ikke foreligger bindende internasjonale avtaler som kan bidra til å regulere utviklingen av Internett på det nasjonale nivået. I tillegg eksisterer det en viss skepsis mot myndighetsinnflytelse når det gjelder utviklingen av Internett (Nasjonal Kommunikasjonsmyndighet, 2015: 39). Blant annet fordi Internett er blitt en sentral arena for tilgang til informasjon, effektiv kommunikasjon, meningsutveksling og mulighet for frie ytringer (NOU 2015:13, 2015: 26). Det kan argumenteres for at DGF kan påvirke tillitten til Internett og endre Internett som en arena for sosial og demokratisk utfoldelse og utvikling. Richards (2013) argumenterer for at myndighetenes overvåking av Internett kan være svært skadelig. Han forklarer at en slik intellektuell form for overvåking, som fanger opp menneskers kommunikasjon, hva de leser og hva de tenker, vil begrense menneskenes demokratiske friheter. Fordi det fører til at folk ikke vil eksperimentere med nye eller kontroversielle ideer samt politiske og sosiale problemstillinger (Richards, 2013: 1935).

Ifølge Datatilsynet (2013) vil myndigheters overvåking gjennom Internett kunne føre til en såkalt nedkjølingseffekt overfor viktige samfunnsverdier. Dersom sporene som etterlates via bruk av Internett fanges opp og benyttes til andre og ukjente formål, kan dette føre til at det legges bånd på hvordan befolkningen deltar i samfunnet. Blant annet kan det tenkes at utstrakt bruk av metadata kan ha en nedkjølingseffekt på ytringsfriheten som er en viktig demokratisk samfunnsverdi. Dersom det i tillegg er uklart hvordan myndighetene bruker disse sporene eller dataene kan det svekke tillitten til myndighetene. Hemmelighold rundt E-tjenestens virksomhet og bruk av dataene vil dermed kunne være problematisk. Spesielt dersom datakildene for innsamling og bruken av disse dataene er skjult. Dette kan være utfordrende både for ulike personverninteresser og for det demokratiske fundamentet for et åpent og velfungerende samfunn (Datatilsynet, 2013: 5, 29).

6.3.2.3 Rettssikkerhet

Funksjonen til menneskerettighetene, og særlig personvernet, kan argumenteres for å ha gått fra å være noe som begrenset myndigheters kontroll til å bli en tilrettelegger for mer inngripende kontroll og overvåking. Det har oppstått en slags glidning av begrepet beskyttelse, hvor beskyttelse ikke lenger primært sett handler om å beskytte personer mot staten, men hvor staten går inn for å beskytte potensielle ofre mot potensiell kriminalitet. Derav har staten og myndighetene i større grad blir en aktør som skal sørge for å ivareta borgernes rett til beskyttelse mot kriminalitet. Denne beskyttelsen foregår vanligvis gjennom lovgivning og rettsforfølgelse. Samtidig er det blitt et større fokus på forebygging av kriminalitet eller uønskede hendelser. Politiet har for eksempel en plikt til å forebygge og avverge kriminalitet. Spørsmålet videre blir således hvor langt prinsippene bak forebygging kan strekkes (Lomell, 2014: 45-47). Ved å handle på usikkert grunnlag, for å være på den sikre siden, skapes det gjerne noen negative konsekvenser i tillegg. Blant annet kan sikkerhetstenkning og føre-var-prinsippet snu om på rettsstatsprinsipper hvor tvilen nå skal komme offeret til gode. Byrden av usikkerhet plasseres på den tiltalte eller potensielt kriminelle, som dermed blir ansett for å være skyldig til det motsatte er bevist. Det anses som et uakseptabelt premiss å for eksempel skulle la tvilen komme en potensiell terrorist til gode. Fokuset rettes således mot å hindre et terrorangrep ved å stoppe det allerede i planleggingsstadiet. Ved å la tvilen komme den potensielle terroristen til gode og dermed vente til vi er på den sikre siden, kan det være for sent. I lys av føre-var-prinsippet og

sikkerhetstenkningen endres dermed strafferetten fra å være reaktiv til å bli pre-aktiv. Usikkerhet knyttet til om planer eller forberedelser faktisk leder til en fullbyrdet ugjerning må komme samfunnets sikkerhet og potensielle ofte til gode, ikke de potensielle gjerningspersonene. Samtidig bidrar dette til å svekke respekten overfor enkeltindividers moralske autonomi. Det vil si at det ikke gis rom for avveininger omkring hvorvidt den potensielle gjerningspersonen av en eller annen grunn kan komme til å ombestemme seg. Å vurdere om en handling vil begås, er fundamentalt forskjellig fra vurderingen av en handling som allerede har blitt begått. Dette nærer opp om spørsmål knyttet til om det er ønskelig med et samfunn hvor strafferetten ikke gir rom for at det er mulig å skifte mening (Lomell, 2014: 53-55). Ikke minst kan det også være usikkerhet knyttet til om systemene, i dette tilfellet DGF, tar feil.

Det ligger gjerne en utfordring mellom de ulike hensynene innen overvåking og rettsstaten. Blant annet vil prinsippet om forutberegnelighet stå i et slags motsetningsforhold til overvåking. Ofte vil det være et poeng i seg selv at overvåkingen foregår ved hjelp av skjulte metoder, slik at den som overvåkes ikke har kunnskap om det. Årsaken til at gjennomføringen foregår skjult er at vedkommende ikke skal kunne innrette seg på en slik måte at det svekker overvåkingens effektivitet. Samtidig kan dette være problematisk i forhold til forutberegneligheten som tilsier at inngrepet skal være relativt kjent. En aktuell løsning vil kunne være at vilkårene og hjemlene for overvåkingen skal være tydelige og tilgjengelige. På den måten får borgerne innsikt i, og kan forholde seg til de ulike rammebetingelsene for overvåkingen (Bruce & Haugland, 2010: 71).

I forhold til DGF kan det argumenteres for at vilkårene og rammene for overvåkingen fremstår som relativt klare. Lysne II-utvalgets rapport (2016) bidrar til å tydeliggjøre hvordan DGF er tenkt implementert, samt hvordan systemet skal fungere og anvendes. Blant annet kommer dette frem gjennom de ulike vilkårene og kontrollmekanismene som skal regulere DGF-systemet. Til tross for at rammene rundt DGF fremstår som klare, kan det tolkes slik at det vil være utfordrende å skulle forutse når, og i hvilke tilfeller, borgernes data vil bli fanget opp og overvåket. Årsaken er at det er vanskelig å kartlegge og forutse hvor datastrømmene vil gå i hvert enkelt tilfelle. For eksempel vil bruken av ulike tjenester som går gjennom fiberkabler noen ganger føre datastrømmene innenlands, mens den andre ganger vil krysse

landegrensen for å nå dataservere som står i utlandet. På den måten kan det være usikkerhet knyttet til når og i hvilke tilfeller DGF vil gjøre seg gjeldene, selv om rammene rundt systemet fremstå som relativt klare. Datatilsynet (2017) viser til det de kaller for «to ledd ut» prinsippet, som handler om at den man kommuniserer med, igjen kan kommunisere med noen som E-tjenesten overvåker eller har interesse for. Hvem dette eventuelt gjelder vil være umulig å vite, noe som dermed kan bidra til å øke nedkjølingseffekten fordi folk begrenser sin kommunikasjon i frykt for å bli fanget opp i DGF-systemet (Datatilsynet, 2017: 15). Denne frykten kan også forsterkes gjennom E-tjenestens arbeidsmetoder hvor det blant annet anvendes ulike inngangsparameter for å igangsette videre undersøkelser. I verste fall kan det føre til at norske personer feilaktig settes under E-tjenestens overvåking. Spørsmålet vil i så måte handle om hvorvidt dette er en risiko som samfunnet kan akseptere, både med tanke på rettsstatlige prinsipper og tillitsforholdet mellom myndighetene og borgerne.

En annen rettsstatlig utfordring er knyttet til at myndighetene potensielt gis tilgang til store mengder data om egne borgere uten at dette i forkant er basert på mistanke eller konkrete sikkerhetsbekymringer (Lysne II-utvalget, 2016: 64). Dette kan blant annet stå i kontrast til det rettsstatlige prinsippet om dataminimering som handler om at det ikke skal samles inn mer data enn det som er nødvendig. I følge NOU 2015:13 (2015) er digital kommunikasjon blitt en viktig forutsetning for samfunnet og demokratiet. Dermed vil DGF også kunne sies å ha noen utfordrende momenter i henhold til både rettsstatlige og demokratiske prinsipper. Ifølge Datatilsynet (2017) vil også samarbeidet mellom E-tjenesten og PST kunne føre til utglidninger for formålet og bruken av DGF. Informasjon som anses for å være overskuddsinformasjon vil etter reguleringen og kontrollmekanismene i DGF-systemet slettes. Informasjon som er av felles interesse kan imidlertid deles med PST gjennom deres ulike samarbeidsordninger, som blant annet gjennom Felles Kontraterrorsenter. Selv om informasjonen ikke kan anvendes som bevis i straffesaker, kan PST for eksempel bruke informasjonen som en inngangsverdi for egen etterforskning (Datatilsynet, 2017: 17). Samtidig skal ikke E-tjenesten kunne samle inn informasjon etter ønske eller anmodning fra andre myndigheter, uten at dette har et utenlandsetterretningsformål (Lysne II-utvalgets rapport, 2016: 61). Dette kan således tolkes slik at E-tjenesten kan foreta søk etter initiativ fra andre myndigheter, så lenge søket også kan forsvares utfra E-tjenestens eget formål (Datatilsynet, 2017: 17). Hva som vil defineres for å være et utenlandsetterretningsformål kan være både uklart og samtidig favne svært bredt. Dersom informasjon fra DGF i tillegg kan

deles med PST gjennom deres samarbeidsordninger, vil det kunne argumenteres for at DGF-systemet kan sies å ha en utfordring i forhold til rettsstatens rammer.

Videre kan det også stilles spørsmål om hvorvidt samfunnet kan godta at det for eksempel finnes konkret informasjon og bevis for alvorlig kriminelle handlinger, som likevel ikke kan brukes til å stille skyldige til ansvar (Datatilsynet, 2017: 19). Politiets sikkerhetstjeneste (2017) mener det vil være uheldig å legge en slik begrensning på potensielle bevis i tilknytning til terrorhandlinger som gjør at informasjon fra DGF ikke kan anvendes til straffeforfølgning. De peker på at staten har et sikkerhetsansvar overfor befolkningen, og dersom disse forventningene ikke imøtekommes kan det få uheldige konsekvenser for rettsstaten (Politiets sikkerhetstjeneste, 2017: 3). Denne problemstillingen er noe som på sikt kan lede til at bruksområdet for DGF utvides, og man får en formålsutglidning av systemets bruksområde og nedslagsfelt (Datatilsynet, 2017: 19).

6.3.2.4 Tillitt

En eventuell innføring av DGF vil i tråd med norske demokratiske hensyn kreve at befolkningens tillitt til myndighetene ivaretas. I tillegg er det viktig at DGF ikke vil påvirke den offentlige debatt og borgernes søken etter informasjon (Lysne II-utvalget, 2016: 52).

I følge Hammerlin (2014) vil den digitale overvåkingsinfrastrukturen innebære en maktforskyvning i relasjonen mellom borger og myndighet. Denne maktforskyvningen kan bidra til å undergrave grunnleggende tillitsrelasjoner i et liberalt demokrati. Den demokratiske samfunnsmodellen og rettsstatlige prinsipper er med på å sette grenser for myndighetens mulighet til å overvåke og kontrollere sine borgere. Uten konkrete mistanker om straffbare forhold er borgernes rettigheter mot vilkårlig maktbruk beskyttet gjennom prinsippene knyttet til rettsstaten og personvernet. Dette er også viktige aspekter knyttet til demokratiske prosesser og myndighetenes legitimitet. Myndighetenes kontroll og overvåkingsmulighet mot egne borgere bør begrenses på bakgrunn av at det kan påvirke de ulike prosessene som bidrar til å forme samfunnet. Disse prosessene handler om borgere som deltar i samfunnet og bidrar til å skape meningsmangfold (Hammerlin, 2014: 76).

Begrensninger på myndighetenes mulighet for å overvåke egne borgere handler på mange måter om tillitt, og da i form av borgernes mistillit til myndighetene. Det finnes en risiko for at myndighetene kan misbruke sine maktmidler, og derfor må det settes grenser for hvordan myndighetene legitimt kan anvende dem. I tillegg handler det om tillitten som myndighetene må utvise overfor borgerne, der myndighetene ikke skal ha full innsikt og kontroll over borgerne. Potensiale i den digitale overvåkingen vil kunne snu om på denne tillittsrelasjonen mellom borgere og myndigheter. For det første vil myndighetenes potensielle maktmisbruk ikke lenger være relatert til borgernes mistillit, men knyttes opp mot borgernes tillitt til at myndighetene ikke misbruker sin makt. I forbindelse med overvåking handler dette om en tillitt til at dataene ikke brukes til noe annet enn det som er formålet. Motsatt vil myndighetenes tillitt til borgerne erstattes med mistillit. Det kan tolkes slik at den brede metoden for overvåking implisitt betrakter alle som potensielle terrorister (Hammerlin, 2014: 77). Når det gjelder DGF så vil ikke overvåkingen være rettet mot norske juridiske og fysiske personer. Dermed kan det argumenteres for at graden av tillitt mellom borger og myndighet ikke vil berøres eller påvirkes av etableringen av DGF. E-tjenesten har også begrensede muligheter til å utøve makt overfor egne borgere, da dette feltet skal dekkes av politimyndighetene. Samtidig kommer det frem at innsamlingen av data vil inneholde informasjon som også omhandler norske personer. Dermed kan det sies at spørsmålet om tillitt aktualiseres gjennom borgernes tillitt til at data som ikke faller inn under E-tjenestens virkeområde blir brukt eller misbrukt. Videre kommer det frem i Lysne II-utvalgets rapport (2016) at E-tjenesten, etter godkjenning av PST, kan iverksette overvåking av norske personer. I tillegg kan E-tjenesten utlevere informasjon til andre samarbeidsland, hvor utveksling av informasjon er en sentral del av samarbeidet (Lysne II-utvalget, 2016: 15). Dette kan bidra til å komplisere tillitsbildet ytterligere, fordi det ikke vil være kjent eksakt hvilken informasjon som overvåkes og heller ikke hvorvidt den eventuelt utleveres til andre lands etterretningstjenester.

På den andre siden kan DGF representere myndighetenes mistillit til borgerne, i og med at all datatrafikk som krysser grensen vil overvåkes. Igjen pekes det på at overvåkingen ikke skal gjelde for norske personer, men at den er rettet mot informasjon som er relevant for utenladsetterretningen. Dermed kan det sies at myndighetenes metode for makt og kontroll gjennom overvåking av borgerne, ikke er gjeldende i tilfellet med DGF, fordi dette ikke handler om overvåking av norske personer. Selv om E-tjenesten ikke vil overvåke norske

personer, så vil innsamlingen av all informasjon som krysser grensen også innebære at betydelig mengder data om norske personer fanges opp av DGF-systemet. Dermed kan det likevel argumenteres for at myndighetenes tillitt til borgerne er en aktuell variabel i tilknytning til DGF, da overvåkingen indirekte rammer norske juridiske og fysiske personer. I den sammenheng kan det også stilles spørsmål om den videre åpenheten omkring DGF og effekten av overvåkingssystemet etter at det eventuelt er etablert. Det var blant annet viktig for myndighetene at rapporten som tar for seg DGF, samt den politiske behandlingen om etableringen av DGF ble gjort tilgjengelig for offentligheten. Derfor kan det også være viktig å diskutere hvordan åpenheten om DGF vil være i fremtiden, for å forsøke å bevare eller ivareta tillitten både til systemet i seg selv og E-tjenestens virksomhet. Et spørsmål kan for eksempel dreie seg om hvorvidt det vil være åpenhet omkring effekten av DGF, og om systemet viser seg å fungere slik det er tiltenkt. Mer konkret kan dette handle om hvorvidt DGF har bidratt til å avverge angrep eller styrke samfunnssikkerheten. Hensynet til disse spørsmålene kan også være aktuelle i tilknytning til aspektene om tillitt.

Norge anses for å være et land med høy grad av tillitt, både mellom borgerne og myndighetene og borgerne seg imellom (Hammerlin, 2014: 78). Denne tillitten bør likevel ikke tas for gitt, da samfunnet og verden stadig endrer seg. I følge Engen et al. (2016) vil tillitt være basert på erfaringer som bygger seg opp over tid. De ulike aktørene og virksomhetene som arbeider med samfunnssikkerhet må derfor kontinuerlig validere sitt arbeid og forsikre om at de er kapable til å løse oppgavene de har ansvar for (Engen et al., 2016: 49). Et spørsmål kan være hvordan tillitten til myndighetene påvirkes dersom DGF etableres og det likevel oppstår terrorangrep mot Norge. Vil det for eksempel være åpenhet om hvorfor systemet ikke klarte å innhente informasjon som kunne stoppet angrepet? Eller vil et slikt scenario kanskje være et insentiv for å intensivere overvåkingen og utvide fullmaktene og den virksomheten som er relatert til DGF-systemet slik trenden ofte har vist seg å være i etterkant av terrorangrep. Engen et al. (2016) forklarer videre at det er vanskelig å bygge opp tillitt, på samme tid som tillitt enkelt kan la seg rive ned. Derfor bør også tillitt inkluderes som en sentral variabel som må vurderes, på samme måte som for eksempel kriteriet om funksjonalitet, for å ivareta og opprettholde samfunnssikkerheten (Engen et al., 2016: 49).

Lysne II-utvalget hevder videre at en eventuell utbygging av DGF ikke vil føre til noe mistillit blant befolkningen i forhold til hvordan E-tjenesten anvender dataene. På bakgrunn av dette vil en eventuell nedkjølingseffekt derfor bli minimal (Lysne II-utvalget, 2016: 67). I tillegg kan det argumenteres for at innføringen av DGF ikke vil føre til en nedkjølingseffekt og endringer i folks internettvaner, fordi mye av internettrafikken ifølge Sveinbjørnsson (2013) allerede blir overvåket gjennom Sveriges variant av DGF; FRA. Samtidig vil DGF stå i en særstilling for norske borgere. Dette fordi overvåkingen vil utføres av egne myndigheter, og ikke av fremmede stater uten videre myndighet og makt over norske borgere. Videre vil nedkjølingseffekten også kunne betraktes som noe som allerede skjer i samfunnet og verden. Noe som tilsier at begrepet nedkjølingseffekt ikke bør begrenses til å utelukkende dreie seg om en risiko som enda ikke har oppstått. Mulighetene for, og myndighetenes bruk av overvåking bidrar til å skape en visshet om at kommunikasjonen kan fanges opp, og dermed legge begrensninger på borgernes frimodighet og ytringsfrihet (Datatilsynet, 2017: 13-14). Fordi frykten for å bli overvåket fører til at mennesker vil handle og tenke annerledes enn de ville gjort dersom overvåkingen ikke var tilstede (Richards, 2013: 1948).

Lysne II-utvalgets rapport (2016) argumenterer for at nedkjølingseffekten vil bli minimal, mens Datatilsynet (2013) hevder at nedkjølingseffekten er en reell risiko. Hva som eksakt kommer til å skje etter en eventuell etablering av DGF er vanskelig å si. Det kan likevel være viktig å ha noen forutsetninger for hvor grensen går, eller hvilke eventuelle samfunnsendringer som må til før det tilsier at DGF bør endres eller avsluttes. Ved å sette en form for mål på usikkerheten knyttet til etableringen av DGF, kan det bidra til å skape mer tillitt og forutsigbarhet både for befolkningen og for myndighetenes videre styring av DGF. Datatilsynet (2017) peker på at de er enig med utvalgets vurdering om at den generelle tillitten i Norge, samt tillitten til E-tjenesten sammen med de ulike kontroll og tilsynsordningene i DGF-systemet, vil kunne bidra til å dempe nedkjølingseffekten. Videre påpekes det at tillitt og omfattende kontrollordninger er viktig i vurderingen av DGF, men at kilden til en eventuell nedkjølingseffekt vil ligge i selve tvilen eller usikkerheten. For det første vil ikke de ulike tilsynsordningene samt de juridiske og teknologiske barrierene, være noe som vanlige borgere har oversikt eller innsikt i. For det andre vil ikke tillitt til E-tjenesten nødvendigvis fjerne usikkerhet og tvil knyttet til hvordan overvåkingen foregår og hvorvidt det foretas undersøkelser knyttet til egen aktivitet og kommunikasjon (Datatilsynet, 2017: 15). I tillegg peker E-tjenesten selv på at det vil være en feilslutning å tro at deres arbeid ikke vil kunne

innebære behandling av informasjon knyttet til norske forhold (Etterretningstjenesten, 2017: 1). Tillitten til E-tjenesten er også noe som kan endres i fremtiden. Kanskje spesielt i forhold til DGF dersom det kommer frem eventuelle problemer eller feil i tilknytning til systemet eller bruken av dataene. Det kan også svekke tillitten dersom effekten av overvåkingen ikke er tilfredsstillende med hensyn til formålsbestemmelsene.

7. Konklusjon

I dette kapittelet samles trådene sammen for å gi svar på studiens problemstilling om hvordan DGF kan true samfunnssikkerheten. Tilslutt gis en kort oppsummering av studiens hovedfunn og de ulike konklusjonene som trekkes.

Samfunnssikkerhet ble innledningsvis definert som «samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. DGF kan ut fra denne definisjonen ha potensiale til å true samfunnssikkerheten på flere områder. I utgangspunktet vil det trolig ikke være slik at DGF direkte vil sette liv og helse i fare. Men samtidig kan DGF true noen av de grunnleggende verdier og funksjoner i samfunnet som igjen er viktige grunnsteiner for samfunnssikkerheten. Blant annet kan DGF true samfunnssikkerheten gjennom den potensielle nedkjølingseffekt det kan ha overfor ulike verdier som anses for å være essensielle for et demokrati. Studien viser også at DGF vil måtte ha strenge kontroll og sikkerhetskrav nettopp fordi systemet er sensitivt. Til tross for kontrollforslagene om både filter, domstolskontroll og tilsyn så kan likevel DGF utgjøre en trussel mot samfunnssikkerheten.

Politisk sett vil det trolig ikke være en vinnersak eller et mål i seg selv å kjempe mot IKT-utviklingen. I utgangspunktet har digitalisering og IKT-innovasjoner gjerne et positivt og godt formål som blant annet kan bidra til å skape trygghet og sikkerhet. På den andre siden ligger det utfordringer knyttet til usikkerheten om konsekvensene ved etablering eller bruk av nye teknologier. Det ligger gjerne en trussel i den avhengigheten og sårbarheten som skapes i samfunnet gjennom digitalisering og IKT-utvikling. Digitalisering og IKT-systemer er gjerne komplekse og uoversiktlige i den forstand at det er både vanskelig å styre, det kan oppstå teknologiske feil, eller det kan misbrukes (Engen et al., 2016, 383-385). Et sentralt moment vil kunne sies å være den risikoen som DGF kan utgjøre i seg selv. Ingenting er sikkert og alt kan i prinsippet hackes. På den måten kan DGF også utgjøre en sårbarhet i seg selv, som igjen kan true samfunnssikkerheten.

DGF vil på mange måter kunne sies å være en del av myndighetenes redskap som blir en del av de ulike funksjonene som er etablert for å verne og beskytte samfunnet. DGF omtales også

som en del av totalforsvaret. I den forstand blir DGF en del av samfunnssikkerheten og dermed noe som kan true samfunnssikkerheten både dersom det oppstår feil, men også med tanke på utformingen av DGF-systemet som implementeres i samfunnet. Som overvåkingsredskap betraktes DGF som en del av myndighetenes metoder for å styrke den nasjonale sikkerheten. Samtidig tilsier både bredden og kapasiteten av overvåkingen i DGF-systemet at det behøves strenge reguleringer. Gjennom studiens analyse kan det tyde på at kontrollmekanismene som skal sørge for mest mulig sikker og riktig bruk av DGF kan være mangelfulle eller ha noen implikasjoner. I tillegg kan det tolkes slik at den interne kontrollen og sikringen av DGF er relativt grundig beskrevet, mens den eksterne sikringen er mindre vektlagt. DGF-systemet må også sikres mot ytre trusler og risikoer, da DGF også kan sies å representere en sårbarhet i deg selv. Trusselaktører kan ha et ønske å ramme DGF for dernest å skape uro eller ustabilitet i form at de norske myndighetene ikke har beskyttet dataene om norske borgere som er lagret i systemet. Dette kan gjøre DGF til et attraktivt mål for ulike trusselaktører som kan ramme samfunnssikkerheten.

I den forstand vil det også være viktig for myndighetene å sikre tillitt til systemet, ikke bare i form av E-tjenestens interne bruk, men også gjennom den eksterne sikringen av datalagrene. Tillitt til systemet og etterretningen er viktig i og med at det omfatter overvåking av det som kan sies å være en upresis og udefinert personkrets. Ifølge Schartum (2010) vil en slik type overvåking være kontroversiell og kreve grundig argumentasjon og begrunnelse for å kunne iverksettes av myndighetene. I tillegg kan etableringen av DGF påvirke samfunnsfunksjoner og ulike verdier. Dersom det oppstår svikt, feil eller angrep mot DGF vil samfunnssikkerheten kunne påvirkes på flere måter. I og med at DGF ikke er en infrastruktur som direkte sørger for funksjonaliteten til bestemte og sentrale samfunnsfunksjoner, så vil trolig ikke konsekvensene være umiddelbare og konkretiserte på samme måte som for eksempel brudd i strømkabler fører til manglende tilførsel av elektrisitet. Men samfunnets verdier og borgernes trygghetsfølelse er viktige bærebjelker for det norske demokratiet, og dermed vil DGF kunne påvirke samfunnssikkerheten gjennom muligheten til å kunne utfordre disse.

Den digitale utviklingen har foregått i et ekstremt raskt tempo som det i mange tilfeller har vært utfordrende å være i forkant av. Det vil si at eventuelle negative konsekvenser knyttet til etablering av ulike IKT-systemer ikke har vært mulig å forutse. De ulike risikoene og

sårbarhetene har ikke blitt oppdaget før, slik at det har vært nødvendig å forsøke å utbedre systemene i etterkant (NOU 2015:13, 2015: 26). De potensielt negative konsekvensene av DGF er omtalt i Lysne II-utvalgets rapport (2016). Dette kan bidra til å skape et informativt og balansert beslutningsgrunnlag for å vurdere etableringen av DGF. Samtidig kan det argumenteres for at det mangler et risikostyringsperspektiv som tar for seg hvordan eventuelle negative utviklingstrekk i etterkant av DGF-etableringen skal håndteres. Årsaken kan være at det vil være vanskelig å skulle forutse eksakt hva som kommer til å skje, men samtidig vil det kunne argumenteres for at det er viktig å ha noen eksakte holdepunkter for hva som kan godtas eller ikke av ulike negative konsekvenser. I dette ligger blant annet hvilke forutsetninger som skal ligge til grunn for å eventuelt avvikle eller iverksette DGF-systemets egen destrueringsmekanisme. Uten klare føringer for kriteriene som vil bli gjeldende i etterkant av en eventuell etablering av DGF, kan derfor også utgjøre en trussel mot samfunnssikkerheten. Blant annet fordi samfunnet kan endre seg på en slik måte at også nedslagsfeltet til DGF og E-tjenesten vil kunne ramme samfunnsverdier- og funksjoner på en mer omfattende og alvorlig måte, da særlig med tanke på hvor inngripende systemet kan være overfor borgernes rettigheter.

Ved å betrakte DGF gjennom perspektiver på risikostyring vil det kunne sies at det ligger ulike risikoer og usikkerhetsmomenter knyttet til eksistensen av DGF i samfunnet. Det kan være usikkerhet knyttet til de vurderingene som ligger bak anbefalingene eller vurderingene av DGF, enten det er usikkerhet i form av hva som kan skje dersom DGF etableres, eller hva som kan skje dersom vi ikke har DGF. Det kan også være usikkerhet knyttet til hvor alvorlig det kan være å ha eller ikke ha DGF. Videre kan det være usikkerhet i forhold til hvordan DGF kan påvirke de ulike samfunnsverdiene som står sentralt i det norske samfunnet. Alvorligheten av å etablere DGF kan være knyttet til hvorvidt DGF kan sies å være forenelig med demokratiske prinsipper og i den forstand være formålstjenlig. Ved at DGF kan true personvernet, sette ytringsfriheten under press, og utgjøre en maktfaktor fra myndighetene vil det kunne sies å utgjøre en risiko for samfunnet, og dermed for samfunnssikkerheten, hvor disse verdiene anses for å være grunnleggende og elementære elementer ved det demokratiske samfunnet. I et rettsstatlig perspektiv vil det også kunne stilles spørsmål ved hvorvidt regnestykket går opp, i den forstand at hele befolkningen i prinsippet settes under overvåking for å finne et fåtall trusselaktører som kan utgjøre en fare for rikets sikkerhet og nasjonale interesser. I og med at DGF kan påvirke samfunnssikkerheten på flere ulike måter, bør det

gjerne stilles strengere krav til etableringsgrunnlaget og behovet for systemet. Spesielt med tanke på mulighetene og trenden innen ulike krypteringstjenester, som dernest kan utfordre selve formålet og effektiviteten av DGF. I tillegg kan også andre alternativer for DGF bidra til å imøtekomme noe av behovet for å sikre rikets sikkerhet og nasjonale interesser.

7.1 Oppsummering av konklusjon

Etableringen av DGF kan true samfunnssikkerheten på flere områder. For det første kan DGF true samfunnssikkerheten ved å bane vei mot et overvåkingssamfunn som kan bidra til å undertrykke dagens samfunnsverdier som anses for å være viktige både i demokratisk, men også i samfunnssikkerhetlig forstand. Overvåkingskapasiteten i DGF-systemet vil kunne argumenteres for å være så omfattende at det også kan stilles spørsmål ved systemets formålstjenlighet og hvorvidt målet helliger middelet. For det andre kan de ulike kontrollmekanismene i systemet utfordres fra et samfunnssikkerhetsfaglig ståsted hvor systemfeil, misbruk eller svikt i kontrollfunksjonene ikke uten videre kan utelukkes. Spørsmålet vil i så måte handle om alvorlighetsgraden av konsekvensene, og om samfunnet kan akseptere eller tåle en eventuell materialisering av dem. For det tredje vil DGF fremstå som en trussel overfor samfunnssikkerheten da systemet i seg selv vil kunne argumenteres for å være en sårbar komponent. Dette handler både om eventuelle sårbarheter i interne kontroll- og tilsynsfunksjoner, men også om den fysiske og digitale sikringen av DGF-systemet mot ytre trusler. Tilslutt kan det sies at DGF, gjennom overvåkingskapasiteten sammen med faren for svikt i kontrollfunksjonene, utgjør en utfordring for samfunnssikkerheten ved at det kan ramme viktige samfunnsverdier. Prinsippene om personvernet presses, faren for nedkjølingseffekt øker, rettssikkerheten utfordres, og tillittsrelasjonene i den norske samfunnet kan på mange måter påvirkes. Tillitten mellom myndighetene og borgerne kan særlig være et element som påvirkes gjennom DGF da dette kan berøre kontroll og maktforholdet mellom borgerne og myndighetene. Tillitt er også noe som i denne sammenheng er viktig både for borgernes trygghetsfølelse, og for stabiliteten i samfunnet som på sin side er sentrale aspekter ved samfunnssikkerheten.

Avslutningsvis påpekes det at DGF i utgangspunktet er foreslått etablert med den hensikt å skulle styrke samfunnssikkerheten. Denne avhandlingen veier ikke nødvendigvis den eventuelle positive effekten som DGF kan ha, opp mot de negative. Det er ikke dermed sagt at

det ene utligner det andre, men det kan viktig å ha reflektert kunnskap og innsikt i hvordan DGF kan påvirke samfunnet i begge retninger. Det kan gis inntrykk av at Lysne II-utvalgets rapport (2016) om DGF fokuserer på hvordan DGF kan bidra til å styrke samfunnssikkerheten, samtidig som enhver problemstilling knyttet til DGF argumenteres for å bli ivaretatt gjennom systemets utforming og mange kontrollfunksjoner. Denne avhandlingen kan forhåpentligvis bidra til å vise hvordan DGF også kan true samfunnssikkerheten på noen områder, og dermed fungere som et informativt og nyttig bidrag i debatten om DGF spesielt, og gjerne om overvåking generelt. Det store spørsmålet som gjenstår er hvilken risiko samfunnet er villig til å akseptere.

8. Videre forskning

I Sverige har de etablert FRA som er en innretning som på mange måter ligner DGF. Det kunne vært interessant å undersøkt nærmere hvorvidt FRA har endret svenskers kommunikasjon- eller internettvaner, eller om det har skapt nye sårbarheter for det svenske samfunnet. Det kunne også vært interessant å sett nærmere på selve FRA-systemet og hvordan det ivaretar sikkerheten for dataene som lagres. I og med at denne avhandlingen argumenterer for at DGF som system kan utgjøre nye sårbarheter og bli et etterretnings- eller angrepsmål i seg selv, kan det være aktuelt å se hvordan FRA i så måte har fungert. En annen problemstilling kan være knyttet til hvorvidt FRA faktisk har vist seg å være nyttig og effektiv i forhold til formålet og etterretningsbehovet. Et studie av FRA kan trolig bidra med nyttig informasjon knyttet til DGF og hvordan det både kan påvirke samfunnssikkerheten og demokratiske verdier og menneskerettigheter. Et annet utgangspunkt kan være å gjøre studier av hvordan andre land som ikke har etablert lignende overvåkingssystemer systemer håndterer og imøtekommer cyber- og terrortrusler.

Videre forskning kan utvide undersøkelsesspekteret ved å for eksempel inkludere andre samfunnsfunksjoner og verdier som kan tenkes å bli berørt gjennom DGF. Det kunne også vært interessant å utelukkende hatt et rettsstatlig fokus, for å eksempelvis kunne gå dypere inn i de ulike problemstillingene knyttet til overvåking i lys av lovverket og ikke minst menneskerettighetene. Det ville også vært interessant å utført et kvantitativt studie med fokus på å undersøke hvordan befolkningen vil forholde seg til DGF, og om det eventuelt vil føre til endringer i kommunikasjonsvaner eller metoder.

Det vil også være spennende og interessant å følge debatten fremover, og ikke minst skjebnen til DGF. Her vil det også kunne være interessante elementer å forske videre på. For eksempel kan et retorisk studie av DGF-debatten være interessant og bidra med mer innsikt om motivasjonen for DGF og hvordan det knyttes opp mot samfunnssikkerhetsaspekter. Dersom DGF endelig vedtas å skulle etableres vil det selvsagt være relevant å studere hvordan DGF faktisk viser seg å påvirke samfunnet og eventuelt hvordan det truer eller påvirker samfunnssikkerheten.

Litteraturliste

Aase T. H., Fossaskåret, E. (2014). *Skapte Virkeligheter. Om Produksjon og Tolkning av Kvalitative Data* (2. utg.). Oslo: Universitetsforlaget.

Aven, T., Boyesen, M., Njå, O., Olsen, K. H., Sandve, K. (2004). *Samfunnssikkerhet.* Oslo: Universitetsforlaget.

Aven, T., og Renn, O. (2010). *Risk Management and Governance. Concepts, Guidelines and Applications*. Berlin: Springer-Verlag.

Bing, J. (2010). *Forord. Overvåkingens mange fasetter.* I: Schartum, D. W (Red.). (2010). *Overvåking i en rettsstat*. Bergen: Fagbokforlaget, s. 5-8.

Bruce, I., og Haugland, G. S. (2010). *Personvern, rettssikkerhet og vern mot alvorlig kriminalitet. Noen utgangspunkter.* I: Schartum, D. W (Red.). (2010). *Overvåking i en rettsstat*. Bergen: Fagbokforlaget, s. 62-83.

Council of Europe (2010). *Den Europeiske Menneskerettighetskonvensjonen.* Hentet fra: https://www.echr.coe.int/Documents/Convention_NOR.pdf [Nedlastet: 18.05.2019]

Datatilsynet (2013). *Big Data – Personvernprinsipper under press.* Hentet fra: https://www.datatilsynet.no/globalassets/global/om-personvern/rapporter/big-data_web.pdf [Nedlastet: 28.04.2019]

Datatilsynet (2017). *Høringsuttalelse – Rapport avgitt av Lysne II-utvalget om digitalt grenseforsvar – Forsvarsdepartementet.* Hentet fra: https://www.datatilsynet.no/globalassets/global/regelverk/avgjorelser-datatilsynet/horinger/2017/horingsuttalelse-dgf-2017.pdf [Nedlastet: 16.03.2019]

DSB (2016). *Samfunnets kritiske funksjoner. Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?* Versjon 1.0. Oslo: Direktoratet for samfunnssikkerhet og beredskap (DSB).

Engen, O. A., Kruke, B. I., Lindøe, P. H., Olsen, K. H., Olsen, O. E. og Pettersen, K.A. (2016). Perspektiver på samfunnssikkerhet. Cappelen Damm AS.

EOS-utvalget (2015). *Årsmelding for 2014.* Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget). Oslo, 8. april 2015. Hentet fra: https://eos-utvalget.no/norsk/arsmeldinger/content/text_1401199471784/1428492476338/_rsmelding_for_2014.pdf [Nedlastet: 28.03.2019]

Etterretningstjenesten (2016). *Høring av rapport avgitt av Lysne II-utvalget om digitalt grenseforsvar.* Hentet fra: https://www.regjeringen.no/contentassets/84a90462cf9b4aebb310d97052083d26/horingssvar-med-merknader-etterretningstjenesten-digitalt-grenseforsvar.pdf?uid=Etterretningstjenesten [Nedlastet: 16.03.2019]

EU direktiv 2006/24/EF (2006). *EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV 2006/24/EF: af 15. marts2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentlig tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF*. Den Europæiske Unions Tidende. L 105/54. Hentet fra: https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:32006L0024&qid=1552045147446&from=EN [Nedlastet 08.03.2019]

Europarådskonvensjonen (2016). *Europaparlaments- og Rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning)*. I: Personopplysningsloven (2018). *Lov om behandling av personopplysninger* (LOV-2018-06-15-38). Hentet fra: https://lovdata.no/lov/2018-06-15-38 [Nedlastet: 05.05.2019]

FN-sambandet (2018). *FNs verdenserklæring om menneskerettigheter.* Vedtatt 10.12.1948. Hentet fra: https://www.fn.no/Om-FN/Avtaler/Menneskerettigheter/FNs-verdenserklaering-om-menneskerettigheter [Nedlastet: 08.05.2019]

Forsvarsdepartementet (2015). *Ekspertgruppen for Forsvaret av Norge- Et felles løft.* Oslo: Forsvarsdepartementet. Hentet fra: https://www.regjeringen.no/globalassets/departementene/fd/dokumenter/et-felles-loft-webversjon.pdf [Nedlastet: 23.01.2019]

Færaas, A. (30.04.2015). E-tjenesten sto i fjor bak ulovlig overvåking av nordmenn i Norge. *Aftenposten.* Hentet fra: https://www.aftenposten.no/norge/i/RzEd/E-tjenesten-sto-i-fjor-bak-ulovlig-overvaking-av-nordmenn-i-Norge [Nedlastet: 28.03.2019]

Hammerlin, J. (2009). *Terrorindustrien.* Oslo: Forlaget Manifest.

Hammerlin, J. (2014). *Tillitt og kontroll.* I: Hausken, L., Yazdani, S. R., Haagensen, T. K. (Red.). (2014). *Fra terror til overvåking. Overvåking i Norge, et kritisk prospekt*. Oslo: Vidarforlaget, s. 63-83.

Halvorsen, K. (2008). *Å forske på samfunnet. En innføring i samfunnsvitenskapelig metode*. Oslo: Cappelen Akademisk Forlag.

Hausken, L. (2014). *Innledning.* I: Hausken, L., Yazdani, S. R., Haagensen, T. K. (Red.). (2014). *Fra terror til overvåking. Overvåking i Norge, et kritisk prospekt*. Oslo: Vidarforlaget, s. 11-37.

Hausken, L., Yazdani, S. R., Haagensen, T. K. (Red.). (2014). *Fra terror til overvåking. Overvåking i Norge, et kritisk prospekt*. Oslo: Vidarforlaget.

Jacobsen, D. I. (2015) *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode.* 3. Utg. Oslo: Cappelen Damm akademisk.

Justis- og beredskapsdepartementet (2017). *Høring – rapport avgitt av Lysne II-utvalget om digitalt grenseforsvar.* Hentet fra: https://www.regjeringen.no/contentassets/84a90462cf9b4aebb310d97052083d26/horingssvar-med-merknader-jd-digitalt-grenseforsvar.pdf?uid=Justis-_og_beredskapsdepartementet_(JD) [Nedlastet: 16.03.2019]

Lomell, H. M. (2014). *Forventninger om beskyttelse.* I: Hausken, L., Yazdani, S. R., Haagensen, T. K. (Red.). (2014). *Fra terror til overvåking. Overvåking i Norge, et kritisk prospekt*. Oslo: Vidarforlaget, s. 39-61.

Lyon, D. (2003). *Surveillance after September 11.* Great Britain: Polity Press

Lyon, D. (2007). *Surveillance Studies – An Overview.* Great Britain: Polity Press.

Lyon, D. (2015). *Surveillance After Snowden.* Cambridge, UK: Polity Press.

Lysne II-utvalget (2016). *Digitalt Grenseforsvar (DGF).* Hentet fra: *https://www.regjeringen.no/globalassets/departementene/fd/dokumenter/lysne-ii-utvalgets-rapport-2016.pdf* [Nedlastet 24.01.2019]

Meld. St. 38 (2016-2017). *IKT-sikkerhet, et felles ansvar.* Justis- og beredskapsdepartementet. Hentet fra: https://www.regjeringen.no/contentassets/39c6a2fe89974d0dae95cd5af0808052/no/pdfs/stm201620170038000dddpdfs.pdf [Nedlastet: 04.02.2019]

Meld. St. 27 (2015-2016). *Digital agenda for Norge. IKT for en enklere hverdag og økt produktivitet.* Kommunal- og moderniseringsdepartementet. Hentet fra: https://www.regjeringen.no/contentassets/fe3e34b866034b82b9c623c5cec39823/no/pdfs/stm201520160027000dddpdfs.pdf [Nedlastet: 04.02.2019]

Nasjonal Kommunikasjonsmyndighet (2015). *Ekomplanen – Innspill til Samferdselsdepartementet fra Nasjonal kommunikasjonsmyndighet.* Hentet fra: https://www.regjeringen.no/contentassets/d2043d6b52934697b8d96e4114cc88ec/nkominnspill.pdf [Nedlastet: 15.03.2019]

Nasjonal Sikkerhetsmyndighet (2015). *Sikkerhetsfaglig råd.* Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/nsm-sikkerhetsfaglig_raad_2015_web.pdf [Nedlastet: 03.04.2019]

Newth, E. (2014). *Overvåkingssamfunnet.* Oslo: Humanist Forlag.

NOU 2006:6 (2006). *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner.* Hentet fra: https://www.regjeringen.no/contentassets/c8b710be1a284bab8aea8fd955b39fa0/no/pdfs/nou200620060006000dddpdfs.pdf [Nedlastet: 16.03.2019]

NOU 2015:13 (2015). *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden.* Oslo: Departementenes sikkerhets- og serviceorganisasjon, Informasjonsforvaltning.

NOU 2016:19 (2016). *Samhandling for sikkerhet. Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid.* Hentet fra: https://www.regjeringen.no/contentassets/816d557c6ab24493a1101837cc2e1cf8/nou-2016-19-samhandling-for-sikkerhet.pdf [Nedlastet. 16.03.2019]

Politiets sikkerhetstjeneste (2017). *Innspill fra PST til rapport avgitt av Lysne II-utvalget om digitalt grenseforsvar*. Hentet fra: https://www.regjeringen.no/contentassets/84a90462cf9b4aebb310d97052083d26/horingssvar-med-merknader-pst-digitalt-grenseforsvar.pdf?uid=Politiets_sikkerhetstjeneste_(PST) [Nedlastet: 16.03.2019]

Prop. 49 L (2010-2011). *Endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett): Tilråding fra Justis- og politidepartementet av 10. desember 2010, godkjent i statsråd samme dag: (Regjeringen Stoltenberg II).* [Oslo]: Justis- og politidepartementet.

Regjeringen.no1 (2016). *Mottok Lysne II-utvalgets rapport om digitalt grenseforsvar.* Pressemelding, Nr: 47/2016. Forsvarsdepartementet. Hentet fra: https://www.regjeringen.no/no/aktuelt/mottok-lysne-ii-utvalgets-rapport-om-digitalt-grenseforsvar/id2510465/ [Nedlastet: 24.01.2019]

Regjeringen.no2 (2016). *Høring av rapport avgitt av Lysne II-utvalget om digitalt grenseforsvar.* Forsvarsdepartementet. Hentet fra: https://www.regjeringen.no/no/dokumenter/horing-av-rapport-avgitt-av-lysne-ii-utvalget-om-digitalt-grenseforsvar/id2513635/?expand=horingssvar [Nedlastet: 24.01.2019]

Regjeringen.no (2017). *Utreder et digitalt grenseforsvar.* Pressemelding, Nr: 18/2017. Forsvarsdepartementet. Hentet fra: https://www.regjeringen.no/no/aktuelt/utreder-et-digitalt-grenseforsvar/id2539809/ [Nedlastet: 24.01.2019]

Regjeringen.no (2019). *Nye nasjonale strategier – et felles løft for digital sikkerhet.* Pressemelding, Nr: 3/2019. Justis- og beredskapsdepartementet, Statsministerens kontor, Forsvarsdepartementet, Kunnskapsdepartementet. Hentet fra: https://www.regjeringen.no/no/aktuelt/nye-nasjonale-strategier--et-felles-loft-for-digital-sikkerhet/id2627193/?expand=factbox2627196 [Nedlastet: 02.02.2019]

Richards, N. M. (2013). *The Dangers of Surveillance.* Harvard Law Review. Hentet fra: https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_richards.pdf [Nedlastet: 22.04.2019]

Samfunnssikkerhetsinstruksen (2017). Instruks for departementenes arbeid med samfunnssikkerhet. Justis- og beredskapsdepartementet. Hentet fra: https://lovdata.no/dokument/INS/forskrift/2017-09-01-1349?q=samfunnssikkerhetsinstruksen [Nedlastet 04.02.2019]

Schartum, D. W. (Red.). (2010). *Overvåking i en rettsstat*. Bergen: Fagbokforlaget.

Sejersted, F. (2002). *Er det mulig å styre utviklingen? Teknologi og samfunn.* Oslo: Pax Forlag.

Søreide, I. E. (2017). *Vi trenger et digitalt grenseforsvar*. Tale/innlegg. Forsvarsdepartementet. Hentet fra: https://www.regjeringen.no/no/aktuelt/vi-trenger-et-digitalt-grenseforsvar/id2573968/ [Nedlastet 20.03.2019]

Sveinbjørnsson, S. (02.12.2013). –Sverige overvåker norsk mobiltrafikk. *Digi.no.* Hentet fra https://www.digi.no/artikler/sverige-overvaker-norsk-mobiltrafikk/288168 [Nedlastet: 18.01.2019]

Thon, B. E. (2014). *Personvern i en brytningstid.* I: Hausken, L., Yazdani, S. R., Haagensen, T. K. (Red.). (2014). *Fra terror til overvåking. Overvåking i Norge, et kritisk prospekt*. Oslo: Vidarforlaget, s. 103-127.

Figurer

Figur 1: *Overordnet beskrivelse av DGF*. Fra Lysne II-utvalget (2016). *Digitalt Grenseforsvar (DGF).* Hentet fra: *https://www.regjeringen.no/globalassets/departementene/fd/dokumenter/lysne-ii-utvalgets-rapport-2016.pdf* [Nedlastet 24.01.2019]