UiO : Det juridiske fakultet

Er digitalt grenseforsvar mot cyberspionasje forholdsmessig i den norske rettsstaten?

Demokratiske og menneskerettslige utfordringer ved sikring av rikets sikkerhet i den digitale tidsalder.

Kandidatnummer: 537

Leveringsfrist: 25. november 2018

Antall ord: 17962

Innholdsfortegnelse

1 Introduksjon

1.1 Problemstilling og bakgrunn

Cyberspionasje fra fremmed etterretning anses å være en av de største truslene mot Norge.[1] Aktørene er stort sett statlige grupper som i hovedsak foretar ulovlig innhenting av informasjon om politiske og militære institusjoner gjennom hacking av datasystemer.[2] På sikt kan slike operasjoner føre til svekkelse av rikets beredskap og sikkerhet. Som svar på cybertruslene har Forsvarsdepartementet oppnevnt Lysne II-utvalget, som etter sin utredning har kommet frem til at det er hensiktsmessig med digitalt grenseforsvar (DGF)[3] i Norge. Med DGF vil all kommunikasjon på tvers av landegrensen kunne overvåkes, og norsk etterretningstjeneste (e-tjenesten) vil derfor være bedre rustet til å avdekke cyberspionasje fra fremmed etterretning. Det er samtidig ikke til å unngå at overskuddsinformasjon om kommunikasjon mellom norske borgere lagres.

Problemstillingen går derfor ut på å drøfte om opprettelse av DGF som tiltak for å sikre rikets sikkerhet er forenelig med vernet om privatlivets fred i Grunnloven § 102, Den europeiske menneskerettighetskonvensjonen (EMK) artikkel 8, Den europeiske unions menneskerettighetscharter (EU-charteret) artikkel 7 og 8 jf. 52(1) og FNs konvensjon om sosiale og politiske rettigheter (SP) artikkel 17. Menneskerettighetene er sammen med demokratiet og rettsstaten en av de norske kjerneverdiene som skal sikres etter Grunnloven § 2 annet punktum. De tre kjerneverdiene er gjensidig avhengig av hverandre for å fungere i praksis. Når menneskerettighetene utfordres, utfordres også demokratiet og rettsstaten fordi det blir et spørsmål om i hvor stor grad statsmaktene med rette kan gripe inn i borgernes liv. Et av premissene for et velfungerende demokrati er nettopp distinksjonen mellom den offentlige og private sfære,[4] en distinksjon som beskytter mot autoritære og totalitære regimer, som kan anses som motsatser til rettsstater. I det videre vil demokrati og menneskerettigheter kategoriseres som rettsstatsidealer.

Balansegangen mellom ivaretakelsen av rikets sikkerhet og rettsstatsidealene ved cyberspionasje er relevant fordi vi står ovenfor et relativt uoversiktlig digitalt trusselbilde som preges av et teknologikappløp i kombinasjon med lite nasjonal og internasjonal lovregulering. Behovet for effektive etterretningsmetoder er nødvendig, men kan fort utfordre rettsstatsidealene gjennom inngripende tiltak som omfattende overvåkning. I tillegg er det utfordrende å utvikle

1 Lysne (2016) s. 28.

2 Etterretningstjenesten (2018) s. 30.

3 Lysne II-utvalgets abbreviasjon for digitalt grenseforsvar.

4 Bauman (2014) s. 136.

tilstrekkelig klar lovgivning på området siden teknologien utvikles raskere enn lovgivningen. Samtidig vil ivaretakelse av rikets sikkerhet innebære beskyttelse av rettsstatsprinsippene, som representerer grunnleggende norske verdier. Ivaretakelsen av rikets sikkerhet og etterlevelse av rettsstatsprinsippene er derfor to måter å verne om de samme verdiene på. Utfordringen ligger i å ikke avbalansere maktforholdet mellom myndighetene og borgerne[5] slik at ikke midlene som skal beskytte rettsstaten på samme tid blir dens trussel.

1.2 Metode

Problemstillingen drøftes i hovedsak gjennom en forholdsmessighetsvurdering i tråd med Den europeiske menneskerettighetsdomstol (EMD) sin metode og praksis, supplert med tilsvarende fra Den europeiske unions domstol (EU-domstolen). Grunnlovens bestemmelser i § 2 og § 102 vil ha størst relevans og vekt i drøftelsen siden problemstillingen knytter seg spesifikt til Norge som rettsstat. Grunnlovens relevans og vekt for problemstillingen overføldiggjør forøvrig drøftelse av lovgivning som supplerer Grunnloven § 2 og § 102, og slik lovgivning vil derfor ikke dekkes nærmere. Rettskildebildet rundt problemstillingen lar seg vanskelig skille fra innholdsbeskrivelsen, og blir derfor beskrevet nærmere i kapittel 2. Av samme grunn vil særskilte rettskildemessige spørsmål knyttet til EMD, EU-domstolen og Grunnlovens bestemmelser, samt forholdet mellom dem, redegjøres for underveis.

Innholdet i Lysne II-utvalgets høring utgjør det innholdsmessige utgangspunktet for problemstillingen. Høringen kan ikke sies å ha særlig autoritet i kraft av å være på et tidlig stadium i lovgivningsprosessen, men dens innhold representerer en dagsaktualitet som det er grunn til å belyse nærmere, særlig i forhold til den internasjonale utviklingen på overvåkingsområdet. Problemstillingen suppleres med øvrige forarbeider og litteratur som gir grunnlag for rettspolitiske drøftelser underveis. Det vil legges inn tekniske forklaringer på hva DGF går ut på i den utstrekning det er nødvendig for å forstå inngrepsgraden det medfører, samt dets forhindringspotensiale i forhold til cyberspionasje.

[5] NOU 2015:13 s. 25.

1.3 Demokratiet og menneskerettighetene som rettsstatsidealer

Begrepet rettsstat forklares best ved å vise til trekk som kjennetegner en rettsstat.[6] Gjennom demokratiske prosesser skal borgerne sikres mot maktmisbruk gjennom at regjeringen og domstolene må holde seg innenfor de lovene som borgerne, gjennom Stortinget, selv har laget.[7] Et vedtak fra regjerningen må derfor forankres i en lov, og domstolene må på selvstendig grunnlag dømme i samsvar med lover vedtatt av stortinget.[8] Dette er også selve kjernen i legalitetsprinsippet.

Forutsetningen for rettsstatens virke er Grunnloven, som gjennom de formelle reglene etablerer og begrenser myndighetenes makt, og derfor legger grunnlaget for den demokratiske prosessen. De materielle reglene i Grunnloven er ment å sikre fundamentale menneskerettigheter, deriblant retten til vern om privatlivets fred i § 102. Sett i sammenheng kan det sies at de formelle reglene bidrar til at grunnleggende materielle regler sikres.[9] Med trinnhøydeprinsippet dannes videre grunnlaget for Grunnlovens funksjon som skranke for lovgivning på lavere nivå.[10] Menneskerettighetene, og derav vernet om privatlivets fred, henger derfor svært høyt, og er samtidig avhengig av at den demokratiske prosessen fungerer som den skal. Videre beror rettsstatens funksjon på at demokratiet og menneskerettighetene ivaretas.

Det er på dette grunnlaget at forholdsmessigheten av DGF drøftes i forhold til Norge som rettsstat. Norge er en rettsstat som setter demokratiet og menneskerettighetene i sentrum. Det er derfor ikke hvilken som helst lovgivning som kan tre i kraft. Om mere overvåkning skal tillates kan derfor ikke utelukkende avgjøres av et demokratisk flertall. Lovgivningen må respektere Grunnlovens skranker i § 102, og domstolene må kontrollere at disse skrankene overholdes. Denne tilsynelatende begrensningen på demokratiet er blitt til gjennom demokratiske prosesser, og er derfor en selvpålagt begrensning. Det er denne demokratiske prosessen som i helhet reflekterer hvilket verdigrunnlag Norge har, og som videre er med på å vedlikeholde dette verdigrunnlaget.[11] Som følge er rettsstatsperspektivet det mest dekkende utgangspunktet for å vurdere hvorvidt DGF er forholdsmessig i Norge.

Spørsmålet om DGF er forholdsmessig i Norge må ses i sammenheng med den økende overvåkningen i samfunnet, som særlig ble aktualisert i kjølvannet av Edward Snowden-

---

6 Knoph (2014) s. 3.

7 Grunnloven §49 og §§76-79.

8 Grunnloven §96.

9 Smith (2014) s. 69.

10 Høgberg (2013) s. 23.

11 Schartum (2010) s. 20-21.

avsløringene i 2013 der NSA sin omfattende samfunnsovervåkning ble avslørt.[12] Det finnes mange former for overvåkning, og i forhold til DGF er hovedformålet at e-tjenesten skal "motvirke alvorlige trusler[.]"[13] Overvåkningen har dermed en preventiv hensikt gjennom at lagret informasjon kan gi grunnlag for å igangsette en etterforskning allerede på forberedelsesstadiet, i stedet for i etterkant av en allerede utført straffbar handling. Schartum har i sin bok lagt til grunn at overvåkning fra myndighetenes side i utgangspunktet er en legitim handling og at problemet derfor omhandler hvor mye overvåkning som kan tillates før den blir for inngripende.[14] Den samme oppfatningen legges til grunn i det videre siden overvåkning fra e-tjenesten på en side kan utøves av hensyn til nasjonal sikkerhet, som igjen er en måte å ivareta rettsstatens virke på gjennom at trusler fra cyberspionasje kan oppdages og avvikles. På den andre siden må det drøftes om trusselen som cyberspionasje utgjør er alvorlig nok til å åpne for overvåkning av det omfanget DGF vil innebære.

Datatilsynets og Personvernnemndas årsmeldinger for 2013, refererer det til den såkalte nedkjølingseffekten, som et resultat av den økende overvåkningen i Norge. Nedkjølingseffekten går ut på at frykt for sanksjoner medfører skepsis til utførelse av legitime handlinger.[15]
Den økte overvåkningen vil altså føre til at rettsstatsidealene utfordres. Som datatilsynets rapport også viser til, kan overvåkningen føre til at borgernes tillit til myndighetene svekkes.[16] Demokratiets funksjon er avhengig av at borgere har tillit til myndighetene. E-tjenestens tilgang til detaljer om borgeres kommunikasjon er svært inngripende, og det blir en hårfin balansegang å skulle ivareta demokratiets beskyttelse mot myndighetsmisbruk, og samtidig ivareta rikets sikkerhet. Selv om det skulle utarbeides kontrollmekanismer for å unngå misbruk av den lagrede informasjonen gjenstår likevel spørsmålet om man for all fremtid og under enhver omstendighet kan stole på at informasjonen ikke misbrukes. Når demokratiet, som utgangspunkt for menneskerettighetenes eksistens utfordres, trues også menneskerettighetenes rekkevidde. Hvor ukrenkelig vernet om privatlivets fred er etter Grunnloven § 102, EMK artikkel 8, og SP artikkel 17 vil avhenge av hva domstolene anser som forholdsmessig tatt trusselbildet i betraktning.

---

12 St. Meld. 23 (2013-2014) s. 5.

13 Lysne (2016) s. 10.

14 Schartum (2010) s. 21.

15 St. Meld. 23 (2013-2014) s. 5.

16 Datatilsynet (2014) s. 34.

1.4 Rikets sikkerhet og cyberspionasje

I det følgende vil det redegjøres for hva rikets sikkerhet og cyberspionasje innebærer, samt hvordan begrepene henger sammen.

1.4.1 Rikets sikkerhet

Begrepet "rikets sikkerhet" favner vidt. De aspektene som har størst betydning for cyberspionasje vil dermed vektlegges i det følgende. Forarbeidene til Sikkerhetsloven legger innledningsvis til grunn at rikets sikkerhet omhandler "rikets indre og ytre sikkerhet."[17] I forhold til cyberspionasje vil rikets sikkerhet i det videre omhandle ytre sikkerhet fordi det er en trussel som kommer utenfra. Forarbeidene omtaler videre begrepet som "en rettslig standard som kan forandre seg med samfunnsutviklingen."[18] Forarbeidene går ikke videre innpå hva som legges i "rettslig standard", men i henhold til EOS-utvalgets rapport til Stortinget handler det om å ivareta statssuverenitet, samt det demokratiske systemet, inkludert dets "digitale samfunnsstrukturer".[19] Denne definisjonen viser at det ikke nødvendigvis er et motsetningsforhold mellom rikets sikkerhet og ivaretakelsen av rettsstaten, men at det handler om en avveiing av hva som til enhver tid er de mest beskyttelsesverdige verdiene. Den videre definisjonen av rikets sikkerhet i forarbeidene til sikkerhetsloven støtter opp om det gjennom å si at begrepet også omhandler beskyttelse av 'vitale samfunnsinteresser', og at det er høy terskel for å anse noe for å true disse interessene.[20] Høy terskel for å anse rikets sikkerhet som truet kan sies å ha sammenheng med at hensynet til rikets sikkerhet ikke skal brukes på altfor generelt grunnlag fordi det legitimerer potensielt inngripende tiltak. I møte med cyberspionasje er dermed hensynet til rikets sikkerhet også en måte å sikre demokratiet, menneskerettighetene og rettsstaten etter Grunnloven § 2.

Det er likevel et spørsmål om cyberspionasje truer vitale samfunnsinteresser i så stor grad at DGF rettferdiggjøres som legitimt middel for å ivareta rikets sikkerhet i betydningen Norge som en selvstendig demokratisk institusjon, med de følgene det får for hensynet til privatlivets fred etter Grunnloven § 102, EMK artikkel 8, EU-charteret artikkel 7 og 8 jf. 52(1), samt SP artikkel 17. I det følgende vil det dermed redegjøres nærmere for hva cyberspionasje er, og hvilke konsekvenser det kan få.

---

17 Ot. Prp. Nr. 49 (1996-1997) s. 64.

18 Ot. Prp. Nr. 49 (1996-1997) s. 64.

19 Dokument 16 (2015-1016) s. 33.

20 Ot. Prp. Nr. 49 (1996-1997) s. 64.

1.4.2 Cyberspionasje i digital kontekst

Det har blitt argumentert at den type krigføring som benyttes reflekterer måten et samfunn skaper velstand på.[21] Informasjon– og kommunikasjonsteknologi (IKT) betegnes som samfunnets bærebjelke. Vesentlige samfunnsinstitusjoners funksjon avhenger av IKT, og sårbarheten ved cyberspionasje er dermed innlysende.[22] I likhet med e-tjenesten peker PST på spionasje fra fremmed etterretning som en av de største truslene Norge står ovenfor. I sin trusselvurdering for 2018 fremhever PST russisk etterretning som den med størst potensielle skadevirkning, men også andre staters etterretningsvirksomhet foretar ulovlig cyberspionasje.[23] Som oftest foregår cyberspionasje gjennom målrettede utsendinger av tilsynelatende legitime e-poster med vedlegg som i realiteten fungerer som spionprogramvare når lenken åpnes.[24] Innsamling av informasjon på denne måten fører til at etterretning og tjenester i andre land opparbeider seg såpass mye informasjon om norsk etterretning at de kan være i stand til å komme det norske forsvar i forkjøp ved krisesituasjoner, og derfor svekke dets effektivitet.[25]

Cyberspionasje kan anses som en moderne strategi for å på ulovlig vis skaffe seg en maktfordel. Det er ikke lengre på slagmarken en stat vinner eller taper makt og innflytelse. Vi ser heller en tendens til en desentralisert slagmark der særlig militære aktører opererer mer presist og målrettet gjennom vel utviklede kommando- og kontrollservere som muliggjør presise og målrettede dataangrep der det til enhver tid er strategisk lønnsomt.[26] Cyberspionasje viser derfor at det er grunnlag for å påstå at måten man fører krig på reflekterer hvilke verdier som er viktige i et samfunn. Gjennom å infiltrere og manipulere IKT-systemer oppnår aktørene oversikt over systemer som er avgjørende for at en stat skal fungere. Cyberspionasje kan derimot ikke kategoriseres som en krigshandling fordi det ikke klassifiseres som "væpnet angrep" som rettferdiggjør selvforsvar under De forente nasjoners pakt (FN-pakten) artikkel 51 jf. Artikkel 2(4) som igjen er ansett som gjeldende rett på cyberområdet gjennom Tallinn Manualen 2.0.[27] [28] Likevel utgjør cyberspionasje en alvorlig trussel fordi sensitiv informasjon som hentes kan legge grunnlaget for et senere cyberangrep.

---

21 Toffler (1993) s. 57-80

22 NOU 2015:13 s. 25.

23 Politiets sikkerhetstjeneste (2018).

24 Nasjonal sikkerhetsmyndighet (2017) s. 5.

25 Politiets sikkerhetstjeneste (2018).

26 Dinniss (2012) s. 19.

27 Schmitt (2017) s. 3.

28 Tallinn Manualen 2.0 fra 2016 er oppfølgeren fra Tallinn Manualen fra 2013. Begge manualene ble til etter initiativ fra NATO, som satte sammen en ekspertgruppe som skulle vurdere hvordan internasjonal rett kan brukes på cyberoperasjoner. Manualene representerer objektive syn på allerede eksisterende internasjonal rett, og har dermed veiledende framfor bindende funksjon, med unntak av der det henvises til folkerettslig sedvane.

Et eksempel er Stuxnet, hvor det iranske atomprogrammet i 2010 ble ødelagt under et cyberangrep som resultat etter lengre tid med omfattende spionasje på atomprogrammet.[29] Angrepet var så omfattende og ødeleggende at det ble ansett som brudd på det internasjonale forbudet mot "bruk av makt" etter FN-pakten artikkel 2(4). På grunn av manglende internasjonal konsensus, ble det likevel ikke ansett å kvalifisere som "væpnet angrep" etter FN-pakten artikkel 51.[30] Til tross for de massive ødeleggelsene kan det fremdeles ikke sies med sikkerhet hvem som står bak Stuxnet. USA og Israel mistenkes for angrepet, men det er ikke tilstrekkelige holdepunkter for å fastslå dette.[31] Det er derfor ingen ansvarlige for det som til nå er et av de mest omfattende cyberangrepene, noe som understreker skadepotensialet ved cyberspionasje.

Det kan ofte være vanskelig å skille mellom cyberspionasje og cyberangrep fordi begge kategoriene innebærer hacking av datasystemer med skadematerialer som utover spionasje kan muliggjøre degradering, forstyrrelse eller ødeleggelse av datasystemet eller dets informasjonsinnhold.[32] Om det som starter som cyberspionasje eskalerer til et cyberangrep kan i verste fall liv gå tapt, eksempelvis gjennom at forsvarets satellittstyrte kommando- og kontrollsystem for kontroll av våpen forstyrres.[33] Når man det konfliktnivået i cyberrommet, er det aktuelt å snakke om cyberkrigføring. Temaet her er cyberspionasje i fredstid, men steget fra cyberspionasje til cyberkrigføring er ikke nødvendigvis langt, så sammenhengen er derfor nevneverdig.

For ordens skyld kan cyberspionasje, cyberangrep og cyberkrig likevel skilles fra hverandre ved følgende hovedtrekk; cyberspionasje dreier seg om innhenting av spesifikk informasjon fra utvalgte aktører som skal brukes på et senere tidspunkt for eksempel i form av et cyberangrep, for å få forhandlingsfordeler, samt industrielle fordeler. Cyberangrep dreier seg hovedsakelig om økonomisk motiverte angrep på mange og ubestemte datasystemer, gjerne for profittmaksimering. Andre motiver for cyberangrep omfatter informasjonstyveri, skade på datasystemer, samt underholdningsaspektet.[34] Cyberkrig er mer diffust, men kan sies å innebære cyberangrep med mål om å svekke statssuverenitet og nasjonal sikkerhet. I henhold til Tallin Manualen 2.0 er det også grunn til å si at cyberangrepet må kvalifiseres som "væpnet angrep" etter FN-pakten artikkel 2(4).

---

29 Lupovici (2016) s. 334 og 336 og Wangen (2015) s. 208.

30 Dev (2015) s. 398.

31 Lupovici (2016) s. 335-336.

32 Tallinn Manualen 2.0 artikkel 32(13).

33 Nasjonal sikkerhetsmyndighet (2017).

34 Wangen (2015) s. 185.

I motsetning til forbudet mot bruk av makt og væpnede angrep som folkerettslig sedvane, finnes det ingen tilsvarende forbud mot spionasje i fredstid.[35] Ekspertgruppen bak Tallinn Manualen 2.0 har derfor ingen eksisterende lovgivning å anvende på cyberspionasje. Det kan likevel ikke slås fast at det er et juridisk vakuum på dette området i internasjonal sammenheng hvis cyberspionasje medfører brudd på annen folkerettslig sedvane, som statssuverenitetsprinsippet og forbudet mot intervensjon.[36] Likevel, en internasjonal lovregulering som direkte angår cyberspionasje i fredstid vil føre til en mer effektiv beskyttelse mot en praksis som vokser i omfang og skadepotensiale. I mangelen av lovregulering på dette området er det desto viktigere at stater kan utvikle systemer som kan fange opp mistenkelig aktivitet i cyberrommet.

For å kunne avverge og håndtere risikoen for effekten av cyberspionasje er første steg på veien å erkjenne at risikoen finnes, for deretter å sette inn konkrete til tiltak. Et DGF vil gjøre en vesensforskjell i forhold til å beskytte Norge mot cyberspionasje. Samtidig må sikkerhetstiltak være forenelige med rettsstatsidealene. Vernet om privatlivets fred og rettsikkerhet henger høyt, og avveiingen mellom sikkerhetstiltak, rettigheter og friheter forbundet med en rettsstat er en krevende øvelse.

Sikkerhetstiltak handler om risikostyring. Som begrepet tilsier handler det om å forholde seg til noe man ikke med sikkerhet vet om kan inntreffe. Effekten av DGF må veies opp mot sannsynligheten for at cyberspionasje medfører alvorlige konsekvenser for rikets sikkerhet. Nytten av et sikkerhetstiltak som DGF kan derfor være vanskelig å fastslå.[37] Samtidig er trusler fra cyberrommet kompliserte å regulere fordi det ofte er vanskelige å finne det ansvarlige datasystemet, hvem som brukte det ansvarlige datasystemet, og hvilken stat eller organisasjon truslene kommer fra.[38] Et system som fanger opp disse uforutsigbare truslene kan derfor potensielt ha stor nytteeffekt.

---

35 Tallinn Manualen 2.0 artikkel 32(5).

36 Tallinn Manualen 2.0 artikkel 32(6).

37 Meld. St. 10 (2016-2017).

38 Glennon (2012) s. 567.

2 Digitalt grenseforsvar: formål og rettskildebilde

I dette kapittelet gis det en mer teknisk fremstilling av hva DGF går ut på for å gi en nærmere forståelse inngrepsgraden det medfører. Deretter redegjøres det ytterligere om formålet med DGF for å belyse effekten det kan ha for nasjonal sikkerhet på tross av inngrepsgraden. Til slutt redegjøres det for innholdet av de nasjonale og internasjonale regelverkene som er aktuelle for å drøfte om det er forholdsmessig med DGF i Norge. Begrunnelsen for en samlet framstilling av de overnevnte temaene er å gi en presisert framstilling av DGF i lys av regelverket, og hvordan særlig Grunnloven § 102 kan ses som en forlengelse av de norske rettsstatsidealene. Framstillingen i dette kapittelet vil også utgjøre innholdet for forholdsmessighetsvurderingen i kapittel 3.

2.1 Nærmere om digitalt grenseforsvar

Gjennom DGF kan e-tjenesten innhente informasjon på tvers av landegrensen i fiberoptiske kabler. Informasjonen som hentes kan både være kommunikasjon mellom flere personer, eller ensidig sending av data. Så lenge dataene overføres, og passerer landegrensen kan de innhentes. Typen informasjon som innhentes kategoriseres i hovedsak som metadata og innholdsdata. Metadata innebærer informasjon om andre data, for eksempel hvem en e-post kommer fra, og til hvem, samt fra hvor e-posten ble sendt og mottatt. Innholdsdata sier noe om innholdet, altså hva som står i selve e-posten. Metadata vil innhentes i bulk på utvalgte kommunikasjonslinjer, noe som går ut på at store mengder data innhentes før den relevante dataen siles ut. Metadata vil da inneholde store mengder kommunikasjonsinformasjon som ikke er relevant for e-tjenesten. Innholdsdata vil derimot innhentes målrettet og ikke i bulk.[39]

Foruten å avverge cyberspionasje fra fremmed etterretning er formålet med DGF også å motvirke terrorvirksomhet gjennom å avdekke kommunikasjon mellom terrorister, spesielt fra IS og Al-Qaida, som ut i fra motiver om politisk makt anses å utgjøre en trussel i forhold til voldelige angrep og bruk av masseødeleggelsesvåpen.[40] Begrunnelsen for å fokusere på DGF i forhold til cyberspionasje fra fremmed etterretning er at det i større grad enn terrorisme direkte angår Norge gjennom at det er avdekket spionasjeaktivitet rettet mot Norge. I henhold til terrorisme er Norge derimot ikke et prioritert mål, men trusselen fremgår i kraft av å være et vestlig land.[41] I følge e-tjenesten utgjør også cyberspionasje mot militære og politiske institu-

[39] Lysne (2016).

[40] Lysne (2016) s. 28.

[41] Etterretningstjenesten (2018) s. 28.

sjoner den største trusselen i det digitale rommet.[42] Sånn sett kan DGF sies å være mest effektivt mot cyberspionasje, og siden DGF er såpass inngripende i privatlivets fred er det mest hensiktsmessig å vurdere effekten opp i mot den trusselen DGF har størst potensiale til å forhindre.

Det foreligger ikke noe mål om å rangere truslene som ligger til grunn for opprettelsen av DGF, for deretter å la digital spionasje definere hvorvidt det er behov for DGF. Utgangspunktet i cyberspionasje framfor terrorisme er begrunnet i at det fremstår som et mer taktisk og subtilt virkemiddel med et enormt skadepotensiale; i det tilfelle at fremmed etterretning får innsyn i kritisk statsinformasjon foreligger de beste forutsetninger for å senere undergrave statens virke. Terrorangrep innebærer synlig vold, med mål om å skape frykt og forstyrrelser i et samfunn. Selv om cyberspionasje i seg selv ikke innebærer vold i tradisjonell forstand, legger det til rette for senere angrep i tillegg til innsyn i vitale statsorganer. Om det skjer, bli det ekstra vanskelig å håndtere en nødsituasjon. Som den estiske politikeren Ene Ergma sa i forbindelse med det massive tjenestenekt-angrepet rettet mot den estiske regjeringens kommunikasjonskanaler i 2007, 'Like nuclear radiation, cyberwar doesn't make you bleed, but it can destroy everything.'[43]

En videre grunn til å fokusere på cyberspionasje fremfor terrorisme er den manglende lovreguleringen av det digitale rom, som resulterer i at det er færre muligheter for sanksjonering ved skadelige cyberoperasjoner. Manglende sanksjoneringsmuligheter aktualiserer ytterligere spørsmålet om det er nødvendig med preventive tiltak mot cyberspionasje.

Til sist kompliserer cyberspionasje særskilt spenningsforholdet mellom rikets sikkerhet på den ene siden, og demokratiet og menneskerettighetene på den andre siden fordi cyberspionasje i større grad enn terrorisme utfordrer selve bærebjelken for rettsstatens funksjon i og med at institusjonene som skal ivareta og beskytte rettsstaten avhenger av IKT-systemer. Mister vi kontroll over de vitale statsinstitusjonene, mister vi også grunnlaget for å kunne håndtere både fysiske og digitale angrep. Samtidig som at staten skal beskytte mot den alvorlige trusselen som cyberspionasje er, med dens uforutsigbarhet og manglende reguleringer, skal også demokratiet og menneskerettighetene ivaretas.

---

42 Etterretningstjenesten (2018) s. 28.

43 Davis (2007).

2.2 Forholdet til norsk og internasjonal rett.

I det følgende skal det redegjøres for grunnlovsbestemmelsene som har størst betydning for rettsstatsidealenes stilling ved opprettelse av DGF, samt de tilsvarende internasjonale bestemmelsene, og forholdet mellom dem. EMD sin tolkning av artikkel 8 tilsvarer FNs menneskerettighetskomités tolkning av SP artikkel 17.[44] Videre er uttalelsene fra FNs menneskerettighetskomité ikke bindende.[45] Av disse grunnene vil ikke FNs tolkning av SP artikkel 17 drøftes særskilt.

2.2.1 Grunnloven § 2 og § 102

Grunnloven skal sikre "demokratiet, rettsstaten og menneskerettighetene" jf. § 2.[46] Med menneskerettighetene siktes det til konvensjonene som er listet opp i menneskerettslovens § 2, og som etter samme lovs § 3 skal gå foran norsk lov ved motstrid.[47] Samtidig må det presiseres at Grunnloven § 92 legger til grunn at menneskerettighetene skal respekteres og sikres "slik de er nedfelt i denne grunnlov og i for Norge bindende traktater om menneskerettigheter." Grunnloven § 92 er i følge Holship-dommen derfor ikke en inkorporasjonshjemmel, men et påbud om "å håndheve menneskerettighetene på det nivået de er gjennomført i norsk rett."[48] Det er altså ikke slik at alle menneskerettighetskonvensjonene som binder Norge har Grunnlovs rang. Men sammen med demokratiet og rettsstaten er menneskerettighetene grunnleggende verdier, og Grunnloven § 2 vil i følge Lønningutvalget ha stor betydning for tolkningen av samtlige bestemmelser i Grunnloven.[49]

Vernet om privatlivets fred er nedtegnet i Grunnloven § 102, der det i første ledd fremgår at hver enkelt har rett til "respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon." Videre fremgår det i annet ledd at det er pålagt myndighetene å verne borgernes "personlige integritet."[50] De mest aktuelle delene av Grunnloven § 102 i forhold til DGF er retten til privatliv og kommunikasjon. Som det fremgår av ordlyden i § 102, favner begrepet "privatliv" vidt. I Maria-dommen viser høyesterett til EMD sin vektleggelse av "menneskets fysiske og psykiske integritet".[51] Det er derfor sentralt å verne om menneskers lovlige råderett

---

44 NOU 2015:13 s. 78.

45 SP artikkel 40(4).

46 Grunnloven § 2.

47 Menneskerettsloven §§ 2, 3.

48 HR-2016-2554-P, i avsn. 70.

49 Dokument 16 (2011-2012) s. 51.

50 Grunnloven § 102.

51 Rt. 2015 s. 93 i avsn. 58.

over livene sine uten frykt for at myndighetene uberettiget skal gripe inn. "Respekten" for privatlivet går derfor ut på å verne mot den slags maktmisbruk fra offentlige myndigheters hold. Hva angår "kommunikasjon" er det i følge Lønningutvalget ment å blant annet sikte til "nye digitale medier" for å kunne dekke alle nye kommunikasjonsmidler.[52]

I forbindelse med grunnlovsendringen i 2014 fremgår det av Lønningutvalget at en motivasjon for den nye § 102 er å på alle rettsområder sikre retten til "privatlivets fred, personvern og personopplysningsvern", samt å løfte fram rettigheten på grunnlovsnivå.[53] Videre trekkes det frem at grunnlovsfestningen er ekstra aktuell i forhold til den raske teknologiske utviklingen, derav økning i mekanismer for overvåking og kontroll, og utfordringene den kommer til å ha for beskyttelse av privatlivets fred, siden lovverket ikke vil kunne utvikles like rast som teknologien. Det påpekes også at hensynet til utviklingen av et velfungerende demokrati vil henge sammen med beskyttelsen av privatlivets fred fordi systemer med utbredt overvåkning og kontroll vil kunne føre til frykt for at personlige opplysninger skal komme på avveie, og derfor medføre redusert livsutfoldelse.[54] Uten at Lønningutvalget bruker begrepet eksplisitt, er det grunn til å si at det vises til det som ovenfor er referert til som "nedkjølingseffekten".

Med utgangspunkt i Lønningutvalgets utredning kan det legges til grunn at retten til privatlivets fred skal stå like sterkt, selv i møte med teknologiens utvikling og alle kontroll- og overvåkningsmekanismer det medfører. Beskyttelsen av privatlivets fred som en sentral menneskerett- og forutsetning for demokratiet, viser Grunnloven § 102 sin forankring i § 2, og dermed hva Norge vektlegger som rettsstat. Selv om ivaretakelse av rikets sikkerhet også er en sentral del av rettsstaten, har altså ikke hensynet til rikets sikkerhet like stor eksplisitt forankring i Grunnloven som en side av hva det innebærer å være en rettsstat. Det vil ha en del å si for vurderingen om hvorvidt DGF mot cyberspionasje vil være forholdsmessig i Norge.

DGF vil medføre innsamling av informasjon som ikke er en del av etterretningen. Det vil derfor medføre et inngrep i norske borgeres privatliv når kommunikasjon er utsatt for overvåkning. I motsetning til EMK artikkel 8 og EU-charteret artikkel 7 og 8 inneholder Grunnlovens bestemmelsen i § 102 ingen unntaksbestemmelse. Det er likevel lagt til grunn at Grunnlovens bestemmelse følger folkeretten på dette området.[55] EMK artikkel 8 og EU-charterets artikkel

---

52 Dokument 16 (2011-2012) s. 178.

53 Dokument 16 (2011-2012) s. 175.

54 Dokument 16 (2011-2012) s. 176

55 Rt. 2015 s. 93 i avsn. 60.

52(1) åpner for unntak fra inngrepsforbudet når det foreligger hjemmel for inngrep, er nødvendig i et demokratisk samfunn, og er av interesse for nasjonal sikkerhet.[56]

2.2.2 Forholdet til parallelle internasjonale bestemmelser

I og med at EMK er inkorporert som norsk lov jf. menneskerettsloven § 3, vil naturligvis EMD sin tolkning av tvillingbestemmelsen i EMK artikkel 8 bli tillagt stor vekt ved anvendelse av Grunnloven § 102. Norge forholder seg til EU-retten gjennom Lov om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS-loven), som i § 2 jf. § 1 har gjort hoveddelen av EØS-avtalen til norsk lov på samme måte som menneskerettsloven § 3 har gjort et utvalg av menneskerettighetskonvensjoner til norsk lov. EU-charteret beskytter privatlivet, personvernet og personopplysningsvernet i artikkel 7 og 8. I følge Høyesterettsdommer Bårdsen, er Grunnloven § 102 inspirert av artikkel 7 og 8 i EU-charteret.[57] EU-domstolens tolkning av disse bestemmelsene vil som følge ha innvirkning på tolkningen av Grunnloven § 102. På EU-rettens område følger det videre av homogenitetsprinsippet i EØS-avtalen artikkel 1 at formålet er identisk tolkning av EØS-regler innad i EØS, samt at EØS-avtalen skal speile EUs regelverk.[58] EU-domstolen har derfor stor betydning for hvordan Norge innretter seg jf. EØS-avtalen artikkel 6 og ODA-avtalen artikkel 3 annet ledd.[59] Kort sagt setter menneskerettslovens § 3 og EØS-lovens § 2 forpliktelser og rammer for norsk lovgivning.[60]

I Maria-dommen uttalte retten likevel på generelt grunnlag at det til syvende og sist er Høyesterett som skal ”tolke, avklare og utvikle Grunnlovens menneskerettigheter.”[61] Høyesteretts uttalelse må ses i sammenheng med at Norge følger dualismegrunnsetningen, som går ut på at norsk rett som hovedregel går foran folkeretten ved motstridstilfeller. Likevel må norsk lov presumeres å være i overenstemmelse med folkeretten.[62] Dualismegrunnsettingen aktualiseres derfor kun ved motstrid.

---

56 EMK art. 8(2).

57 Bårdsen (2017) s. 6.

58 Bårdsen (2017) s. 3.

59 Arnesen (2014) s. 223.

60 Knoph (2014) s. 49.

61 Rt. 2015 s. 93 i avsn. 57.

62 Rt. 2007 s. 234 i avsn. 54.

3 Forholdsmessigheten av digitalt grenseforsvar

Den videre framstillingen berører selve kjernen i problemstillingen, altså hvorvidt DGF bør innføres i Norge basert på Lysne II-utvalgets utredning holdt opp i mot de nasjonale og internasjonale forpliktelsene som nevnt ovenfor. Det tas utgangspunkt i praksis fra EMD og EU-domstolen i forhold til EMK artikkel 8 og EU-charteret artikkel 7 og 8 jf. 52(1). I hovedsak vil EMK artikkel 8 med følgende tolkning fra EMD være den viktigste pekepinn på rammeverket ved opprettelse av DGF fordi EMD har størst direkte relevans for Norge. EU-domstolen har også direkte betydning for Norge, men under nærmere betingelser, noe som vil belyses nærmere i 2.2.2 og 2.3. EU-domstolens praksis vil derfor i hovedsak ha supplerende effekt på analysen.

Analysen struktureres etter samme metode som EMD og EU-domstolen anvender, altså ved å spørre om det foreligger inngrep, om det finnes tilstrekkelig lovhjemmel, om formålets gyldighet, og hvorvidt inngrepet er nødvendig i et demokratisk samfunn. Det er nødvendigheten i et demokratisk samfunn som er hovedgrunnlaget for bedømmelsen av forholdsmessigheten av DGF, men de andre momentene vil drøftes for å gi et helhetlig inntrykk av de utfordringene DGF medfører for rettsstatsidealene. Siden spørsmålet om DGF er til høring vil analysen få en prinsipiell karakter, og derfor koke ned til spørsmålet om overvåkning fra myndighetenes side er i ferd med å gå for langt i forhold til hva som etter Grunnloven er en rettsstat verdig. Derunder vil Lysne II-utvalgets foreløpige utredning og de internasjonale skrankene være retningslinjer på hvor lista bør ligge i forhold til overvåkningens omfang. Analysen vil underveis suppleres med rettspolitiske betraktninger rundt problemstillingen.

3.1 Praksis fra EMD og EU-domstolen

Forholdet mellom EMD og EU-domstolen på menneskerettighetenes område er langt på vei samkjørt gjennom Traktaten om Den europeiske union (TEU) artikkel 6(2), der det fremgår at EU skal være medlem av EMK,[63] noe som blant annet tilsier at EU er villig til å rette seg etter EMD som en ekstern domstolskontroll.[64] Det fremgår også av TEU artikkel 6(1) at EU-charteret skal ha samme status som de øvrige traktatene. I EU-charteret artikkel 52(3) er EMK omtalt som generelle prinsipper for tilsvarende menneskerettigheter innad i EU. EMK fungerer derfor som menneskerettslige minimumsstandarder som EU har pålagt seg selv å etterleve.[65]

---

63 TEU art. 6(2).

64 Lock (2012) s. 109-110.

65 Lock (2012) s. 110.

På samme tid har EMD uttalt at det er aktuelt å vektlegge EU-domstolens tolkning og anvendelse av EU-charterets bestemmelser om retten til privatlivets fred i artikkel 7 og 8 i møte med den stadige utviklingen av avanserte overvåkningsmetoder. Hensynet bak EMD sitt skråblikk på EU-domstolens håndtering av overvåkningsspørsmål er å sikre en rettsutvikling som etter beste evne ivaretar konvensjonsrettighetene.[66] Erkjennelsen av at samarbeid er nødvendig for å på best mulig vis utvikle lovverket i tråd med den teknologiske utviklingen er et viktig steg på veien til ivaretakelse av det felles verdigrunnlaget som både EMK og EU-charteret gir uttrykk for. På det viset kan lovverket stå sterkere mot fristelsen til impulsiv lovgivning som i øyeblikket kan virke effektiv, men som på sikt har nedbrytende effekt på rettsstatsidealene. Samtidig må det erkjennes at hver stat står overfor ulike alvorlighetsgrader av trusler, og at blant annet politisk kultur kan ha innvirkning på hvorvidt et overvåkningssystem mot cyberspionasje utgjør en reell trussel mot rettsstaten.

I tråd med den raske teknologiske utviklingen, er domstolspraksisen på kommunikasjonsovervåkning i stadig utvikling. De to mest relevante dommene for DGF er EMD sin Big Brother Watch and Others v. The United Kingdom (Big Brother Watch) og Centrum för Rättvisa v. Sweden (Centrum-dommen). Begge dommene kom ut i 2018, og behandler hemmelig bulk innsamling av data som tiltak for beskyttelse av rikets sikkerhet i forhold til EMK artikkel 8. Som Lysne II-utvalget fastslår, innebærer DGF blant annet bulk innsamling av data. Dommene legger til grunn at bulk innsamling av data i seg selv ikke er konvensjonsstridig.[67] Hvorvidt bulk innsamling utgjør uforholdsmessige inngrep i privatlivets fred kommer an på om det foreligger tilstrekkelig lovhjemmel, og kontrollmekanismer for søk i dataene.[68] I Big Brother Watch ble det fastslått brudd på EMK artikkel 8,[69] mens det i Centrum-dommen ble fastslått å ikke foreligge brudd.[70]

Fra EU-retten er det særlig storkammersaken Digital Rights Ireland v. Minister of Communications & Others[71] (Digital Rights Ireland) og den prejudisielle Tele2 Sverige AB v. Post- och telestyrelsen[72] (Tele2-saken). I Digital Rights Ireland ble det avgjort at Datalagringsdirektivet stred mot EU-charteret artikkel 7 og 8[73] blant annet fordi direktivet overskred det som var strengt nødvendig for å ivareta rikets sikkerhet.[74] To år senere fulgte EU-domstolen opp med

---

66 Szabó-dommen, avsn. 68.

67 Big Brother Watch, avsn. 112, Centrum-dommen avsn. 314.

68 Lysne (2016) s. 39.

69 EMD rapport 221(2018).

70 Centrum-dommen, avsn. 181.

71 Sak C-293/12.

72 Sak C-203/15.

73 Sak C-293/12, avsn. 69.

74 Sak C-293/12, avsn. 62.

Tele2-saken, som er relevant for gjennomføring av DGF i Norge fordi Kommunikasjonsdirektivet er inkludert i EØS-avtalens vedlegg XI, og er i norsk lov gjennomført gjennom personopplysningsloven, ekomloven og ekomforskriften.[75] I Tele2-saken ble det i tråd med Digital Rights Ireland lagt til grunn at EU-charteret artikkel 7 og 8 ikke tillater generell og utskillingsløs lagring av trafikk- og lokaliseringsdata fra brukere av digitale kommunikasjonsmidler.[76]

Begge dommene fra EU-domstolen legger til grunn at det er målrettet, og ikke generell overvåkning som på nærmere vilkår kan tillates. Det samme er dessuten lagt til grunn i Szabó and Vissy v. Hungary (Szabó-dommen) fra EMD, som i likhet med Tele2-saken kom ut i 2016. På den måten sett er de tre sistnevnte dommene forskjellig fra Big Brother Watch- dommen og Centrum-dommen. EU-dommene og Szabó-dommen er likevel relevante for DGF fordi e-tjenesten ved søk i innsamlet data vil gå mer målrettet til verks enn ved selve lagringen av bulk data.

Samlet sett er alle dommene på sitt vis relevant som rettslige rammer for DGF. EMD of EU-domstolen er stort sett samstemte med tanke på hvordan overvåkning skal reguleres, men det er likevel noen nyanser i forhold til hva dommene legger særlig vekt på. Formålet med anvendelsen av dommene er først og fremst å redegjøre for det fullstendige regelsettet som Norge må forholde seg til ved innføring av DGF. Hvorvidt for eksempel EU-domstolen går lengre enn EMK i beskyttelsen av privatlivets fred vil belyses, men ikke drøftes særskilt med mindre det har relevans for innføring av DGF i Norge.
Dommene gir også grunnlag for å påstå at det har skjedd en utvikling i rettspraksis fra EMD sin side, i og med at lagring av bulk data ikke lenger anses som konvensjonsstridig. Denne utviklingen gir ytterlig grunnlag for en rettspolitisk drøftelse om hvorvidt overvåkning er i ferd med å bli uforholdsmessig utbredt.

[75] Senter for europarett (2017).

[76] Sak C-203/15, avsn. 112.

3.2 Inngrep og proporsjonalitet

Felles for EMK og EU-charterets bestemmelser om retten til privatliv er at de er inngrepshjemler, og derfor ikke absolutte i motsetning til for eksempel forbudet mot tortur i EMK artikkel 3. Ved drøftelsen av hvorvidt det foreligger brudd på privatlivets fred etter Grunnloven § 102 jf. EMK artikkel 8 og EU-charteret artikkel 7 og 8 jf. 52(1) må det først spørres om det foreligger et inngrep. Lysne II-utvalget legger selv til grunn at DGF vil føre til et inngrep i "privatliv og korrespondanse,"[77] så den delen av vurderingen er det ikke grunn til å gå videre innpå.

Når det er slått fast at det foreligger et inngrep i privatlivets fred ved innføring av DGF må det foretas en proporsjonalitetsdrøftelse for å vurdere om inngrepet likevel er tillatt etter konvensjonen. Proporsjonalitetsdrøftelsen er derfor et redskap for å drøfte forholdsmessigheten mellom DGF og rettsstatsidealene, med retten til privatlivets fred som et premiss for demokratiets funksjon. Forholdsmessighet blir dermed et dekkende begrep for proporsjonalitetsprinsippet, som består av flere typer drøftelser. I den videre drøftelsen vil "proporsjonalitet" bli anvendt som et mer presiserende begrep enn forholdsmessighet.

Proporsjonalitetsprinsippet avgjør hvor langt staten kan gå i sitt inngrep basert på målet og middelet, og kan dermed anses som en skranke for statens myndighet. Hvordan hver stat avgjør forholdet mellom retten til privatlivets fred og nasjonal sikkerhet har ingen universell formel, men kommer an på hver stats demokratiske tradisjon, og historie.[78] Denne individuelle vurderingen for hver stat understreker viktigheten av at DGF drøftes innenfor relevante internasjonale rammer, men også gjennom en selvstendig drøftelse i forhold til det norske demokratiet i tråd med Grunnloven § 2 og § 102.

I vid forstand karakteriseres proporsjonalitetsprinsippet som en drøftelse av et tiltaks lovlighet og legitimitet. Lovlighetskravet innebærer at ethvert inngrep må ha hjemmel i lov. Legitimitetskravet kan betegnes som proporsjonalitet i ordinær forstand, og innebærer at ethvert inngrep må motiveres av et lovlig formål, og at det iverksettes gjennom forholdsmessige tiltak. Proporsjonalitet i snever forstand innebærer at det forholdsmessige tiltaket blir gjenstand for en interesseavveiing utover det konkrete tilfellet.[79] I det følgende vil det foretas en vurdering av proporsjonalitet i vid forstand fordi det ved opprettelse av DGF er grunn til å belyse utfordringer ved lovkravet, formålet og nødvendigheten i et demokratisk samfunn. På den måten

---

77 Lysne (2016) s.39.

78 Barak (2010) s. 4.

79 Strand (2015) s. 79.

kan omfanget av DGF best belyses, og dermed gi et dekkende grunnlag for å vurdere hvorvidt det er et forholdsmessig tiltak mot cyberspionasje.

3.3 Lovkravet

Lovkravet reflekterer maktfordelingen som et grunnlag for demokratiet. Det står sentralt at borgere skal kunne kjenne til hvilke regler som forplikter, samt gir rettigheter og friheter, for deretter å kunne innrette seg etter reglene.[80] Et generelt legalitetsprinsipp ble grunnlovsfestet i § 113 ved grunnlovsendringene i 2014.[81] EMD sin praksis på lovkravet reflekterer den demokratiske grunnsetningen i Sunday Times v. The United Kingdom. I dommen fremgår det at to kumulative krav må være oppfylt for at lovkravet skal være oppfylt. Først må det foreligge tilstrekkelig grunnlag i nasjonal lovgivning, videre må lovhjemmelen ha tilstrekkelig presisjon som gjør at det går an å se for seg hvilke konsekvenser en handling kan få.[82] EMD sin uttalelse kan ses parallelt med det som på norsk kalles det formelle og materielle legalitetsprinsippet; det formelle aspektet ved legalitetsprinsippet omhandler kompetansen til vedtakene, og vedtaksformen. Selve innholdet i regelen har dermed mindre betydning.[83]

Det materielle legalitetsprinsippet omhandler krav til presisjon til innholdet i lovgivning som åpner for inngrep, samt tilgjengelighet. Forutberegnelighetshensynet ligger til grunn for det materielle legalitetsprinsippet.[84] Beslektet med det materielle legalitetsprinsippet er det som blant annet Smith refererer til som et "relativt legalitetsprinsipp,"[85] som går ut på at det bør være strengere krav til presisjon i lovhjemmel jo større inngrep det er snakk om. Smith bruker rettigheter med grunnlovsvern som eksempler på lover som bør ha klar hjemmel. I følge Smith har det i norsk rett vært mer fokus på det formelle lovkravet fremfor det materielle.[86] Likevel, med grunnlag i Sunday Times-dommen fremgår det at EMD vektlegger lovgivningens materielle kvaliteter i større grad enn de formelle kvalitetene, for eksempel gjennom uttalelsen "prescribed by law constitutes not only statute but also unwritten law."[87]

I dag eksisterer det ikke lovgivning som omhandler DGF og utfordringene det medfører. Lysne II-utvalget har selv uttalt at det nødvendigvis må komme ny lovgivning på dette fel-

---

80 Smith (2014) s. 230.

81 Smith (2014) s. 228.

82 Sunday Times v the United Kingdom avsn. 49.

83 Smith (2014) s. 232.

84 Smith (2015) s. 370.

85 Smith (2014) s. 231.

86 Smith (2014) s. 370.

87 Sunday Times v the United Kingdom avsn. 47.

tet.[88] Det er ikke det formelle lovkravet som er problematisk, men heller det materielle. Ut i fra Smiths påstand om hovedfokus på det formelle lovkravet i norsk rett, blir det interessant å se hvordan ny lovgivning om DGF forholder seg til folkerettens krav til presisjon. I og med at lovgivningen vil legitimere inngrep i en grunnlovsfestet rettighet vil det utvilsomt måtte settes høye krav til presisjon. I det videre vil folkerettens krav til lovhjemmelen redegjøres for, samt utfordringene det medfører.

I alle dommene problematiseres det materielle lovkravet, og ikke det formelle. Samtlige av EMD-dommene legger videre til grunn at det må foreligge lovgivning av god kvalitet, som i sin tur innebærer at lovgivningen må være tilgjengelig og forutsigbar.[89] Tele2-saken legger til grunn at lovene må være klare og presise, samt inneholde minstegarantier mot misbruk av lagret data.[90] Lysne II-utvalget problematiserer ikke lovkravet på samme måte som selve forholdsmessighetsvurderingen. Det legges til grunn at ny lovgivning ved innføring av DGF vil etterleve de folkerettslige kravene til "klarhet og presisjon."[91] Det er klart at forholdsmessighetsvurderingen vil være av større betydning, men det er likevel grunn til å belyse utfordringer ved lovkravet.

For å unngå maktmisbruk ved søk i kommunikasjonsdata er det i Szabó-dommen, Centrum-dommen og Big Brother Watch vist til seks minimumskriterier som må fremgå av hjemmel i lov som er utviklet i rettspraksis. Kriteriene gjelder for både bulk innsamling og målrettet innsamling av informasjon. For det første må det framgå hvilken type handlinger som gjør at man kan komme i søkelyset, deretter hvilken kategori mennesker som er aktuelle for overvåkning, deretter en begrensning på varigheten av overvåkningen, så en metode for eksaminering, bruk og oppholdelse av data, så forhåndsregler ved videreføring av data til andre aktører, og til slutt redegjørelse for tilfeller der data kan eller må tilintetgjøres.[92] Momentene i kravet til lovhjemmel i EMD-dommene tydeliggjør at det ikke er hvem som helst som kan bli utsatt for overvåkning. Sånn sett foreligger det begrensninger som er viktig for lovverkets forutsigbarhet, og for ivaretakelsen av borgernes tillit til myndighetene.

Lysne II-utvalget fastslår at det blir nødvendig å angi kvalifiserende vilkår for datasøk, samt kontrollmekanismer. Blant annet må ny lovgivning under enhver omstendighet inneholde krav om strengt målrettet etterretningsmessig bruk av lagret informasjon, sletting av overskuddsinformajson, forbud mot å bruke tilfeldig informasjon som bevis i straffesaker, samt forsikring

---

88 Lysne II (2016) s. 62.

89 Szabó-dommen avsn. 59, Centrum-dommen avsn. 100, Big Brother Watch avsn. 305.

90 Sak C-203/15 avsn. 109.

91 Lysne II (2016) s.39

92 Szabó-dommen avsn. 56, Centrum-dommen avsn. 103, Big Brother Watch avsn. 307.

om lik beskyttelse av personvernet uavhengig av nasjonalitet, livssyn og andre personlige særtrekk som det ellers ikke er grunn til å foreta søk på.[93] Videre vil vilkårene for søk avhenge av kontrollmekanismene. Det er med dette grunn til å gå ut ifra at det ved lovgivningen vil etterstrebes å følge kriteriene fra EMD.

Lysne II-utvalget oppgir likevel at et hovedvilkår for søk i både metadata og innholdsdata vil være at det er snakk om situasjoner hvor det er "rimelig grunn" til å undersøke basert på etterretningsmessige formål i tråd med etterretningstjenestelovens § 1 og § 3.[94] I Big Brother Watch mente den saksøkende part at det i tillegg til de seks kriteriene måtte legges til et ytterlig kriterium om "reasonable suspiscion" ved søk i dataene av hensyn til omfanget av informasjon som kan hentes frem ved søk.[95] EMD uttalte at siden bulk innsamling per definisjon ikke er målrettet, vil objektive beviskrav for tilgang til data umuliggjøre funksjonen ved bulk innsamling av data, og ser derfor bort fra nødvendigheten av et slikt krav. Det kan se ut som at Lysne II-utvalget med dette legger til grunn strengere kriterier enn det EMD gjør. Siden de seks kriteriene er minimumsvilkår står Norge fritt til å legge til et slikt kriterium, og vil dermed redusere sannsynligheten for maktmisbruk fra myndighetenes side.

I Szabó-dommen var det spørsmål om den nasjonale lovgivningen var detaljert og presis nok til å være tilstrekkelig forutsigbar. EMD uttalte at kravet til forutsigbarheten i lovgivning som angår kommunikasjonsovervåkning nødvendigvis må være annerledes enn på andre områder. Lovgivningen kan ikke være detaljert nok til at aktører med onde hensikter kan omgå lovgivningen. Samtidig, på områder som angår grunnleggende rettigheter må lovgivningen indikere omfanget av, og omstendighetene som legitimerer kommunikasjonskontroll. Det kan leses ut av Szabó-dommen at det må kunne vises en sammenheng mellom kategorien av aktuelle personer og ivaretakelsen av rikets sikkerhet.[96] For eksempel vil det ikke være nok å referere til "rikets sikkerhet" eller "terrortrussel". Big Brother Watch viser også til denne uttalelsen som bakteppe for de seks minimumskriteriene til lov som hjemler overvåkning.[97]

Lysne II-utvalget erkjenner at enkelte regulatoriske momenter med DGF ikke kan være tilgjengelige av hensyn til etterretningens virke. Inngrep i privatliv og korrespondanse er alvorlig. Det er en vanskelig lovteknisk øvelse å skulle etterleve kravet til presisjon samtidig som at hjemmelen ikke skal fungere som oppskrift på hvordan man kan kommunisere uten å komme i søkelyset. Utfordringene med presis lovgivning fremgår av både Big Brother Watch

---

93 Lysne II (2016) s. 60-61.

94 Lysne II (2016) s. 63.

95 Big Brother Watch, avsn. 316.

96 Szabó-dommen avsn. 67.

97 Big Brother Watch avsn. 306.

og Szabó-dommen, der det ble slått fast at det forelå brudd på EMK artikkel 8 blant annet fordi lovverket rundt kommunikasjonsoveråkning ikke ga tilstrekkelig sikkerhet mot myndighetsmisbruk.[98]

I Tele2-saken vektlegges det særlig at lovgivningen må gi indikasjoner på hvilke omstendigheter og betingelser som kan åpne for kommunikasjonskontroll for å sikre at overvåkningen begrenses til det som er "strictly necessary." Tele2-saken sier i forlengelsen av dette at nasjonal lovgivning må oppgi omstendigheter hvor hemmelig søk kan forekomme.[99] Det kan se ut til at EU-domstolen legger strengere krav til grunn for hvilke kriterier som kan legges til grunn siden de må være "strictly necessary." Nødvendighetskravet skal drøftes nærmere under avsnitt 3.5.2, men det er likevel relevant å påpeke under lovkravet fordi det kan påvirke hvilke kriterier loven må oppstille for å være tilstrekkelig klar og presis til å legitimere hemmelig søk.

Til tross for retningslinjene fra EMD og EU-domstolen er det på prinsipielt grunnlag fremdeles aktuelt å diskutere lovverkets forutberegnelighet. Generelt er det en utfordring å få lovgivningen til å henge med på den teknologiske utviklingen; det utvikles stadig mer sofistikerte instrumenter og metoder for å forhindre cyberspionasje, samtidig som det stadig utvikles metoder for å omgå disse systemene, for eksempel kryptering, som beskytter informasjonskonfidensialitet. Kryptering har økt i tilgjengelighet og styrke etter Snowden-avsløringen, noe som kommer til å skape utfordringer for etterretningstjenesten. DGF kan avdekke noe kryptert informasjon, men vil ha større problemer med å avdekke den informasjonen som er sterk kryptert.[100]

Begrepet "sorte svaner" er brukt om slike uventede hendelser, som ofte får alvorlige konsekvenser, men som likevel kan forklares ut i fra på tidspunktet tilgjengelig informasjon som likevel blir ansett for å vær ubetydelig før en alvorlig hendelse inntreffer.[101] Teknologien overrasker stadig, og dens raske utvikling tilsier at lite kan utelukkes. Samtidig er det velkjent at lovgivning ofte tar noe tid å få etablert. Det er også påpekt at det tillates mer og mer overvåkning, noe som kan være et resultat av teknologiens raske utvikling, kanskje fordi det er lettere å tillate mer enn det er å begrense det, når rettssystemer uansett tvinges til å forholde seg til den teknologiske utviklingen.

---

98 Big Brother Watch avsn. 388, Szabó-dommen avsn. 86.

99 Sak C-203/15 avsn. 109.

100 Lysne II (2016) s. 49.

101 Meld. St. 10 (2016-2017) s. 28.

Det at lovgivning som åpner for økt overvåkning ikke problematiseres her og nå, trenger ikke å bety at det for all framtid vil være like uproblematisk. Man må forholde seg til teknologi, men ikke glemme at den skaper utfordringer. Det er derfor viktig med et langtidsperspektiv på konsekvensene av den teknologiske utviklingen. Det gjelder også hvordan lovverket utvikler seg. Hvorvidt man kan skape et forutsigbart lovverk for lagring av, og søk i data ved opprettelse av DGF kommer an på hvor fort teknologien utvikler seg. Loven bør ikke tolkes for vidt i møte med nye teknologiske utfordringer fordi det fort kan føre til svært inngripende handlinger på altfor tynt rettslig grunnlag.

3.4 Formålskravet

I forhold til formålskravet fremgår det av EMK artikkel 8(2) jf. EU-charteret artikkel 52(1) at hensynet til nasjonal sikkerhet er et lovlig formål. Det samme fremgår av etterretningstjenesteloven § 1a som sier at det skal tilrettelegges for en effektiv kartlegging og motvirkning av "ytre trusler mot rikets selvstendighet og sikkerhet".[102] I Szabó-dommen nevner EMD den generelle grunnsetningen at vurderingen av hva som til enhver tid er nødvendig for å ivareta nasjonal sikkerhet i stor grad faller innenfor medlemsstatenes skjønnsmargin. Det nevnes samtidig at demokratiet er sårbart ved bruk av overvåkning for å beskytte nasjonal sikkerhet, og at det derfor er viktig med kontrollmekanismer for å forhindre misbruk av informasjon.[103] Gjennom sin uttalelse belyser EMD at påberopelse av nasjonal sikkerhet ved et så inngripende tiltak som overvåkning er legitimt i den utstrekning det er nødvendig i et demokratisk samfunn. Det er her grensen mellom målet og middelet blandes, og denne grensen vil drøftes nærmere i 3.5 og 3.6. Det er likevel verdt å nevne at det spesifikke formålet ikke ubegrunnet kan påberopes som et skalkeskjul for det som egentlig er maktmisbruk fra myndighetenes side.

Lysne II-utvalget viser til sikkerhetsutfordringer som begrunnelse for DGF fordi digitale trusler er på fremmarsj, og at de ikke kan kontrolleres med tilgjengelige instrumenter. Formålets lovlighet i seg selv kan dermed ikke bestrides. Det må likevel drøftes om hensynet til nasjonal sikkerhet står såpass sterkt i dette tilfelle at de konkrete tiltakene og konsekvensene som DGF medfører er nødvendige.

---

[102] Etterretningstjenesteloven §1a.

[103] Szabó-dommen avsn. 57.

3.5 Nødvendig i et demokratisk samfunn?

Hovedutfordringen er hvorvidt DGF er nødvendig i et demokratisk samfunn. Nasjonal sikkerhet skal derfor vurderes i forhold til rettsstatsidealene demokrati og menneskerettigheter. Som nevnt er det ikke et motsetningsforhold mellom nasjonal sikkerhet og rettsstatsidealene. Et tema som belyser det er risikoaspektet. Som følge vil risikoaspektet redegjøres for før selve interesseavveiingen, og vil fungere som et gjennomgående hensyn ved interesseavveiingen. Det er også grunn til å drøfte hva EMD og EU-domstolen legger i nødvendighetskravet før selve interesseavveiingen. Grunnen er at rettspraksis tilsier en viss utvikling de siste to årene, noe som får betydning for hvilke momenter som skal vektlegges ved interesseavveiingen. Utviklingen av innholdet i nødvendighetskravet er forøvrig et eget moment i vurderingen om hvorvidt Norge bør innføre DGF.

3.5.1 Risikoaspektet

Avveiingen i det følgende går ut på å finne et balansepunkt mellom rikets sikkerhet og retten til privatliv innenfor rammene av et demokratisk samfunn. Som nevnt innledningsvis vil betydningen av rikets sikkerhet variere med tiden, og må som følge defineres ut i fra samfunnsutviklingen. Statsviter Kristian Åtland har i sin artikkel om utviklingen av sikkerhetsbegrepet vist til litteratur som påpeker at det moderne sikkerhetsbegrepet ikke lenger kun er knyttet til den tradisjonelle staten og militærmakten, men at også individer og internasjonalisering, samt flere samfunnssektorer dekkes av begrepet. I tillegg er det påpekt at nasjonal sikkerhet må ses i sammenheng med risiko.[104] Åtland viser blant annet til Ulrich Beck sitt risikobegrep, som går ut på at det er moderniseringen selv som har skapt de risiki vi lever med i dag, og at vi må fokusere på "boomerang-effekten" av våre egne handlinger framfor å knytte risiko til et "oss og dem" perspektiv.[105] Dette betyr at trusler utenfra ikke bare kommer fra stater, men at trusselbildet i større grad preges av individuelle aktører. Dessuten, den teknologiske utviklingen fører til at geografi ikke er en hindring i forhold til hvor trusler og angrep kommer fra.[106] For eksempel har Kina like stor mulighet til å spionere på Norge som det Russland har.[107] Siden statlig cyberspionasje er hovedtema i denne oppgaven, kan Becks teori virke selvmotsigende. Statlig cyberspionasje må likevel ses som en av mange cybertrusler, og det er ikke ubestridt at trusselen fra individuelle aktører er minst like fremtredende.[108] Et typisk karaktertrekk ved cyberspionasje er at det ofte foregår mellom stater.[109] I tillegg har norsk etterretning avdekket

---

104 Åtland (2008).

105 Fra Ulrich Becks bok *Risk Society: Towards a New Modernity,* 1992.

106 Åtland (2008).

107 Platt (2012) s. 160.

108 NOU 2016:19 s. 56.

109 Platt (2012) s. 159.

statlig spionasje, og det har mest for seg å fokusere på trusler som man med sikkerhet vet eksisterer i forhold til spørsmålet om DGF er forholdsmessig.

I forarbeidene til den nye sikkerhetsloven som ennå ikke har trådt i kraft, vises det også til en mer risikobasert tilnærming i forhold til rikets sikkerhet, og som derfor har blitt lagt til grunn ved forslag til ny sikkerhetslov. Videre påpekes det at trusselbildet er mer utfordrende enn på lenge grunnet kombinasjonen av statlige og ikke statlige aktører, samt at teknologi bidrar til et uforutsigbart og uoversiktlig trusselbilde.[110]

Becks teori om "boomerang-effekten" kan derfor sies å være reell: mennesker skaper og utvikler teknologien. Vi gjør oss avhengig av den gjennom IKT-systemer. Samtidig skaper vi våre egne sårbarheter. Teknologien slår tilbake på oss fordi den er den mest effektive måten å skade et IKT-avhengig samfunn på. I tillegg er den uforutsigbar og uoversiktlig, og bærer derfor med seg stor risiko. Som det påpekes i NOU 2016:19, så lever vi i et risikosamfunn. Det å skape sikkerhet i et risikosamfunn er et spørsmål om hva vi må akseptere å leve med, holdt opp imot hva vi kan forhindre gjennom kontrollmekanismer. Det er derfor grunn til å si at begrepet "rikets sikkerhet" nødvendigvis må inkludere risikoaspektet.

Hva vi skal kontrollere gjennom kontrollmekanismer er i sin tur et demokratisk spørsmål. Det at vi kan kontrollere noe betyr ikke nødvendigvis at vi bør kontrollere det. Det må erkjennes at teknologien har skapt nye risiki, og vi tvinges til å forholde oss til dem når de utfordrer det demokratiske samfunnet vi ønsker å ivareta. Vedtak om å kontrollere et uforutsigbart og uoversiktlig cyberrom krever naturligvis sterke mekanismer. Velger vi å foreta de nødvendige grepene kan vi ikke på samme tid forvente at vernet om privatlivets fred vil stå like sterkt. Om det videre legges til grunn at vernet om privatlivets fred er selve premisset for et velfungerende demokrati kan det deretter spørres om ikke demokratiet også svekkes ved tiltakene for å øke rikets sikkerhet. Det er viktig at myndighetene spiller med åpne kort om denne avveiingen, slik at borgere er innforståtte med hva DGF vil innebære. Kun på det grunnlaget kan det skapes et legitimt lovverk ved innføring av DGF om det skulle aktualiseres. Skal den demokratiske modellen endres, må borgerne velge det selv.

Den andre siden av saken er muligheten for at DGF kan bidra til å opprettholde rettsstatsidealene demokrati og menneskerettigheter gjennom å forhindre en større skade på det norske samfunnet i det tilfelle at cyberspionasje medfører alvorlige konsekvenser, som svekkelse av forsvarets beskyttelsesevne, samt manipulering av essensiell infrastruktur som elektrisitet, flytrafikk, internettilgang osv. Om dette skulle skje vil hele grunnlaget for en fungerende

[110] Prop. 153 L (2016-2017) s. 16.

rettsstat falle sammen. Men disse eksemplene er de verst tenkelige konsekvensene. Det har i alle tider blitt spekulert i dommedag, med frykten for atomkrig under den kalde krigen som et nyere eksempel. Paranoia kan også true fundamentet for en velfungerende rettsstat.

Betraktningene ovenfor angående innholdet av begrepene rikets sikkerhet og rettsstat vil fungere som et bakteppe i den videre forholdsmessighetsvurderingen. Lysne II-utvalgets konkrete vurderinger av DGF vil veies opp mot rammene fra EMD og EU-domstolen, etterfulgt av en drøftelse av hvor gjennomførbart DGF er i det norske samfunnet.

3.5.2 Innholdet i nødvendighetsvurderingen

En dom som på generelt grunnlag oppsummerer innholdet av vurderingen om hvorvidt et inngrep er nødvendig i et demokratisk samfunn er Silver and Others v. The United Kingdom. I dommen uttales det at nødvendighetskravet forutsetter "a pressing social need"[111] – det er altså ikke nok at inngrepet er hensiktsmessig, samtidig behøver det ikke å være uunngåelig.[112]

I forlengelsen av at inngrepet må være nødvendig i et demokratisk samfunn uttaler EMD videre at inngrepet må være "proportionate to the legitimate aim pursued." I forhold til DGF vil vurderingen gå ut på å drøfte om det er tilstrekkelig sammenheng mellom opprettelse av DGF og bekjempelse av cyberspionasje – altså hvorvidt DGF er egnet og nødvendig for å ivareta rikets sikkerhet, og hvorvidt inngrepet som DGF vil utgjøre er forholdsmessig for å sikre rikets sikkerhet.[113]

EMD poengterer at statene har en skjønnsmargin ved avgjørelsen om det skal foretas et inngrep i borgernes rettigheter fordi den enkelte stat står nærmest i å avgjøre hva som er nødvendig å foreta i den konkrete situasjonen som tilsier at inngrep er nødvendig. EMD har likevel siste ord i saken når det kommer til nødvendigheten av inngrepet.[114]

Det er fastslått at innsamling av informasjon i bulk er tillatt etter EMD i kraft av å falle innenfor staters skjønnsmargin.[115] Det er likevel vektlagt at det må foreligge "adequate and effective guarantees against abuse," og at vurderingen deretter går ut på om "the nature, scope and duration of the possible measures, the grounds required for ordering them, the competent to

---

111 Silver and Others v. The United Kingdom avsn. 97.

112 Høstmælingen (2013) s. 128.

113 Strand (2015) s. 79.

114 Silver and Others v. The United Kingdom avsn. 97.

115 Centrum-dommen avsn. 112, Big Brother Watch avsn. 314, jf. Weber and Saravia v. Germany, Liberty and Others v. The United Kingdom.

authorise, carry out and supervise them, and the kind of remedy provided by the national law."[116] Utfordringen ligger dermed i å forvalte informasjonen på en lovlig og så etisk måte som mulig, noe Lysne II-utvalget også erkjenner. I Big Brother Watch er det lagt til grunn at de seks minimumskravene til lovhjemmel som nevnt i 3.3 må oppfylles for å unngå at overvåkning misbrukes til myndighetens fordel. De seks minimumskravene er nå ansett å gjelde for både generell og målrettet overvåkning.[117] Det kan med dette se ut til at EMD nå legger større vekt på mekanismer for å unngå maktmisbruk framfor en høy terskel for å tillate overvåkning. På samme måte argumenterer den franske professoren i internasjonal rett, Theodore Christakis.[118]

Szabó-dommen, Digital Rights Ireland og Tele2-saken legger til grunn et skjerpet nødvendighetskrav for å tillate overvåkningsteknologi som innebærer hemmelig søk i data om personlige opplysninger om borgere.[119] Det skjerpede nødvendighetskravet må anses som en ytterligere presisering av det generelle nødvendighetskravet jf. Silver and Others v. The United Kingdom, og kan sies å ha sammenheng med omfanget av inngrepet som overvåkningsteknologi innebærer. I Szabó-dommen utdyper EMD at det skjerpede nødvendighetskravet må ses i to henseender; for det første må inngrepet være nødvendig på generelt grunnlag, for eksempel i kraft av å beskytte demokratiske institusjoner. For det andre må inngrepet være nødvendig på et spesifikt grunnlag, for eksempel informasjonssøk i en konkret operasjon. Det skjerpede nødvendighetskravets to komponenter må derfor anses som kumulative vilkår for den typen inngrep som søk i kommunikasjonsdata utgjør. Videre nevner EMD at det skjerpede nødvendighetskravet må ses i sammenheng med behovet for et kontrollorgan overfor vedtak om datasøk; inngrepet bør bedømmes av domstolene framfor politiske organer som for eksempel justisministeren for en mest mulig upartisk og uavhengig vurdering av inngrepets nødvendighet.[120]

I Centrum-dommen og Big Brother Watch legges det ikke et skjerpet nødvendighetskrav til grunn. Det kan forklares ved at det i Szabó-dommen, Digital Rights Ireland, og Tele2-sakene tas utgangspunkt i spesifikke hemmelige søk mot bestemte personer, mens det i Centrum-dommen og Big Brother Watch tas utgangspunkt i generell innsamling av informasjon gjennom bulk data.

---

116 Big Brother Watch, avsn. 308, Centrum-dommen avsn. 104.

117 Big Brother Watch avsn. 315.

118 Christakis (2018).

119 Szabó-dommen avsn. 73, Sak C-293/12 avsn. 62, Sak C-203/15 avsn. 110.

120 Szabó-dommen avsn. 73.

I og med at EMD gjennom Szabó-dommen i likhet med EU-domstolen la til grunn retningslinjer for overvåkning under forutsetning at den er målrettet, kan det nå se ut til at EMD i Big Brother Watch nyanserer regelverket i forhold til om det er snakk om målrettet eller generell overvåkning.[121] Det argumentet kan forsterkes med å vise til at EMD i Centrum-dommen noen måneder tidligere, la til grunn at innsamlet data som det ikke foretas søk i ikke kan anses å utfordre EMK artikkel 8, og at det i stedet er det fra det øyeblikket informasjonen kommer under behandling at bestemmelsen potensielt kan utfordres.[122] Dette fraviker forbudet mot generell og udifferensiert lagring av data, som ble lagt til grunn av EU-domstolen i Digital Rights Ireland, og som senere ble fulgt opp av Szabó-dommen og Tele2-saken.

Uansett om det er snakk om generell eller målrettet overvåkning skal altså de seks minimumskravene til lovhjemmel nå legges til grunn som garanti mot myndighetsmisbruk. Hvorvidt det betyr at EMD med dét utgangspunktet ser bort fra kravet om streng nødvendighet også ved målrettede søk til fordel for grundige sikringsmekanismer mot myndighetsmisbruk kan ikke sies med sikkerhet, men det tyder på at det er et generelt skifte mot lavere terskel for å tillate overvåkning til fordel for strengere kontrollmekanismer for å unngå misbruk av informasjonen som overvåkningen lagrer. Hvorvidt EU-domstolen trekker i samme retning er foreløpig usikkert. Om EU-domstolen tar avstand fra EMD sin praksis vil det oppstå nye problemstillinger som ligger på utsiden av temaet i denne oppgaven.

[121] Christakis (2018).

[122] Centrum-dommen avsn. 146.

3.6 Nødvendighetsvurderingen i forhold til digitalt grenseforsvar

Den videre vurderingen vil ta utgangspunkt i de faste momentene ved nødvendighetsvurderingen, supplert med retningslinjene fra Big Brother Watch som en presisering av vurderingsmomentene i overvåkningskontekst. Den raske digitale utviklingen gjenspeiles i domstolspraksisen; både Tele2-saken og Szabó-dommen kom ut i 2016. Når det to år senere kommer ut en avgjørelse som nyanserer tidligere praksis, er det grunn til å ta utgangspunkt i den. Lysne II-utvalget tar naturligvis stilling til nødvendighetskravet i sin utredning, men nevner ikke direkte det skjerpede nødvendighetskravet, selv om Szabo-dommen og Tele2-saken, i likhet med høringen, kom ut tidlig i 2016, og derfor burde vært veiledende. Sånn sett kan det sies at Lysne II-utvalget refererer til det nødvendighetskravet som vist til i Silver and Others v. The United Kingdom.

3.6.1 Er digitalt grenseforsvar egnet til å ivareta nasjonal sikkerhet?

I Big Brother Watch uttaler EMD om lagring av bulk data at det er en verdifull mekanisme for å ivareta nasjonal sikkerhet, særlig i møte med global terrorisme og alvorlige kriminelle handlinger.[123] Det er verdt å merke at EMD her tar et steg videre fra Centrum-dommen i forhold til aksept for samfunnsovervåkning. Fra å la overvåkning falle under statenes skjønnsmargin ved ivaretakelse av nasjonal sikkerhet,[124] uttrykker EMD nå at det er fordelaktig med bulk innsamling av kommunikasjonsinformasjon. Denne endringen i synet på overvåkning bidrar til å bekrefte at EMD og EU-domstolen for øyeblikket ser noe forskjellig på overvåkning.

Selv om EMD har lagt til grunn at lagring av bulk data er en verdifull metode for å sikre nasjonal sikkerhet, er det er samtidig bemerket at det er en risiko for at hemmelig overvåkning kan ødelegge demokratiet under påstanden om å beskytte det.[125] Det er derfor avgjørende at det foreligger "adequate and efficient guarantees against abuse". Det kan altså legges til grunn at DGF er egnet til å ivareta nasjonal sikkerhet så lenge det foreligger tilstrekkelige garantier mot misbruk av lagrede data. Utover de rent tekniske egenskapene til DGF, vil derfor også en vurdering av kontrollmekanismene ved DGF inngå under vurderingen av hvorvidt DGF er egnet til å ivareta nasjonal sikkerhet. Lysne II-utvalget legger også lignende forutsetninger til grunn. Utover det å ha etterretningsmessig verdi, er grunnleggende premisser for DGF at det innføres i tråd med det som er lovmessig og teknologisk mulig, samt at innføringen ikke reduserer borgeres tillit til etterretningen.[126]

---

123 Big Brother Watch, avsn. 386 jf. avsn. 385.

124 Centrum-dommen avsn. 112.

125 Big Brother Watch avsn. 308, jf. Centrum-dommen avsn. 104.

126 Lysne (2016) s. 70.

3.6.1.1 Teknisk egnethet

Om den tekniske funksjonen til DGF forklarer Lysne II-utvalget at DGF vil fange opp spionasjemateriale som treffer norske datasystemer, og som derifra overfører informasjon til aktøren. Lysne II-utvalget sammenligner verdien av DGF med nåværende system hvor noen få av de viktigste institusjonene har lokale sensorer som fanger opp angrep, men som ikke evner å gi et fullstendig bilde av omfanget av angrepet fordi sensorene kun registrerer trafikk seg imellom, og kan dermed ikke si noe om, og i tilfelle hvilke andre institusjoner som er rammet. Dessuten er det vanskelig å detektere hvem som står bak angrepet fordi det som oftest plasseres mange brukere bak IP-adressen som spionprogramvaren kommer fra.[127] DGF vil derimot lagre all metadata, altså kommunikasjonstrafikk. Om det søkes etter IP-adressen til agenten bak spionprogramvaren avslører den om det foreligger trafikk mot flere mål enn de som allerede er fanget opp av lokale sensorer.[128] På dette viset gir altså DGF et mer presist og tidlig bilde på aktører og omfanget av cyberspionasje, som videre gir bedre grunnlag for å sette i gang mottiltak og skadereduserende tiltak. Med tanke på potensielle konsekvenser av cyberspionasje fra fremmed etterretning som redegjort for i 1.4.2 er det ikke tvilsomt at DGF er en teknisk verdifull mekanisme for å ivareta nasjonal sikkerhet.

3.6.1.2 Rettsstatlige utfordringer

Hvorvidt DGF er en like verdifull mekanisme i kampen mot cyberspionasje med tanke på hvordan DGF påvirker den norske rettsstaten er nå neste vurdering. Som retningslinjer under hva som er ”adequate and efficient guaarantees against abuse” er ”the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and superwise them, and the kind of remedy provided by the national law.”[129]

Lysne II-utvalget refererer til DGF som et instrument for ”innhenting, bearbeiding og analyse”[130] av selektert informasjon som krysser landegrensen. Det distingveres mellom innsamling av metadata og innholdsdata, der metadata samles inn i bulk, og innholdsdata samles inn målrettet. Hvorvidt denne distinksjonen tilsvarer EMD sin distinksjon mellom generelle og målrettede søk fremgår ikke tydelig av dommene og Lysne II-utvalget, men det er grunn til å si at det har likhetstrekk med distinksjonen mellom generell og målrettet innsamling av data.

---

[127] Lysne (2016) s. 72.

[128] Lysne (2016) s. 73.

[129] Jf. Szabó-dommen avsn. 57, Centrum-dommen avsn. 104, Big Brother Watch avsn. 308.

[130] Lysne-II (2016) s. 10.

Lysne II-utvalget viser til etterretningstjenesteloven § 1 og § 3 om ansvaret for å beskytte vitale funksjoner for landets "selvstendighet, sikkerhet og andre viktige nasjonale interesser."[131] Lysne-utvalget knytter også ivaretakelsen av slike vitale funksjoner til Grunnloven §2,[132] altså som en måte å ivareta demokratiet, rettsstaten og menneskerettighetene på. Dette viser til spenningsnivået mellom nasjonal sikkerhet på den ene siden, og rettsstatsprinsipper på den andre siden, noe som Lysne II-utvalget også erkjenner.

Lysne II-utvalget fokuserer mer på hvordan data skal unngå å misbrukes når den er samlet inn. På det grunnlaget er Lysne II-utvalgets utredning mer i tråd med Big Brother Watch, der det blant annet legges til grunn at det ved målrettet datasøk må være strengere krav til adgangen til å foreta søkene siden så godt som all informasjon vil bli analysert. Ved søk i bulk data vil det derimot være adgang til større mengder med informasjon, men strengere kontrollmekanismer ved filtrering og eksaminering av relevant informasjon.[133]

Lysne II-utvalget uttaler at målrettet lagring av innholdsdata ikke vil medføre problemer i forhold til privatlivets fred siden det er uproblematisk å sikre at lageret kun inneholder relevant data siden metadatalageret blant annet har som funksjon å filtrere bort innholdsdata.[134] Sånn sett er det teknisk lettere å sørge for at irrelevant informasjon ikke lagres i innholdslageret. I tillegg må domstolene godkjenne informasjonen som havner i innholdsdatalageret.[135]
Den generelle lagringen av metadata byr derimot på større problemer. Metadatalageret filtrerer bort innholdsdata uten problem, men filtreringen av metadata med irrelevant informasjon for etterretningen er mer utfordrende fordi den vil være "teknisk og resursmessig krevende å filtrere bort".[136] Resultatet blir at metadatalageret inneholder store mengder kommunikasjonsinformasjon mellom norske borgere.

[131] Lysne II (2016) s. 63.
[132] Lysne II (2016) s. 37.
[133] Big Brother Watch avsn. 329.
[134] Lysne II (2016) s. 54.
[135] Lysne II (2016) s. 55.
[136] Lysne II (2016) s. 54.

3.6.1.2.1 Omfanget av metadata

Det er grunn til å spørre om kriteriene for innsamling av, og søk i generell og målrettet informasjon bør være ulike. Selv om DGF kategoriseres som et instrument for innsamling av bulk data, altså generell innsamling av informasjon gjennom masselagring av metadata, og tidvis mulighet for innholdssøk etter nærmere reguleringer, vil DGF i prinsippet innebære både generell og målrettet lagring av informasjon, med metadata som den generelle informasjon, og innholdsdata som den målrettede informasjonen. Lysne II-utvalget vektlegger at det er forskjell mellom metadata og innholdsdata, og at lagring av, og søk i innholdsdata gir informasjon på detaljnivå. Behandling av innholdsdata anses derfor som mer inngripende, og er underlagt strengere rutiner. I Big Brother Watch konstaterte EMD for første gang at lagring av metadata kan være like inngripende som innholdsdata.[137] Den erkjennelsen er viktig for å vurdere premissene for innføring av DGF siden Lysne II-utvalget distingverer mellom inngrepsgraden lagring av metadata og innholdsdata utgjør.

Tidligere generalrådgiver i NSA, Stewart Baker, har uttalt at "Metadata absolutely tells you everything about somebody's life...if you have enough metadata, you don't really need content". [138] Tidligere direktør i NSA, Michael Hayden, har bekreftet Bakers uttalelse med å legge til; "We kill people based on metadata."[139] En kortfattet forklaring på uttalelsene fra NSA er at det ved hjelp av data-algoritmer kan navigeres fram til informasjon om borgeres privatliv, og på den måten kan metadata til og med anses som mer inngripende enn søk i innholdsdata fordi man i prinsippet kan få tilgang på samme informasjon som innholdsdata uten å en gang gå veien om domstoltillatelse, samt foreta avlesning og avlytting på samme måte som man ville vært nødt til ved søk i innholdsdata. Søk i metadata blir derfor også mer kostnadseffektivt enn søk i innholdsdata.[140]

Lysne II-utvalget nevner så vidt skadepotensialet som metadata utgjør,[141] men kan ikke sies å ta tilstrekkelig stilling til dette. I og med at metadata potensielt kan være minst like inngripende som innholdsdata er det alvorlig at dette ikke belyses nærmere, spesielt siden Lysne II-utvalget erkjenner at det vil være vanskelig å filtrere bort den irrelevante metadataen – altså kommunikasjonsinformasjon mellom norske borgere.

---

137 Big Brother Watch avsn. 356.

138 Cole (2016) s. 683.

139 Cole (2016) s. 683.

140 Cole (2016) s. 683.

141 Lysne II (2016) s. 26.

3.6.1.2.2 Statens informasjonsfordel

Som nevnt ovenfor påpeker Lysne II-utvalget at et absolutt kriterium for å innføre DGF er at tilliten til etterretningen ikke reduseres. Det å ikke problematisere grensen mellom metadata og innholdsdata i større grad kan anses som utilstrekkelig kommunikasjon til norske borgere om hva DGF vil innebære, og derfor svekke tilliten til etterretningen og grunnlaget for den demokratiske prosessen ved bestemmelse om DGF skal innføres i Norge. Det som kalles "informatial deficit" går ut på at staten vet mye mer om borgere enn det borgere vet om staten.[142] Selv om det naturligvis vil være noe skjevhet i mengden informasjon som staten bærer på om sine borgere, har teknologien nå ført til en økning i mengden informasjon om borgere til staten, uten en tilsvarende økning i informasjon om staten til borgere.[143]

Wessel-Aas påpeker også det han kaller en "disproporsjonal informasjonsfordel" og hvordan den utfordrer demokratiet; det er myndighetene som skal ivareta borgernes interesser på grunnlag av å ha fått den makten av borgerne. Av det følger det videre at borgere bør ha mest mulig innsyn i hvordan myndighetene ivaretar interessene, samtidig som at staten skal ha minst mulig innsyn i borgernes private sfære. Likevel er det et spenningsforhold her; når hensynet til rikets sikkerhet medfører tilbakeholdenhet av informasjon, samtidig som at kontrollmidler øker, minsker det opposisjonsmulighetene ytterligere, og på den måten svekkes demokratiet.[144]

Lysne II-utvalgets rapport om DGF kan ikke sies å på generelt grunnlag være tilbakeholden med informasjon. Tvert imot beskrives fordeler og ulemper med DGF lettfattelig og med høy grad av presisjon. Det er likevel problematisk at forskjellen mellom metadata og innholdsdata ikke fremstilles nærmere. Hvis det er manglende kunnskap som begrunner at forskjellene ikke redegjøres for nærmere, kan det spørres om norske myndigheter er modne for å ta i bruk denne teknologien i det hele tatt, noe som utfordrer et av Lysne II-utvalgets absolutte kriterier om teknologisk gjennomførbarhet som forutsetning for at DGF kan innføres. Det utfordrer også spørsmålet om egnethet siden en forutsetning for å bedømme om DGF bør innføres er å ha tilstrekkelig kompetanse på alt det vil innebære. Selv om teknologien utvikler seg raskt, er analytisk og langsiktig tenkning vesentlig ved innføring av DGF.
Når det nå er gode holdepunkter for å si at metadata kan være like inngripende som innholdsdata, er det et godt eksempel på at det er sider med teknologien som mennesker ikke ser konsekvensene av med det samme, men som dukker opp senere, jf. begrepet "sorte svaner" under

142 Robbins (2017) s. 583.
143 Robbins (2017) s. 583.
144 Wessel-Aas (2012).

3.3. Hvorvidt det er for sent å sikre at metadata ikke misbrukes i fremtiden kan være vanskelig å si. Det siste poenget viser til "boomerang-effekten" som nevnt under 3.5.1.

Samtidig er det utfordrende å forholde seg til utviklingen på en gjennomtenkt og balansert måte når tilsvarende tiltak ofte haste-innføres av mektige stater.[145] Det er derfor viktig at Norge foretar selvstendige vurderinger på dette området. Å kunne ta tilstrekkelig informerte valg på hva som skal beskytte norske borgere er av demokratisk og menneskerettslig interesse fordi det som skal beskytte borgeres rettigheter ikke må risikere å ødelegge de samme rettighetene. Da blir det også vanskelig å bedømme om ugjennomtenkte og inngripende valg lar seg forsvare i en forholdsmessighetsvurdering. Selv om ivaretakelse av rikets sikkerhet innebærer å forholde seg til risiko, kan ikke ubegrunnet uvitenhet om inngripende tiltak sies å være en gyldig aksept av risiko.

Om manglende informasjon om forholdet mellom metadata og innholdsdata er begrunnet i bevisst tilbakeholdelse av informasjon som kan endre norske borgeres syn på hvorvidt DGF bør innføres, står vi overfor en utvikling med stort skadepotensiale for demokratiet og menneskerettighetene. Det er allerede belyst at Norge ikke er unntatt det økende presset på rettsstatsidealene som følge av sterkere og mer uforutsigbare inngrep i borgeres privatliv.[146] Opprettelse av DGF kan ses som et utslag av denne utviklingen. Uforutsigbarheten fremheves når det ikke redegjøres for effekten av DGF på en tilstrekkelig måte. Uforutsigbarhet minsker i sin tur tillit til myndighetene, og dermed svekkes demokratiet og følgelig fundamentet for beskyttelsen av menneskerettighetene. Selv om statene har en viss skjønnsmargin i forhold til tiltak som skal verne mot rikets sikkerhet, er det viktig å påse at hensynet til rikets sikkerhet ikke brukes i alt for vid forstand.[147] Det kan fort gå for langt hvis informasjon som kan påvirke borgeres demokratiske valg tilbakeholdes av sikkerhetsmessige årsaker. Om informasjon holdes tilbake som følge av myndighetenes frykt for at DGF framstår som mer inngripende enn det egentlig er, så fremstår det som umyndiggjøring av norske borgeres evne til fornuftig og autonom beslutningsevne. Den holdningen er ikke kompatibel med Grunnloven § 2.

Oppsummeringsvis må borgere få muligheten til å ta valg på informert grunnlag. Ved å holde tilbake informasjon, eller ikke ta ansvar for tilstrekkelig konsekvensutredning ved tiltak for nasjonal sikkerhet, vil borgere fratas muligheten til å velge ut ifra fullstendig forståelse av et tiltaks innvirkninger. Følgelig øker sannsynligheten for at borgere oppfatter at tiltak får uforutsette konsekvenser. Når tiltak får uforutsette konsekvenser, vil borgers tillit til myndighete-

[145] Wessel-Aas (2012).

[146] Wessel-Aas (2012).

[147] Wessel-Aas (2012).

ne reduseres, og det blir følgelig grunn til å snakk om nedkjølingseffekten.[148] I henhold til DGF er det nødvendig å ta nærmere stilling til om´ metadata og innholdsdata skal anses å ha samme grad av inngrepspotensiale, og behandles deretter. Til tross for en ellers presis og informativ utredning om hva DGF vil innebære, så er det grunn til å si at Lysne II-utvalgets nåværende stilling til metadata og innholdsdata trekker i retning av at "the nature, scope and duration" av DGF kan få en nokså inngripende karakter. Selv om stater nå har ganske vid skjønnsmargin i forhold til tiltak som skal sikre rikets sikkerhet, så gjenstår likevel spørsmålet om DGF, som presentert i Lysne II-høringen, er i tråd med Grunnloven § 2 og § 102. Sånn som paragrafene er beskrevet i avsnitt 2.2.1 kan det se ut til at DGF kommer til å bryte med de norske rettsstatsprinsippene.

3.6.1.3 Kontrollmekanismene

Et motargument til manglende skille mellom metadata og innholdsdata kan være at kontrollmekanismene ved tilgang til søk i datalagrene vil hindre misbruk av informasjon. I det følgende skal derfor EMD og EU-domstolens rammer for kontrollmekanismer redegjøres for og drøftes. Deretter skal Lysne II-utvalgets stilling i forhold til disse rammene, samt forholdet til Grunnloven § 2 og § 102 drøftes.

I Big Brother Watch er det lagt til grunn at domstolautorisasjon kan være den beste kontrollmekanismen for å unngå misbruk, men at det likevel ikke nødvendigvis er avgjørende eller tilstrekkelig for å forsikre overholdelse av EMK arikkel 8.[149] Med det til grunn uttrykker EMD større aksept for kontroll-alternativer sammenlignet med Centrum-dommen, der det ble uttalt at alternativer til domstolskontroll kan anses å være i tråd med konvensjonen så lenge de utviser tilstrekkelig uavhengighet fra organet som utsteder tillatelse til gjennomgang av data, samt utøver effektiv og kontinuerlig kontroll.[150] I Szabó-dommen er det uttrykt at det bør foretas domstolkontroll før både generell og målrettet overvåkning igangsettes,[151] men at et alternativt organ likevel kan forhåndkontrollere så lenge det foreligger en juridisk etterhåndskontroll av lovligheten av overvåkningen.[152] Tilsvarende syn legges til grunn av EU-domstolen i Tele2-saken.[153]

---

148 Robbins (2017) s. 584-585.

149 Big Brother Watch avsn. 320.

150 Centrum-dommen avsn. 153.

151 Szabó-dommen avsn. 79.

152 Szabó-dommen avsn. 77.

153 Sak C-203/15 avsn. 120.

Det er grunn til å si at EMD-dommene viser en gradvis utvikling mot større fleksibilitet i hvilket kontrollorgan som skal foreligge så lenge kontrollorganet er tilstrekkelig uavhengig. Det foreligger foreløpig ingen bestemmelse fra EU-domstolen som uttrykker en tilsvarende fleksibilitet i hvilket kontrollorgan som skal foreligge. Økt fleksibilitet i kontrollorgan og anerkjennelsen av bulk innsamling av data som et verdifullt redskap, peker i retning av at overvåkning i økende grad normaliseres og tilrettelegges for i EMD.

Det må spørres hvor uavhengig et ikke-juridisk kontrollorgan har mulighet til å være, spesielt i et såpass lite land som Norge. Det jobbes for ytterligere samarbeid på tvers av ulike myndigheter og private aktører i møte med sikkerhetsutfordringer. Samtidig erkjennes den sentrale utfordringen det er å avklare grenser for ansvar og fullmakt mellom de ulike aktørene, samt hvordan et tilsynsorgan skal fungere ved det økte samarbeidet.[154] Det er på det rene at slikt samarbeid kan effektivisere motstandsdyktigheten mot trusler, derav cyberspionasje. Samtidig øker risikoen for myndighetsmisbruk i større grad sammenlignet med et domstolorgan som kontrollmyndighet ved tilgang til lagrede data.

Lysne II-utvalget foreslår en kontrollinstans i tre deler bestående av "DGF-domstolen", "DGF-tilsynet" og EOS-utvalget.[155] Selv om særlig forhåndsgodkjenning av en domstol vil kunne forhindre e-tjenestens adgang til ønskede søk, mener utvalget at det av hensyn til folkets tillit til systemet må foreligge domstolsautorisasjon. Sånn sett kan Lysne II-utvalget sies å legge til grunn strengere kontrollmekanismer enn det EMD åpner for i Big Brother Watch. Siden den dommen er helt ny, gjenstår det å se om Lysne II-utvalget holder fast ved domstolsautorisasjon fremfor ikke-juridiske kontrollorganer, som jo kan tilføre en mer kostnadseffektiv behandling av overvåkningsspørsmål.

DGF-domstolen vil i følge Lysne II-utvalget bestå av noen få dommere med spesialkunnskap om etterretning og trusler for å sikre en mest mulig effektiv kontroll. Det presiseres at DGF-domstolen av hensyn til "gradering og sikkerhet" må være en spesialdomstol framfor å inngå i Oslo tingrett.[156] Som Lysne II-utvalget selv påpeker så er det en risiko for at dommerne blir for lojale til e-tjenestens behov. Det er heller ikke usannsynlig at dommerne vil følge EMD sin utvikling, som ser ut til å tillate mer og mer overvåkning. Da blir det særlig aktuelt å være bevisst på Grunnlovens skranker i § 2 og § 102 for å overholde det verdigrunnlaget som Norge bygger på.

---

154 NOU: 2016 s. 120.

155 Lysne (2016) s. 57-59.

156 Lysne (2016) s. 58.

Grunnloven understreker demokratiets stilling i Norge gjennom § 2. Hensynet til det demokratiske samfunnet viser dets gjennomgående vekt i det moderne samfunnet, og at det skal bestå uansett hvilke politiske og religiøse strømninger som til enhver tid preger samfunnet. Grunnlovsfestningen av ivaretakelsen av demokratiet viser at det skal ha full motstandskraft mot lovgivning og påvirkning utenfra som utfordrer demokratiets funksjon.[157] Grunnlovens funksjon som skranke vil likevel avhenge av de norske domstolenes tolkning og anvendelse av dens bestemmelser. Videre vil Norges forpliktelser etter EMK medføre at EMD sin dynamiske tolkningsstil tilpasses politiske strømninger og andre trekk med samfunnsutviklingen som potensielt kan utfordre demokratiet, for eksempel gjennom at informasjonssamling i bulk tillates.

Det er viktig å være bevisst på hva denne overvåkningstrenden gjør med samfunnet. Eksempelvis kan det spørres om terminologien "innsamling av data i bulk" er et finere ord for masseovervåkning. Tilhengere av NSA etter Snowden-avsløringene brukte "bulk access" istede for "mass surveilance" som betegnelse på den omfattende overvåkningen.[158] Det må her minnes om at EMD anvender betegnelsen "bulk access". På denne måten formes språkbruken på grunnlag av en politisert debatt. Språkets betydning kan derfor formes på et ikke-nøytralt politisk grunnlag, som igjen påvirker regelverket. Betydningen av terminologien vil formodentlig EMD presisere i tråd med sin praksis, men det er likevel grunn til å belyse at språkvalget har påvirkningskraft på hva man assosierer med et konsept.

Siden samfunnet har skapt sine egne sårbarheter gjennom avhengighet av IKT-systemer, tvinges rettssystemet til å forholde seg til sårbarhetene siden teknologiens utvikling uansett ikke kan stoppes med det første. EMD sin dynamiske tolkning er et uttrykk for dette; det vokser frem flere digitale trusler. Det handler om å velge hvordan man skal forholde seg til dem. I forhold til Norge er det viktig at domstolene erkjenner den norske konteksten i forhold til hvordan digitale trusler skal håndteres. Det er ikke nødvendigvis slik at en stats overvåkningssystem er direkte overførbart til Norge, særlig med tanke på nasjonale rammer i lovverket, politisk kultur og trusselbildets omfang.

DGF-tilsynet skal på sin side være et forvaltningsorgan som i hovedsak skal kontrollere bruken av DGF-systemet, samt domstolsavgjørelsene om DGF. Hensynet bak DGF-tilsynet er å ha et "kontinuerlig og uavhengig" kontrollorgan ved opprettelse av DGF. Avvik fra domstolsvedtak og ellers lovmessig bruk av DGF vil rapporteres til EOS-utvalget[159] som i sin tur har i

[157] Smith (2014) s. 346.

[158] Bauman (2014) s. 140.

[159] Lysne (2016) s. 59.

oppgave å sikre at e-tjenesten opererer innenfor de lovlige rammene,[160] som beskrevet i etterretningstjenesteloven § 3 jf. § 4.

DGF-tilsynet bidrar som et ekstra kontrollorgan til EOS-utvalget. Det betyr at etterretningstjenestens virksomhet må forholde seg til flere kontrollmekanismer, noe som kan øke bevisstheten på rettmessig bruk av systemet. Denne ytterlige kontrollmekanismen er i tråd med Lysne II-utvalgets mål om å ikke svekke borgernes tillit til e-tjenesten. I tillegg vil den tilføre mer teknisk ekspertise, noe som er viktig for å kunne forstå omfanget av, og potensialet til DGF. Økt teknisk ekspertise vil som følge også bidra til mer effektiv overvåkningskontroll i et samfunn som bæres av IKT-systemer.

EOS-utvalget er nokså unikt i og med at det er utnevnt av stortinget framfor regjeringen, samt at det er et fullstendig uavhengig organ,[161] med særlig stor innsynsrett.[162] Det kan spørres om ikke EOS-utvalget alene hadde vært et tilstrekkelig kontrollorgan etter EMD sin standard, siden det i Big Brother Watch legges til grunn at det viktigste med et kontrollorgan er "the actual operation of the system..., including the checks and balances of the exercise of power, and the existence of any evidence of actual abuse"[.][163] Et av hovedpoengene med EOS-utvalget er nettopp å sikre at hemmelige tjenester, deriblant e-tjenesten ikke begår myndighetsmisbruk ved beskyttelse av rikets sikkerhet.[164] En slik kontroll vil ha skjerpende effekt på e-tjenesten og tillitsskapende effekt på borgerne. Samtidig, tidligere leder i EOS-utvalget, Helga Hernes, har uttalt at EOS-tilsynet ikke kan garantere at de hemmelige tjenestene bedriver utelukkende lovlig arbeid, men at EOS-tilsynets hovedoppgave er å forhindre ulovlig handlinger, og at vissheten om at det foreligger et kontrollorgan har hatt positiv virkning på de hemmelige tjenestenes virke. Hun poengterer videre at økt internasjonalt fokus på, og politiske strømninger i favør av "overvåkning og etterretning" som midler for samfunnssikkerhet, særlig etter 9/11, legger press på kontrollmyndigheters arbeid for å sikre rettssikkerheten.[165] I og med at EMD nå går lengre og lengre i å tillate overvåkning som svar på disse politiske strømningene er det ikke utenkelig at det kan ha smitteeffekt på kontrollmyndighetene.

Spørsmålet om hvorvidt EOS-utvalget vil kunne tilsvare et tilstrekkelig kontrollapparat under EMD, er i hovedsak ment for å understreke at Lysne II-utvalget har planer om et grundig kontrollberedskap som kan sies å overgå EMD sin standard. Men uansett hvor pålitelig og grun-

---

160 EOS-kontrollloven § 6(4) nr. 2.

161 EOS-kontrolloven § 3 jf. § 1(5).

162 EOS-kontrolloven § 8.

163 Big Brother Watch avsn. 320.

164 Hernes (2010) s. 320.

165 Hernes (2010) s. 320.

dig EOS-utvalgets arbeid er, har dets uttalelser ingen juridisk bindende virkning.[166] EOS-utvalget kan dermed ikke endre en avgjørelse fra DGF-domstolen, men bare uttale seg og gi utredninger, deriblant om forhold de finner ulovlig eller klandreverdig.

Til tross for noen svakheter som for så vidt gjelder på generelt grunnlag i ethvert system med domstols- og kontrollorgan kan det alt i alt legges til grunn at Lysne II-utvalgets planlagte kontrollapparat for håndtering av DGF er nokså grundig. Hvorvidt det veier opp mot manglende og delvis utilstrekkelig planlegging av hvordan metadata og innholdsdata skal behandles er derimot ikke overbevisende. Derfor, om det utvikles bedre mekanismer for behandling av metadata og innholdsdata kan det legges til grunn at DGF er et egnet tiltak mot cyberspionasje. Det gjenstår likevel å vurdere om DGF er et nødvendig og proporsjonalt tiltak.

3.6.2 Er digitalt grenseforsvar nødvendig for å ivareta nasjonal sikkerhet?

Nødvendighetsvurderingen beror på om det er andre mekanismer som kan erstatte DGF, og som er like effektive i møte med cyberspionasje. De alternative tiltakene må vurderes på bakgrunn av trusselen som cyberspionasje utgjør holdt opp i mot inngrepsgraden som DGF utgjør. Cyberspionasje er en av flere kategorier av cyberkriminalitet. Alternative tiltak er ikke nødvendigvis rettet direkte mot cyberspionasje, men gjelder generelt for aktiviteter som innebærer ulovlig hacking av datasystemer. Tiltakene kan derfor anses som mekanismer for å fremme cybersikkerhet generelt.

Cyberspionasje er et internasjonalt problem som utfordrer nasjonal sikkerhet i mange stater. Spionasjevirksomhet er referert til som verdens andre eldste yrke,[167] men det er ikke dermed noen grunn til å romantisere spionasjevirksomhet, særlig ikke i tilfellet av den moderne formen, som gir direkte og målrettet tilgang til vital statsinformasjon. Tiltak mot cyberspionasje bør derfor starte på et internasjonalt nivå. Det kan generelt skilles mellom offensive tiltak, som innebærer forbud og sanksjonering mot cyberspionasje, og defensive tiltak, som går ut på å beskytte IKT-system mot cyberspionasje. Offensive og defensive tiltak kan i son tur ses som underkategorier til regulative- og tekniske alternativer til DGF.

[166] EOS-kontrolloven § 14.

[167] Wangen (2015) s. 183.

3.6.2.1 Regulative alternativer

I forhold til offensive tiltak vil et naturlig første steg være et internasjonalt forbud mot uautorisert spionasje i fredstid på samme måte som forbudet mot "bruk av makt" og "væpnet angrep" er forbudt etter FN-pakten artikkel 2(4) og 51. Det må presiseres at et slikt forbud ikke vurderes i forhold til rikets sikkerhet, men fremstilles som et alternativ med forhindringspotensiale i forhold til cyberspionasje uten at stater trenger å innføre tiltak som utfordrer rettsstatsidealene. Selv om Tallinn Manualen 2.0 er et steg på veien i å regulere cybertrusler, er det fremdeles ingen regel som forbyr cyberspionasje jf. avsnitt 1.4.2. Sanksjonering ved eventuelt brudd på en sånn regel kan videre ha avskrekkede effekt. I og med at cyberspionasje er en moderne måte å skaffe seg maktfordel på, er en internasjonal hjemmel mot cyberspionasje svært aktuelt med det økende omfanget, og skadepotensialet cyberspionasje har. Krigføring endrer seg, jf. avsnitt 1.4.2, og det er som følge ikke nødvendigvis slik at etterkrigstidens definisjon av krigføring i FN-pakten er like aktuell lenger. Cyberspionasje kan riktig nok ikke anses som krigføring, men det er altså konsekvensene det kan ha som er relevant å sikte til, jf. Stuxnet.

Om ikke et internasjonalt forbud mot cyberspionasje er gjennomførbart med det første kan et alternativ være å utvikle lovgivning som tillater mottiltak ved cyberangrep som følge av cyberspionasje. Til tross for at cyberangrep i hovedsak ikke resulterer i ødeleggelser som tradisjonelt er kategorisert som "bruk av makt" under FN-pakten artikkel 2(4), kan det tenkes at artikkel 2(4) bør tolkes dynamisk så bestemmelsen kan dekke bruk av økonomisk og politisk makt for å oppnå en uberettiget maktfordel.[168] For å gå tilbake til tesen i 1.4.2 om at måten krigføring drives på reflekterer måten et samfunn skaper velstand på, så kan det spørres om ikke systematisk og sofistikert spionasje og angrep på IKT-systemer vil bli en dominerende metode å drive krigføring på. Det vi vet helt sikker er at cyberspionasje og cyberangrep er utbredt, og at samfunnet avhenger av IKT-systemene som cyberspionasje og cyberangrep retter seg mot. Svikt og forstyrrelser i IKT-systemene gjør samfunnet vårt svært sårbart på samme måte som en svekket hær gjorde samfunn sårbare tidligere. Om det tradisjonelle innholdet av "bruk av makt" omdefineres for å inkludere flere ulovlige cyberoperasjoner, vil det i det minste medføre at destruktive handlinger i fremtiden vil være ulovlige. Det er ikke noe poeng i å drive med cyberspionasje hvis utnyttelse av informasjonen tar form av handlinger som uansett er ulovlige gjennom et omfattende lovverk. I og med at det er sannsynlig at konsekvenser av cyberspionasje inntreffer i fremtiden har både nasjonale og internasjonale lovgivere tid til å utvikle lovverk og samarbeid som er resistent mot cyberspionasje.

---

[168] Dinnis (2012) s. 41.

Internasjonale forbud og sanksjoner mot handlinger som utfordrer rikets sikkerhet kan potensielt gi bedre forutsetninger for Norge som rettsstat fordi det i hovedsak er trusselen, og ikke samfunnet som kontrolleres. DGF er derimot et eksempel på et tiltak som plasserer ansvaret hos statene som utsettes for cyberspionasje framfor statene som utfører cyberspionasje. Med færre trusler i omløp vil klimaet for demokrati og menneskerettigheter vokse fordi det ideelt sett gir myndighetene mindre grunn til å foreta inngripende samfunnskontroll som rettferdiggjøres av hensyn til nasjonal sikkerhet. Selv om risikoen for cyberspionasje ikke forsvinner med det første, vil den reduseres. Tiltak for nasjonal sikkerhet må justeres i tråd med risikobildet for å unngå uforholdsmessig forskyving av maktbalansen mellom myndighetene og borgere.

I forhold til DGF er det for Norge sin del likevel et spørsmål om det er forsvarlig å vente på et slikt internasjonalt lovverk. Selv om innføring av nye lovverk og endring av allerede eksisterende lovverk kan ha preventiv effekt er det likevel en utfordring å nå tilstrekkelig internasjonalt konsensus på endring av, og tilføyelse av nye regler. Et nylig eksempel på samarbeidsutfordringer er signeringsavslagene fra USA, Russland og Kina på et omfattende cybersikkerhetsinitiativ fra Frankrike. Initiativet ble signert av 51 stater, deriblant alle EU-medlemslandene.[169] Mektige og ikke-allierte stater drar fordeler av å kunne spionere på hverandre for å vedlikeholde eller øke makt og innflytelse.[170] Gjennomførbarheten av regulerende tiltak er derfor ikke selvsagt.

Om regulerende tiltak som nevnt ovenfor er gjennomførbare, så gjenstår likevel bevisproblemer i forhold til hvor spionasje og angrep kommer fra. De fleste omfattende tilfeller av cyberspionasje og cyberangrep har ikke en sikker skyldig stat.[171] Det er unødvendig å si, men sanksjonerende lovverk mister sin effekt når den skyldige aktøren ikke kan detekteres.

Det er her det blir desto viktigere med defensive tiltak som beskytter mot cyberspionasje, altså beskyttelse av IKT-systemer. Like viktig som internasjonalt samarbeid ved bekjempelse av cyberspionasje, er tverrsektorielt samarbeid mellom offentlige og private institusjoner ved utvikling av beskyttelsesstrategier mot cyberspionasje.[172] Direktivet om nettverks- og informasjonssikkerhet (NIS-direktivet) ble som det første lovverket for cybersikkerhet i EU nylig gjennomført. NIS-direktivet skal bidra til økt beskyttelse av nettverks- og informasjonssystem gjennom å pålegge stater å utvikle strategier for å sikre IKT-systemer, blant annet ”computer

169 Archer (2018).

170 Scmitt (2016) s. 44.

171 Wangen (2015) s. 202 og Sharma (2018) s. 562.

172 Meld. St. 38 (2016-2017) s. 28.

security incidence teams"[173] (CSIRTS). Det pålegges videre tverrsektorielt samarbeid for å kunne stå samlet mot angrep jf. artikkel 10, samt samarbeid mellom medlemsstater.[174] Norge har uttrykt interesse for internasjonalt og regionalt samarbeid, særlig med EU.[175] Implementering av NIS-direktivet, samt styrking av ENISA[176] sin rolle som ekspertrådgiver og operativ funksjon har prioritet blant EU og EFTA-landende i 2018.[177] NorCERT[178] og VDI[179] er Norges responsteam ved cyberangrep. Det er grunn til å tro at deres funksjon vil bli styrket gjennom EU-samarbeidet, særlig hvis ENISA får styrket sin innflytelse.

Tverrsektorielt samarbeid gir de beste forutsetninger for å sette sammen mangfoldet av relevant ekspertise, for deretter å kunne utvikle et så sofistikert beskyttelsessystem som mulig. Samtidig, samarbeid krever fleksibilitet mellom, og innsyn i de ulike sektorene. Det må foreligge en maktbalanse mellom de ulike aktørene, sånn at for eksempel byråkratiet ikke blir for dominerende i forhold til de private aktørene med IT-ekspertise. Samarbeid forutsetter med andre ord tydelige ansvarsområder for hver aktør, samt tillit til hverandres ekspertise.[180]

Som det første lovverket for cybersikkerhet i Europa, viser NIS-direktivet at cybersikkerhet for alvor er på agendaen i Europa. Med klare regler for CSIRTS, og samarbeid mellom aktører og medlemsland er det klima for å skape et solid forsvar i møte med cyberspionasje. Samtidig, NIS-direktivet overlater i stor gard til statene å utvikle konkrete strategier for best mulig cybersikkerhet.[181] Lovverket bidrar derfor i størst grad med å sette rammer for hvordan hver stat kan utvikle et best mulig forsvar, framfor konkrete tiltak. Dessuten er NIS-direktivet helt nytt, og det er foreløpig tidlig å si noe om hvorvidt cybersikkerheten i Europa har økt. Regulering av internasjonalt og tverrsektorielt samarbeid gir derfor ikke tilstrekkelig svar på om det er et mer forholdsmessig tiltak mot cyberspionasje enn DGF.

NIS-direktivet gjenspeiler generelt eksisterende og planlagte lovverk på cybersikkerhetsområdet; det er stort sett enighet om at det må samarbeides om økt cybersikkerhet, men manglende forslag på konkrete tiltak som for eksempel DGF. En grunn til det kan være at det er behov for fleksible lovverk så det er rom for tiltak som kan svare til nye trusler. Staters fleksi-

---

173 NIS-direktivet artikkel 9(1).

174 NIS-direktivet artikkel 11.

175 Utenriksdepartementet (2017) s. 7.

176 EUs Network Information Security Agency.

177 Stortinget (2018).

178 Norwegian Computer Emergency Response Team.

179 Varslingssystemet for digital infrastruktur.

180 Christou (2016) s. 49.

181 NIS-direktivet artikkel 7(1).

bilitet ved tiltak for cybersikkerhet understreker viktigheten av å hele tiden behandle tiltak for cybersikkerhet parallelt med demokratiske og menneskerettslige problemstillinger.

3.6.2.2 Tekniske alternativer

I det videre skal det redegjøres for eksempler på det som ovenfor er referert til som "konkrete tiltak" i møte med cyberspionasje. EU-kommisjonen foreslo i fjor å ta i bruk IPv6, som muliggjør å lokalisere individer bak enhver IP-adresse. Som følge blir det umulig å gjemme seg som en av opp til mange tusen brukere bak samme IP-adresse, som er typisk ved cyberspionasje.[182] IPv6 vil derfor gjøre det enklere å finne ut hvem som står bak cyberspionasje.

En rekke øvrige tiltak er foreslått av professor Christopher Yoo fra universitetet i Pennsylvania. For det første er det mulig å isolere sårbare datasystem fra omverden, såkalte "air gaps". For eksempel vil e-tjenestens nettverk med denne løsningen bli et lukket system som ikke kan ta imot noe fra omverdenen. Hovedutfordringen med dette tiltaket er at det er en dyr og komplisert prosess å innføre.[183]

Et annet alternativ er å innføre en "kill switch" funksjon, som går ut på at informasjon beskyttes gjennom å tilintetgjøre informasjonen, eller ubrukeliggjøre datamaskinen i det informasjon ulovlig blir forsøkt stjålet, uten at autorisert personell mister tilgang på systemet. Å gjøre informasjon verdiløs på denne måten skal altså demotivere angripere.[184] Det går an å tenke seg at de omfattende ødeleggelsene ved Stuxnet kunne vært forhindret med et slikt system. Samtidig kan det være utfordrende å føre kontroll med et slikt system, ikke minst i forhold til maktmisbruk fra myndighetenes side.

Et tredje tiltak er et "firewall" system, som filtrerer bort ukjent trafikk, gjennom et innside- og utsidesystem, der kun trafikk fra innsidesystemet får tilgang.[185] Svakheter med dette tiltaket er at det ikke beskytter mot angrep fra innsiden av systemet. Dessuten har det vanskeligheter med å fange opp nytt virusmateriale.[186]

Et siste tiltak som Yoo belyser er forbedringer i programvareutviklingen. Han mener det er for lett å utnytte programvare sånn som kvaliteten er nå, og peker blant annet på at det er mere rom for masseproduksjon av programvare framfor kvalitetssikring. Siden det er utnytting av

---

182 JOIN (2017) 450.

183 Yoo (2016) s. 22.

184 Techopedia.

185 Yoo (2016) s. 24.

186 Secpoint.

svak programvare som muliggjør de fleste cyberangrep, er dette tiltaket svært sentralt.[187] Det må legges til at regulering av kvalitet på programvare burde vært regulert i NIS-direktivet, noe det ikke er per i dag. Utover det er programvareutvikling et eksempel på at samarbeid mellom aktører er nødvendig for cybersikkerhet. Selv om masseproduksjon av programvare er lønnsomt for aktørene, er det viktig å anerkjenne at de samme aktørene er en sentral brikke i bekjempelse av alvorlige cybertrusler.

En fellesnevner for de alternative tekniske tiltakene ovenfor er at de muliggjør en mer lokal beskyttelse av informasjon sammenlignet med DGF, som vil medføre store mengder overskuddsmateriale i beskyttelsen mot cyberspionasje. Tiltakene kan dermed sies å utgjøre en mindre trussel mot rettsstaten sammenlignet med DGF. En ytterlig fellesnevner for tiltakene er at de har sine sårbarheter, som ikke er til å komme unna med den farten som teknologien utvikler seg i. Dessuten er det en kostbarhetskalkyle i det hele – det er naturligvis ikke ubegrenset med ressurser som kan brukes på slike sikkerhetstiltak.

3.6.2.3 Tiltakenes verdi i forhold til DGF og trusselbildet

I forhold til nødvendigheten av DGF mot cyberspionasje, så er det altså forebyggende potensiale i form av offensive tiltak gjennom internasjonale lovverk som FN-pakten, og den rådgivende Tallin Manualen 2.0. NIS-direktivet legger også til rette for utvikling av defensive mottiltak på regionalt nivå. Selv om det foreligger potensiale for bedre cybersikkerhet er det et poeng å kunne handle raskt. Å hvile i at cybersikkerhet kommer til å bli bedre med tid er ikke nødvendigvis grunn nok til å avslå DGF som uforholdsmessig. Likevel, det finnes alternative konkrete tekniske mottiltak som er mindre inngripende, men muligens mere kostbare. Det kunne vært et poeng å drøfte alternative mottiltak i Lysne II-utvalgets utredning. Iallfall å redegjøre for alternativer, og deretter forklare hvorfor de eventuelt ikke er bedre egnet. Fullstendige utredninger går tilbake til argumentet om å sørge for å gi borgere valg på så opplyst grunnlag som mulig.

Et problem med cyberspionasje er at det er vanskelig å fastslå konsekvensene. I tillegg er det ikke usannsynlig at konsekvensene slår ut i framtiden.[188] Det reiser spørsmålet om hvorvidt det er grunn til å gå såpass langt på dette tidspunktet i henhold til å bekjempe cyberspionasje, særlig siden det tross alt finnes andre metoder for å sikre informasjonssystemer. Om alternative metoder som unngår like store inngrep i privatlivets fred er for kostbare, så kan det spørres om hensynet til demokratiet, menneskerettighetene og rettsstaten i praksis er så tungtveiende

[187] Yoo (2016) s. 25.

[188] Wangen (2015) s. 207.

som Grunnloven § 2 jf. § 102 gir uttrykk for. Uansett graden av egnethet og nødvendighet, er den ikke avgjørende for tiltakets proporsjonalitet, som nå blir den siste og avgjørende drøftelsen.

3.6.3 Er det proporsjonalitet mellom rikets sikkerhet og rettsstatsidealene?

Drøftelsen kan for ordens skyld kategoriseres som "proporsjonalitet i snever forstand"[189], og handler om å finne en balanse mellom nasjonal sikkerhet og ivaretakelse av rettsstatsidealene med utgangspunkt i retten til privatlivets fred. Konkret handler drøftelsen om den relative verdien av DGF mot cyberspionasje, holdt opp i mot den relative verdien av å forhindre inngrep i privatlivets fred.[190]

Vi vet nå at begrepet "rikets sikkerhet" er en rettslig standard som favner vidt og som endrer seg med samfunnsutviklingen. Samtidig er det et gjennomgående mål å beskytte statssuvereniteten og demokratiet. Beskyttelsen av "digitale samfunnsstrukturer" er ansett som et konkret tiltak for å ivareta statssuvereniteten og demokratiet, jf. avsnitt 1.4.1. Tatt i betraktning at samfunnets funksjon avhenger av IKT-systemer, utgjør de et naturlig beskyttelsesverdig mål. Rettsstatens virke avhenger av beskyttelse mot trusler mot statssuvereniteten og demokratiet. Vi ser samtidig at demokratiets funksjon avhenger av at visse grunnleggende menneskerettigheter overholdes. Privatlivets fred er en kjernerettighet for demokratiets funksjon fordi det fremmer personlig autonomi og integritet, som igjen er fundamentalt for å kunne ta del i den demokratiske prosessen, som til syvende og sist skal opprettholde riktig maktbalanse mellom myndighetene og borgerne.[191]

Når hensynet til rikets sikkerhet både kan beskytte og true rettsstatens virke, understreker det betydningen av å finne riktig balanse mellom rikets sikkerhet og rettsstatsidealene. Likevel, i og med at forarbeidene til den nye sikkerhetsloven sier at det skal være høy terskel for å anse rikets sikkerhet som truet, jf. avsnitt 1.4.1, så underbygger det betydningen av demokratiet og menneskerettighetene som tungtveiende komponenter for den norske rettsstatens virke.

Samtidig påvirkes det norske samfunnet av strømninger utenfra. USA og Europa har vektlagt nasjonal sikkerhet i større grad enn hensynet til sivile og politiske rettigheter etter terrorangrepet i USA i 2001.[192] EMD normaliserer overvåkning i økende grad, og Norge vurderer nå DGF.

---

189 Strand (2015) s. 79.

190 Barak (2010) s. 8.

191 Bruce (2010) s. 65.

192 Wessel-Aas (2012).

Når grunnlovfestingen av § 102 ble ansett som ekstra aktuell i forhold til den teknologiske utviklingen og økt samfunnsovervåkning, er det ikke tvil om at beskyttelse av privatlivets fred er en kjernerettighet. Samtidig må det erkjennes at Norge, i likhet med de aller fleste stater i verden må stå til rette for den teknologiske utviklingen, med de truslene den har skapt. Det blir igjen aktuelt å snakke om "boomerang-effekten", som beskrevet i avsnitt 3.5.1; teknologien har ført til at Norge i prinsippet kan trues fra hvor som helst i verden på et hvilket som helst tidspunkt. Det er en risiko vi er nødt til å forholde oss til.

Når DGF i følge Lysne II-utvalget kan forhindre slike trusler på et helt annet nivå enn det e-tjenesten til nå har hatt mulighet til, er det god grunn til å ikke umiddelbart avslå tiltaket av hensynet til rettsstatsprinsippene. Samtidig, ved en nærmere analyse av Lysne II-utvalgets plan for DGF blir det tydelig at vesentlige samfunnsinteresser potensielt kommer i sterk ubalanse.

Selv om det vil komme ny lovgivning som regulerer DGF vil forutsigbarheten av dette lovverket likevel være skjør, både på grunn av at loven ikke kan være for presis, og fordi teknologien er i stadig utvikling. Teknologisk utvikling er en gjennomgående utfordring for rettens forutsigbarhet i vår tid,[193] men DGF kan i særlig grad true rettsikkerheten i kraft av å være et potensielt særlig inngripende tiltak. Til tross for at det vil innføres strenge kontrollmekanismer for søk i innsamlet data, så vil lovverkets uforutsigbarhet påvirke domstolenes praksis. Graden av rettsbeskyttelse med disse utfordringene vil derfor avhenge av jurister som evner å se når lovverket og domstolene fraviker kjerneverdiene i Grunnloven § 2 og § 102. Som Graver påpeker, så er "evnen til å stå i mot angrep på rettsstaten innenifra gjennom samfunnet selv med dets ordinære kanaler" like viktig som å stå i mot trusler utenifra.[194] Juristers evne og vilje til å forsvare rettsstaten er ikke er en selvfølge i tider der demokrati og menneskerettigheter settes på prøve.[195]

Vissheten om at e-tjenesten uspesifisert lagrer data gir også grunn til å belyse nedkjølingseffekten nærmere. Datatilsynets rapport fra 2014 om personvern, kom etter en undersøkelse blant norske borgere frem til at 26% av de spurte hadde frastått å undertegne på et opprop av frykt for å bli konfrontert med handlingen på et senere tidspunkt. Videre oppga 12% å ha meldt seg ut av et sosialt medium av samme grunn.[196] I samme undersøkelse kom det også frem at 27% av befolkningen ville bli mer påpasselige med hva de søkte opp på nett, og 18%

[193] Sand (2011) s. 111.

[194] Graver (2011) s. 111.

[195] Graver (2011) s. 113.

[196] Datatilsynet (2014) s. 27.

ville blitt mer påpasselig med hvem de kommuniserte med i det hypotetiske tilfelle at norsk og utenlandsk etterretning kunne overvåke folks elektroniske kommunikasjon.[197]

Ut i fra Datatilsynets rapport fremgår det altså at det i 2014 var større bevissthet rundt den økende overvåkningen, og at den hypotetiske etterretningsovervåkningen ville føre til en nedkjølingseffekt i den forstand at ikke bare bevisstheten rundt overvåkning ville øke, men folk sine handlinger vil også bli påvirket som følge av frykten for hvordan etterretningen vil bruke den lagrede informasjonen på et senere tidspunkt. Det er derfor relevant å snakke om nedkjølingseffekten ved innføring av DGF. Vel vitende om personlig autonomi og integritet som forutsetninger for demokratiet, er det grunn til å si at DGF vil påvirke den demokratiske prosessen.

Det kan diskuteres hvorvidt det er realistisk å kunne ivareta privatlivets fred i like stor grad som Grunnloven § 102 legger opp til med de digitale utfordringene vi står overfor. Samtidig har den diskusjonen begrenset relevans siden § 102 per nå er det avgjørende rammeverket som DGF må balanseres opp i mot, med Grunnloven § 2 som gjennomgående hensyn.

Selv om det ikke kan sies at nedkjølingseffekten av e-tjenestens overvåkning er særlig stor, så er den fremdeles der. Den utgjør en forskjell, om aldri så liten. Nedkjølingseffekten indikerer redusert tillit til myndighetene. Sannsynligheten for at DGF kan få uforutsette konsekvenser er også til stede med tanke på den manglende beskrivelsen av hvor inngripende søk i metadata er. I tillegg er Lysne II-utvalget åpne om at det er en utfordring å håndtere metadata så spesifikt som mulig. Disse utfordringene er nokså store selv om de ikke utredes for i tilstrekkelig grad. Om DGF skulle få uforutsette konsekvenser som følge av utilstrekkelig redegjørelse for inngrepet, vil det kunne svekke tilliten til myndighetene ytterligere.

Det kan argumenteres med at advarslene mot økt overvåkning baseres på potensielle indre trusler mot rettsstatsidealene fremfor faktiske trusler,[198] og at det derfor blir et tynt grunnlag å kritisere DGF på. Til det argumentet må det understrekes at rettsstaten er skjør. Mange små innskrenkninger i demokratiet og menneskerettighetene kan over tid legge til rette for en uforholdsmessig autoritær stat. Tatt i betraktning at det er en generell tendens til å la nasjonal sikkerhet går foran politiske og sivile rettigheter om nødvendig, er det desto viktigere å tenke langsiktig i forhold til hvilken retning samfunnet beveger seg i. I liket med de indre truslene mot rettsstatsidealene er truslene som cyberspionasje utgjør også usikre fordi de kan slå ut

[197] Datatilsynet (2014) s. 33.

[198] Bygrave (2010) s. 60.

lengre frem i tid, hvis de i det hele tatt slår ut. En forutsetning for å beskytte rettsstaten fra trusler utenifra er uansett at rettsstaten ivaretas innenifra.

Som Schartum legger til grunn på spørsmålet om hvor mye overvåkning som skal tillates, jf. avsnitt 1.3, så bør utgangspunktet være at jo mindre målrettet overvåkning, jo mer pressende må behovet for overvåkningen være.[199] Risikoen for cyberangrep som følge av cyberspionasje er til stede, men det er vanskelig å se at det er pressende nok til å innføre DGF med de usikkerhetene rundt håndteringene det medfører, særlig når det samtidig foreligger holdepunkter for at DGF vil endre norske borgeres adferd i form av nedkjølingseffekten. Når det også foreligger alternative og mindre inngripende tiltak mot cyberspionasje, samt stort potensiale i ytterlig sikring av programvare, så taler det for at behovet for DGF ikke er pressende nok til å utfordre Grunnloven § 2 og § 102 i den graden DGF gjør.

[199] Schartum (2010) s. 27.

4 Konklusjon

Digitale trusler setter rettsstaten under press. Teknologien utvikler seg raskt, og det må som følge handles raskt når teknologien slår tilbake på samfunnet med et nytt og uoversiktlig trusselbilde. Håndtering av trusselbildet forutsetter en viss samfunnskontroll. Hvor langt myndigheten skal gå i å kontrollere samfunnet for å beskytte det mot trusler er et spørsmål om hvor pressende truslene er. Cyberspionasje utgjør en risiko som vi ikke vet med sikkerhet om vil slå ut. Men det vi vet helt sikkert er at skadepotensalet er enormt. Samtidig er det ingen direkte internasjonal regulering på cyberspionasje, i tillegg til at det er vanskelig å oppdage omfanget av, og hvor spionasje kommer fra. I møte med slike trusler er det nødvendig å utvikle systemer som beskytter mot cyberspionasje, slik som DGF. Bulk innsamling av data har på kort tid blitt normalisert i USA og Europa. Til tross for at det er ment å ivareta nasjonal sikkerhet, er det nødvendig å tenke kritisk rundt denne utviklingen som i økende grad åpner for overvåkning. Hvis maktfordelingen skal være reell, så må det holdes fast på utgangspunktene i Grunnloven § 2 og § 102, uansett om EMD og EU-domstolen åpner for å innskrenke rekkevidden av privatlivets fred. Jo mer kunnskap den norske staten har om sine borgere, jo mer makt har den. Om det ikke merkes mye til effekten av overvåkningen i dag, så vil den kunne slå ut i krisetider, og det er gjerne krisetider som viser hvor makten faktisk ligger.

Det kan være at DGF fungerer som en midlertidig løsning, men på sikt er det ikke veien å gå av tre grunner. For det første er nedkjølingseffekten reell. For det andre så eksisterer det alternative tiltak mot cyberspionasje. For det tredje så ser vi utvikling i cyberregulerende lovverk, som for eksempel NIS-direktivet, samt ytterlig regulerende potensiale i allerede eksisterende lovverk, som FN-pakten. Til tross for at utviklingen av lovverk med adekvat regulerende effekt går sent, så er det en start som det er god grunn til å tro at vil fortsette i riktig retning. Selv om tiltak for rikets sikkerhet er en måte å beskytte rettsstaten på, så vil DGF gi staten en uforholdsmessig maktfordel siden behovet for DGF ikke er pressende nok til å innskrenke rekkevidden av privatlivets fred, med de konsekvenser det får for demokratiet og menneskerettighetene - altså selve fundamentet for rettsstaten.

Kildeliste

Norske rettskilder

Lover

1814	Lov 17.mai 1814 Kongeriket Norges grunnlov (Grunnloven).
1992	Lov om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven).
1995	Lov om kontroll med etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-kontrolloven).
1998	Lov 20.mars 1998 nr. 5 om Etterretningstjenesten (Etterretningstjenesteloven).
1999	Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (Menneskerettsloven).

Forarbeider

Ot. Prp. Nr. 49 (1996-1997)	Lov om nasjonal sikkerhet (Sikkerhetsloven).
Dokument 16 (2011-2012)	Rapport til Stortingets presidentskap fra Menneske-rettighetsutvalget om Menneskerettigheter i Grunnloven.
Dokument 16 (2015-1016)	Rapport til Stortinget fra Evalueringsutvalget for Stor-tingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-utvalget).
NOU:2015	Digital sårbarhet - sikkert samfunn.
NOU:2016	Samhandling for sikkerhet. Beskyttelse av grunnleggen-de samfunnsfunksjoner i en omskiftelig tid.
Prop. 153 L (2016-2017)	Lov om nasjonal sikkerhet (sikkerhetsloven).

St. Meld. 23 (2013-2014) Datatilsynets og Personvernnemndas årsmeldinger for 2013.

St. Meld. 10 (2016-2017) Risiko i et trygt samfunn.

Norsk rettspraksis

Rt. 2007 s. 234.

Rt. 2015 s. 93.

HR-2016-2554-A.

Internasjonale rettskilder

Traktater/Direktiver

EMK Den europeiske menneskerettskonvensjon, Roma 4. november 1950.

EU-Charteret Den europeiske unions menneskerettighetscharter (2012/C 326/02). Lisboa 1. desember 2009.

SP FNs konvensjon om sivile og politiske rettigheter, New York 16. desember 1966.

FN-pakten De forente nasjoners pakt, San Francisco 24 oktober 1945.

ODA-avtalen Avtalen mellom EFTA-statene om opprettelse av et Overvåknings og en Domstol. 2 mai 1992.

TEU Traktaten om den Europeiske Union. Konsolidert versjon 2016 (EUT 2016/C 202/01).

NIS-direktivet	Directive 2016/1148 of the European Parliament and the Council of July 2016 concerning measures for high common level of security of network and information systems across the Union (2016) Official Journal of the European Union. L 194/2. [NIS-direktivet].

Rettspraksis

Den Europeiske menneskerettighetsdomstol/EMD

Sunday Times v. the United Kingdom	Case of Sunday Times v. the United Kingdom, Application no. 6538/74, 26.04.1979.
Silver and Others v. The United Kingdom	Case of Silver and Others v. The United Kingdom, Application nos. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, 25.03. 1983.
Szabó and Vissy v. Hungary	Case of Szabó and Vissy v. Hungary, Application no. 37138/14, 12.01.2016.
Centrum för Rättvisa v. Sweden	Case of Centrum før rettvisa v. Sweden, Application no. 35252/08, 19.06.2018.
Big Brother Watch and Others v the United Kingdom	Case of Big Brother Watch and Others v. The United Kingdom, Application nos. 58170/13, 62322/14 og 24960/15, 13.09.2018.

EU-domstolen

Sak C-293/12 Digital Rights Ireland v. Minister of Communications & Others.	ECLI:EU:C:2014:238
Sak C-203/15 Tele2Sverige AB v Post- och telestyrelsen	ECLI:EU:C:2016:970.

Litteratur

Archer (2018) — Archer, Joseph. (2018) ”US, Russia and China refuse to back French cybersecurity initiative”, *The Telegraph*, 12. november 2018. https://www.telegraph.co.uk/technology/2018/11/12/us-russia-china-refuse-back-french-cybersecurity-initiative/ [Sitert 18.11.2018].

Barak (2010) — Barak, Aharon. ”Proportionality and Principled Balancing”, *Law & Ethics of Human Rights*, vol. 4 nr. 1 (2010), side 1-16. https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/lehr4&id=2&men_tab=srchresults# .

Baumann (2014) — Baumann, Zygmundt, Didier Bigo, Paulo Esteves, mfl. ”After Snowden: Rethinking the Impact of Surveillance”, *International Political Sociology* vol. 8 nr. 2 (2014) s. 121-144. https://doi.org/10.1111/ips.12048.

Beck (1992) — Beck, Ulrich. *Risk Society: Towards a New Modernity*. London: Sage Publications, 1992.

Bruce (2010) — Bruce, Ingvild, Geir Sunde Haugland. ”Personvern, rettssikkerhet og vern mot alvorlig kriminalitet. Noen utgangspunkter”, i *Overvåkning i en rettsstat,* Dag Wiese Schartum (red.). Oslo: Fagbokforlaget Vigmostad & Bjørke AS, 2010, s. 62-83.

Bygrave (2010) — Bygrave, Lee A. ”Captain Surveillance v. Mr. X. An Essay on the Semantics and Politics of ’Surveillance Society’”, i *Overvåkning i en rettsstat,* Dag Wiese Schartum (red.). Oslo: Fagbokforlaget Vigmostad & Bjørke AS, 2010, s. 49-61.

Bårdsen (2017) — Bårdsen, Arnfinn. *Grunnloven, overvåkning og domstolenes rolle* (2017). https://lovdata.no/pro/JUS/bardsen-a-2017-04 [Sitert 10.10.2018].

Christakis (2018) — Christakis, Theodore. "A Fragmentation og EU/ECHR Law on Mass Surveillance: Initial Thoughts on the Big Brither Watch Judgement." *European Law Blog*. September 20, 2018. [Sitert 29.10.2018]. http://europeanlawblog.eu/2018/09/20/a-fragmentation-of-eu-echr-law-on-mass-surveillance-initial-thoughts-on-the-big-brother-watch-judgment/.

Christou (2016) — Christou, Georg. *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. London: Palgrave Macmillan, (2016). https://link.springer.com/book/10.1057/9781137400529.

JOIN (2017) 450 — European Commission. Joint Communication to the European Parliament and the Council."Resilience, Deterrence and Defence: Building strong cybersecurity for the EU". (Sitert fra eur-lex.eu).

Cole (2016) — Cole, David. D. "After Snowden: Regulating Technology-Aided Surveillance in the Digital Age", *Capital University Law review*, nr. 4 (2016), s. 677-692. https://heinonline-org.ezproxy.uio.no/HOL/P?h=hein.journals/capulr44&i=725.

Datatilsynet (2014) — Datatilsynet. *Personvern 2014 – tilstander og trender*. (2014). https://www.datatilsynet.no/globalassets/global/om-person-vern/rapporter/persovern_tilstandogtrender_2014.pdf .

Davis (2007) — Davis, Joshua. (2007) ”Hackers take down the most wired country in Europe”, *Wired*, 21. August 2007. https://www.wired.com/2007/08/ff-estonia/ [Sitert 1.11.2018].

Dev (2015) — Dev, Priyanka R. “Use of Force and Armed Attack Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response”. *Texas International Law Journal* vol. 50, nr. 2 (2015) s. 381-401. https://heinonline.org/HOL/Page?lname=&public=false&handle=hein.journals/tilj50&page=381&collection=journals.

Dinniss (2012) — Dinniss, Heather Harrison. *Cyber Warfare and the Laws og War,* Cambridge: Cambridge University Press, 2012.

EMD rapport 221(2018) — European Court of Human Rights. *Information Note on the Court´s case-law 221*. August-september 2018. http://hudoc.echr.coe.int/eng-press?i=003-6187848-8026299 [sitert 17.09.2018].

Etterretningstjenesten (2018) — Etterretningstjenesten. *Fokus 2018. Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer.* (2018). https://forsvaret.no/fakta_/ForsvaretDocuments/Fokus2018_bokmaal_oppslag_godkjent.pdf. [Sitert 28.08.2018].

Glennon (2012) — Glennon, Michael J. ”The Dark future of International Cybersecurity Regulation”, *Journal of National Security Law & Policy* vol. 6 nr. 2 (2012), s. 563-570. https://heinonline.org/HOL/Page?lname=&public=false&handle=hein.journals/jnatselp6&page=563&collection=journals.

Graver (2011) — Graver, Hans Petter. *Hva er rett*, Oslo: Universitetsforl., 2011.

Hernes (2010) — Hernes, Helga. ”EOS-utvalgets kontroll av ”de hemmelige tjenester””, i *Overvåkning i en rettsstat,* Dag Wiese Schartum (red.). Oslo: Fagbokforlaget Vigmostad & Bjørke AS, 2010, s. 306-321.

Høgberg (2013) — Høgberg, Benedikte Moltumyr. *Statsrett kort forklart*, Oslo: Universitetsforl., 2013.

Høstmælingen (2013) — Høstmælingen, Njål. *Internasjonale Menneskerettigheter*, 2. utg., Oslo: Universitetsforl., 2013.

Lilleholt (2014) — Lilleholt, Kåre. ”Rett og rettsregler”, i *Knophs oversikt over Norges rett*, Ragnar Knoph, 14.utg., Oslo: Universitetsforl., 2014, s. 1-3.

Lock (2012) — Lock, Tobias. ”Accession of the EU to the ECHR. Who would be responsible in Strasbourg? ”, i *The European Union after the Lisbon Treaty,* Ashiagbor, Diamond, Nicola Countouris, Ioannis Lianos, Cambridge: Cambridge University Press, 2012, s. 109-135. https://doi.org/10.1017/CBO9781139084338.

Lupovici (2016) — Lupovici, Amir. ”The ”Attribution Problem” and the Social Construction of ”Violence”: Taking Cyber Deterrence Literature a Step Forward”, *International Studies Perspectives* vol. 17, nr. 3 (2016), s. 322-342. https://doi.org/10.1017/CBO9781139084338.

Lysne (2016) — Lysne, Olav. *Digitalt grenseforsvar (DGF). Lysne II-utvalget.* (2016). https://www.regjeringen.no/contentassets/ca1f705dbebd48cb9a61889d4cfee6bf/digitalt-grenseforsvar-lysne-ii-utvalget.pdf [Sitert 04.09.2018].

Nasjonal sikkerhetsmyndighet — Nasjonal sikkerhetsmyndighet. *Håndtering av digital spionasje*. https://nsm.stat.no/globalassets/dokumenter/norcert/apt_2015_web.pdf [Sitert 30.08.2018].

Nasjonal sikkerhetsmyndighet (2017) — Nasjonal sikkerhetsmyndighet. *Helhetlig IKT-risikobilde 2017*. *https://nsm.stat.no/globalassets/rapporter/helhetlig_ikt-risikobilde_2017_orig_enkeltsider_low.pdf* [Sitert 05.09.2018].

Politiets sikkerhetstjeneste (2018) — Politiets sikkerhetstjeneste. *Trusselvurdering 2018*. (2018). https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2018/. [Sitert 30.08.2018].

Robbins (2017) — Robbins, Scott, Adam Henschke. "Designing for Democracy: Bulk Data and Authoritarism." *Surveillance & Society* 15, no. 3-4 (2017), s. 583-589. https://doi.org/10.1017/CBO9781139084338.

Sand (2011) — Sand, Inger-Johanne. *JFEXFAC04 Rett, samfunn, tekster og legitimitet*, Oslo: Unipub, 2011.

Schartum (2010) — Schartum, Dag Wiese. *Overvåkning i en rettsstat,* Bergen: Fagbokforlaget, 2010.

Schmitt (2017) — Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2.utg., Cambridge: Cambridge University Press, 2017. https://doi-org.ezproxy.uio.no/10.1017/9781316822524.

Schmitt (2016) — Schmitt, Michael N., Vihul, Liis. "The Nature of International Law Cyber Norms", i *International Cyber Norms: Legal Policy & Industry Perspectives*, Anna-Maria Osula and Henry Roigas (red.), Tallinn: NATO Cooperative Cyber Defence Center of Excellence, 2016, s. 23-47. https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_Ch2.pdf.

Secpoint — Secpoint. *What is the weakness of a firewall.* *https://www.secpoint.com/what-is-the-weakness-of-a-firewall.html* [Sitert 29.10.2018].

Sejersted (2014) — Sejersted, Fredrik, Finn Arnesen, Osle-Andreas Rognstad mfl. *EØS-rett*, 3.utg., Oslo: Universitetsforl., 2014.

Senter for europarett — Senter for europarett. "Plikt til datalagring i strid med EUs charter". *Eurorett* nr. 2 (2017), (Sitert fra Lovdata.no).

Sharma (2018) — Sharma, Rohit, Dr. Mona Purhoit. "Emerging Cyber Threats and the Challenges Associated with them", *International Research Journal of Engineering and Technology*, Vol. 5 nr. 2. (2018), s. 560-563. https://www.irjet.net/archives/V5/i2/IRJET-V5I2127.pdf.

Smith (2015) — Smith, Eivind. *Konstitusjonelt demokrati. Statsforfatningsretten i prinsipielt og komparativt lys*, 3.utg., Oslo: Fagbokforl., 2015.

Stortinget (2018) — Stortinget. ”Cybersikkerhet på agendaen”, i *EU/EØS-nytt*. (2018), https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/EU-EOS-informasjon/EU-EOS-nytt/2018/eueos-nytt---18.-januar-2018#cybersikkerhet [Sitert 29.10.2018].

Strand (2015) — Strand, Vibeke Blaker, Kjetil Mujezinović Larsen. *Menneskerettigheter i et nøtteskall*. Oslo: Gyldendal juridisk, 2015.

Technopedia — Technopedia. *Kill Switch.* https://www.techopedia.com/definition/4001/kill-switch [Sitert 29. 10.2018].

Toffler (1993) — Toffler, Alvin and Heidi. *War and Anti-war. Survival at the Dawn of the 21st Century*, 1. Utg., New York: Little Brown & Co., 1993.

Utenriksdepartementet (2017) — Utenriksdepartementet. *Internasjonal Cyberstrategi for Norge.* (2017), https://www.regjeringen.no/globalassets/departementene/ud/dokumenter/sikpol/cyberstrategi_web.pdf [Sitert 29.10.2018].

Wangen (2015) — Wangen, Gaute. ”The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism”, *Information*, vol. 6, nr. 2 (2015), s. 183-211. https://doi.org/10.1017/CBO9781139084338.

Wessel-Aas (2012) — Wessel-Aas, Jon. ”Krigen mot terror og den norske rettsstaten”, *Internasjonal Politikk* vol. 70 nr. 1 (2012). (Sitert fra Idunn.no).

Yoo (2016) — Yoo, Christopher S. ”Cyberespionage or Cyberwar?”, i *Cyberwar: Law and Ethics for Virtual Conflicts.* Jens David Ohlin, Kevin Govern, Claire Finkelstein (red.), Oxford: University Press, 2016. https://doi.org/10.1017/CBO9781139084338.

Åtland (2008) — Åtland, Kristian. ”Hva er sikkerhet? En drøfting av sikkerhetsbegrepets innhold og utvikling fra Antikken til det 21. Århundre”, *Norsk statsvitenskapelige tidsskrift* vol. 24 (2008) (Sitert fra Idunn.no).