Digitalt grenseforsvar (DGF)

Lysne II-utvalget

26. august 2016

Til Forsvarsdepartementet

Utvalget ble oppnevnt ved Forsvarsdepartementets brev av 24. februar 2016 med mandat å utrede sentrale problemstillinger knyttet til Etterretningstjenestens mulige tilgang til elektronisk informasjon som kommuniseres i fiberoptiske kabler inn og ut av Norge.

Utvalget legger med dette frem sin utredning. Utredningen er i sin helhet ugradert. Utredningen er enstemmig.

Oslo, 26. august 2016

Olav Lysne
leder

Trond Grytting *Eva Jarbekk*

Einar Lunde *Christian Reusch*

INNHOLD

SAMMENDRAG

Etterretningstjenestens samfunnsoppdrag består i å fremskaffe informasjon om norske interesser sett i forhold til fremmede stater, organisasjoner og individer. Informasjonen skal benyttes til å varsle om trusler mot Norge og norske interesser, og til å understøtte politiske beslutningsprosesser knyttet til norsk utenriks-, sikkerhets- og forsvarspolitikk. E-tjenesten sitt fokusområde er således utenlandsk aktivitet. Formålet for informasjonsinnhentingen er beslutningsstøtte for myndighetene, og ikke straffeforfølgning, og tjenesten er avgrenset mot overvåkning av nordmenn i Norge.

Digitalt grenseforsvar (DGF) brukes i denne rapporten om en innretning og en virksomhet som gir E-tjenesten innsyn i digitale datastrømmer som krysser den norske landegrensen. I dag går hovedmengden av slike strømmer i fiberoptiske kabler som enten er landbasert eller ligger på sjøbunnen. E-tjenesten har ikke noen DGF-installasjon i dag, men både tidligere og nåværende sjef for tjenesten har argumentert for at det burde opprettes.

DGF som virkemiddel for etterretning er aktualisert av to utviklingstrender. Den ene trenden er endringer i trusselbildet. Vi er vitne til en kraftig eskalering av cybertrusler mot Norge og norske interesser, både i volum av angrep og i angrepenes kompleksitet. Videre er truslene fra internasjonal terrorisme økende, og vi ser at nettbasert koordinering av terrorvirksomhet på tvers av landegrenser blir mer vanlig. Den andre trenden som aktualiserer DGF er at teknologiutviklingen erstatter tidligere kommunikasjonskanaler med internettbaserte løsninger. E-tjenestens ønske om DGF kan således begrunnes i at eldre etterretningskapasiteter må fases ut og erstattes av nye.

Hvorvidt DGF bør opprettes må imidlertid vurderes i et bredt perspektiv. Saken berører juridiske spørsmål knyttet til personvern og menneskerettigheter, og den influeres av hvilke løsninger som er teknisk mulige. Begrensninger som legges på en eventuell DGF-installasjon vil kunne redusere den etterretningsmessige verdien av DGF til et punkt hvor det ikke lenger er et effektivt verktøy.

Sentrale kompliserende faktorer i denne diskusjonen er av teknologisk art. Den intuitive forståelse av at kommunikasjonskablene som krysser landegrensen kun vil bære kommunikasjon mellom Norge og utlandet, er ikke riktig. En stor og stigende andel av kommunikasjonene mellom personer som befinner seg i Norge, krysser landegrensen og vil således kunne plukkes opp av DGF. Likeledes vil mange elektroniske tjenester som benyttes av et individ kun for dettes formål innebære kommunikasjon over landegrensene. Skybaserte lagringstjenester er et eksempel på dette. Noe av denne trafikken vil maskinelt kunne filtreres bort før den tas vare på. Nøyaktig filtrering slik at kun informasjon som er relevant for E-tjenestens oppdrag slipper gjennom, er imidlertid ikke mulig. En DGF-installasjon vil nødvendigvis plukke opp en god del informasjon som E-tjenesten ikke skal ha innsyn i. En eventuell DGF-installasjon må derfor ligge under et strengt kontrollregime som består av både teknologiske og menneskelige kontrollmekanismer.

En eventuell innføring av DGF må også gjøres på en måte som ikke strider mot folkeretten eller mot norsk lov. Det finnes flere bestemmelser både i norsk lovverk og i internasjonale avtaler og konvensjoner med relevans for dette spørsmålet. EU-domstolens beslutning fra 2014 om å kjenne Datalagringsdirektivet for ugyldig illustrerer at det ikke har vært opplagt hvor de juridiske grensene for datalagring for samfunnstjenlige formål går. De juridiske grensene på dette området vil trolig klargjøres noe i tiden som kommer, ved at flere relevante saker får sin avgjørelse. Vi ser det som viktig at en eventuell innføring av DGF ikke lider den skjebne at den ved et senere tidspunkt blir kjent ulovlig.

Hensynet til befolkningens tillit til de hemmelige tjenestene kan i noen grad ivaretas ved at DGF holder seg innenfor oppsatte grenser gitt av menneskerettighetene og personvernlovgivningen. På de fleste andre samfunnsområder vil man også benytte åpenhet og transparens som befordrer av generell tillit. På etterretningsområdet vil det imidlertid være klare begrensninger på hvor åpne og transparente man kan være, uten at effektiviteten til etterret-

ningsvirksomheten svekkes. Tillit til hvordan en eventuell DGF-installasjon blir benyttet kan derfor ikke bygges på åpenhet alene. Den må baseres på sikkerhetsklarerte kontrollinstanser som har innsyn i virksomheten på befolkningens vegne.

Utvalget har vurdert at DGF kan innføres på en måte som kombinerer hensynene til teknisk realiserbarhet, juridisk gangbarhet, personvernmessige forhold, etterretningsmessig verdi og tillit i befolkningen. Konklusjonen forutsetter flere forhold. Dels er den betinget av et bestemt teknologisk oppsett og dels er den betinget av omfattende tilgangsregler, formålsskranker og kontrollregimer. Videre forutsetter utvalget at DGF forankres i et tilstrekkelig klart lovgrunnlag. For å oppnå et rettslig forsvarbart DGF, er det etter utvalgets oppfatning ikke mulig å fravike dette oppsettet i stor grad, og selv små svekkelser i kontrollmekanismene kan føre til at menneskerettigheter og personvernhensyn vil bli ansett som brutt.

Kontrollmekanismene består av en domstol som står for forhåndsgodkjenninger, et tilsyn som overvåker bruken av DGF i nær sanntid, samt at EOS-utvalget styrkes for å etterhåndskontrollere E-tjenestens bruk av DGF. Installasjonen består av lagrede data, filtre som filtrerer ut hvilke data som skal kunne lagres, og maskinell kontroll med hvilke søk som tillates utført i disse dataene. Detaljene i samspillet mellom installasjonen og kontrollmekanismene er å finne i rapporten.

Utvalgets konklusjoner er som følger:

- DGF kan utformes juridisk holdbart og forholdsmessig i et menneskeretts- og personvernperspektiv ved at filtrene, begrensninger på søk i dataene, formålsbegrensninger og kontrollmekanismene vi har beskrevet implementeres. Dette forutsetter at et tilstrekkelig klart lovgrunnlag vedtas.

- DGF er et potensielt svært personverninngripende virkemiddel, og utvalget kan ikke anbefale innføring av DGF med svakere kontrollmekanismer og tekniske filtre mv. enn det som er beskrevet i rapporten.

- DGF anses som nødvendig for nasjonens sikkerhet, særlig gjelder dette beskyttelse mot sabotasje og spionasje i det digitale rom.

- DGF slik utvalget anbefaler gir etterretningsmessig verdi og er teknologisk realiserbart.

- DGF vil kunne bidra til høyere grad av presisjon i nasjonalt sikkerhetsarbeid og vil derigjennom over tid også virke modererende på det samlede nasjonale overvåkingstrykket.

- DGF bør benyttes utelukkende til utenlandsetterretning. Ikke under noen omstendighet bør informasjon fremskaffet ved DGF kunne benyttes som bevis mot tiltalte i straffesaker.

- DGF slik det er beskrevet i rapporten anbefales innført.

1 UTVALGETS MANDAT, SAMMENSETNING OG ARBEID

1.1. Mandatet

Utvalget ble gitt følgende mandat:

"*Forsvarsministeren nedsetter et utvalg for å utrede sentrale problemstillinger knyttet til Etterretningstjenestens mulige tilgang til elektronisk informasjon som kommuniseres i fiberoptiske kabler inn og ut av Norge (digitalt grenseforsvar). Bakgrunnen er at informasjonen som følge av den teknologiske utviklingen i stor grad flytter seg til informasjonskilder der Etterretningstjenesten i dag ikke har tilgang.*

I sin utredning skal utvalget foreta en vurdering av behovet for digitalt grenseforsvar i lys av gjeldende trusselbilde, og se hen til Etterretningstjenestens tilgang til informasjon fra andre kilder. Utvalget skal også se på behovet i sammenheng med overvåking og innsamling av informasjon som i dag gjøres av andre nasjonale myndigheter.

Utvalget kan i sine vurderinger se hen til lovgivning i andre land, samt relevante rettsavgjørelser og åpne vurderinger.

Formål som særlig skal vurderes er:

1. *Formålet med Etterretningstjenestens tilgang til det digitale kommunikasjonsnettet og rettslige rammer for bruk og lagring av innsamlet informasjon. I dette ligger også en vurdering av hvilke tilleggsgevinster man kan få med digitalt grenseforsvar sammenlignet med de overvåkningstiltakene som allerede er iverksatt i regi av NSM NorCERT, andre CERT/CSIRTer samt tilgang til informasjon som Etterretningstjenesten har fra andre kilder.*

2. *Grunnloven § 102 og eventuelle skranker av relevans for tilgang til og innsamling av informasjon, samt eventuelle skranker etter Norges folkerettslige forpliktelser, særlig sett hen til den europeiske menneskerettskonvensjonen artikkel 8, FN-konvensjonen om sivile og politiske rettigheter artikkel 17, EUs personverndirektiv 95/46/EF og Europarådets konvensjon nr. 108.*

3. *Hvordan formålet med tilgang og innsamling av informasjon står i forhold til personvernmessige prinsipper og lov om behandling av personopplysninger. Spesielt skal tilleggsgevinstene av tilgang ses i relasjon til hvor inngripende slik tilgang er i personvernet.*

4. *Mekanismer som motvirker formålsutglidning.*

5. *Behovet for ytterligere og/eller forsterkede godkjennings-/kontrollfunksjoner ut over den eksisterende kontrollen som i dag gjennomføres av kontrollutvalget for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget).*

6. *Vurdere faren for, og konsekvensene ved, at utenforstående får tilgang til overvåkningsutstyr og/eller den innsamlede informasjonen.*

Forsvarsdepartementet skal bistå og legge til rette for at utvalget får tilgang til informasjon som er nødvendig for å foreta sine vurderinger. Den endelige utredningen skal være ugradert og fremlegges for Forsvarsdepartementet innen 30. juni 2016."

1.2. Hvordan utvalget har tolket mandatet

Utvalget har lagt til grunn at formålet med utredningen først og fremst har vært å vurdere de prinsipielle sider ved en eventuell tilgang for Etterretningstjenesten (E-tjenesten) til digital kommunikasjon som transporteres inn og ut av Norge.

Hensikten med utredningen er å stimulere til en bred offentlig prinsipiell debatt, basert på et opplyst faktum om hva digitalt grenseforsvar er og hva det ikke er. Et offentlig ordskifte er viktig, og i tråd med anbefalingen i NOU 2015:13 *Digital sårbarhet – sikkert samfunn* (pkt. 21.11.8). Dette primærformålet, sammenholdt med tidsrommet utvalget har fått til rådighet, har medført behov for å gjøre noen avgrensninger og mandatpresiseringer.

Utvalget har lagt vekt på å utrede hensyn som taler for og mot en slik eventuell tilgang, samt vurdert trender som kan påvirke behovet for digitalt grenseforsvar i tiden fremover. Dernest har utvalget lagt hovedvekt på å vurdere hvorvidt og hvordan en eventuell tilgang kan ivareta og balanseres mot grunnleggende hensyn i et demokratisk samfunn. Utvalget har konkludert med at mandatet åpner for at utvalgets medlemmer tar stilling til om E-tjenesten bør få tilgang til elektronisk informasjon som kommuniseres i fiberoptiske kabler inn og ut av Norge.

Digitalt grenseforsvar – i utredningen her forkortet DGF – er i mandatet definert som «Etterretningstjenestens (…) tilgang til elektronisk informasjon som

kommuniseres i fiberoptiske kabler inn og ut av Norge». Utvalget antar at termen «fiberoptiske kabler» er valgt fordi dette er den dominerende teknologiske realitet per i dag for transport av elektronisk kommunikasjon. Den teknologiske utviklingen skjer raskt. Utvalget har tatt høyde for at både nye kommunikasjonsruter, nye kommunikasjonsmåter og ny teknologi for transport av kommunikasjon vil være en realitet i fremtiden, slik at de prinsipielle avveininger så langt mulig skal være gyldige uavhengig av dagens teknologiske fremføringsmåter.[1]

Både mandatet og tidshensynet har foranlediget at utvalget ikke har vurdert E-tjenestens (eksisterende eller fremtidige) metoder i bredt. Utvalget har imidlertid gjort seg kjent med tjenestens kommunikasjonsetterretning slik den gjennomføres i dag. Utvalget har også vurdert verdien av DGF opp mot andre informasjonskilder. Utvalget har videre sett nærmere på samspillet mellom DGF og andre etterretningsdisipliner, og vurdert behovet for DGF i lys av annen innsamling av informasjon som i dag gjøres av øvrige nasjonale myndigheter. Selv om mandatgiver trolig har hatt norske nasjonale myndigheter i tankene, har utvalget ikke ansett dette mandatpunktet for å være til hinder for å vurdere behovet sett i forhold til innsamling som gjøres av andre lands myndigheter og som kan tenkes delt med E-tjenesten.

Det fremgår av mandatet at utredningen skal være ugradert, hvilket ligger i sakens natur når formålet er å stimulere til offentlig debatt. I enkelte henseender kan dette være utfordrende når det dreier seg om virksomheten til en hemmelig tjeneste som E-tjenesten. Utvalget har mottatt sikkerhetsgradert bakgrunnsinformasjon og orienteringer fra tjenesten. Av sikkerhetsmessige grunner kan utvalget ikke beskrive i detalj hvem tjenesten samarbeider med og hva samarbeidet innebærer. Av samme grunn kan utvalget ikke gå nærmere inn på tjenestens kilder, metoder eller kapasiteter annet enn på et generelt nivå. I forhold til de prinsipielle problemstillinger som ligger i kjernen av utvalgsmandatet, har dette imidlertid ikke voldt problemer for utvalget. Utvalget har ikke hatt behov for å underbygge noen av sine vurderinger eller slutninger med å henvise til sikkerhetsgradert informasjon. Utvalget peker også på at trusselbildet i dag beskrives i ugraderte publikasjoner fra både E-tjenesten og Politiets sikkerhetstjeneste.

Utvalget antar at enkelte land har aksess til grenseoverskridende kommunikasjon, uten at dette fremkommer klart i åpent nasjonalt regelverk. Beskrivelsen av situasjonen i andre land er derfor ikke komplett. Utvalget har lagt til grunn at noen land ikke ønsker oppmerksomhet om denne tilgangen. En har vært klar over faren for at oppmerksomhet fra et offentlig utvalgs side rettet mot disse forhold i andre land kan medføre negative reaksjoner og konsekvenser for E-tjenestens partnersamarbeid, og har derfor avstått fra å gå nærmere inn på dette. Det forhold at enkelte land kan ha ordninger basert på et hemmelig samarbeid med hjemlig ekomindustri, har imidlertid ikke vært avgjørende for noen av utvalgets vurderinger eller konklusjoner.

Verken mandatet, tiden til rådighet eller utvalgets sammensetning har tilsagt at utvalget skal utrede konkrete tekniske løsninger for etablering og innfasing av et eventuelt DGF i Norge. Dette krever uansett forutgående grundige analyser og dialog med bl.a. utvalgte større tilbydere av ekomnett og ekomtjenester i Norge. Utvalget har imidlertid vurdert konseptuelle løsninger som grunnlag for utvalgets prinsipielle avveininger.

Det ligger utenfor utvalgets mandat å utrede eller foreslå konkret lovgivning. Ut i fra mandatets formål om å utrede prinsipielle problemstillinger som grunnlag for offentlig debatt, har utvalget også konkludert med at utredningsinstruksens bestemmelser om å utrede sakskompleksets administrative og

[1] «Fiberoptiske» er et ord knyttet til en teknologisk realitet som kan være tidsbegrenset. Selv om dette benyttes i mandatet og enkelte steder i utredningen, fordi dette for tiden er det mest aktuelle overføringsmedium, er det utvalgets intensjon at vurderingene i hovedsak vil være anvendelig også for nye fremtidige løsninger. Det spesifikke medium for kommunikasjonsoverføring er i utgangspunktet av underordnet betydning. Det vil imidlertid være enkelte rettslige og faktiske forskjeller mellom innhenting av trådløs og ikke-trådløs kommunikasjon, blant annet med hensyn til behovet for å regulere E-tjenestens relasjon til tjenestetilbydere. Teoretisk kunne man tenke seg et fremtidig teknologiskifte hvor overføring av kommunikasjon over landegrensene skjer 100% trådløst. Utvalgets avveininger er derfor så langt mulig søkt å være metode- og teknologinøytrale. Det er det prinsipielle knyttet til kontrollmuligheter av grensekryssende trafikk utvalget har vektlagt å utrede. Utvalget peker i denne forbindelse på at E-tjenestens innhentingshjemmel per i dag er metode- og teknologiuavhengig. Det samme gjelder de mest aktuelle rettslige begrensningene for inngrep i kommunikasjonsfriheten og den enkeltes personvern.

økonomiske konsekvenser, herunder hvilke eventuelle investeringer som er påkrevet i E-tjenesten, ikke har vært utvalgets oppgave. Dette må utredes senere dersom det blir truffet en beslutning på politisk nivå om videre prosess med sikte på å innføre DGF i Norge.

Utvalget har konkludert med at det ligger utenfor mandatets kjerne å vurdere hvilke beføyelser og hvilken innhentingsvirksomhet E-tjenesten bør ha i beredskapssituasjoner og væpnet konflikt som berører norsk territorium, samt hvilke nasjonalrettslige og folkerettslige bestemmelser som vil regulere virksomheten i slike situasjoner. Utvalget har derfor ikke sett behov for å vurdere beredskapslovgivningen, nasjonalt planverk og tjenestens planverk for krise og krig. Utvalget har heller ikke i de folkerettslige vurderingene analysert muligheten for midlertidig å fravike menneskerettslige regler i krisesituasjoner, f.eks. med hjemmel i Den europeiske menneskerettskonvensjonen artikkel 15.

1.3. Utvalgets sammensetning og arbeid

Forsvarsdepartementet oppnevnte utvalget i brev til medlemmene av 24. februar 2016.

Utvalget har hatt fem medlemmer:

- Professor Olav Lysne (utvalgsleder)
- Kontreadmiral (p) Trond Grytting
- Advokat Eva Jarbekk
- Avdelingsdirektør Einar Lunde
- Advokat Christian Reusch

E-tjenesten har ivaretatt sekretariatsfunksjonen for utvalget, og de fleste av utvalgets møter har av praktiske og sikkerhetsmessige årsaker funnet sted i E-tjenestens lokaler.

Utvalget har gjennomført 11 møter. Utvalget vurderte i lys av allerede tilgjengelig informasjon, samt avveining mellom merverdi og tidsforbruk, å ikke prioritere å gjennomføre studiebesøk til andre land. Utvalget ble først formelt oppnevnt mot slutten av februar. Dette forhold, sammenholdt med kompleksiteten ved og omfanget av de problemstillinger som har stått sentralt for utvalget, medførte at utvalget i brev ultimo mai 2016 ba Forsvarsdepartementet om fristutsettelse til 1. september 2016. Anmodningen ble innvilget ved brev av primo juni 2016 fra departementet til utvalget.

Utvalget har ikke funnet behov for å sette ut utredningsoppdrag til eksterne, men har innhentet en skriftlig uttalelse fra Nasjonal Institusjon for Menneskerettigheter (NIM) som er vedlagt utvalgets rapport.

Utvalget har gjennomført møter med Samferdselsdepartementet, Nasjonal sikkerhetsmyndighet, Politiets sikkerhetstjeneste og Datatilsynet. To av utvalgets medlemmer har gjennomført et møte med Telenor Norges ledelse. For øvrig har utvalget gjennomført flere møter med berørte fagmiljøer i E-tjenesten.

1.4. Rapportens inndeling

Utredningens innledende del (kapittel 1-4) omhandler – foruten sammendrag av utvalgets vurderinger og konklusjoner og et kapittel om utvalgets mandat, mandatforståelse og arbeid - grunnleggende bakgrunnsinformasjon som bakteppe for utvalgets vurderinger. Denne delen består av en beskrivelse av hva som menes med DGF, en redegjørelse for E-tjenestens samfunnsoppdrag, en fremstilling av den teknologiske og samfunnsmessige utvikling, samt en redegjørelse for DGF-lignende ordninger i andre land.

Dernest (kapittel 5-6) drøftes faktorene som etter utvalgets syn taler henholdsvis for og mot DGF. Utvalget redegjør videre for de rettslige rammene for DGF, særlig knyttet til menneskerettigheter og personvern (kapittel 7), og drøfter tekniske løsninger og begrensninger (kapittel 8).

Utvalgets samlede vurderinger av DGF fremgår av kapittel 9. Først presenteres DGF-systemet med kontrollmekanismer. Dernest vurderes kontrollmekanismene i mer detalj. Hovedvekten legges videre på vurderingene av om DGF er nødvendig og forholdsmessig, og hvilke tiltak og vilkår som utvalget mener bør være på plass som forutsetning for utvalgets konklusjon. Avslutningsvis (kapittel 10) sammenfattes utvalgets konklusjoner.

Som vedlegg til utredningen følger 1) to scenarier knyttet til hhv. cyberspionasje og internasjonal terrorisme som er ment å illustrere merverdien ved DGF, 2) en redegjørelse for forholdene i andre land, 3) uttalelse til utvalget fra Nasjonal Institusjon for Menneskerettigheter (NIM), og 4) forklaring av forkortelser og sentrale begreper som er benyttet i utredningen.

2. HVA SOM MENES MED DIGITALT GRENSEFORSVAR (DGF)

2.1. Definisjon

Digitalt grenseforsvar (DGF) kan defineres slik:

> E-tjenestens målrettede innhenting og analyse av utenlandsetterretningsrelevant informasjon, basert på aksess til elektronisk kommunikasjon som går inn og ut av Norge, i den hensikt å kartlegge og motvirke mulige ytre trusler mot rikets sikkerhet og selvstendighet og andre viktige nasjonale interesser

DGF er den betegnelsen utvalgets oppdragsgiver har valgt å benytte.[2] Noen har også benyttet betegnelsene digital grensekontroll, digital grenseovervåking og kabelaksess. Felles for betegnelsene er at det dreier seg om ordninger som inkluderer innhenting av/aksess til informasjon i bulk. Med bulk-innhenting/bulk-aksess[3] menes at etterretningstjenester må samle inn eller på annen måte ha tilgang til store mengder data *før* tjenestene målrettet og med bruk av utvalgte søkekriterier (f.eks. en IP-adresse) kan trekke ut relevant informasjon fra den større datamengden, og at datamengdene som det søkes i vil inneholde et betydelig mengde informasjon som ikke er relevant for utenlandsetterretningsformålet.

DGF dreier seg om innhenting, bearbeiding og analyse av utvalgt kommunikasjon som går inn og ut av Norge i landbaserte eller sjøbaserte fiberoptiske kabler.[4] Innhenting av innhold i kommunikasjon vil kun bli innsamlet målrettet, og ikke i bulk. Metadata vil derimot bli innsamlet i bulk på de kommunikasjonslinker man velger ut, og vil derfor også inneholde betydelige mengder informasjon knyttet til kommunikasjon som ikke er av interesse for E-tjenesten. En nærmere teknisk og konseptuell beskrivelse følger av kapittel 8 og 9.2.

DGF vil gjelde kommunikasjon over landegrensen. Det understrekes at kommunikasjonsbegrepet ikke krever at det dreier seg om kommunikasjon mellom to eller flere parter. Også ensidig overføring av lyd, tekst, bilder eller andre data omfattes. Det er nødvendig for bl.a. å fange opp cyberangrep som ikke innebærer gjensidig kommunisering mellom to eller flere aktører. DGF omfatter ikke innhenting av lagrede data, f.eks. data lagret i skyen, kun elektronisk kommunikasjon som overføres i et system for signaltransport ved hjelp av nett og tjenester.

Definisjonen reflekterer at det dreier seg om å fremskaffe informasjon som er av interesse for en utenlandsetterretningstjeneste. E-tjenesten er Norges eneste utenlandsetterretningstjeneste, og er landets sivile og militære utenlandsetterretningstjeneste. Forsvarsbegrepet henspeiler på at det dreier seg om et førstelinjeforsvar for å skaffe kunnskap om de mest alvorlige trusler, slik at de kan motvirkes før de materialiserer seg.

2.2. Formål

Det overordnede formålet med DGF er å sikre at den nasjonale COMINT-tjenesten[5] - det vil i Norge si E-tjenesten - i lys av den teknologiske utviklingen i fremtiden skal ha tilgang til utenlandsetterretningsrelevant informasjon, der slik informasjon finnes og kommuniseres. Dette er viktig for Norges evne til å kartlegge, varsle og motvirke alvorlige trusler, både i fredstid og i sikkerhetspolitiske krisesituasjoner.

---

[2] Betegnelsen er også benyttet av *Ekspertgruppen for Forsvaret av* Norge, som la frem sin utredning for Forsvarsdepartementet i april 2015.

[3] Sml. U.S. Presidential Policy Directive/PPD-28 on Signals Intelligence Acitivities, datert 17. Januar 2014, som definerer dette slik: "*References to signals intelligence in 'bulk' mean the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.).*" Denne definisjonen er på enkelte områder uklar. Særlig gjelder det dersom man bruker vide selektorer, f.eks. «Syria» som seleksjonsterm. I det tilfellet vil separasjonen av all trafikk til og fra Syria etter definisjonen fremstå som målrettet, og ikke som bulkinnhenting. Motsatt ville en innhenting av all trafikk som går over en spesiell kommunikasjonskanal som kun brukes av to personer, være å anse som bulkinnhenting, fordi man ikke benytter selektorer («discriminants») som grunnlag for innhentingen. I en rapport fra 2015 utarbeidet av det amerikanske National Research Council (NRC) – *Bulk Collection of Signals Intelligence: Technical Options* – tas det heller til orde for at «*if a significant portion of the data collected is not associated with current targets, it is bulk collection; otherwise, it is targeted*". Rapporten uttaler også at "*there is no precise definition of bulk collection, but rather a continuum with no bright line separating bulk from targeted*". I rapporten erkjennes det at begrepet "*significant*" i seg selv er et upresist begrep.

[4] Jf. dog mandatdrøftelsen i kapittel 1 om teknologiuavhengighet.

[5] COMINT: Communications Intelligence – kommunikasjonsetterretning.

E-tjenesten har etter gjeldende lovgivning oppdrag om å samle inn informasjon og drive kunnskapsorientert analyse i den hensikt å bidra til å kartlegge og motvirke ytre trusler mot rikets selvstendighet og sikkerhet og andre viktige nasjonale interesser. COMINT er innrettet mot å innhente informasjon om fremmede stater, organisasjoner og personer av relevans for dette oppdraget. Formålet med DGF er å innhente etterretninger om utenlandske trusselaktører og relevante utenlandske mål innenfor det oppgavesettet som i dag er tillagt E-tjenesten.

I det globale kommunikasjonsnettet formidles det informasjon som det er av vital betydning for norske myndigheter å ha kunnskap om. Nettet benyttes videre til virksomhet som kan utgjøre en ytre trussel mot landet og viktige nasjonale interesser. Trusselbildet er komplekst og dynamisk. Grenseoverskridende trusler som digital spionasje, cyberangrep, terrorisme og spredning av masseødeleggelsesvåpen antas å forsterkes ytterligere i årene som kommer.

De mest alvorlige trusler mot rikets sikkerhet og selvstendighet er nesten uten unntak trusler med en internasjonal opprinnelse, eller i hvert fall med utenlandske forbindelser i en eller annen form. Trusselaktørene kommuniserer over landegrensene. Avanserte IT-verktøy har gitt både større og mindre stater, samt ikke-statlige aktører, en evne til å ramme norske interesser som de tidligere ikke hadde. De mest avanserte aktørene gjennomfører spionasjeoperasjoner som kan pågå i flere år uten å bli oppdaget, også i Norge, med de betydelige negative økonomiske, sikkerhetsmessige og samfunnsmessige konsekvenser dette har. Digitale etterretningsoperasjoner er målrettede og komplekse. Aktørene er kapable, pågående og effektive. Operasjonenes mål spenner fra politiske og militære til teknologiske og økonomiske.

Elektronisk kommunikasjon benyttes i dag av trusselaktører bl.a. til å gi og formidle oppdrag, rapportere om gjennomførte tiltak, planlegge og gjennomføre operasjoner, fremskaffe etterretninger om mulige mål, motivere og radikalisere trusselaktører, og rekruttere nye medlemmer til trusselaktøren. Tidlig etterretning om slike forhold vil bedre responsevnen og muligheten til å kunne velge mellom ulike virkemidler fra norske myndigheters side. Det finnes en rekke eksempler på hvordan Internett har blitt benyttet av utenlandske trusselaktører for å infiltrere viktig samfunnsinformasjon og viktige samfunnsfunksjoner. Motivet kan være spionasje, av både økonomisk og sikkerhetspolitisk karakter, men en slik tilgang kan også bli brukt til sabotasje dersom den sikkerhetspolitiske situasjonen skulle tilsi det. Internett har også, i flere tilfeller, blitt trukket frem som et viktig verktøy for planlegging av og rekruttering til terrorvirksomhet. Flere terrorhandlinger har blitt stanset som følge av etterretningsvirksomhet i det digitale rom. Det foreligger nære eksempler på dette.[6] Terrorister bruker i økende grad sosiale media, spesielle applikasjoner og åpne og lukkede chatterom, bl.a. for planlegging og koordinering av terrorhandlinger. Trusselen fra terrorgrupper vedrørende cyberangrep med alvorlige samfunnsmessige konsekvenser er i dag marginal, men dette kan endres raskt. Enkelte terrorgrupper søker aktivt å forbedre evnen til å planlegge og gjennomføre slike angrep, enten på egen hånd eller gjennom samarbeid med andre ikke-statlige aktører.

Grensen mellom politisk påvirkning og krigføring er ikke så skarp som tidligere. Et digitalt angrep kan, avhengig av omstendigheter som angrepets formål og legitimitet, styrke og konsekvenser, i dag sidestilles med militært angrep og ulovlig maktbruk etter FN-paktens bestemmelser. Dette er lagt til grunn av de fleste toneangivende stater og av organisasjoner som NATO. Et formål med DGF er derfor å bidra til at Norge etablerer et troverdig forsvar mot slike angrep. DGF vil også gi bedre og økt etterretning på andre områder av betydning for norsk utenriks-, forsvars- og sikkerhetspolitikk.

Det digitale rom er i dag et krigføringsdomene. Et av formålene med DGF er å styrke forsvarsevnen mot angrep og sabotasje overfor en motstander som benytter det digitale rom som arena for slik

[6] Det kan bl.a. vises til intervju med sjefen for Säpo i Sverige, Anders Thornberg, i Dagens Nyheter 11. januar 2015, hvor han uttaler at man i løpet av de siste halvannet år har lykkes med å stanse to planlagte terroranslag i Sverige, og at signalspaning fra FRA er helt avgjørende for å kunne stanse slike anslag. Videre vises til rapport av 2014 fra det amerikanske *Privacy and Civil Liberties Oversight Board (Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act)*, s. 104 flg. Det kan også vises til at den britiske regjeringen, i dokumentet «*Operational Case for Bulk Powers*» fra 2015, konkluderer med at det er klare bevis for at informasjon innsamlet ved bulk aksess bl.a. har spilt en betydelig rolle i alle kontraterrorsaker de siste 10 år, «*including in each of the seven terrorist attack plots disrupted since November 2014*».

virksomhet. Uansett hvordan Norge gjennom forebyggende sikkerhetstiltak søker å gjøre det vanskelig for en motstander å nå frem med angrep, vil en avansert motstander utnytte svakheter i bl.a. informasjonssystemer og driftsrutiner. Angrep og sabotasje kan også finne sted utenfor rammen av en åpenbar væpnet konflikt. Et eksempel på dette kan være hendelsen 23. desember 2015, hvor to regionale elkraftselskaper i Ukraina ble utsatt for sabotasjehandlinger som medførte omfattende strømbortfall. Ifølge åpne kilder hadde angriper trolig så tidlig som i mars 2015 plantet skadevare i de to kraftselskapenes datanettverk, og dermed sikret kontroll over ressurser og tjenester.

Det kan i denne sammenhengen vises til regjeringens langtidsplan for forsvarssektoren, som ble fremmet for Stortinget 17. juni 2016, hvorfra hitsettes:[7]

«Digitale angrep har i økende grad blitt en integrert del av militære operasjoner. Slike angrep kan forstyrre, påvirke og hindre nasjonale beslutningsprosesser i sikkerhetspolitiske kriser og væpnet konflikt. Evne til å motstå angrep i og gjennom det digitale rom for å sikre egen handlefrihet vil derfor være viktige elementer i et lands forsvar, selv om maktanvendelse gjennom det digitale rom sannsynligvis ikke vil kunne avgjøre mellomstatlige konflikter alene. En forutsetning for å kunne motstå slike angrep er å ha tilstrekkelig kapasitet og et rettslig rammeverk for å kunne oppdage og håndtere digitale angrep som har sin opprinnelse utenfor Norges grenser.»

Når Norge iverksetter en ny langtidsplan for Forsvaret, så dreier det seg om å ha et forsvar som nasjonalt og i en NATO kontekst også kan beskytte nasjonen mot et trusselspektrum ut over det klassisk konvensjonelle militære. Nasjonen må kunne beskyttes mot såkalte hybride angrep fra en aktør som ønsker å utøve makt eller press. Maktbruken vil kunne ha som formål å påtvinge norske myndigheter en politisk innrømmelse eller avståelse av suverenitet. En fiende vil søke å beherske informasjonsdomenet, og kampen vil i mangt kunne dreie seg om det kognitive (dvs. befolkningens opplevelse av hva som skjer snarere enn det som faktisk foregår). Hybrid krigføring kan være et sett av handlinger som er satt i kombinasjon; økonomisk press, geografisk posisjonering, utpressing, psykologiske operasjoner, propaganda og desinformasjon, militær demonstrasjon, infiltrasjon med kamuflerte spesialenheter, planting av digitale våpen som vil slå ut kritisk infrastruktur, villedning og nedstengning av kommunikasjonskanaler – alt forberedt over tid gjennom spionasje og infiltrasjon.

Et vesentlig formål med DGF – ut over å motvirke cyberspionasje, avverge terroranslag og støtte norske styrker i internasjonale operasjoner – vil derfor være å styrke Norges forsvar mot både klassiske militære angrep og hybrid krigføring. E-tjenesten har et særlig ansvar for å identifisere og varsle en aktørs mulige oppbygging av angrep mot Norge og norske interesser.

[7] Prop. 151 S (2015-2016), *Kampkraft og bærekraft – Langtidsplan for forsvarssektoren*, s. 35.

3. ETTERRETNINGSTJENESTENS SAMFUNNSOPPDRAG OG INFORMASJONSTILGANG

3.1. Etterretning som historisk fenomen

Etterretning har foregått i alle tider. Etterretningens kjerne er den samme i dag. Etterretning benyttes for å samle inn den informasjonen som en motpart vil holde skjult. Om nødvendig må slik informasjon stjeles ved fordekte metoder som ellers ikke er tillatt i samfunnet. Kun metodene har forandret seg gjennom tidene. Fremveksten av nasjonalstater og det moderne diplomatiet etter middelalderen bidro til å utvide etterretningens funksjon og rolle, fra et grunnleggende selvforsvarsbehov, via en fase preget av ekspansjon og erobring, og frem til en politisk strategisk rådgivningsfunksjon. Nye oppfinnelser, herunder mer moderne kommunikasjonsformer, innebar at etterretningstjenestenes muligheter for å innhente informasjon med ulike metoder økte.

Norges moderne etterretningshistorie startet i 1905, men først under og etter den annen verdenskrig etablerte regjeringen et eget norsk etterretningsvesen. Stiftelsesdagen regnes for å være 6. februar 1942, da Forsvarets overkommandos avdeling II ble opprettet. Norske etterretningskapasiteter vokste deretter raskt i volum, og etter hvert også i kvalitet, som beskrevet i Moland og Riste: *Strengt hemmelig – norsk etterretningshistorie 1945-1970*. Man samarbeidet nært med enkelte allierte, men regjeringen fremhevet tidlig at Norge, som en suveren stat, forutsetningsvis må disponere en egen etterretningstjeneste. Det ble fra starten av satset sterkt på bl.a. elektronisk etterretning, med utbygging av radio-, radar- og sonarstasjoner, spesielt i Nord-Norge. Før murens fall var etterretningsfunksjonen innrettet mot den kalde krigens fiendebilde. Senere har en rekke andre utviklingstrekk bidratt til å forme norsk etterretning, herunder Norges geopolitiske beliggenhet, bruken av avansert teknologi på en del områder, det bilaterale etterretningssamarbeidet, Lundkommisjonen, innføring av lov om Etterretningstjenesten, terrorutfordringer i kjølvannet av terrorangrepene i USA 11. september 2001, samt norske styrkers deltakelse i internasjonale operasjoner under og etter Balkan-operasjonene fra midten av 1990-tallet.

3.2. E-tjenesten som nasjonal strategisk utenlandsetterretningstjeneste i dag

I Forsvarssjefens etterretningsdoktrine av mai 2013 er etterretning – i realiteten *utenlands*etterretning[8] – definert slik:

> Etterretning er systematisk innhenting og bearbeiding av informasjon som angår utenlandske forhold ervervet med åpne og fordekte metoder i en statlig legal ramme. Produktene skal redusere usikkerhet, skape forståelse og har ofte en prediktiv karakter. Begrepet brukes om produktet, aktiviteten og organisasjonen som utøver aktiviteten.

E-tjenesten er landets nasjonale – sivile og militære – og sektorovergripende strategiske utenlandsetterretningstjeneste. Tjenesten har utviklet seg til en helhetlig nasjonal tjeneste med en økende andel oppdragsgivere utenfor forsvarssektoren.

E-tjenesten har i dag tre hovedoppgaver:[9]

1. Fremskaffe informasjon om og varsle trusler mot Norge og norske interesser
2. Understøtte viktige politiske beslutningsprosesser med relevant informasjon vedrørende fokusområder for norsk utenriks-, sikkerhets- og forsvarspolitikk
3. Støtte Forsvarets operasjoner hjemme og ute i verden

Tjenestens oppdragsgivere forventer i økende grad å få kunnskap[10] om omverdenen basert på unik informasjon som holdes skjult av andre. Etterspørselen etter etterretningsvurderinger er stigende, noe

[8] Definisjonen bygger på NATOs tilsvarende definisjon, og skiller utenlandsetterretning fra annen innsamling og bearbeiding av informasjon, enten det gjøres av andre offentlige myndigheter (f.eks. politiets/PSTs kriminaletterretning) eller private aktører (f.eks. "business intelligence").

[9] Oppgavesettet er ytterligere detaljert i og i medhold av lov, se kap. 3.3.2 nedenfor.

[10] Det er også en økende forventning om at en utenlandsetterretningstjeneste skal kunne gjennomføre operasjoner som ikke bare har til hensikt å frembringe informasjon, men som også kan bidra til å minimere en trussel eller påvirke en tilstand. E-tjenesten er også pålagt oppdrag som per definisjon ikke er etterretning. Et eksempel er at tjenesten er tillagt ansvaret for gjennomføring av offensive cyberoperasjoner med annet formål enn å

som må forstås på bakgrunn av endringer som gjør Norge mer synlig globalt. En rekke forhold retter oppmerksomhet mot Norge. Norges samlede etterretningsbehov er som følge av dette tettere knyttet til globale og regionale prosesser enn vår størrelse og beliggenhet skulle tilsi. I tillegg kommer at Norge tradisjonelt har ført en mer aktiv utenrikspolitikk enn småstater flest, noe som bidrar til å forsterke spennvidden i etterretningsbehovene. Tilsvarende er koblingen mellom hendelser på taktisk og strategisk nivå blitt tettere, ikke minst som følge av at informasjon spres og er tilgjengelig globalt kort tid etter en hendelse.

3.3. Folkerettslige og nasjonalrettslige rammer for E-tjenesten

3.3.1. Folkeretten

I folkeretten er utenlandsetterretningsvirksomhet lite regulert. Det finnes ingen generell internasjonal norm som forbyr eller begrenser virksomheten[11], selv om spesifikke normer i folkeretten selvsagt også skal etterleves av utenlandsetterretningstjenester. De mest relevante folkerettslige regler relatert til utvalgets utredningsmandat er behandlet i kapittel 7. Her skal kun fremheves at etterretningsvirksomhet har et dualistisk forhold til legalitet:

a. På den ene siden viser statspraksis, som er den viktigste rettskilde i folkeretten, at strategisk utenlandsetterretningstjeneste både er lovlig og legitim virksomhet. I mellomstatlig sammenheng anses virksomheten endog å kunne ha viktige positive effekter, bl.a. fordi kunnskap om hverandres egentlige kapasiteter og intensjoner kan ha en stabilitetsfremmende effekt og motvirke at hendelser eskalerer til konflikt gjennom misforståelser av f.eks. aktørers intensjoner.
b. På den annen side ligger det i etterretningens natur at metodebruken vil kunne medføre brudd på den nasjonale lovgivningen i en annen stat, med mindre det foreligger særskilt avtale eller annet rettslig grunnlag. Fordekt innhenting av informasjon som ønskes hemmeligholdt av annen stat vil ofte være straffebelagt av den stat innhentingen er rettet mot, og særlig dersom etterretningsvirksomheten skjer innenfor denne statens jurisdiksjonsområde. E-tjenesten er eneste offentlige myndighet i Norge som er autorisert gjennom lov og instruks til å bryte lovgivningen i andre stater[12]. Slik aktivitet representerer imidlertid ikke brudd på folkeretten. Stater kan dessuten vanskelig beskytte seg gjennom nasjonal lovgivning mot etterretningsvirksomhet som foregår utenfor dens jurisdiksjonsområde (eksempelvis fra åpent hav eller fra rombaserte etterretningsplattformer).

3.3.2. Lov og instruks om Etterretningstjenesten

E-tjenestens overordnede oppgaver og virksomhet er regulert i E-loven.[13] Loven overlater til regjeringen å regulere enkelte sider ved tjenestens virksomhet, men fastslår grunnleggende prinsipper og viktige grenser for virksomheten. Loven er utdypet i E-instruksen.[14] Annet offentlig tilgjengelig regelverk er instruks om samarbeidet mellom E-tjenesten og PST[15], og Forsvarsdepartementets utfyllende bestemmelser om innsamling mot norske personer i utlandet samt for utlevering av personopplysninger til utenlandske samarbeidende tjenester.[16] I tillegg gjelder personopplysningsloven[17] for E-tjenestens behandling av personopplysninger, enten opplysningene kan knyttes til en norsk eller ikke-norsk fysisk enkeltperson.

E-tjenesten skal i fred, krise og krig gi norske myndigheter og militære sjefer pålitelig, rettidig og relevant etterretningsstøtte. For at tjenesten skal kunne utføre sine lovpålagte oppgaver, har tjenesten aksess til og behandler omfattende mengder med informasjon, herunder opplysninger som kan knyttes til enkeltpersoner. Dersom informasjonen har direkte tilknytning til ivaretakelse av tjenestens oppgaver eller er direkte knyttet til en persons arbeid eller oppdrag for tjenesten, kan tjenesten også oppbevare og behandle informasjon som gjelder norske fysiske eller juridiske personer (E-loven § 4 annet ledd). Denne bestemmelsen synliggjør at tjenesten har behov for å behandle opplysninger om

innhente informasjon, innenfor rammen av norsk lov og norske folkerettslige forpliktelser.

[11] Utviklingen etter Snowden har ikke endret på forannevnte rammer, men det er enkelte som i debatten har tatt til orde for at etterretningsvirksomhet burde reguleres nærmere i folkeretten. Få om noen stater har imidlertid argumentert for dette.

[12] Sjefen for E-tjenesten opplyste i intervju med NTB i desember 2015 at «*Norske etterretningsagenter bryter til stadighet loven i land de opererer og løper stor risiko.*»

[13] Lov 20. mars 1998 nr.11 om Etterretningstjenesten.

[14] Kgl res 31. august 2001 nr. 1012 om Etterretningstjenesten.

[15] Kgl res 13. oktober 2006 nr. 1151.

[16] Fastsatt 24. juni 2013.

[17] Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).

norske personer, selv om § 4 første ledd forbyr tjenesten å drive fordekt innhenting rettet mot norske personer på norsk territorium.

E-tjenestens lovbestemte oppdrag er fastsatt slik i E-loven § 3 første ledd:

«Etterretningstjenesten skal innhente, bearbeide og analysere informasjon som angår norske interesser sett i forhold til fremmede stater, organisasjoner eller individer, og på denne bakgrunn utarbeide trusselanalyser og etterretningsvurderinger i den utstrekning det kan bidra til å sikre viktige nasjonale interesser, herunder

a) utformingen av norsk utenriks-, forsvars- og sikkerhetspolitikk,
b) beredskapsplanlegging og korrekt episode- og krisehåndtering,
c) langtidsplanlegging og strukturutvikling i Forsvaret,
d) effektiviteten i Forsvarets operative avdelinger,
e) støtte til forsvarsallianser som Norge deltar i,
f) norske styrker som deltar i internasjonale militære operasjoner,
g) tilveiebringelse av informasjon om internasjonal terrorisme,
h) tilveiebringelse av informasjon om overnasjonale miljøproblemer,
i) tilveiebringelse av informasjon om ulike former for spredning av masseødeleggelsesvåpen og utstyr og materiale for fremstilling av slike våpen, og
j) grunnlaget for norsk deltakelse i og oppfølging av internasjonale avtaler om nedrustnings- og rustningskontrolltiltak.»

Oppregningen er ikke uttømmende. Hva som er andre «viktige nasjonale interesser», vil avhenge av hvilke sikkerhetsutfordringer Norge til enhver tid står overfor, jf. E-instruksen § 7 annet ledd. Oppgavene vil imidlertid til enhver tid være ytterligere detaljert og prioritert fra oppdragsgivernes side, i det årlige prioriteringsdokumentet som er nevnt i E-instruksen § 12 og som utgis av Forsvarsdepartementet. For oppdukkende prioriteter benyttes RFI-systemet (*Request For Information*) fra oppdragsgiver. Dette innebærer at all innhenting og behandling av informasjon som E-tjenesten gjennomfører, skal kunne knyttes direkte til et oppdrag nedfelt i prioriteringsdokumentet eller i en RFI fra overordnet myndighet. Innsamlingsoppdraget er derfor til enhver tid formålsavgrenset. E-tjenesten innhenter aldri etterretninger for egen skyld eller for andre formål enn de som politiske myndigheter til enhver tid prioriterer.

Iht. E-loven § 3 annet ledd kan E-tjenesten etablere og opprettholde etterretningssamarbeid med andre land. Utveksling av informasjon med samarbeidende tjenester i utlandet er en forutsetning for og en viktig del av slikt samarbeid.[18]

E-loven § 4 første ledd fastsetter at E-tjenesten ikke skal overvåke eller på annen fordekt måte innhente informasjon om norske fysiske eller juridiske personer på norsk territorium. Bestemmelsen er primært begrunnet i en geografisk ansvarsinnsnevring av E-tjenestens virkeområde, spesielt av hensyn til å unngå uklare grenser mellom E-tjenesten og politiets overvåking av personer i Norge i kriminalitetsbekjempelsesøyemed. Lovens forarbeider forutsatte at eventuelle gjenstående uklare ansvarsgrenser mellom E-tjenesten og PST skulle løses gjennom instruksregulering.

E-instruksen regulerer enkelte forhold knyttet til innhenting av informasjon vedrørende norske fysiske eller juridiske personer. Etter E-instruksen § 5 har tjenesten adgang til å innhente informasjon om fremmed etterretningsvirksomhet i Norge, herunder om norske personer som driver slik virksomhet. Dette er i hovedsak begrunnet med tjenestens behov for å beskytte egen virksomhet mot slik etterretning, og kan bare skje gjennom eller med samtykke fra PST. Av lovens forarbeider fremgår det at forbudet i § 4 mot informasjonsinnhenting om norske personer på norsk jord ikke skal tolkes motsetningsvis. Det er altså ikke slik at tjenesten fritt kan samle informasjon om norske borgere i utlandet eller utenlandske borgere i Norge. Forbudet i § 4 første ledd mot fordekt innhenting på norsk territorium er dessuten på generelt grunnlag antatt også å gjelde for utenlandske statsborgere som har lovlig opphold i Norge, midlertidig eller permanent, hvor reelle hensyn tilsier at personene bør ha samme rettssikkerhetsgarantier som norske borgere. Til-

[18] Det følger av forarbeidene til E-loven at tjenesten kan innhente informasjon som er i samarbeidende tjenesters interesse, fordi slik innhenting indirekte også vil ha betydning for norske interesser i lys av at E-tjenesten ofte får viktig informasjon tilbake ut fra et gjensidighets- og informasjonsbytteperspektiv («e-valuta»).

knytning til fremmed stat kan imidlertid tilsi at enkelte utenlandske personer ikke har samme krav på beskyttelse mot etterretning på samme måte som andre utenlandske statsborgere som lovlig oppholder seg i Norge. I forarbeidene til E-loven[19] er det presisert at det vil være tilfeller hvor forbudet ikke kommer til anvendelse. Særlig nevnes «fremmed aktivitet» på norsk territorium, som må forstås som utenlandsk aktivitet som utføres på vegne av fremmed stat eller internasjonal organisasjon. Det fremheves at «*Bestemmelsen vil derfor ikke ramme innhenting av informasjon om utenlandske statsborgere som oppholder seg i Norge og annen fremmed aktivitet i Norge, såfremt dette er nødvendig for å gjennomføre Etterretningstjenestens oppgaver som angitt i lovforslaget*.» Det følger imidlertid av fast praksis i tjenesten at tjenesten ikke fordekt innhenter informasjon om utenlandske statsborgere i Norge, med mindre disse opptrer på vegne av en fremmed makt. Et moment for å videreføre denne praksisen er at PST i stor grad ser det som sin oppgave å foreta fordekt innhenting mot utenlandske borgere i Norge, riktignok for andre formål enn de formål som er styrende for E-tjenestens virksomhet. Dersom E-tjenesten foretar slik innhenting parallelt, vil de to tjenestene lett kunne gå i beina på hverandre. I tillegg vil effektivitetshensyn til en viss grad tilsi at oppgavesettene ikke i for stor grad bør overlappe hverandre.

Ytterligere begrensinger for E-tjenestens innhentingsvirksomhet i Norge kan følge av legalitetsprinsippet, blant annet slik at inngripende metoder ikke kan tas i bruk i Norge uten hjemmel i lov. Inngripende metodebruk er hjemlet i E-lovens innhentingshjemmel (§ 3), men forholdsmessighet og nødvendighet ved inngrepet må vurderes konkret i den enkelte sak. E-tjenesten står friere til å benytte metoder for informasjonsinnsamling som ikke rammes av legalitetsprinsippet, for eksempel søk i åpne kilder eller observasjoner i det offentlige rom. Tjenesten kan også passivt motta informasjon om norske og utenlandske borgere som befinner seg på norsk territorium fra personer som tar kontakt på eget initiativ. All slik virksomhet må imidlertid ligge innenfor E-loven og E-instruksens angivelse av tjenestens formål og oppgaver, slik at disse også begrenser tjenestens virkeområde.

Med «norske personer» menes

a. norske og utenlandske statsborgere som har fast eller midlertidig lovlig opphold i Norge og som ikke opptrer på vegne av fremmed makt, eller
b. norske og utenlandske juridiske personer som har hovedkontor i Norge eller på annen måte lovlig opererer på norsk territorium eller har annen særlig primærtilknytning til riket og som ikke opptrer på vegne av fremmed makt, uavhengig av hvilke(n) ikke-statlig(e) fysisk(e) eller juridisk(e) person(er) som eier eller kontrollerer virksomheten.

En person som befinner seg i utlandet skal anses som ikke-norsk person med mindre det foreligger eller fremkommer klare holdepunkter for at vedkommende er norsk person. En person som befinner seg på norsk territorium skal anses som norsk person med mindre det foreligger eller fremkommer klare holdepunkter for at vedkommende ikke er norsk person. Ved tvil om vedkommende befinner seg på norsk territorium eller i utlandet, skal legges til grunn det som fremstår som mest sannsynlig basert på den informasjon som er tilgjengelig eller som kan skaffes til veie fra PST, åpne kilder eller annen lovlig innhenting.

Tjenesten er avhengig av å kunne innhente og lagre rådata for å løse sitt oppdrag. Rådata som innhentes og lagres er ikke tilfeldig valgt ut. Det velges eksempelvis ut kommunikasjonsstrømmer, basert på visse kriterier, som antas å fremskaffe mest mulig utenlandsetterretningsrelevant informasjon blant rådataene. All rådata som tjenesten innsamler vil imidlertid kunne inneholde data som også kan knyttes til norske personer eller utenlandske personer som ligger utenfor tjenestens interessefelt. Det er langvarig praksis for at tjenesten lagrer slike data. Utvalget er kjent med at EOS-utvalget i lys av denne praksis har reist noen prinsipielle tolkningsspørsmål knyttet til E-loven § 4 første ledd.[20]

Tjenestens målrettede innsamlingen av informasjon (søk etter og uttrekk av informasjon fra lagrede data) er ikke rettet mot norske forhold og personer. I forhold til behandlingen av personopplysninger knyttet til norske personer, er lagringen hjemlet i personopplysningsloven § 8 d) og e), fordi behandlingen er helt nødvendig for at tjenesten skal kunne

[19] Ot prp nr 50 for 1996-97 side 11.

[20] Se *Særskilt melding til Stortinget fra Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget) om rettsgrunnlaget for Etterretningstjenestens overvåkingsvirksomhet*, som ble avgitt 17. juni 2016 og som i skrivende stund ligger til behandling i Stortingets kontroll- og konstitusjonskomité.

utføre sine lovpålagte oppgaver. Tekniske, praktiske og økonomiske årsaker medfører at det er umulig å foreta rutinemessig manuell gjennomgang av alle rådata for å vurdere deres etterretningsrelevans. Dette skjer først når data aktivt trekkes ut av rådatamaterialet og overføres til tjenestens prosesserings- og analyseverktøy og således kan vurderes av mennesker.[21]

E-tjenesten skal være under nasjonal kontroll, se E-instruksen § 4. Det gjelder også den informasjonen som deles med utenlandske samarbeidspartnere, noe som bl.a. innebærer at det ikke er anledning til å videreformidle rådata som tjenesten ikke kjenner karakteren eller innholdet av.

For øvrig skal E-tjenestens oppgaver utføres innenfor rammen av den alminnelige lovgivning, administrative og militære instrukser samt ulovfestet rett. Tjenesten kan dermed f.eks. ikke benytte virkemidler som er i strid med norske strafferettslige regler. Dette gjelder likevel bare så langt de aktuelle straffebestemmelsene kommer til anvendelse i utlandet, eller det ikke følger av bestemmelsen selv eller den generelle strafferettslige rettsstridsreservasjonen eller doktrinen om lovlige myndighetshandlinger at tjenestens virksomhet ikke rammes.

3.3.3. Personopplysningsloven

E-tjenestens adgang til å lagre informasjon om norske personer er, som berørt ovenfor, uttrykkelig regulert i E-loven § 4 annet ledd, der det heter at E-tjenesten bare kan oppbevare informasjon som gjelder norske fysiske eller juridiske personer dersom informasjonen har direkte tilknytning til ivaretakelsen av tjenestens oppgaver, eller er direkte knyttet til en slik persons arbeid eller oppdrag for tjenesten. I tillegg gjelder personopplysningsloven med forskrifter for tjenestens behandling og lagring av personopplysninger. E-tjenesten er unntatt fra personopplysningslovens regler om melde- og konsesjonsplikt samt fra Datatilsynets og Personvernnemndas tilgang til og kontroll med opplysninger i tjenesten, jf. personopplysningsforskriften § 1-2. Tjenestens behandling av personopplysninger kontrolleres i stedet av EOS-utvalget.[22]

E-tjenesten kan bare behandle personopplysninger, uavhengig av om personen er norsk eller ikke, dersom behandlingen kan antas å ha betydning for ivaretakelsen av tjenestens oppgaver etter E-loven § 3 og prioriteringsdokumentet fastsatt i medhold av E-instruksen § 12. Personopplysninger kan ikke behandles til formål som er uforenlig med det opprinnelige formålet med innsamlingen, uten forutgående samtykke fra den person opplysningene kan knyttes til. Personopplysninger kan heller ikke behandles dersom opplysningene anses utilstrekkelige eller irrelevante for formålet med behandlingen. E-tjenesten skal ikke behandle personopplysninger utelukkende på bakgrunn av hva som er kjent om en persons etnisitet eller nasjonale bakgrunn, politiske, religiøse eller filosofiske overbevisning, fagforeningstilhørighet eller opplysninger om helsemessige eller seksuelle forhold.

E-tjenesten skal ikke lagre personopplysninger lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. Hvis ikke personopplysningene deretter skal oppbevares i henhold til arkivloven eller annen lovgivning, skal de slettes.[23] Nødvendighets-/relevansvurderingen er en etterretningsfaglig vurdering, som kan variere etter fagområde/tema og andre omstendigheter. Nærmere bestemmelser fremgår av E-tjenestens interne regelverk. For behandling av store datamengder er automatisk/maskinell filtrering og sletting eneste mulighet; manuell siling og sletting er rett og slett for tid- og ressurskrevende. Tjenesten utreder for tiden et helhetlig og generelt regelverk for behandling av personopplysninger i tjenesten, for å sikre en enda mer effektiv implementering av personvernhensyn i alle deler av tjenestens virksomhet, samtidig som det må tas hensyn til etterretningsfagets langsiktige fokus som beskrevet over. E-tjenesten ansatte i 2014 en personvernrådgiver for ytterligere å styrke innsatsen på disse områdene.

3.4. Kontroll, styring og rapportering

I demokratiske politiske systemer er åpenhet en sentral forutsetning for at de styrte skal ha den nødvendige tillit til de styrende. Men også demokratier må ha muligheten til å forsvare seg mot ytre og indre fiender. Virksomhet der visse deler er unndratt

[21] Utvalget har registrert at enkelte har argumentert for at selve den teoretiske aksessen på et tidlig stadium til store ubearbeidede datamengder i seg selv ikke kan anses for å være innsamling eller registrering (behandling av personopplysninger). Utvalget finner for sin del ikke holdepunkter for at en slik argumentasjon kan føre frem.

[22] jf. lov 3. februar 1995 nr. 7 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste og instruks 30. mai 1995 nr. 4295 om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste.

[23] Se personopplysningsloven § 28 første ledd.

offentlig innsyn er et akseptert og legitimt redskap for å ivareta et lands grunnleggende nasjonale interesser og borgernes sikkerhet. De hemmelige tjenesters fullmakter, som gjør dem i stand til å løse sine oppgaver, står i et potensielt motsetningsforhold til borgernes individuelle rettigheter. For å sikre at borgernes demokratiske og juridiske rettigheter ikke blir krenket av de hemmelige tjenestenes virksomhet, er tjenestene underlagt særskilte regimer som utøver styring og kontroll på vegne av det politiske systemet.

Forsvarsministeren er parlamentarisk og konstitusjonelt ansvarlig for E-tjenestens virksomhet, og utøver styring og kontroll både gjennom Forsvarssjefen og direkte overfor E-tjenesten. E-tjenestens løpende oppgaver og prioriteringer reguleres i det årlige prioriteringsdokumentet fra Forsvarsdepartementet, som er gradert og som oppdateres gjennom en løpende oppdragsdialog. Sentralt i den løpende politiske styring og kontroll står også E-tjenestens foreleggelsesplikt overfor Forsvarsdepartementet (regulert i E-instruksen § 13). Foreleggelsesplikten gjelder for etablering av samarbeid og avtaler med utenlandske tjenester og organisasjoner, organisering av okkupasjonsberedskapen, iverksetting av særskilte etterretningsoperasjoner som kan reise politiske problemstillinger og andre saker av særlig viktighet eller prinsipiell karakter. Innføring av nye innsamlingskapasiteter og iverksetting av nye former for etterretningsoperasjoner vil falle inn under foreleggelsesplikten og derfor være underlagt politisk kontroll. Forsvarsdepartementet har videre en styringsfunksjon i forhold til hvem E-tjenesten skal rapportere til (regulert i E-instruksen § 16). Rapportering til instanser utenfor Forsvaret skal skje gjennom departementet eller etter departementets anvisninger. Rapportering til militære brukere bestemmes av Forsvarssjefen.

E-tjenesten er underlagt flere styrings- og kontrollordninger som har til hensikt å sikre Stortinget, regjeringen og Riksrevisjonen innsikt i virksomheten:[24]

- Stortinget informeres om tjenestens virksomhet gjennom en *årlig orientering for Stortingets president*, der også riksrevisor og leder og nestleder i Utenriks- og forsvarskomiteen er til stede.

- Det parlamentariske kontrollorganet, *Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget)*, har som oppgave å sikre at virksomheten skjer innenfor de rammer som er fastlagt. Utvalgets medlemmer (nylig utvidet til 8 personer) velges av Stortinget, og utvalget rapporterer hvert år til Stortinget gjennom en årsmelding og ellers ved behov.[25]

- *Koordineringsutvalget for Etterretningstjenesten*, omtalt som K-utvalget, ledes av departementsråden i Forsvarsdepartementet. Forsvarssjefen og sjefen for E-tjenesten er medlem av utvalget, sammen med enkelte avdelingssjefer i Forsvarsdepartementet. Riksrevisjonen er også representert. K-utvalget gjennomgår og kontrollerer tjenestens budsjetter, planer, personellrammer, regnskapsoversikter og større materiellanskaffelser. Utvalget fungerer således som E-tjenestens forvaltningsmessige styringsorgan. I tillegg revideres tjenestens regnskap av Riksrevisjonen, på lik linje med all annen statlig virksomhet.

E-tjenesten har etablert internkontrollfunksjoner for å sikre en lovlig og hensiktsmessig utøvelse av tjenestens virksomhet. Disse er av ulik karakter og i nødvendig utstrekning tilpasset disiplin og fagområde. Funksjonene er nedfelt i interne bestemmelser, instrukser og retningslinjer.[26] I tillegg kommer

[24] Tidligere var også *Koordinerings- og rådgivningsutvalget for etterretnings-, overvåkings- og sikkerhetstjenesten (KRU)* en del av den samlede styrings- og koordineringsordningen. KRU var et samarbeidsorgan med representanter fra Utenriks-, Forsvars- og Justis- og beredskapsdepartementet, som ledet utvalgets arbeid på omgang. Sjefene for E-tjenesten, PST og NSM var også medlemmer av utvalget, hvis oppgave var å koordinere virksomheten til de tre tjenestene og gi råd til myndighetene i relevante spørsmål. Utvalgets virksomhet er nylig nedlagt, men funksjonene er delvis overtatt av Kriserådet.

[25] EOS-utvalget inspiserer E-tjenestens virksomhet flere ganger hvert år, både hovedkvarteret på Lutvann og stasjonene. Om EOS-utvalgets kontroll med E-tjenesten vises ellers til Evalueringsutvalgets innstilling av 29. februar 2016 til Stortingets presidentskap, samt til EOS-utvalgets årsmeldinger og lov og instruks for EOS-utvalget.

[26] Internkontrollfunksjonene er samlet sett ment å utgjøre et system som både er systematisk og helhetlig. Tjenesten har bl.a. gjennom prosedyrer pålagt seg selv en rekke interngodkjennings-, kontroll- og notoritetsmekanismer. Mekanismene er delvis automatiserte og delvis manuelle. Internkontrolltiltak kan særlig ta form av at godkjenning fra flere instanser i tjenesten er påkrevd før iverksettelse, eller ved særskilt periodisk rapportering og/eller gjennomgang av enkeltsaker for å sikre regelverksetterlevelse. Et eksempel på en slik mekanisme er at innhenting av informasjon om norske rettssubjekter i utlandet eller deling av personopplysninger om norske personer med samarbeidende tjenester i andre land forelegges ledelsesnivået i tjenesten i hvert

andre typer ordninger, bl.a. opplæringstiltak samt særskilt rådgivning fra og rapportering til tjenestens personvernrådgiver og tjenestens juridiske enhet. Tjenesten gjennomfører rutinemessig opplæring av ansatte i gjeldende regelverk og prosedyrer innen de ulike etterretningsdisipliner. Det er videre etablert et system for avviksrapportering. Når et brudd avdekkes, foretas det rutinemessig en etterfølgende vurdering av hvorvidt det dreier seg om systemsvikt eller et enkeltstående avvik. Det er avgjørende for tjenestens håndtering av bruddet og for hvilke prosesser som iverksettes i etterkant. Avviksrapporter forelegges rutinemessig for EOS-utvalget.[27]

Det interne regelverket og dertil knyttede internkontrollmekanismer vurderes jevnlig. For tjenesten er det vesentlig å ha en dynamisk tilnærming til internt regelverk, slik at det på en forsvarlig måte kan tilpasses den kontinuerlige utviklingen innen teknologi og andre operative forhold. Interne kontrollordninger drøftes rutinemessig med EOS-utvalget, og tilpasses så langt mulig også EOS-utvalgets kontrollbehov.

3.5. Etterretning og informasjonsbehandling

3.5.1. Analyse, målutvikling og vilkår for informasjonsbehandling

Etterretningsvirksomhet er i mange tilfeller et møysommelig puslespill som krever behandling og sammenstilling av informasjon fremkommet gjennom mange kilder og ved ulike metoder. På den måten vil E-tjenesten etablere den nødvendige helhetlige og forsvarlige kunnskapen tjenesten trenger for å kunne utarbeide trusselanalyser og etterretningsvurderinger. Dette langsiktige perspektivet, sammenholdt med fokus på utenlandske forhold, er noe av det som skiller E-tjenesten fra andre offentlige virksomheter. Virksomheten er tidkrevende, og fordrer at opplysninger oppbevares og analyseres i et langsiktig perspektiv. Bl.a. kreves en langvarig oppbygging av forståelsen for et normalsituasjonsbilde for å kunne detektere avvik fra det normale. Etterretningspersonell er av natur og fag «samlere» av informasjon. Historisk sett har man vektlagt dokumentasjonshensyn fremfor hensyn til sletting av ikke relevant informasjon.

Etterretningsvirksomhet er i større grad informasjonsorientert enn personorientert. Man innhenter relevant informasjon der det er lettest å frembringe denne. Det er i prinsippet irrelevant om personer som tjenesten innhenter informasjon om, er mistenkt for å planlegge eller ha begått straffbare handlinger. Det avgjørende er om innhenting kan fremskaffe utenlandsetterretningsrelevant informasjon. Dette gjelder også på kontraterrorfeltet.

Målutvikling er prosessen for å finne nye trusselaktører (eller andre legitime etterretningsmål) eller mer informasjon rundt allerede kjente mål. Målutvikling er grunnstammen i og forutsetningen for all etterretningsvirksomhet. Uten målutvikling er det ikke mulig å drive etterretningsvirksomhet. Normalt gjøres målutvikling basert på historiske data så snart en eller annen form for inngangsparameter foreligger. Et inngangsparameter kan være et telefonnummer til en nylig avslørt terrorist. E- tjenesten har eksempelvis fått telefonnummeret av en samarbeidende tjeneste. E-tjenesten vil da umiddelbart prøve å finne ut:

- Har aktøren være i kontakt med andre terrorister vi ikke kjenner til?
- Har aktøren andre identifikatorer (e-postadresser osv.)?

For å kunne gjøre disse analysene, er historiske data helt avgjørende, også fordi telefonnummeret trolig ikke lenger er i bruk. Ved å nøste i den historiske aktiviteten kan andre ledetråder komme frem, som er avgjørende for å gi etterretningsinformasjon som kan bidra til at ansvarlige myndigheter kan rette inn sine virkemidler, rulle opp nettverket og forhindre terror. Mange målutviklingsprosesser er mer avanserte enn eksemplet ovenfor, da både teknologi og trusselaktørene blir mer avanserte, men det gir likevel et bilde av de viktigste momentene innen målutvikling.

Av forannevnte grunner har det alltid vært en lav terskel for etterretningstjenester i forhold til å behandle usikker informasjon. Det er en grunnleggende feilslutning at innhenting må være basert på *mistanke* eller lignende individualbaserte terskler for innhenting og behandling av informasjon, etter ana-

enkelt tilfelle. Et annet eksempel er at det er etablert et eget element i tjenesten som utelukkende har til oppgave å sørge for intern legalitetskontroll i forhold til tjenestens tekniske innhentingsvirksomhet.

[27] Det er ikke avdekket regelverksbrudd de senere år som tjenesten ikke selv har oppdaget og rapportert til EOS-utvalget. For øvrig nevnes at tjenesten har implementert en varslingsmekanisme (varslingskanal) som tjenestens ansatte blant annet kan benytte til å innrapportere brudd på regelverk eller tjenestens etiske regler. Rapporteringen kan skje anonymt.

logi fra justissektoren og straffeprosessen. Her skiller utenlandsetterretningstjenester seg grunnleggende fra politiorganers formål og virksomhet. Mens tradisjonelle politiorganer (*law enforcement*) fokuserer på å bygge opp en juridisk sak relatert til en kriminell handling som er begått eller forberedes begått (historisk perspektiv med stor vekt på beviskjede), er etterretningstjenesters fokus å redusere usikkerhet hos viktige beslutningstakere, med et særlig fokus på å predikere fremtiden – å vurdere fremmede trender og handlinger hos stater, organisasjoner og personer, uavhengig av om disse har gjort eller vil gjøre noe straffbart, og uten å være styrt av å måtte beskytte informasjonens integritet på en slik måte at den kan benyttes i en rettslig prosess.

For E-tjenesten kan dette skjematisk uttrykkes slik, se fig. 1: For å finne den ukjente informasjonen som er av interesse (målutvikling), er eneste terskel for å behandle opplysninger at letingen må basere seg på legitime formål; letingen må knyttes til et legitimt etterretningsbehov slik dette er fastsatt at overordnede myndigheter. Etter at et antatt mål av interesse er identifisert, vil terskelen for å innhente informasjon om vedkommende være noe høyere (rimelig grunn til å undersøke om innhentingen vil frembringe utenlandsetterretningsrelevant informasjon), men fremdeles lavere enn at det må godtgjøres sannsynlighetsovervekt for at innhenting av informasjon rettet mot vedkommende vil frembringe slik informasjon. Utenlandsetterretningstjenester forholder seg ikke til høyere «beviskrav», som f.eks. skjellig grunn til mistanke, rett og slett fordi slike krav i praksis vil gjøre det umulig å frembringe etterretninger. De to øverste radene i fig. 1 er derfor de eneste terskelvilkårene for innsamling som er relevante for E-tjenesten. Dette er naturligvis ikke til hinder for at informasjon så langt mulig må kvalitetssikres, for å øke verdien av etterretningsanalysen og vurderingene. Men til syvende og sist er det et faktum at stater ofte må basere seg og handle på basis av usikker informasjon.

Vilkår for innsamling	Sammenlignbare vilkår på engelsk	Utfyllende forklaring
Målutviklingsformål (legitimt formål)	Target discovery purpose (legitimate purpose)	Eneste terskel er at virksomheten må være formålsstyrt iht oppdrag og e-behov. Kan baseres på rene antagelser/gjetninger eller å se etter ukjente mønstre.
Rimelig grunn til å undersøke (RGU)	Reasonable articulable suspicion (RAS)	Må foreligge fornuftige, objektive og etterprøvbare holdepunkter ut over ren vilkårlighet eller rene antagelser/gjetninger. Trenger ikke godtgjøre sannsynlighetsovervekt.
Skjellig grunn til mistanke	Probable cause	Sannsynlighetsovervekt (51% sannsynlighet eller høyere).
Bevist utover enhver rimelig tvil	Proven beyond a reasonable doubt	Høy grad av sannsynlighet

Fig. 1. Vilkår for innsamling.

3.5.2. Informasjonstilgang

3.5.2.1. E-tjenestens egne kilder og metoder

E-tjenestens egne kilder er de kilder som tjenesten selv kan skaffe seg tilgang til og benytte. Kildene er de stedene hvor man finner informasjon og data. Disipliner og metoder er utviklet og innrettet for å kunne tappe disse kildene for informasjon slik at E-tjenesten kan løse gitte konkrete oppdrag.

I etterretningsterminologien benytter man begrepene «etterretningsdisiplin» og «innhentingsmetode». Uansett hvilken disiplin eller metode som benyttes, vil alltid informasjonen ha sin opprinnelse i en kilde. Et hovedskille for tjenestens innhentingsmetoder går mellom menneskebasert innhenting (HUMINT) og teknisk innhenting. Begrepet «kilde» benyttes både for menneskebasert og tekniske innhentingsdisipliner. Ved menneskebasert innhenting er det en person som gir tilgang til informasjon, og ved teknisk innhenting er det f.eks. signaler gjennom luften eller i fysiske ledere som samles inn. Det er innsamlingen av informasjon og data, analysen, bearbeidingen og viderefordelingen av resultatet

som til sammen kalles for «etterretning», se også definisjonen av etterretning i kap. 3.2.

Teknisk etterretning er en samlebetegnelse for etterretninger utledet av informasjon og data fra tekniske objekter; det være seg radar, kommunikasjonsbærere i det elektromagnetiske spektrum, akustikk eller andre former for signaler og utstråling. Teknisk innhenting inkluderer etterretningsdisipliner som signaletterretning (SIGINT, som igjen deles inn i kommunikasjonsetterretning - COMINT - og elektronisk etterretning - ELINT), bildeetterretning (IMINT), akustisk etterretning (ACINT), radaretterretning (RADINT), etterretning ved bruk av åpne kilder (OSINT) og geografisk etterretning (GEOINT).

Etterretningsbehovet vil ofte være styrende for valg av innhentingsmetode. HUMINT vil gjennom et godt etablert kildenettverk eller en godt plassert enkeltkilde f.eks. kunne skaffe verdifull informasjon om aktørers tankesett, verdensbilde og intensjoner. Ved behov for en detaljert oversikt over fysiske installasjoner og deres geografiske plassering, er IMINT en bedre egnet metode. Ved disiplinen SIGINT avsøkes gjerne et meget bredt datatilfang, for deretter gjennom analyse å kunne trekke ut det som er viktig for etterretningsformål.

Anvendbarheten av den ene fremfor den annen metode vil ofte være kontekstavhengig i forhold til etterretningsbehovet som foreligger og hvilket miljø en opererer i. Informasjon som kommer fra én kilde vil i en del tilfeller kunne besvare et konkret etterretningsbehov, mens innhenting fra flere uavhengige kilder og ved bruk av ulike disipliner og metoder vil kunne ha en gjensidig forsterkende effekt i besvarelsen av et annet etterretningsbehov. Som regel gir kombinasjonen av flere innhentingsmetoder bedre forutsetninger for å besvare et etterretningsbehov. En forutsetning for det hele er at det er der kommunikasjon og informasjon finnes, at E-tjenesten må lete.

Det er den løpende trussel- og risikovurdering, og bestillingen fra oppdragsgiver (f.eks. FD og UD), som ligger til grunn for hvordan og hvor mye tjenesten utnytter sine kilder. I utgangspunktet bør E-tjenesten ved den informasjon tjenesten får fra sine egne kilder, langt på vei kunne løse sitt oppdrag. Tilgang fra egne kilder er imidlertid ikke tilstrekkelig for å dekke etterretningsbehovet. E-tjenesten er derfor avhengig av samarbeid med og informasjon fra andre nasjonale og utenlandske tjenester. Det alt vesentlige av kommunikasjon går nå også over fiberoptiske kabler. Det betyr at E-tjenesten i økende grad ikke har tilgang til en kilde der det er viktig informasjon av etterretningsverdi.

3.5.2.2. Informasjon fra andre nasjonale myndigheter

Samarbeidet med PST og NSM har blitt stadig bedre og tettere. Godt partnerskap med nasjonale partnere er og vil fortsatt være helt nødvendig for at E-tjenesten skal kunne løse sitt oppdrag. For E-tjenesten er det viktig å opprettholde og videreutvikle evne til å levere etterretningsstøtte på svært spesialiserte, komplekse og ressurskrevende fagområder, utvikle velfungerende mekanismer for informasjonsutveksling, samt gode prosesser for samarbeid innen taktisk og strategisk analyse.

Intensivert samarbeid med nasjonale partnere skyldes bl.a. et endret og mer komplekst trusselbilde. Oppfølgingen av hovedkonklusjonene og anbefalingene fra 22. juli-kommisjonens rapport knyttet til sikkerhets- og etterretningstjenestene bidro til et ytterligere styrket samarbeid.

I dag er det et avklart og godt grensesnitt mellom disse tre tjenester. En videre styrking av samarbeidet med PST og NSM kan forventes. Det er særlig forholdet til NSMs og PSTs informasjonsinnhenting som har berøringspunkter til E-tjenesten. De har enkelte oppgaver som tenderer mot E-tjenestens ansvarsområder. Særlig gjelder det PST, ved at både PST og E-tjenesten har et ansvar for å innhente informasjon om enkelte kategorier trusselaktører. NSM innhenter også informasjon, men ikke om trusselaktører og kun for forebyggende sikkerhetsformål.

Mens PST har ansvar for rikets indre sikkerhet, skal E-tjenesten kartlegge og motvirke ytre trusler mot Norge. Samarbeidet er tett og nært på alle nivåer, særlig innenfor områdene kontraterror, kontraetterretning og kontraproliferasjon (arbeidet mot spredning av masseødeleggelsesvåpen).[28] Det utveksles informasjon begge veier.

[28] Samarbeidet er nærmere regulert i kgl res 13. oktober 2006 nr. 1151 om instruks for samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste.

Det er imidlertid også betydelige forskjeller mellom de to tjenestenes rolle og oppgaver, jf. kap. 3.2. Kriminalitetsbekjempelse er i seg selv ikke et lovlig formål for E-tjenestens innsamling av informasjon, mens dette utelukkende er styrende for PSTs innhentingsformål. E-tjenesten er ikke et politiorgan, og skal heller ikke innrette sin virksomhet som et bistandsorgan for politiet.

Formålet med E-tjenestens innhenting er ikke å avdekke lovbrudd eller bruke informasjon som bevis i straffesaker. Politiets virksomhet retter seg mot enkeltpersoner som det er rimelig grunn til å undersøke/skjellig grunn til å mistenke om har begått visse straffbare handlinger eller forbereder slike. E-tjenesten har et annet formål med sin informasjonsinnhenting, og må gå bredt ut og innhente en rekke informasjoner om fremmede stater, organisasjoner og individer for å løse sitt oppdrag. Det er som nevnt tidligere grunnleggende rettslige og prinsipielle forskjeller mellom polisiære og straffeprosessuelle tvangsmidler på den ene siden, som blant annet bygger på strafferammekrav som grunnvilkår for å ta i bruk de ulike tvangsmidlene, og E-tjenestens metodebruk for å innhente informasjon på den andre siden.
Ulike oppgaver og roller tilsier at det også er enkelte begrensninger for samarbeidet. Hver av tjenestene kan kun samarbeide så langt dette ligger innenfor den enkelte tjenestes eget rettsgrunnlag.[29] Dette er sentralt for å unngå at en av tjenestene ber den andre om å gjøre noe som anmodende tjeneste ikke selv kan gjøre innenfor egne rettslige rammer. Dersom E-tjenesten som ledd i løsningen av sine oppgaver mottar overskuddsinformasjon av interesse for PST, kan imidlertid slik informasjon deles med PST (og slettes i E-tjenesten), se E-instruksen § 5 første ledd. Med overskuddsinformasjon menes informasjon som ligger utenfor tjenestens ansvarsområde, men som tjenesten likevel kommer i besittelse av som følge av dens virksomhet rettet mot forhold innenfor ansvarsområdet.[30] Etableringen av Felles Kontraterrorsenter (FKTS) mellom PST og E-tjenesten endrer ikke på ovennevnte prinsipper.[31]

De ulike rettsgrunnlagene er i hovedsak ikke til hinder for at de to tjenestene deler informasjon med hverandre og oppbevarer slik informasjon. De utfordringene som har oppstått, har i det vesentlige blitt løst gjennom konstruktivt samarbeid, men enkelte skranker for nødvendig informasjonsdeling er likevel blitt identifisert.[32]

En DGF-kapasitet kan medføre gravitasjon mot å bruke kapasiteten til andre formål enn opprinnelig bestemt (formålsglidning). Fra PSTs side mener man at dette motvirkes gjennom strenge regler for deling av DGF-generert informasjon mellom tjenestene, samt et effektivt kontrollregime.

I kapittel 9 redegjøres det for hvordan utvalget mener at faren for en eventuell formålsglidning skal motvirkes.

[29] Med mindre man er utenfor utenlandsetterretningsdomenet og E-tjenesten bistår PST etter kriteriene og vilkårene som fremgår av politiloven § 27a, innenfor PSTs rettsgrunnlag og etter styring og instruks fra PST.

[30] Se instruksen om samarbeidet mellom E-tjenesten og PST § 9 første ledd annet punktum.

[31] På kontraterrorområdet samarbeider PST og E-tjenesten nært, blant annet gjennom Felles kontraterrorsenter (FKTS). Hensikten med FKTS er primært knyttet til tidsriktig/rask informasjonsdeling mellom tjenestene. Senteret sammenstiller også analyser og trusselvurderinger fra tjenestene. Senteret driver ikke egeninnhenting, men følger saker og sakskomplekser og koordinerer mellom tjenestene ved behov. Utveksling av informasjon om hverandres prioriteringer og fokus bidrar til effektivt samspill og oversikt hos tjenestene. Det bidrar også til en mer hensiktsmessig fokusering av innhentingskapasitetene i de respektive tjenester.

[32] I 2011 tok PST opp med Justis- og beredskapsdepartementet enkelte lovmessige begrensninger i adgangen til å dele informasjon med E-tjenesten, med sikte på en avklaring og om nødvendig en endring av lov eller instruks. Terrorangrepet i Norge den 22. juli 2011 bidro til å aksentuere denne problemstillingen. Initiativet munnet ut i forslag fra regjeringen om endringer i straffeprosessloven og politiloven, som ble sendt på offentlig høring 1. februar 2016 med høringsfrist 1. mai 2016. Uavhengig av dette lovendringsforslaget vil det fortsatt være enkelte rettslige skranker for informasjonsdeling mellom tjenestene. For E-tjenestens deling med PST kan sikkerhetsloven, kildevern og prinsippet om utstederkontroll (tredjepartsregelen) i et konkret tilfelle hindre deling. For PSTs deling med E-tjenesten kan også politiregisterloven hindre deling i det enkelte tilfelle. All informasjonsdeling er videre underlagt en risiko- og forholdsmessighetsvurdering for å sikre kvalitet og notoritet. Det kan stilles vilkår knyttet til mottakers bruk av informasjonen. Mottaker plikter også i alle tilfeller av eget tiltak å vurdere om informasjonen kan behandles som nødvendig og relevant (formålsbestemthet) opp mot vilkårene for behandling etter eget rettsgrunnlag og lovpålagte oppgavesett. Politiregisterloven kapittel 5 har generelle regler om utlevering av opplysninger som gjelder for PST. De nærmere vilkårene følger av kapittel 6 og bestemmelsene om taushetsplikt. I politiregisterforskriften del 3 kapittel 9-11 spisses vilkårene ytterligere, herunder stilles krav til saksbehandlingen. Politiregisterloven § 8 annet ledd i.f. har en særregel for utlevering av opplysninger som behandles innenfor firemånedersregelen. Politiregisterloven § 20 har særlige regler om utlevering av ikke-verifiserte opplysninger. Jf også politiregisterforskriften § 21-7, som gjelder særskilt for PST.

NSM er Norges nasjonale forebyggende sikkerhetstjeneste, hvis hovedoppgaver er regulert i sikkerhetsloven. NSM er et direktorat direkte underlagt Forsvarsdepartementet (FD), med instruks- og rapporteringsplikt til både FD og Justis- og beredskapsdepartementet (JD). NSM skal koordinere forebyggende sikkerhetstiltak og føre tilsyn med sikkerhetstilstanden i de virksomheter som omfattes av sikkerhetsloven, samt forestå enkelte andre oppgaver, blant annet kontroll med luftfotografering og drift av *Norwegian Computer Emergency Response Team (NorCERT*) som nasjonal nettverksovervåkingsenhet. Forebyggende sikkerhetstjeneste omfatter tiltak for å sikre skjermingsverdig informasjon og skjermingsverdige objekter mot sikkerhetstruende hendelser. E-tjenesten samarbeider med NSM – og omvendt – blant annet gjennom Cyberkoordineringsgruppen (CKG).

NSMs viktigste element når det gjelder deteksjon av alvorlige trusler, er Varslingssystem for Digital Infrastruktur (VDI). VDI er et sensornettverk for å avdekke forsøk på datainnbrudd mot kritisk infrastruktur på tvers av sektorer, hittil basert på samtykke fra de virksomheter sensorene er utplassert i. Systemet er basert på deteksjon ved hjelp av signaturer, men dette kan endre seg i fremtiden. NSM lagrer VDI-metadata. Ved alarm skjer utvidet lagring. Ifølge NSM er det stadig mer utfordrende å detektere de mest alvorlige truslene. IP-adresser får mindre betydning for å identifisere trusler. NSM evne til deteksjon utfordres i økende grad av kryptering. NSM har derfor tatt et strategisk valg om å flytte sensorene nærmere endepunktene. For øvrig vises til vedlegg 1 om forholdet mellom DGF og lokale sensorer.

Det er E-tjenestens internasjonale etterretningssamarbeid som i dag skaper den største merverdi for NSM i forhold til avanserte trusler. Det meste av det NSM detekterer av alvorlige cyberhendelser er i dag basert på slike tips via E-tjenesten. Informasjon fra E-tjenesten kan peke NSM i riktig retning. NSM kan deretter i enkelte tilfeller bruke informasjonen til å lage egne vurderinger, som forenkler delingen nasjonalt.
E-tjenesten vil ha flere formål med DGF. Kun ett av disse, støtte til *Cyber Defence*, er viktig også for NSM. Merverdien for NSM er ikke avhengig av at E-tjenesten får full dekning av all trafikk inn og ut av Norge. Metadataanalyser/trafikkanalyser, og samarbeid med tjenestetilbyderne, vil kunne gi gevinster.

3.5.2.3. Informasjon fra samarbeidende tjenester i andre land

E-tjenesten har et omfattende internasjonalt partnernettverk. Internasjonalt samarbeid er avgjørende for å løse tjenestens informasjonsbehov. Som en relativt sett liten tjeneste er norsk etterretningstjeneste avhengig av større partnere med andre aksesser til informasjon enn man selv har. E-loven fremhever at E-tjenesten kan etablere og opprettholde etterretningssamarbeid med andre land. E-tjenesten vektlegger slikt samarbeid både i den operative virksomheten og i forhold til utveksling av produkter. Det bi- og multilaterale samarbeidet Norge har med relevante land, er avgjørende for at norsk etterretning skal kunne løse sitt oppdrag. Den teknologiske og konseptuelle utviklingen må holdes synkronisert og avstemt med de viktigste partnere for å sikre relevans og kvalitet i samarbeidet i dag, og inn i fremtiden. Se også kap. 5.4 om dette.

Norges geopolitiske posisjon og endringene i trusselbildet understreker viktigheten av tett internasjonalt etterretningssamarbeid med allierte i NATO. NATO er bærebjelken i norsk utenriks- og sikkerhetspolitikk. Norge er derfor tett integrert i NATOs militære struktur og har et omfattende samarbeid med en rekke medlemsland, også innen etterretning. De fleste NATO-land betrakter imidlertid etterretning som et nasjonalt anliggende, og etterretningssamarbeidet er helt avhengig av landenes bidrag. Alliansen har felles etterretningselementer som bearbeider og distribuerer etterretninger, men har få egne innhentingskapasiteter. Medlemslandenes evne og vilje til å dele etterretninger er derfor kritisk viktig for alliansens funksjon både under rutinemessige operasjoner og i krise. For å sikre kvalitet i samarbeidet og dermed bedre forutsetninger for å møte de felles utfordringene medlemslandene står overfor, vektlegges utvikling av felles doktrine, taktikk og prosedyrer.

4. DEN TEKNOLOGISKE OG SAMFUNNSMESSIGE UTVIKLING

4.1. Digitalisering og avhengighet

Norge har i global sammenheng en høy grad av digitalisering både i privat og offentlig sektor. Regjeringens digitale agenda[33] er tydelig på ytterligere høye ambisjoner for digitalisering av offentlig sektor, og offentlig sektors kommunikasjon til befolkningen ønskes i størst mulig grad gjennomført via elektroniske informasjonssystemer som bl.a. sikker digital postkasse.

Statistisk sentralbyrås måling av hvor stor andel av befolkningen som har brukt Internett siste tre måneder er 96 % for 2015.[34] Dette tallet har økt med ca. ett prosentpoeng hvert år de siste fem år, og forteller oss at så godt som alle husstander er tilknyttet Internett, og bruker det. Samme kilde viser til at Internettilknytningen brukes til formål som e-post, elektronisk handel, lesing av aviser/surfing/strømming, banktjenester, sosiale media m.m. I den yngre del av befolkningen er det en klar trend at bruk av PC for Internettilgang går ned til fordel for en vekst i bruk av mobile enheter. Graden av deling av egenprodusert informasjon øker.

I takt med en økende grad av digitalisering av både offentlig og privat sektor, blir det vanskeligere og vanskeligere å stå utenfor. Man kan fremdeles velge digitalt utenforskap i for eksempel sin relasjon til staten, mens mange nye tjenester i det private markedet er forbeholdt digital tilgang. Den reelle muligheten til å velge *ikke* å være en del av det digitale samfunnet blir ventelig mindre og mindre.

4.2. Internett som felles plattform[35]

Nasjonal kommunikasjonsmyndighet (Nkom) viser i en rapport[36] til at global Internettrafikk vokser eksponentielt. Medio 2016 var det ca. 3,4 milliarder internettbrukere[37], og den globale IP-trafikken er mer enn femdoblet sammenlignet med 2010. Årsakene til trafikkveksten er blant annet et stadig økende antall tilkoblede individer og enheter på Internett, mer video på Internett og raskere Internettlinjer. Det er verdt å legge merke til at svært mange av tjenestene som vokser mest fra et sluttbrukerperspektiv, er mobile.

Rapporten fra Nkom peker videre på at både nasjonalt og globalt utgjør Internett, inkludert applikasjoner og data som er tilgjengelig på Internett, en grunnleggende *samfunnsressurs* med meget stort potensial for innovasjon og vekst på nær sagt alle samfunnsområder. Internett er blitt avgjørende for sosial og kulturell kommunikasjon, og for utvikling av fremtidsrettede private og offentlige tjenester. Tillit til at Internett og tjenestene som leveres over Internett er stabile og sikre, er grunnleggende for fortsatt utvikling av nett og tjenester både nasjonalt og globalt. Samfunnets sårbarhet både når det gjelder villede hendelser som sabotasje og bevisste angrep, og ikke-villede hendelser som naturkatastrofer og sårbarheter i maskinvare og programvare, er stor.

IP-protokollen[38] fungerer som en felles plattform for produksjon av ulike applikasjoner, som e-post, webtilgang og liknende. Det er relativt sett enkelt, både teknisk, merkantilt og formelt, å forholde seg til et åpent IP-basert nett som Internett fra en tjenesteprodusents ståsted. Etter hvert som Internettet har tatt rollen som felles global kommunikasjonsløsning, har dette ført til fremveksten av dedikerte tjenesteleverandører som i større grad enn før er løsrevet fra den markedsaktøren som gir tilgang til selve Internettet. Aktørene refereres ofte til som *Over The Top (OTT)*-aktører eller *Content and Application Providers (CAP)*-aktører. Disse aktørene leverer ofte tjenester på tvers av landegrenser, og er i varierende grad omfattet av den samme nasjonale regulering som de tradisjonelle leverandørene av ekomtjenester.

[33] Meld. St. 27 (2015-2016) Digital agenda for Norge.

[34] Statistikken er en enkel måling av hvor mange i aldersgruppen 16-79 år som har vært tilkoblet Internett i løpet av en tremånedersperiode. Se for øvrig kap. 6.1 om vårt digitale liv.

[35] Store deler av den etterfølgende teksten bygger på «Dokument 16 (2015-2016), vedlegg 3; Innspill til evaluering av EOS-utvalget. Teknologiske aspekter».

[36] Ekomplan - Innspill til Samferdselsdepartementet fra Nasjonal kommunikasjonsmyndighet 14. august 2015

[37] Antall individer med tilgang til Internett hjemme iht www.internetlivestats.com som bygger på tall fra den internasjonale teleunion (ITU), Verdensbanken og befolkningsstatistikk fra FN.

[38] Avsnittet bygger på beskrivelse av OTT-tjenester i rapporten «Ekomtjenester, -nett og –utstyr - utvikling og betydning for PT» utgitt av Post- og teletilsynet juni 2014.

Utviklingen har ført til at stadig nye applikasjoner tilbys over Internett, og noen av disse er svært vellykkede, også som erstatninger til tradisjonelle telefoni- og kringkastingstjenester. Velkjente eksempler på generelle anvendelser er Facebook og Twitter, eksempler på erstatningstjenester for tradisjonell telefoni er Skype, Viber og Google Voice, og eksempler på erstatningstjenester for tradisjonell kringkasting og fjernsyn er YouTube, iTunes og Netflix. Felles for OTT-tilbyderne er at de ofte opererer og utfordrer på tvers av landegrenser og jurisdiksjon. Dette har skapt gråsoner hva angår private aktørers behandling av personopplysninger. Innsamlet informasjon hos private aktører kan i prinsippet tilgjengeliggjøres også for myndighetsorganer for deres behandling, avhengig av gjeldende jurisdiksjon. Enkeltindividets evne til både å kunne vite om, og i neste instans påvirke hvorvidt egne data eller informasjon om egen tjenestebruk krysser landets grenser, er mindre enn tidligere.

Det er videre en sterk trend at man i økende grad ser at objekter (ting) er koblet til Internett og kommuniserer med hverandre både med og uten individer involvert. Trenden refereres ofte til som «Tingenes Internett» eller «Internet of Things (IoT)». Anvendelsesområdene er mange. Begrep som kroppsnære sensorer, e-helse, intelligent trafikkstyring, smarte hjem, bedrifter og byer er eksempler. IoT er et viktig element knyttet til stordatatrenden – primært hva angår tilhørende mulighet for utnyttelse av informasjon til andre formål enn opprinnelig tiltenkt, sammenstilte analyser mv.

Bruken av mobile tjenester har det ved seg at man legger igjen geografiske spor, i tillegg til informasjon om den tjenesten som er brukt eller den type innhold som er konsumert eller lagret. Dette skjer ofte uten at brukeren er bevisst problemstillingen. Den omtalte IoT-utviklingen, med mange kroppsnære ting koblet til Internett, forsterker dette bildet.

Videre er det naturlig å peke på betydningen av moderne skytjenester. Skytjenester er langt fra noe nytt, men det har nå fått en slik utbredelse, pris, skalerbarhet og fleksibilitet at svært mange sektorer, infrastruktureiere mv. for alvor tar dette i bruk nå. Det samme gjelder individer. Skytjenester kan i mange tilfeller representere sikre og gode alternativer til andre former for tjenesteleveranser. Men grunnleggende er det også slik at mange skytjenester representerer en utfordring på tvers av sektorgrenser, landegrenser og jurisdiksjoner.

4.3. Spesielt om metadata

Metadata (fra gresk meta «om» og latin data «opplysninger») er data som beskriver andre data. I etterretnings- og overvåkningssammenheng skiller man ofte mellom metadata og innholdsdata. F.eks. vil metadata om en telefonsamtale typisk være hvilken abonnent (nummer) som ringer til hvem (nummer) og hvor lenge varer samtalen varer. Dersom mobiltelefoner er involvert i samtalen, vil også informasjon om hvilken basestasjon som telefonen er koblet til være å regne som metadata. Dette vil da si noe om lokasjonen til den som ringer[39] når det ringes. Selve *innholdet* i samtalen vil derimot karakteriseres som innholdsdata. Metadata knyttet til Internettbruk vil typisk – hvis samlet inn og analysert – bl.a. inneholde en oversikt over hvilke internettdomener en bruker har besøkt.

Et eksempel på metadata fra den fysiske verden er informasjonen som påføres på utsiden av en konvolutt for å sende brev. Her vil mottaker stå på forsiden av brevet og avsender på baksiden. I tillegg vil konvolutten stemples med dato. Dette er sammenlignbart for en epost i den digitale verden. En epost vil inneholde metadata i form av en avsender epostadresse, mottaker epost-adresse og tidspunkt for når eposten ble sendt. Dette kan anses som mindre sensitive data i forholdet til selve innholdet i brevet eller eposten, selv om også slike data er å anse som personopplysninger. Lagring og sammenstilling av denne type metadata er av avgjørende betydning når en ny trussel blir avdekket. Ved å gjøre tilbakeskuende (retrospektive) søk i metadata i form av f.eks. et telefonnummer eller epostadresse knyttet til en ny trussel, vil det være mulig å danne seg et bilde av for eksempel størrelsen av et terrornettverk basert på analyse av kommunikasjonsmønster, eller omfanget til et cyberangrep basert på analyse av IP-adresser og tilhørende trafikkdata.

På globalt plan er det mye som tyder på at bulkinnsamling av metadata i statlig regi de senere år har

[39] I tillegg til «ordinære» metadata genereres også *signaleringsdata* definert i ekomforskriften § 7-2 som «data som genereres mellom terminalen og tilgjengelig basestasjon og angir terminalens geografiske plassering når den er slått på, uten at trafikkdata formidles». Dette er informasjon som mobilnettet genererer og lagrer for rent tekniske formål, men som inneholder betydelig informasjon om en brukers posisjon og bevegelser uten at telefonen trenger å være i bruk.

vært omfattende.[40] Flere stater skiller lovmessig mellom etterretnings- og overvåkningstjenestenes adgang til å samle inn og analysere metadata på den ene siden, og innholdsdata på den andre siden. Bulkinnsamlet metadata har et betydelig iboende skadepotensial, blant annet avhengig av adgangen til sammenstilt analyse og lagringstid. Eksempelvis vil en sammenstilling av opplysninger om at en person har ringt Kirkens SOS, fastlegen og forsikringsselskapet samme formiddag bety noe mer enn det hver enkelt hendelse forteller. Dette selv om man ikke skulle ha adgang til å innhente innholdsdata fra disse samtalene.

4.4. Spesielt om stordata

Stordata er en betegnelse på store mengder av potensielt både strukturert, ustrukturert og delvis strukturert informasjon. Bearbeiding og analyse av stordata kjennetegnes gjerne av kravene til å kunne håndtere store datavolum med forskjelligartet struktur og med økende grad av hastighet. De store datavolumene og tilvekstraten for ny, relevant informasjon, er til hinder for «ordinær» behandling av datamengdene ved eksempelvis sortering, strukturering og lagring i en relasjonsdatabase for påfølgende analyse. For å kunne trekke meningsfull informasjon ut av den type data og datavolum som kvalifiserer til å bli kalt stordata, er man helt avhengig av maskinelt basert analyse hvor lærende programvare benytter komplekse algoritmer for å gjenkjenne mønstre og deretter legge til rette for sammenstilling og analyse.

For å anskueliggjøre hvilke datamengder det er snakk om, er det relevant å vurdere både datavolum og dataenheter som deles. Tall fra IBM om volum sier at det *hver dag* produseres og lagres 2,5 trillioner byte, eller sagt på en annen måte 2,5 billioner megabyte (MB) som er en vanligere forkortelse. Til sammenligning er det samlede innhold av skrevet materiale *i historisk tid* (tilgjengelig i analog form som bøker, aviser o.l.) estimert til 5 billioner MB. Sagt med andre ord produseres det altså digital informasjon tilsvarende all historisk tilgjengelig analog informasjon i løpet av kun to dager. Vekstraten er i tillegg både høy og økende; ca. 90 % av verdens samlede datamengde er produsert kun i løpet av de siste to år. Det er også et poeng at idéen om at informasjon slettes, veldig ofte er en illusjon: Teknisk sett innebærer sletting ofte bare at det er opplysningene om hvor informasjonen lagres som slettes.

I tillegg til volum er det viktig å forstå omfanget av informasjonsenheter som skapes, utveksles og lagres. Informasjonsenheter kan være alt ifra en Facebook-oppdatering til et digitalt bilde eller et spor lagt igjen i en mobiloperatørs nettverk som forteller om brukerens lokasjon og aktivitet uten at bruker selv er klar over det. Noen eksempler på hva som skjer på globalt nivå *hvert minutt*[41] av handlinger som er styrt og antatt bevisste:

- Facebook-brukere deler 2,5 million informasjonsenheter
- Det twitres nær 300.000 ganger
- Det lastes opp ca. 220.000 nye bilder på Instagram
- Det lastes opp 72 timer med video på YouTube
- Det sendes over 200 millioner e-poster

Dette er eksempler på informasjon som, i hvert fall i første instans, har en klar avsender og ansvarlig for produksjon, lagring og distribusjon. I tillegg til denne type informasjonsenheter blir det skapt mange andre datatyper som har en individdimensjon i seg, direkte eller indirekte.

Datatilsynet viser i en rapport[42] hvordan man som individ kan spores gjennom forskjellige teknikker – bruk av informasjonskapsler (cookies), kjennskap til IP-adresse eller et mer direkte digitalt fingeravtrykk. Et digitalt fingeravtrykk kan gi identifikasjon av en enhet basert på kombinasjon av kunnskap om IP-adresse, hvilken nettleser som brukes og andre tekniske forhold som brukerutstyret gir fra seg uten at det gis eller trengs tillatelse til dette fra bruker. Informasjon om interesser, bruk av tjenester, livssituasjon mv. kan og blir avledet av å følge en identifisert enhet over tid, og det er velfungerende auksjonslignende markeder for omsetning av denne type informasjon, jf. nevnte rapport.

4.5. Spesielt om kryptering

Kryptering er en fundamental sikkerhetsmekanisme for bl.a. å sikre informasjonens konfidensialitet. Fra å være en strengt kontrollert og regulert virksomhet og teknologi under den kalde krigen, har sterk kryptering etter hvert blitt tilgjengelig for store grupper som kan implementere løsninger på egenhånd.

[40] Fremkommer i flere kilder; rettsdokumenter, politiske prosesser, høringer, medialekkasjer mv.

[41] The Data Explosion in 2014 Minute by Minute, Susan Gunelius ACI blog juli 2014

[42] Det store datakappløpet, Rapport om hvordan kommersiell bruk av personopplysninger utfordrer personvernet - Datatilsynet, november 2015

Mange lands etterretnings- og overvåkningstjenester rapporterer at et av de tydeligste spor etter Snowden er at flere som har ønske om å skjule sin informasjon gjør det, fordi de nå i langt større grad er klar over at de kan bli sett når de bruker informasjons- og kommunikasjonssystemer.

Flere har tatt til orde for strengere kontroll med distribusjon og tilgang til sterke kryptografiske metoder, eventuelt å ivareta statens behov for innsyn gjennom etablering av bakdører eller samarbeidsfunderte løsninger for å kunne lese kryptert innhold. Med den allerede betydelige utbredelsen av kryptografiske metoder, vurderes et forbud eller streng regulering av kryptografi først og fremst å ramme individer og virksomheter med legitime beskyttelsesbehov, snarere enn å lette oppdragsløsningen for etterretnings- og sikkerhetstjenestene. Debatten om tilgang til sterk kryptografi vil fortsette, men mye tyder på at etterretnings- og overvåkningstjenester må belage seg på at de i fremtiden i langt større grad enn før må forholde seg til informasjon hvor de ikke kan lese innhold, i hvert fall ikke i nær sann tid. Det betyr ikke at informasjonen i transportfasen er uten interesse; det vil ofte være deler av informasjonen om trafikken på nettet som kan brukes til å *skape* innhold selv om selve innholdet i kommunikasjonen er beskyttet. En annen effekt er at selv om informasjon i større grad enn før krypteres når den *transporteres*, så er ikke nødvendigvis det samme tilfellet for informasjonen når den *lagres*. Det kan føre til økt grad av interesse for å få tilgang til informasjon på eksempelvis et apparat (mobiltelefon, nettverk, PC), i et internt nettverk eller i en skytjeneste.

Kryptering kan skje på flere nivå, både for hele linjer/linker og på tjenestenivå. De ulike tjenestene som overføres i samme kabel/linje benytter gjerne ulike protokoller og kryptering. I mange tilfeller vil dermed ikke tilrettelegging fra tilbyder av ekomnett være tilstrekkelig for å få tilgang til informasjonen i ikke-kryptert format. I de tilfeller hvor en relevant tjeneste er kryptert eller på annen måte uleselig, vil tilgang til informasjonen i ikke-kryptert format også kunne innebære at tilbyder av ekomtjenesten pålegges å tilrettelegge for tilgang til den elektroniske kommunikasjonen, i den utstrekning tilbyder av ekomtjenesten har teknisk mulighet for dette.

Detaljer rundt hvordan E-tjenesten jobber med kryptert kommunikasjon er svært sensitivt. Økt bruk av kryptering vil trolig representere en betydelig utfordring for etterretningstjenester i tiden fremover. Samtidig vil det fortsatt eksistere muligheter for å avdekke og følge utenlandske trusler mot Norge gjennom et DGF, ikke minst når dette sees i sammenheng med E-tjenestens øvrige kapabiliteter. Flere etterretningsbehov kan dekkes gjennom trafikkanalyse, selv om innholdet i kommunikasjonen er kryptert. Det er under enhver omstendighet klart at uten aksess til relevante informasjonsstrømmer vil det heller ikke være mulig å hente ut relevant informasjon fra datastrømmene. Utvalget viser til nærmere analyse av betydningen av krypteringstrenden i kap. 8.3 nedenfor.

4.6. DGF-lignende ordninger i andre land

I dag har de fleste land i verden, deriblant mange sammenlignbare stater som Sverige, Tyskland, Frankrike, Storbritannia, USA og Canada, i større eller mindre grad aksess for etterretningsformål til grenseoverskridende kommunikasjon som går i fiberoptiske kabler. Andre sammenlignbare stater er i ferd med etablere slik aksess. Tilgang til utenlandsetterretningsrelevant informasjon som passerer eget lands grense kan karakteriseres som en «hjemmebanefordel»; en etterretningsfordel sett i forhold til trusler mot eget land som genereres i utlandet men som på en eller annen måte materialiserer seg ved kommunikasjon over landegrensen.

Forholdene i andre land har direkte betydning for norsk etterretning og hensynet til nasjonal kontroll. E-tjenesten får i dag varsler og informasjon som er basert på slik aksess hos samarbeidende tjenester. Samtidig kommer disse varslene ofte for sent, og ofte som et biprodukt i forhold til landenes egne nasjonale prioriteter. Norge kan ikke forvente at andre lands etterretningstjenester skal ha et primærfokus på å beskytte norske interesser. Dette reiser spørsmål om nasjonal evne til å fange opp sikkerhetsmessige utfordringer mot Norge og norske interesser. Det er videre en etisk-moralsk problemstilling, dersom et norsk DGF ikke innføres, at Norge like fullt vil være avhengig av partnerinformasjon som ofte vil være fremskaffet gjennom partners egen aksess til kommunikasjon i fiberoptiske kabler.

I vedlegg 2 til utvalgets rapport gis det en oversikt over noen av landene (Sverige, Frankrike, Storbritannia, Canada, Tyskland, Nederland, Sveits og Finland) som gir eller vurderer å gi deres utenlandsetterretningstjenester tilgang til kommunikasjonsdata som transporteres i fiberoptiske kabler. Utvalget understreker at fremstillingen utelukkende bygger på åpne kilder.

5. FAKTORER SOM TALER FOR DGF

5.1. Generelt om verdien av DGF i lys av sikkerhetsutfordringene

Staten vil til enhver tid gjøre vurderinger av trussel og risiko knyttet til omverdenen og forhold ute som kan påvirke Norge som nasjon og samfunn. Regjeringen har nylig uttalt at terrorisme og voldelig ekstremisme forblir en alvorlig trussel mot nasjonal og internasjonal fred og sikkerhet, og at en rekke terrorangrep og avdekte planer om terror de siste årene viser hvor grenseløs og kompleks trusselen er.[43] Videre hevder E-tjenesten at nettbaserte etterretningsoperasjoner nå er, sammen med terror, den mest alvorlige og akutte trussel mot norske interesser. I et lengre perspektiv sies det at tilbakekomsten av mellomstatlig væpnet konflikt er et viktig utviklingstrekk. Utviklingen i Russland og nordområdene har alltid vært en dimensjonerende oppgave for E-tjenesten, og vil fortsette å være det. Norge befinner seg i et sikkerhetspolitisk landskap der det er av vesentlig betydning å følge utviklingen av den russiske militærmakt i Norges nærområder.

Cybertruslene er i brutal vekst. Digitaliseringen av samfunnet innebærer at lagring og behandling av data blir et stadig mer sentralt element i all menneskelig aktivitet. Dette gjør samtidig samfunnet mer sårbart for trusler. Fremmede staters etterretningsoperasjoner i det digitale rom representerer i dag en alvorlig og økende trussel mot nasjonale myndigheter og virksomheter. Det vises også til beskrivelsen av hybride operasjoner og krigføring i kap. 2.2. Stater, grupper og personer søker kunnskap om forhold i Norge som brukes politisk, økonomisk eller militært. E-tjenesten har åpent uttalt at det er russiske og kinesiske aktører som står bak de mest alvorlige nettverksbaserte etterretningsoperasjonene mot Norge. Begge land har høy kompetanse og viser stor grad av pågåenhet i sin tilnærming mot norske mål.

Terrortrusselen mot vestlige interesser er alvorlig og kompleks. Den er alvorlig og skaper så mye usikkerhet i befolkningene at de fleste vestlige land – Norge inkludert – er villige til å bruke militærmakt og delta i væpnede konflikter for å få bukt med problemet. I all hovedsak er det terrororganisasjonene Den islamske staten i Irak og Levanten (ISIL) og al-Qaida som representerer den største trusselen. Norge er ikke et prioritert mål, men som et vestlig land som deltar i koalisjonen mot ISIL og al-Qaida, er Norge en del av disse organisasjonenes fiendebilde. I mange år fremover er det rimelig å anta at terrorisme som virkemiddel vil fortsette å representere en alvorlig utfordring, både i og utenfor Vesten. Det er antagelig et tidsspørsmål før verden vil erfare nye former for terrorangrep. Terroristers bruk av masseødeleggelsesvåpen understreker ytterligere at internasjonal terrorisme kan true statssikkerheten direkte. Både ISIL og al-Qaida har aktivt forsøkt å tilegne seg slike våpen, og terroristers bruk av kjemiske våpen har man allerede sett eksempler på i Syria.[44] Motivasjonen for å bruke vold som politisk virkemiddel vil være til stede så lenge grunnforutsetningene for slik bruk av vold ikke endres. Fellesnevnere for terrorutsatte land utenom Vesten i dag er interne voldelige konflikter, polariserte religiøse og ideologiske motsetninger, svake statlige styringsstrukturer og høy sosial og økonomisk ulikhet. Selv om antall drepte i vesten pga. terrorisme fremdeles er lavere enn de siste tiår i forrige århundre, og vesentlig lavere enn f.eks. omkomne i trafikkulykker, tilsier de særegne forhold ved terrortrusselen samt utviklingen i hvorledes terrorangrep gjennomføres og hvilke mål som rammes at denne trusselen står i en særstilling som må møtes med robuste virkemidler.

E-tjenesten har i dag kun i meget begrenset grad evne til å kunne fange opp utenlandsk kommunikasjon over landegrensen til Norge som kan utgjøre alvorlige sikkerhetsutfordringer for landet. Eksempelvis har tjenesten i liten grad mulighet til å avdekke at en kjent terrorleder i utlandet kommuniserer med ukjente personer i Norge. Et annet eksempel er at norske myndigheter i dag har minimal mulighet til å avdekke at andre stater driver spionasje mot norske offentlige og private virksomheter i og ved hjelp av det digitale rom. Det medfører at de mest avanserte trusler i det digitale rom relatert til rikets sikkerhet – statlig spionasje og forberedelser til cyberangrep, samt kommunikasjon mellom kjente terrorister i utlandet og ukjente personer i Norge – i de fleste tilfeller ikke kan avdekkes innenfor gjeldende lovverk og kapasiteter. Alternativet for tjenesten er å til enhver tid følge alle potensielle terrortrusler i utlandet. Det vil være en uoverkommelig

[43] Prop. 151 S (2015-2016) Kampkraft og bærekraft – Langtidsplan for forsvarssektoren, s. 34 sp.1.

[44] Enkelte historiske tilfeller foreligger, f.eks. angrepet med sarin rettet mot T-banen i Tokyo 20. mars 1995.

oppgave. Det vil være langt mer hensiktsmessig å kunne fange opp kommunikasjonen når truslene retter sin virksomhet og kommunikasjon mot Norge. En kombinasjon vil være det mest hensiktsmessige.

Dagens mangelfulle aksess har negative konsekvenser for myndighetenes evne til å håndtere digital spionasje og infiltrasjon, digitale anslag mot samfunnskritisk infrastruktur og terrorisme. DGF vil ifølge E-tjenesten være et viktig tiltak for å møte trusselen fra internasjonal terrorisme, og vil være et avgjørende tiltak mot de mest alvorlige truslene i det digitale rom (spionasje og sabotasje) i fred, krise og væpnet konflikt. DGF vil også gi bedre og økt etterretning på andre områder av betydning for viktige norske interesser. PST og NSM støtter begge at E-tjenesten blir gitt aksess til grensekryssende digital kommunikasjon. Etablering av DGF vil imidlertid ikke innebære at PST og NSM får noen ny eller direkte tilgang til E-tjenestens informasjonstilgang. Det lovmessige og prinsipielle forblir enten uforandret, eller kan bli strengere ved f.eks. ytterligere begrensninger på å dele overskuddsinformasjon.

Den altoverveiende delen av kommunikasjon ut av og inn i Norge går i fiberoptiske kabler. Tilleggsinformasjon E-tjenesten kan få ved DGF vil gi E-tjenesten betydelig mer informasjon, og innen enkelte områder avgjørende informasjon, som tjenesten ikke kan skaffe seg i dag. Slik aksess gir følgelig nasjonen en mulighet til å beskytte og forsvare seg. Viktige nasjonale interesser, hensynet til rikets sikkerhet og beredskapshensyn tilsier derfor at E-tjenesten bør gis mulighet til å innhente relevant kommunikasjon fra fremmede aktører når denne krysser grensen til norsk territorium ved tilgang til ekomtjenester og ekomnett underlagt norsk jurisdiksjon og lovgivning, innenfor de begrensninger som allerede gjelder for E-tjenestens informasjonsinnhenting, innenfor de prioriterte informasjonsbehov som overordnede politiske myndigheter fastsetter, og innenfor nye lovfastsatte begrensninger.

I vedlegg 1 til rapporten her fremstilles to scenarioer – ett knyttet til cyberspionasje, og ett knyttet til internasjonal terrorisme – som mer konkret illustrerer hvordan DGF i praksis vil tilføre merverdi i etterretningsarbeidet med å avdekke, forebygge og motvirke alvorlige trusler.

5.2. Prinsipielle argumenter for DGF

Det kan på prinsipielt grunnlag anføres at siden E-tjenesten er avhengig av å basere sine vurderinger på tilgang til unik kommunikasjon og unike data, vil innsamling av informasjon og data for etterretningsproduksjon nødvendigvis skje der relevant kommunikasjon foregår, med teknisk mulighet til faktisk tilgang til denne. Og for å finne den relevante informasjonen, må man nødvendigvis også søke i datamengder hvor det også befinner seg ikke-relevant informasjon.

E-tjenesten innhenter og lagrer i dag store mengder data. DGF vil ikke endre dette prinsipielt. E-tjenesten innhenter i dag internettkommunikasjon som transporteres i luftgrensesnittet (over satellitt) eller som er tilgjengelig gjennom åpne kilder. Kommersielle eller praktiske hensyn, samt automatiserte prosesser, kan avgjøre om trafikk formidles på den ene eller annen måte. I dette perspektiv er det ingen vesentlige forskjeller mellom etterretning i det digitale rom og mer tradisjonelle former for kommunikasjonsetterretning. DGF vil ikke utvide E-tjenestens oppgaver, ansvarsområde eller hvilken *type* informasjon tjenesten skal ha tilgang til. Formålet vil være å sikre tjenesten teknisk tilgang til en informasjonskilde som i dag ikke er tilgjengelig.

I forhold til menneskerettighetene er det prinsipielt sett ikke forskjell mellom innsamling av utenlandsetterretningsinformasjon gjennom ekomnett og innsamling gjennom andre kommunikasjonsbærere. De aller fleste sammenlignbare land opererer heller ikke med et slikt skille når det gjelder kommunikasjon.

5.3. Hensynet til nasjonal selvstendighet og suverenitet

Norge kan ikke forvente at andre lands etterretningstjenester skal ha et primærfokus på å beskytte norske interesser. Det er i dag en alvorlig utfordring for rikets sikkerhet at de mest avanserte trusler i det digitale rom – statlig spionasje og forberedelse til digitale angrep, samt kommunikasjon mellom kjente terrorister i utlandet og ukjente personer i Norge – i de fleste tilfeller ikke kan avdekkes med dagens kapasiteter. Dette gjør E-tjenesten (og PST) avhengig av å få slik informasjon fra samarbeidende tjenester. Varsler kommer ofte for sent, og ofte som biprodukt i forhold til partneres nasjonale prioriteter. Det er derfor en betydelig sårbarhet – politisk og ut fra et suverenitetsperspektiv – at Norge i dag er helt avhengig av partnerinformasjon for i det hele tatt å kunne fange opp denne typen sikkerhetsmessige utfordringer mot Norge og viktige norske interesser. Det er også et paradoks at informasjon som E-tjenesten i dag mottar fra partnere, i betydelig

grad må antas å være basert på DGF-lignende ordninger. Egen aksess vil derfor både gjøre Norge mindre avhengige av, og mer relevante i forhold til, andre land. På sikt kan DGF muligens vise seg avgjørende for om Norge i fremtiden kan opprettholde en sterk nasjonal evne til utenlandsetterretning, slik at norske politiske myndigheter får et like godt beslutningsgrunnlag som andre stater til å treffe avgjørelser i ulike situasjoner.

5.4. Evne til å bidra i internasjonalt etterretningssamarbeid

Egenproduserte etterretninger kan ved deling med internasjonale partnere gi tilgang til etterretninger som man ikke evner eller finner hensiktsmessig å produsere selv. Dette gir større innsikt i globale problemstillinger av interesse for Norge, og det styrker den nasjonale beslutningsevne. Av samme hensyn er operativt samarbeid en stadig viktigere forutsetning for at E-tjenesten skal kunne løse sitt oppdrag. Internasjonalt etterretningssamarbeid er i norsk interesse.

E-tjenesten har hatt kapasiteter, kompetanse og aksess som over tid har medført at Norge har kunnet bidra substansielt i dette samarbeidet. Det har også bevirket at andre lands tjenester deler informasjon med E-tjenesten i større grad enn de ellers ville gjort. Å opprettholde et nært etterretningssamarbeid krever at tjenesten opprettholder evne til å bidra med etterretninger også innenfor relevante sivile områder som partnere er opptatt av. Uten aksess til informasjon i det digitale rom vil dette ikke være mulig.

Noen vil kunne hevde at så lenge Norge fokuserer på innhenting og analyse knyttet til tradisjonelle militære områder, og er gode på dette, kan man dernest «bytte epler mot appelsiner» og få høyverdig etterretningsinformasjon på sivile områder tilbake. Erfaring viser imidlertid at dette i praksis er urealistisk. Normalt kreves oppbygging av en langvarig, gjensidig og tillitsfull relasjon innenfor samme etterretningsområde og –disiplin, som forutsetning for utstrakt informasjonsdeling av den mest relevante og sensitive informasjonen. Videre har andre land organisert sin utenlandsetterretningsvirksomhet på andre måter enn i Norge, herunder gjort et skille mellom organisasjoner med sivilt og militært oppgavesett eller etablert separate SIGINT-tjenester. Dette medfører ytterligere vansker med å få aksept for en «arbeidsdeling» på vidt forskjellige områder.

5.5. DGF i lys av samspill mellom etterretningsdisipliner

Dersom E-tjenesten blir gitt en regulert tilgang til de kommersielle ekomnettene, vil informasjon fremskaffet på denne måten inngå som én komponent sammen med de andre kilder, metoder og kapabiliteter. I forhold til noen sentrale informasjonsbehov poengterer E-tjenesten at det vesentligste vil kunne dekkes ved tilgang til ekomnettene gjennom et etablert DGF. Samspillet mellom det tradisjonelle og en utvidet DGF aksess vil på mange måter foregå slik samspill og sammenstilling i dag virker internt i E-tjenesten og mellom E-tjenesten og nasjonale og internasjonale partnere. Den store forskjell og gevinst ved DGF er at E-tjenesten selv vil kunne få mulighet til å fremskaffe kritisk informasjon fra en kilde og datastrøm som blir stadig viktigere. Å lene seg på partnere er som beskrevet ovenfor ikke tilstrekkelig.

5.6. Andre staters praksis og rettsoppfatninger

Det fremgår av kap. 4.6 og vedlegg 2 at de fleste toneangivende land, herunder de største landene i NATO, har etablert ordninger tilsvarende DGF for utenlandsetterretningsformål.

De fleste stater har kanskje i liten grad ønsket å tilkjennegi dette synspunktet direkte i offentligheten, eller i det hele tatt offentlig kommunisere omkring egne kapasiteter og metoder innen kommunikasjonsetterretning. Men i forbindelse med lovgivning eller søksmål kommer statene ikke bort fra en viss offentlig kommunikasjon om dette. Det sees også en tendens til i økende grad å offentliggjøre mer detaljert regelverk om håndtering av bulkaksess, for å vise at innhentingen er målrettet og underlagt tilstrekkelige rettslige mekanismer for å ivareta rettssikkerheten til de personer som berøres.[45]

I all hovedsak er det staters syn at bulkaksess har vært lovlig og bør fortsette, og at tilgang til store datamengder i seg selv ikke innebærer ulovlig masseovervåkning. De fleste stater mener at verdifull etterretning har fremkommet gjennom tilgang til slik kommunikasjon, og at slik informasjon har bidratt til å redde liv og hindre alvorlige terroranslag, samt avverget eller redusert konsekvensene av svært skadelige cyberoperasjoner.

[45] Et eksempel på dette er at den britiske regjeringen nylig har offentliggjort flere dokumenter som i mye større utstrekning enn tidligere er åpen om verdien av bulk-innsamling. Dette gjelder f.eks. *Operational Case for Bulk Powers* (mars 2016) *Bulk Personal Datasets – Impact Assessment (IA)* av 6. juli 2016, og David Anderson: *Report of the Bulk Powers Review* (August 2016).

Det er intet som tyder på at stater mener det er behov for å skape ny bindende folkerett på dette området eller behov for grunnleggende endringer i nasjonale lovgivninger.[46] Det er heller ikke innført ny lovgivning i andre vestlige land som har medført grunnleggende endringer i adgangen til å innhente og behandle utenlandsetterretninger. Det pågår en rekke utredninger og debatter, men hovedkonklusjonene er at selv om det kan være behov for å oppdatere lovgivningen og kontrollmekanismer, bør etterretningstjenestene fortsatt drive sin målrettede virksomhet gjennom prosessering av internettkommunikasjon.[47] I den utstrekning ny lovgivning er innført i den senere tid, blant annet i Frankrike, Canada og Danmark, har disse gitt etterretnings- og sikkerhetstjenester større snarere enn snevrere fullmakter. Dette må også sees i lys av terrorangrepene i disse land.

At det i større grad enn tidligere har vært en omfattende debatt om personvern og overvåkning, er en god ting. Og på enkelte områder kan det være grunn til å foreta nasjonale oppdateringer av lovgivning, kontrolltiltak og rettssikkerhetsreguleringer. Men debatten har ikke medført grunnleggende justeringer av statenes balansering av personvern og sikkerhet.

5.7. Folkerettslige forpliktelser

Norge har en folkerettslig plikt til å unngå at norsk territorium brukes som transittland for fremmede aktørers cyberoperasjoner.[48] Norge er videre folkerettslig forpliktet, gjennom en rekke konvensjoner og bindende resolusjoner fra FNs sikkerhetsråd, til å bekjempe internasjonal terrorisme og terroristers støttespillere. I forhold til spredning av masseødeleggelsesvåpen og deres leveringsmidler mv. foreligger det også internasjonale normer og sanksjonsregimer som Norge er forpliktet til å etterleve. Et sideformål med DGF er derfor å oppfylle norske folkerettslige forpliktelser, og å etablere og hevde norsk suverenitet i det digitale rom.

5.8. Konsekvenser dersom DGF ikke etableres

Uten aksess til elektronisk informasjon som overføres ved hjelp av moderne kommunikasjonstjenester vil truslene bli vanskeligere å oppdage og varsle om, eventuelt blir de ikke oppdaget i det hele tatt. En fremmed trussel må avdekkes tidligst mulig, og fortrinnsvis allerede på planleggingsstadiet. Aksess til store mengder data er særlig nødvendig for å kunne finne nye trusler.[49] Manglende aksess vil medføre dårligere etterretningsprodukter til norske politiske myndigheter, herunder negative konsekvenser for tjenestens fremtidige evne til å yte etterretningsstøtte til nasjonale beslutningstakeres utforming av norsk utenriks-, forsvars- og sikkerhetspolitikk. Over tid vil det også medføre en betydelig svekket posisjon sett i forhold til etterretningssamarbeid og informasjonsutveksling med andre lands tjenester. Tjenestens posisjon som internasjonal samarbeidspartner vil reduseres. Dette vil samlet medføre flere uheldige forhold. Muligheten for å kartlegge og motvirke ytre trusler mot rikets selvstendighet og sikkerhet og andre viktige nasjonale interesser (herunder evne til å håndtere digitale anslag mot samfunnskritisk infrastruktur, terrorisme og andre alvorlige utfordringer) vil bli kritisk svekket, og for enkelte trusler helt fraværende.

En slik utvikling vil medføre press i to retninger – for det første i retning av økt aktivitet fra E-tjenesten i utlandet, og for det andre i retning av økt innsats fra NSM og PST innenlands.

For E-tjenesten vil bruk av andre informasjonskilder og innhentingsdisipliner ikke kunne frembringe den samme etterretningsinformasjon som DGF vil kunne gi. Dersom DGF ikke innføres, vil E-tjenesten likevel så langt mulig måtte prøve å frembringe deler av denne informasjonen gjennom SIGINT og HUMINT nærmere trusselaktørene og øvrige utenlandsetterretningsrelevante aktører i utlandet. Dette må både risikomessig og ressursmessig klart forventes å være

[46] Eksempelvis har ny amerikansk lovgivning ikke medført vesentlige endringer i forhold til NSAs utenlandsetterretningsrelaterte programmer.*US Freedom Act* gjelder primært metadatainnsamling fra telefonsamtaler mellom amerikanere, altså innenlandstrafikk. Prinsippet om NSAs tilgang til slike data opprettholdes, selv om måten de får tilgang til disse på endres (lagres av teleoperatørene og ikke av NSA, og tilgang krever nå kjennelse fra *FISA Court*). Utenlandsetterretningsinnsamling som baseres på andre hjemler berøres ikke av den nye lovgivningen.

[47] Et eksempel på dette er den såkalte Anderson-rapporten i UK; *A Question of Trust – Report of the Investigatory Powers Review*, av juni 2015.

[48] I folkeretten gjerne utlagt som det sedvanerettslige *due diligence*-prinsippet.

[49] U.S. Presidential Policy Directive/PPD-28 on Signals Intelligence Acitivities, datert 17. Januar 2014, begrunner dette slik: "*Locating new or emerging threats and other vital national security information is difficult, as such information is often hidden within the large and complex system of modern communications. The United States must consequently collect signals intelligence in bulk in certain circumstances in order to identify these threats.*"

mer belastende enn ved å innføre DGF. Det kan heller ikke utelukkes at enkelte av disse metodene kan være meget inngripende.

PST har overfor utvalget understreket at de støtter at E-tjenesten får ansvar for DGF, fordi dette vil styrke samfunnets samlede evne til å avdekke og motvirke trusler mot Norge fra utlandet. Det vil øke sjansen for tidlig varsling, styrke nasjonal kontroll, bidra til at PST får hurtigere svar fra E-tjenesten i akutte saker med større grad av kvalitet, samt bidra til en styrket felles situasjonsforståelse. I dag er PST avhengig av informasjon fra internasjonale partnere fordi E-tjenesten ikke har egen aksess. Det er ulemper med dette, fordi det ofte tar lang tid å få svar fra internasjonale partnere, og fordi det ofte er usikkert i hvilken utstrekning andre stater prioriterer norske behov. Dagens situasjon fordrer også utstrakt deling av personopplysninger om norske borgere med utenlandske tjenester. DGF antas i vesentlig grad å styrke PSTs informasjonstilfang, og dermed gi sikrere og tryggere data å agere på, selv om det i forkant av en eventuell etablering selvsagt er vanskelig å si akkurat hvor stor effekt DGF vil ha, hvilket også vil bero på hvilket konsept som implementeres. PST får positive tilbakemeldinger fra søstertjenester i andre land som har tilsvarende aksess nasjonalt, om verdien av slik aksess for landenes sikkerhet. Særlig ved akutte hendelser vil DGF kunne bidra med tidskritisk informasjon. Dette er også viktig i perspektivet nasjonal kontroll og suverenitet. I Norge har man hatt konkrete hendelser hvor både forsvar og politi var nær ved å initiere omfattende tiltak. Ved slike hendelser vil det også være viktig å ha evne til å tilveiebringe informasjon som kan bidra til å avklare den reelle trusselen, for å unngå unødvendig full beredskapsmobilisering.

Dersom DGF ikke etableres, antas dette å ha konsekvenser både for det digitale forsvaret av landet innenfor landegrensene, og for behovet for en bredere anlagt overvåking av aktører eller aktørgrupper fra PSTs side. Hva angår førstnevnte har NSM tidligere[50] påpekt at dagens nasjonale sensorutrustning basert på VDI-sensorene kommer til kort både hva angår utbredelse i antall og i forhold til bredden av virksomheter som er dekket. Det foreslås tiltak på området. I tillegg til dette fører bl.a. økt bruk av kryptering til et behov for å komme tettere inn på sluttbrukerne (virksomhetene) med de lokale sensorene. DGF overflødiggjør ikke dette behovet, men kopletterer informasjonsbildet. Etablering av DGF gir mulighet for deteksjon av truende trafikk basert på høyt graderte signaturer. E-tjenesten kan i dag ofte ikke dele graderte signaturer mottatt fra partnere. Egenutviklede signaturer kan i større grad deles nasjonalt. Dette vil igjen gi grunnlag for langt mer målrettet bruk av overvåkings- og deteksjonsressursene i de nasjonale nettene. Fraværet av DGF kan forventes å bety større behov for lokal overvåking på generelt grunnlag og større behov for tilgang til trafikkinnhold, og beskyttelseseffekten vil ikke bli tilsvarende.

Hva angår kontraterroroppdraget og arbeidet mot spredning av masseødeleggelsesvåpen spesielt, antas fraværet av DGF å måtte søkes kompensert med betydelig økt innenlandsk overvåkning fra PSTs side. Det gjelder særlig innenfor kontraterror, for å søke å få kontroll på ukjente norske personer som kommuniserer med kjente terrorister i utlandet. Dette må forventes å øke overvåkingstrykket i Norge sammenlignet med DGF som alternativ. PST må – for å finne de ukjente trusselaktørene i Norge – gå bredt ut og samle inn informasjon om de mange for å identifisere de få som er av interesse. Det samlede overvåkingstrykket i Norge kan derfor antas å bli større enn ved etablering av DGF, bl.a. som følge av at PST retter seg mot innenlandske personer og forhold. Samtidig vil økt innenlandsk overvåkning neppe evne å avdekke de mest alvorlige trusler og fenomener i utlandet som kommuniserer med og mot ukjente personer og infrastruktur på norsk territorium.

[50] Sikkerhetsfaglig råd, rapport fra Nasjonal sikkerhetsmyndighet, 10. september 2015.

6. FAKTORER SOM TALER MOT DGF

6.1. Vårt digitale liv - særtrekk ved DGF

DGF vil skille seg fra annen kommunikasjonstilgang ved at en stor andel av metadatalageret (se kap. 9.2 om dette) vil inkludere kommunikasjon (herunder norsk-norsk kommunikasjon) som faller utenfor det som er relevant for E-tjenesten. En annen forskjell vil være at E-tjenesten ikke lett kan skaffe seg tilgang til kommunikasjonen uten at de private virksomhetene som tilbyr ekomnett og ekomtjenester får en plikt til å tilrettelegge for tjenestens tilgang. En slik plikt fordrer en særskilt lovhjemmel, som ikke finnes i dag. I tillegg vil det være enkelte andre særtrekk sett fra vanlige brukeres ståsted. Det gjelder det faktum at vanlige brukere av digitale kommunikasjonstjenester som oftest ikke vil ha noen formening om datatrafikken går kun innenlands eller også utenlands, at det for praktiske formål ikke er mulig å unngå bruk av kommunikasjonskanaler som i prinsippet vil omfattes av DGF, og at kommunikasjonsvolumet er stort.

I kapittel 4 beskrives viktige teknologiske og samfunnsmessige utviklingstrekk av relevans for vurdering av DGFs påvirkning på det enkelte individ og dettes personvern. Norge er allerede et digitalisert samfunn på mange områder. Dette er likevel fremdeles i sterk utvikling og ikke minst vil vår digitale samhandling med det offentlige øke ytterligere i tiden som kommer. Oppdaterte estimater[51] pr juli 2016 viser at Norge ligger helt i verdenstoppen hva angår tilgang til Internett med skyhøye 98 % tilgang i befolkningen, mens Statistisk sentralbyrås statistikk for andre kvartal 2015 viser at 96 % av befolkningen i aldersgruppen 16-79 år hadde brukt Internett siste tre måneder. I tillegg til at dette er høye tall i seg selv, kommer at mye av Internettbruken nå er på mobile plattformer som også genererer informasjon om f.eks. lokasjon. I tillegg til det enkelte individs bevisste bruk av digitale tjenester, hvor man til en viss grad kan ha en formening om at det legges igjen spor, kommer annen form for potensiell kartlegging som f.eks. passering i bomstasjoner, økende omfang av videoovervåking og registrering av mobiltelefoner som vandrer mellom nett og snakker med omgivelsene uten brukerens medvirkning. I denne digitale verden er privat innsamling og lagring av informasjon om individer – anonymisert eller ikke – blitt et eget forretningsområde av betydning. Data samles gjerne inn for fremtidig bruk, og sammenstilling av informasjon kan avdekke sensitive forhold. Med tilstrekkelig datagrunnlag kan antatt anonyme datasett likevel knyttes til individer etter analyse.

Selv om staten fortsatt aksepterer digitalt utenforskap, jobber den systematisk for å minimalisere dette. Muligheten for det enkelte samfunnsdeltakende individ til å stå utenfor blir mindre med tiden.

Det er mange forhold knyttet til denne utviklingen som sterkt utfordrer personvernet, men dette er imidlertid utenfor rammen av vurderingene i denne rapporten. Imidlertid må det påpekes at en etablering av DGF i utgangspunktet er en måte for staten å tre inn i dette domenet på som reiser mange problemstillinger i seg selv. En svært stor andel av lagret informasjon i et DGF-system vil ikke være relevant for E-tjenesten. Er det da riktig å tillate DGF?

Disse forhold, vurdert opp mot legalitetsprinsippet og personvernrettslige rammer, begrunner hvorfor et mulig DGF utvilsomt må underlegges særskilte rammer og kontrollmekanismer sammenlignet med andre av tjenestens innsamlingsmetoder.

6.2. Formålsglidning

Formålsglidning er et uttrykk for gradvis endret eller utvidet bruk av teknologi, system eller innsamlet informasjon ut over det formålet som teknologien, systemet eller informasjonen var tiltenkt. Ved innføring av nye systemer, som DGF, er det essensielt at det gjennomføres grundige og etterprøvbare forholdsmessighetsanalyser. Disse er nødvendig for å kunne mene noe kvalifisert om gevinstene systemet gir for det bestemte formålet i relasjon til den konkrete inngripen i den enkeltes personvern.

Formålet med DGF er å sette E-tjenesten bedre i stand til å innhente etterretninger om utenlandske trusselaktører og relevante utenlandske mål innenfor det oppgavesettet som i dag er tillagt tjenesten.

[51] Antall individer med tilgang til Internett hjemme, iht. www.internetlivestats,com, som bygger på tall fra den internasjonale teleunion (ITU), Verdensbanken og befolkningsstatistikk fra FN.

Den typiske utfordringen er at så snart informasjonen er samlet inn eller kapasiteten etablert, så vil andre interessenter potensielt hevde at det ikke er hensiktsmessig ut fra et ressurs- eller kapasitetsperspektiv å avgrense bruken av systemet kun til det opprinnelige formål. Hvorfor skal ikke systemet kunne benyttes til avdekking og straffeforfølgning av grov økonomisk kriminalitet, distribusjon av barnepornografi eller lignende? Endringene i Sverige hvor sikkerhetspolitiet og andre deler av politiet fikk anledning til å gi oppdrag til den svenske SIGINT-tjenesten, er av noen trukket frem som et eksempel på formålsglidning.

Dersom det etter en tid åpnes for bruk av systemet for andre formål enn opprinnelig bestemt, vil dette typisk representere en formålsglidning. En formålsglidning er først og fremst problematisk fordi den diskvalifiserer den opprinnelige forholdsmessighetsvurderingen. Man risikerer altså å innføre et system – gjerne under sterk tvil – på et spesifikt premiss, for deretter å endre selve premisset. Det er mange eksempler på at de bakenforliggende mekanismene for formålsglidning både er sterke og fungerer.

Denne type mulige formålsglidning er bekymringsverdig i et lengre tidsperspektiv, gitt DGFs iboende skadepotensiale for personvernet. På den annen side er det intet som er statisk. Det vil ikke nødvendigvis være slik at enhver endring i formål med DGF vil være «feil» eller uforholdsmessig. Det må imidlertid sikres at forholdsmessighetsvurderingene i så fall gjøres på nytt og i en oppdatert kontekst.

Uansett grundighet i de opprinnelige vurderingene, så er det slik at dersom man etablerer en kapasitet som DGF, vil det være et latent skadepotensiale knyttet til utvidet bruk. Endrede sikkerhetspolitiske forhold, eller endringer i det politiske klima etter eksempelvis alvorlige terrorhandlinger på norsk jord, vil kunne endre verdisettet som man bygger vurderingene på. Noen vil da hevde at man aldri bør åpne denne døren selv om den initielle forholdsmessighetsvurderingen borger for det. En slik tilnærming vil representere et offensivt forsvar av personvernet, men mange vil hevde at tilnærmingen kanskje ikke i samme grad tar inn over seg det reelle behovet for informasjon for beskyttelse av landet og landets befolkning.

6.3. Nedkjølingseffekt

Nedkjølingseffekten, også kjent som «chilling effect», har lenge vært omtalt som en etablert sannhet om at generell overvåkning i samfunnet gir lavere eller endret privat og offentlig meningsbrytning. Antakelsen er at dersom man vet at myndighetene overvåker kommunikasjon, så vil man endre adferd og unnlate å søke på eller skrive forhold som kan gi grunnlag for mistanke mot en selv.

Dersom dette er riktig, så vil nedkjølingseffekten innvirke på den demokratiske debatt på en negativ måte, og det vil særlig ramme de som er i randsonen for hva som er gjengs oppfatning. Dette er ikke en ønsket utvikling for et demokrati som Norge. Det finnes så langt få objektive studier på fenomenet, men i kjølvannet av at NSAs overvåkningsprogrammer ble kjent, kommer det nå flere undersøkelser som støtter at fenomenet eksisterer.

I Datatilsynets årsrapport fra 2014 gjengis en undersøkelse som viser at bl.a. 16 % av de spurte har unnlatt å foreta søk på Internett fordi de er usikre på hvordan opplysningene om søket vil bli brukt senere, samt at 8 % av de spurte har «tenkt seg om en ekstra gang før de brukte visse ord i sin korrespondanse og internettsøk». Det vises også til at et mye brukt debattsted for juridiske diskusjoner stengte sine sider fordi de ikke vil eksponere brukerne for myndighetsovervåkning.

Jonathon W. Penney ved Oxford University har nylig publisert en artikkel med en foreløpig beskrivelse av de empiriske funnene knyttet til antall søk på Wikipedia i artikler med ord som «al Qaida», «car bomb» og «Taliban» etter at NSAs søk i elektronisk kommunikasjon ble kjent.[52] Studien viser at antall slike søk gikk ned med 20 %. Jon Penney skriver at det er en utfordring for demokratiet dersom befolkningen unnlater å søke objektiv informasjon om bl.a. terrorisme for selv å unngå å havne i søkelyset.

Elizabeth Stoycheff, ved Wayne State University, har nylig publisert en annen studie på fenomenet i *Journalism and Mass Publication quarterly*.[53] Studien viser empirisk at *«online surveillance programs may threaten the disclosure of minority views and contribute to the reinforcement of majority opinion"*.

[52] Artikkelen heter *Chilling effects: Online Surveillance and Wikipedia Use* og er tilgjengelig på http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645

[53] Tilgjengelig på http://mjmq.sagepub.com/content/early/2016/02/25/1077699016630255.full.pdf?ijkey=1jxrYu4cQPtA6&keytype=ref&siteid=spjmq

I denne sammenhengen er også Jeremy Benthams teori om Panoptikon relevant. Fengslene som ble bygget etter Panoptikon-modellen gikk ut på at fangers oppførsel endres når de vet at fengselsbetjenten *har mulighet* for å overvåke dem på ethvert tidspunkt, selv om fangene vet at overvåkningen ikke er konstant. Poenget er at fangene da til enhver tid oppfører seg som om de var overvåket. Det er grunn til å tro at prinsippet også vil gjelde for digital overvåkning.[54] I DGF-sammenheng vil dette bety at selv om innsamlingen ikke er konstant, så kan det medføre at borgernes oppførsel endres.

Reelt demokrati og debatt forutsetter ytringsfrihet. Ytringsfrihet forutsetter tilgang til kommunikasjonskanaler. Når ytringsfriheten er avhengig av digitale løsninger, har myndighetene et ansvar for å innrette disse slik at ytringsfriheten og mulighet for meningsbrytning ivaretas. På denne bakgrunn foreligger det et klart spenningsforhold mellom ønsket om å innføre DGF og de prinsipielle konsekvensene av DGF.

Nedkjølingseffekten har tradisjonelt vært omtalt i forhold til myndigheters overvåkning av borgerne. Det kan stilles spørsmål ved om det også skjer en atferdsendring hos borgerne som følge av private kommersielle aktørers stadige innsamling av personopplysninger. Datatilsynets undersøkelse som er nevnt over, antyder dette. Undersøkelsen viser at «vesentlige deler av befolkningen har unnlatt å gjøre enkelte aktiviteter fordi de er usikre på hvordan opplysningene kan bli brukt senere».[55] Mange private aktører har et enormt tilfang av kunnskap om sine brukere. En søkemotor vil for eksempel vite langt mer om enkeltindividet enn staten gjør, og aktører som faller utenfor europeisk personvernrett vil ofte ha større muligheter til å sammenstille data og gjøre økonomisk bruk av opplysningene. For myndigheter vil det kunne være fristende å søke rettslig tilgang i slike datamengder. Det kan ikke utelukkes at tilgang til et godt regulert DGF vil kunne minske myndigheters press på informasjon lagret hos private aktører.

6.4. Inngrep i enkeltpersoners menneskerettigheter

Utvalget vil i kapittel 7 nedenfor redegjøre for menneskerettslige rammer av betydning for DGF. Som redegjørelsen vil vise, er det på det rene at DGF vil innebære et inngrep i retten til privatliv etter Grunnloven § 102 og EMK artikkel 8. Den potensielle nedkjølingseffekten av DGF har også en side til ytringsfrihet etter Grunnloven § 100 og EMK artikkel 10. Et sentralt materielt vilkår vil da være at DGF anses som nødvendig og ikke uforholdsmessig inngripende. For å ta stilling til det, vil en måtte avveie de fordeler DGF gir for E-tjenestens virksomhet, mot de negative virkninger DGF vil ha for den enkeltes privatliv. Dette vil stå sentralt i utvalgets vurderinger i kap. 9.

Selv om en kommer til at DGF kan tillates innenfor de rammene Grunnloven og menneskerettskonvensjonene oppstiller, mener utvalget at DGF ikke bør innrettes slik at en balanserer helt på grensen av disse rammene. Ledende synspunkter på nøyaktig hvordan grensene skal trekkes vil kunne endres, og innretningen for DGF vil bli labil og lite robust om en til enhver tid skulle søke å tangere disse grensene.

6.5. Inngrep i kommunikasjonsvernet

Kommunikasjonsvernet har tradisjonelt stått sentralt i Norge og i de internasjonale menneskerettskonvensjonene. Kommunikasjonsvernet i folkeretten og norsk rett har betydning langt ut over ekomsektoren, men er også relevant for DGF.

Kommunikasjonsvern omfatter rettslig og faktisk beskyttelse av informasjon i transitt. Dette er delvis overlappende med personvern, men kan også omfatte vern av annen informasjon enn personopplysninger. Kommunikasjonsvernet verner både innholdsdata og metadata, og ivaretas grovt sett gjennom *dataminimalisering* (at det ikke skal behandles mer data enn nødvendig om brukers kommunikasjon), *behandlingsbegrensning* (at data som behandles bare benyttes til definerte formål) og *informasjonssikkerhet* (at data og tjenester sikres tilfredsstillende).[56]

Den teknologiske og samfunnsmessige utviklingen, jf. kapittel 4, understreker behovet for et bevisst forhold til og et sterkt forsvar av kommunikasjonsvernet for å sikre grunnleggende menneskerettigheter. Med den eksplosive vekst i utbredelse og bruk av elektronisk kommunikasjon og elektroniske kommunikasjonstjenester, følger en tilsvarende vekst i

[54] Det arbeides med dette, bl.a. av professor Melissa Terres ved University College London.

[55] Datatilsynets årsrapport for 2014, side 28.

[56] Utvalget viser ellers til mer utfyllende omtale av kommunikasjonsvern i NOU 2015:13 *Digital sårbarhet – sikkert samfunn* kapittel 11 og Meld. St. 27 (2015-2016) *Digital agenda for Norge* kapittel 33.

mengden av informasjon man genererer og lagrer om forhold som egen adferd, preferanser og interesser. Dette er informasjon som potensielt er interessant for flere aktører, statlige så vel som kommersielle. Det at vi som individer grunnleggende kan stole på at det er et effektivt vern rundt bruken av og innhold i elektronisk kommunikasjon, er svært viktig for den opplevde kommunikasjonsfrihet og dermed for grunnleggende demokratiske verdier. Dette gjenspeiles i ekomregelverkets generelle og spesifikke krav til vern av selve informasjonen og om bruken av elektroniske kommunikasjonstjenester.

Inngripen i kommunikasjonsvernet kan gjøres med hjemmel i lov for forhold knyttet til nasjonens sikkerhet eller kriminalitetsbekjempelse, innenfor de internasjonale forpliktelser som følger av bl.a. EMK artikkel 8 og EUs kommunikasjonsverndirektiv.

Regjeringen vektlegger i *Digital Agenda for Norge*[57] betydningen av et forutsigbart, godt og ordnet regelverk for person- og kommunikasjonsvern, også av hensyn til næringsutvikling og Norges posisjon internasjonalt som attraktiv partner for datasenter og tjenesteproduksjon. Dette stiller også krav til klarhet i og transparens om inngripen i kommunikasjonsvernet.

6.6. Risiko for misbruk

Et misbruk vil være forårsaket av at noen ønsker å ville tilegne seg informasjon, eller bruke informasjon, på en måte som er i strid med lov, forskrifter eller bestemmelser.

DGF kan misbrukes ved at overskuddsinformasjon, som ikke skal deles, likevel blir delt med PST eller andre. Myndigheter kan se gjennom fingrene med håndhevelse av kontroll for å få tak i informasjon som oppleves spesielt viktig i en gitt situasjon. E-tjenesten kan lete etter ulovlig informasjon, eller tilfeldig oppdage den, og så misbruke den. Det som også kan lede til et misbruk, er dersom lovgiver endrer kravene til DGF systemet, dets kontroll og sikringsmekanismer for å lette opp i begrensninger som oppleves uheldige. Det vil kunne lede til en ikke tilsiktet formålsglidning, med den konsekvens at risiko for misbruk blir større. Allerede i dag opererer EOS-tjenestene systemer og datastrømmer med informasjon som kan misbrukes. Ved eventuell innføring av DGF åpnes det opp for et større informasjonstilfang. Det kan også øke risiko for misbruk at personer vil ha kunnskap om muligheten til å skaffe seg uhjemlet sensitiv informasjon.

Det er tre parter som hypotetisk kan stå for et misbruk. Det ene er myndighetene selv, den andre er E-tjenesten som organisasjon og den tredje er enkeltpersoner i organisasjonen. Innbrudd og angrep forårsaket av kriminelle og fiender vil ikke være å betrakte som misbruk i denne sammenheng.

Ved eventuell opprettelse av DGF må det treffes tiltak som reduserer risiko for misbruk. DGF-systemets omfang må reduseres til det strengt nødvendige. Sikrings- og kontrollregimet må være meget strengt, og personer som skal operere systemet må være nøye sjekket og klarert. Uansett strenge sikkerhetstiltak kan intet system bli perfekt. Det vil således alltid være en restrisiko, om enn meget liten, for at DGF vil kunne bli misbrukt og at en gruppe eller enkeltperson dermed vil kunne lide overlast.

[57] Meld. St. 27 (2015-2016) *Digital agenda for Norge* kapittel 33.

7. RETTSLIGE RAMMER FOR DGF

7.1. Grunnleggende hensyn

Norge er et fritt og selvstendig rike. Grunnloven § 2 angir grunnleggende verdier for vår stat og statsform. Det fremgår av § 2 annet punktum at Grunnloven skal sikre demokratiet, rettsstaten og menneskerettighetene. Utvalget tar utgangspunkt i dette som grunnleggende hensyn.

Hele formålet med E-tjenestens virksomhet, herunder også DGF, er å verne om Norge som fri og selvstendig stat. På den måten ivaretas også vårt demokrati. Demokrati som grunnleggende hensyn tilsier på den annen side at DGF skjer under demokratisk kontroll og innenfor klare, lovgitte rammer.

Rettsstaten ivaretas bl.a. gjennom enkeltbestemmelser av menneskerettslig karakter som er inntatt i Grunnloven kapittel E. Ved grunnlovsvedtak 13. mai 2014 ble en rekke menneskerettighetsbestemmelser innarbeidet i Grunnloven. I stor grad er de nye bestemmelsene utformet etter modell av tilsvarende bestemmelser i internasjonale menneskerettighetskonvensjoner som Norge er bundet av. En del av disse skal behandles nedenfor. Grunnlovenes menneskerettighetsbestemmelser suppleres av flere konvensjoner på området, som er gjort til en del av norsk lov gjennom menneskerettsloven av 21. mai 1999.

Av generell betydning er at myndighetenes inngrep overfor den enkelte må ha hjemmel i lov. Dette legalitetsprinsippet fremgår av Grunnloven § 113.

Den praktisk viktigste menneskerettskonvensjonen er Den Europeiske menneskerettighetskonvensjonen av 4. november 1950 (heretter EMK) med tilleggsprotokoller. Denne konvensjonen kjennetegnes at den har etablert sin egen domstol (Den europeiske menneskerettighetsdomstolen, heretter EMD) og en *individklageordning*. Som følge av dette foreligger en rik praksis fra domstolen som autoritativt avklarer fortolkningen av konvensjonen. FN-konvensjonen av 16. desember 1966 om sivile og politiske rettigheter (heretter SP) gir anvisning på mange av de samme rettighetene som EMK, men har ikke det samme systemet med domstol. Begge disse konvensjonene skal ved motstrid gå foran det som ellers måtte følge av annen norsk lov, jf. menneskerettsloven § 3.

Personvern er i seg selv et hensyn som er ivaretatt gjennom flere menneskerettighetsbestemmelser. Det vises til Grunnloven § 102, EMK artikkel 8 og SP artikkel 17. Personvern er også regulert mer detaljert i en rekke ulike regelverk. Det redegjøres for disse nedenfor.

Folkeretten – som regulerer forholdet mellom stater – vil kunne legge begrensninger for E-tjenestens virksomhet. Metodene som tas i bruk for etterretningsformål kan for eksempel ikke stride mot suverenitetsprinsippet eller maktforbudet i FN-pakten. Det vises til omtalen av disse i NOU 2015: 13 *Digital sårbarhet – sikkert samfunn*, punkt 10.2 og 10.3. Slik utvalget forstår det, er det forutsatt at DGF gjennom kabelaksess skal skje på norsk territorium. Det er da ikke grunn til å gå nærmere inn på hjemmels- og jurisdiksjonsspørsmål ved etterretning andre steder[58]. De for utvalget praktiske viktige spørsmål er å identifisere hvilke krav som stilles til lovgivningen for å være i samsvar med Grunnloven og de relevante konvensjonene.

7.2. Krav om lovhjemmel

Som nevnt knesetter Grunnloven § 113 legalitetsprinsippet. Bestemmelsen lyder:

> *«Myndighetenes inngrep overfor den enkelte må ha grunnlag i lov.»*

Bestemmelsen ble inntatt i Grunnloven ved grunnlovsvedtak 13. mai 2014. Det fremgår av komiteens merknader i Innst. 186 S (2013-2014) s. 31-32 at grunnlovfestingen ikke var ment å endre rettstilstanden. Formålet var å bidra til at Grunnloven beskriver de sentrale deler av vår statsskikk, også de som tidligere kun var ulovfestet. Legalitetsprinsippet ville gjeldt uansett i norsk rett og hatt den

[58] Utvalget er klar over den pågående internasjonale faglige diskurs om hvorvidt menneskerettighetene kommer ekstraterritorielt til anvendelse ved inngrep i personvernet gjennom det digitale rom, uten at den stat som gjennomfører inngrepet har territoriell kontroll eller effektiv kontroll over en person i tradisjonell forstand. For DGFs del legger utvalget imidlertid til grunn at norsk rett og E-tjenestens virksomhet skal tilfredsstille menneskerettighetene uavhengig av de formelle jurisdiksjonsspørsmål. Og under enhver omstendighet kommer menneskerettighetene direkte til anvendelse for E-tjenestens virksomhet i forhold til prosessering og analyse av data som skjer innenfor norsk jurisdiksjon, selv om data kan være innsamlet i utlandet.

samme gjennomsIagskraften. Også for en del av de menneskerettsbestemmelsene som behandles nedenfor, vil det kreves grunnlag i lov. Dette fremgår bl.a. uttrykkelig av formuleringen i EMK art. 8 nr. 2, og er innfortolket i andre relevante bestemmelser.

Grunnloven fastslår at inngrepet «må ha grunnlag i lov». Ideelt sett vil det innebære at inngrepet og vilkårene for å foreta det er presist beskrevet i formell lov. Ofte vil imidlertid hjemmelen for myndighetenes inngrep være angitt i en forskrift, som igjen er forankret i lov. Legalitetsprinsippet er imidlertid i en viss grad relativt. Innenfor strafferetten, der hensynet til bl.a. forutberegnelighet og rettssikkerhet gjør seg gjeldende med stor tyngde, gjelder de strengeste kravene til klar lovhjemmel. På andre rettsområder vil det være noe mindre strenge krav. Som Høyesterett fremholdt i Rt-1995-530 (Fjordlaks) må «kravet til lovhjemmel (...) nyanseres blant annet ut fra hvilket område en befinner seg på, arten av inngrepet, hvordan det rammer og hvor tyngende det er overfor den som rammes.» Utvalget kommer tilbake til dette særlig ifm. redegjørelsen for EMK art. 8 nedenfor.

Kravet til lovhjemmel ved DGF gjør seg gjeldende i to relasjoner:

- *For det første* vil det kunne være et inngrep overfor kabeleierne og andre som råder over ekominfrastruktur. Med mindre disse frivillig vil gi E-tjenesten tilgang (herunder også til kryptering) vil det kreves en lovhjemmel for at E-tjenesten skal få tilgang. Utvalget ser her bort fra muligheten til fordekt aksess.
- *For det andre* vil det kunne være et inngrep overfor dem som er parter i den kabelbaserte kommunikasjonen. Det er spesielt i denne relasjonen at det oppstår menneskerettighetsspørsmål og personvernspørsmål.

Kontroll med den praktiske gjennomføringen av DGF er viktig i et demokratisk perspektiv. Kontroll vil også ha betydning for å trekke opp grensene for hva slags inngrep Grunnloven og menneskerettighetskonvensjonene tillater.

For den som mener å ha vært utsatt for ulovlig inngrep, blir det spørsmål om lovligheten av inngrepet skal kunne bringes inn for en norsk domstol, jf. Grunnloven § 95, eller andre overprøvingsmuligheter. Etter EMK artikkel 13 kreves tilgang til et effektivt prøvingsmiddel («effective remedy»). Utvalget viser generelt til professor Husabøs utredning *Hvilke krav stiller Grunnloven og EMK til etterfølgende kontroll av sikkerhets- og etterretningstjenestenes inngrep i menneskerettigheter?*.[59]

Denne typen for kontroll basert på individuelle krav om kontroll, vil imidlertid ikke kunne være tilstrekkelig i seg selv. Utvalget antar at det må suppleres enten med forhåndskontroll, med mer systematisk etterkontroll eller en kombinasjon av disse. Utvalget kommer noe tilbake til de rettslige krav til kontrollmekanismer nedenfor.

7.3. Grunnloven § 102

Grunnloven § 102 fastslår at

> *«Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller.*
>
> *Statens myndigheter skal sikre et vern om den personlige integritet.»*

Bestemmelsen viderefører i første ledd annet punktum § 102, slik den ble vedtatt allerede i 1814. Bestemmelsens første ledd første punktum og annet ledd ble inntatt i Grunnloven den 13. mai 2014. Forut for grunnlovsendringen i 2014 hadde § 102 neppe noen betydning som skranke for DGF. Det hovedsakelige tolkningsspørsmål den gang var hva som kunne anses som «hus», herunder om det var strengt avgrenset til bolig eller om også andre lokaler kunne omfattes.[60]

Rent språklig gir de tilføyelsene i § 102 som ble vedtatt i mai 2014, liten veiledning om hvilken betydning paragrafen har som skranke for lovgivning om DGF. Såvel «respekt for» som «sitt privatliv ... og sin kommunikasjon» er relativt åpne for fortolkning.

Endringene i Grunnloven § 102 i mai 2014 ble utformet etter mønster av EMK artikkel 8. EMDs autoritative praksis om fortolkningen av EMK artikkel 8, frem til grunnlovsendringen ble vedtatt, vil derfor også stå sentralt ved fortolkningen av grunnlovsbestemmelsen. Høyesterett har lagt dette metodologiske

[59] Utredningen er inntatt som vedlegg 4 til Dokument 16 (2015-2016), Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-utvalget).

[60] Se Marius Stub, *Tilsynsforvaltningens kontrollvirksomhet*, s. 114 -122.

synet til grunn.[61] Det må derfor antas at betydningen av Grunnloven § 102 som skranke for lovgivning om DGF vil falle sammen med det som kan utledes av EMK artikkel 8 slik den er fortolket av EMD frem til nå, og som utdypes nedenfor. Nettopp sammenhengen med EMK artikkel 8 er sentral ved forståelsen av Grunnloven § 102. På samme måte som EMK artikkel 8, skal Grunnloven § 102 forstås slik at inngrep i privatlivet – for å være i samsvar med vernet etter bestemmelsen – må være lovhjemlet og forholdsmessig.

7.4. EMK og praksis fra EMD

EMK artikkel 8 verner om retten til privatliv. Bestemmelsen lyder i norsk oversettelse slik:

«Art 8.Retten til respekt for privatliv og familieliv
1. Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.
2. Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.»

EMK artikkel 8 oppstiller et vern om bl.a. privatliv og korrespondanse. Vernet fremgår av artikkel 8 nr. 1. Som det fremgår av nr. 2, er vernet ikke absolutt. Det kan likevel gjøres inngrep i privatliv og korrespondanse på nærmere vilkår.

Alle typer korrespondanse vil være vernet etter nr. 1, uavhengig av teknisk plattform (papirbasert eller elektronisk). EMD har lagt til grunn at innsamling av trafikkdata eller metadata også er vernet. Så vel innsamling av kommunikasjon, lagring og bruk av personlige opplysninger, samt deling av informasjon som utvider gruppen med kjennskap til personlige opplysninger, utgjør selvstendige inngrep i privatlivet.[62]

Utvalget legger til grunn at DGF vil utgjøre et inngrep i privatliv og korrespondanse. Det blir dermed spørsmål om og under hvilke forutsetninger DGF likevel vil være tillatt etter artikkel 8 nr. 2. For å være tillatt etter nr. 2, må inngrepet være i samsvar med loven, og det må være nødvendig i et demokratisk samfunn av hensyn til et legitimt formål.[63]

Formålet med DGF er å gjøre E-tjenesten i stand til å utføre sitt oppdrag ved å kartlegge og motvirke trusler mot rikets selvstendighet og sikkerhet og andre viktige nasjonale interesser. Oppdraget følger av formålsparagrafen i lov om Etterretningstjenesten § 1 bokstav a. Dette må være et legitimt formål etter artikkel 8 nr. 2.

Mer krevende spørsmål oppstår ved vurderingen av lovkravet. For hemmelig kommunikasjonskontroll kreves det at hovedelementene i regelverket kommer til uttrykk i formell lov, som eventuelt kan suppleres med bestemmelser gitt i medhold av lov. EMDs praksis viser at det stilles strengere krav til loven med hensyn til klarhet og presisjon hvis det er tale om større inngrep.[64] Konkret blir det spørsmål om E-loven § 3 og regelverket som supplerer loven (E-instruksen og utfyllende bestemmelser fastsatt av Forsvarsdepartementet) på dette området gir tilstrekkelig klarhet og presisjon. Utvalget ser det ikke som nødvendig å ta konkret stilling til dette spørsmålet, fordi utvalget legger til grunn at DGF under enhver omstendighet vil fordre ny lovgivning som tilfredsstiller kravet til klarhet og presisjon.

Kjernen i vurderingen av om DGF er nødvendig i et demokratisk samfunn, vil være en vurdering av forholdsmessigheten mellom det som oppnås med å tillatte inngrepet, avveid mot hensynet til privatliv og korrespondanse.[65] Utvalget kommer nærmere tilbake til den konkrete forholdsmessighetsvurdering for DGF i kap. 9.5 nedenfor.

Kravet til lovhjemmel og kontrollmekanismer er avgjørende for å ivareta rettssikkerhet på dette området. Hva slags kontrollsystem som er etablert, vil ha betydning ved vurderingen av forholdsmessighet.[66] Utvalget kommer nærmere tilbake til disse spørsmål i kapittel 9.

Utvalget er kjent med at EMD i storkammer har til behandling en klagesak mot Storbritannia, saken

[61] Se Dok. 16 (2011-2012) s. 90 og Rt-2015-93 avsnitt 57.
[62] Se NOU 2015: 13 punkt 10.3.1 med videre henvisninger og Husabø punkt 3.1.
[63] Se NOU 2015: punkt 10.3.1 med videre henvisninger og Husabø punkt 3.2 - 3.4
[64] Se Husabø punkt 3.2.1 med videre henvisninger
[65] Se Husabø punkt 3.4 med videre henvisninger
[66] Se Husabø punkt 3.5 med videre henvisninger

Big Brother Watch vs. UK (sak 58170/13) som gjelder artikkel 8 og kontroll med elektronisk kommunikasjon. Saksforholdet er i korte trekk dette:[67] Klagen fra tre frivillige organisasjoner ble utløst av mediedekning av Snowden-saken. Klagerne hevder at det er sannsynlig at deres elektroniske kommunikasjon har vært gjenstand for generisk overvåkning av den britiske *Government Communications Headquarters (GCHQ)* og/eller at de britiske sikkerhetstjenestene kan ha mottatt slikt materiale fra utenlandske samarbeidende tjenester. Det er i klagen anført at inngrepet ikke er i samsvar med lovkravet i artikkel 8. Videre er det anført at inngrepet uansett ikke er underlagt kontrollmekanismer som oppfyller de minstestandarder EMD gjennom sin praksis har etablert. Endelig er det anført at inngrepet er et uforholdsmessig inngrep i privatlivet til svært mange mennesker. Det er foreløpig ikke kjent når EMDs avgjørelse av klagen vil foreligge. Den direkte relevansen for DGF i Norge vil bero på EMDs avgjørelsesgrunner. Herunder vil det bl.a. ha betydning om det er forskjeller i hjemmelsgrunnlaget og kontrollmekanismene. Det er i noen grad redegjort for den britiske reguleringen av bulk aksess i vedlegg 2. Som det fremgår der, er den britiske lovgivningen for tiden under revisjon. Menneskerettighetsaspektet ble vurdert av parlamentets *Joint Committee on Human Rights*. Komiteen har i sin rapport av 25. mai 2016 som hovedkonklusjon at bulk aksess ikke i seg selv er uforenlig med det menneskerettslige vernet om privatliv, og at det vil kunne tillates dersom lovgrunnlaget er tilstrekkelig klart, det anses nødvendig og forholdsmessig og ledsages av tilstrekkelig kontrollmekanismer.

Utvalget viser videre til at organisasjonen *Centrum för Rättvisa* klaget Sverige inn for EMD i 2008,[68] med påstand om at praksis og lovgivning knyttet til den svenske SIGINT-myndighetens etterretningsinnsamling av kommunikasjon inn og ut av Sverige strider mot EMK artikkel 8 og 13. [69] Den internasjonale juristkommisjonens norske avdeling[70] har intervenert i saken til fordel for klageren. Klagerens anførsler er i hovedsak de samme som i saken mot UK omtalt i foregående avsnitt. Det er foreløpig uklart når saken vil bli avgjort. I likhet med saken mot UK omtalt foran, vil relevansen av en eventuell avgjørelse for DGF i Norge bero på EMDs avgjørelsesgrunner.

7.5. FN-konvensjonen om sivile og politiske rettigheter

SP artikkel 17 verner, som EMK artikkel 8, om retten til privatliv. SP artikkel 17 lyder i norsk oversettelse slik:

«Art 17.
1. Ingen må utsettes for vilkårlige eller ulovlige inngrep i privat- eller familieliv, hjem eller korrespondanse, eller ulovlige inngrep på ære eller omdømme.
2. Enhver har rett til lovens beskyttelse mot slike inngrep eller angrep.»

Som det fremgår er bestemmelsen noe annerledes utformet enn EMK artikkel 8. SP artikkel 17 nr. 1 verner mot «vilkårlige eller ulovlige» inngrep i privatliv og korrespondanse, og gir etter nr. 2 enhver rett til «lovens beskyttelse» mot slike inngrep.

Rent språklig synes ikke artikkel 17 å legge begrensninger for hva slags lovbestemmelser som kan gis på området, så lenge inngrep går klar av å være vilkårlige. Denne forståelsen kan imidlertid ikke legges til grunn. Det foreligger praksis fra FNs menneskerettskomité om fortolkningen av artikkel 17. Denne praksisen er mindre omfattende enn EMDs praksis om EMK artikkel 8, og praksis fra menneskerettskomiteen er heller ikke bindende. Likefullt indikerer praksis at vurderingstemaene ved vurderingen av om et inngrep har krenket konvensjonens vern om privatliv og korrespondanse, vil følge de samme vurderingstemaene etter begge konvensjonene.[71] Utvalget vil derfor i den mer inngående drøftelsen av DGF nedenfor i hovedsak knytte drøftelsen til EMK artikkel 8, og antar at det også vil være dekkende for de skranker for lovgivning på området som vil kunne utledes av SP artikkel 17.

[67] Basert på EMDs *Information Note om the Court's case-law No. 170,* januar 2014 (http://www.echr.coe.int/Documents/CLIN_2014_01_170_ENG.pdf)
[68] Application no. 35252/08, fremmet 14. juli 2008.
[69] Domstolen har stilt en rekke spørsmål til Sverige, senest besvart av den svenske regjeringen 19. november 2015. Sverige har svart at klageren ikke har anført å selv ha blitt gjenstand for overvåking, at det ikke har foregått et inngrep i forhold til klagerens menneskerettigheter, og at klagen derfor bør avvises *ratione personae* (manglende partskompetanse), *ratione materiae* (ikke i strid med konvensjonsreglene) og uansett «*as being manifestly ill-founded*»
[70] ICJ-Norway.
[71] Se NOU 2015:13 punkt 10.3.1 (s. 78 v. spalte øverst)

7.6. Foreløpig sammenfatning av menneskerettslige rammer for DGF

Redegjørelsen ovenfor viser at menneskerettslige regler i Grunnloven og i internasjonale konvensjoner Norge er bundet av, legger viktige rammer for eventuell innføring av DGF. For det første må det kreves tilstrekkelig klar og presis lovhjemmel som angir vilkårene for at E-tjenesten kan innhente datatrafikken, inngrepet må være nødvendig ved at fordelene for tjenesten anses å veie tyngre enn ulempene som påføres den enkelte, og det må foreligge adekvate kontrollmekanismer. Noe generelt forbud mot bulk aksess kan etter utvalgets syn ikke utledes verken av Grunnloven eller internasjonale konvensjoner Norge er bundet av.

7.7. Personvernregler

7.7.1. Europarådets personvernkonvensjon

Norge ratifiserte Europarådets konvensjon nr. 108 av 28. januar 1981 om personvern i forbindelse med elektronisk databehandling av personopplysninger, den 20. februar 1984. Konvensjonen er ratifisert av 46 stater, og er den eneste internasjonale konvensjonen om personopplysninger som regulerer grenseoverskridende datastrømmer. Formålet med konvensjonen er nedfelt i dens artikkel 1, som angir at konvensjonen skal:

«… sikre respekt for enhver enkeltpersons rettigheter og grunnleggende friheter og især retten til privatlivets fred på territoriet til enhver part, uten hensyn til statsborgerskap eller bopel, i forbindelse med elektronisk databehandling av personopplysninger som vedrører ham.»

Konvensjonen gjelder ikke bare statens egne borgere eller personer med lovlig opphold i staten. Konvensjonens forklarende rapport angir:

«The guarantees set out in the convention are extended to every individual regardless of nationality or residence. This provision is in accordance with the general principle of the Council of Europe and its member States with regard to the protection of individual rights. Clauses restricting data protection to a State's own nationals or legally resident aliens would be incompatible with the convention."

Konvensjonen definerer personopplysninger vidt: *«enhver opplysning som gjelder en bestemt eller identifiserbar enkeltperson»*, jf. konvensjonens art. 2 bokstav a.

Ved bearbeiding av denne type opplysninger ved elektronisk databehandling, skal de iht. konvensjonens art. 5:

«a) innsamles og bearbeides på rettferdig og lovlig vis;
b) lagres for bestemte og lovlige formål og ikke nyttes på en måte som er uforenlig med disse formål;
c) være adekvate, relevante og ikke for omfattende i relasjon til de formål de lagres til;
d) være nøyaktige og, der det er nødvendig, holdt a jour;
e) oppbevares på en måte som ikke gir anledning til å identifisere datasubjektene lenger enn nødvendig for det formål som disse opplysningene lagres til.»

Konvensjonen gir enhver rett til å vite om det eksisterer et elektronisk persondataregister, registerets formål og til å få vite om man er registrert og eventuelt korrigert eller slettet opplysninger som er lagret i strid med konvensjonen, samt ha klageadgang dersom disse rettighetene ikke respekteres, jf. konvensjonens art. 8. Konvensjonens art. 6 peker på kategorier av særlig sensitive opplysninger som skal nyte et særskilt vern:

«Personopplysninger som åpenbarer rasemessig opprinnelse, politiske oppfatninger samt religiøs eller annen tro, så vel som personopplysninger vedrørende helse eller seksualliv, kan ikke behandles elektronisk med mindre intern lovgivning gir tilstrekkelig vern. Det samme skal gjelde for personopplysninger som gjelder domfellelser for straffbare handlinger.»

Det kan gjøres unntak fra konvensjonens art. 5, 6 og 8, nevnt ovenfor, når dette er fastsatt i lov og er et nødvendig tiltak i et demokratisk samfunn av hensyn til a) beskyttelse av statens sikkerhet, offentlig sikkerhet, statens økonomiske interesser eller bekjempelse av kriminelle handlinger eller b) beskyttelse av datasubjektet eller andres rettigheter og friheter. Dette er relevant i forhold til DGF. Vurderingstemaene er stort sett sammenfallende med ordlyden i EMK art. 8 nr. 2.

Det arbeides med en protokoll om endringer i konvensjonen med sikte på å modernisere denne, men endringene forventes ikke å medføre grunnleggende justeringer av de prinsipper som fremkommer i konvensjonen.

7.7.2. Norges forpliktelser som følger av EØS-avtalen - personverndirektivet

EØS-avtalen er Norges mest omfattende folkerettslige avtale. Avtalen omfatter 31 land; 28 EU-stater samt EFTA-statene Island, Liechtenstein og Norge. For å delta i EUs indre marked forpliktet Norge seg til å gjennomføre EU-retten på samme måte som det gjøres internt i EU. Reglene skal fortolkes og anvendes på samme måte som i medlemslandene. Det

betyr at EU-domstolens avgjørelser også er bindende for Norge.

Gjeldende norsk lovgivning om behandling av personopplysninger, personopplysningsloven, er gjennomført som del av EØS-avtalen ved personverndirektiv 95/46/EF. Reglene er forankret i EMK artikkel 8, som er omtalt ovenfor i kap. 7.4.

Personopplysningsloven bygger på et sett med grunnleggende personvernprinsipper som har som bærebjelke at alle skal ha bestemmelsesrett over personopplysninger om dem selv. Personopplysninger skal bare behandles når det er nødvendig. Når det er nødvendig å behandle personopplysninger, skal behandlingen først og fremst baseres på samtykke eller annet rettslig grunnlag. For DGF vil det være nødvendig med et selvstendig lovgrunnlag. Selv om DGF er foreslått å ha grunnlag i lov, er de nedenstående momentene fra personopplysningsloven grunnleggende prinsipper som må hensyntas i vurderingen av DGF, se nærmere i kap. 9.4:

- Et prinsipp i personopplysningsloven er at bruk av personopplysninger begrenses til et minimum for å sikre privatlivets fred og den enkeltes personlige integritet.
- Overskuddsinformasjon, sett i forhold til det formålet man behandler opplysninger for, skal unngås.
- Videre må behandlingen av opplysninger ikke medføre noen urimelig belastning for den registrertes integritet eller selvråderett. Det skal være en balanse mellom hensynet til den som registrerer og den som blir registrert, og registreringen må være proporsjonal med formålet. Dersom det foreligger flere alternativer, skal man velge det alternativet som griper minst inn i personvernet til den enkelte.
- Personopplysninger skal ikke brukes til noe annet enn det de i utgangspunktet ble samlet inn for. Personopplysninger skal heller ikke utleveres til andre, bortsett fra hvis den registrerte har samtykket til utleveringen eller det foreligger annet rettslig grunnlag. Innsamlede data som ikke lenger er nødvendige for det angitte formålet, må slettes eller anonymiseres. Personopplysninger skal være relevante, korrekte og fullstendige i forhold til hva de skal brukes til. Det betyr at opplysningene skal være oppdaterte og nøyaktige slik at det ikke fattes beslutninger om en person på feil grunnlag.
- Videre gjelder at den registrerte i utgangspunktet har rett til å bli informert om innsamling og bruk av vedkommendes personopplysninger, samt mulighet til å få slettet eller korrigert opplysninger som er feilaktige eller misvisende. I tillegg gjelder omfattende bestemmelser om at den som oppbevarer personopplysninger må sikre opplysningene mot uautorisert tilgang, endring, ødeleggelse og spredning. Dersom de aktuelle personopplysninger er sensitive, gjelder strengere regler og vurderinger.

EU har arbeidet med å revidere personverndirektivet siden 2012. Kommisjonen har foreslått to nye regelverk: en generell forordning om beskyttelse av personopplysninger og et direktiv for myndighetenes behandling av personopplysninger i politi- og straffesektoren. EU-parlamentet vedtok regelverkene i april 2016. Personvernforordningen vil erstatte gjeldende direktiv i 2018. Det overordnede målet med EU-kommisjonens forslag til reform har vært å oppdatere og modernisere personvernprinsippene som er nedfelt i 1995-direktivet, i tråd med den digitale utviklingen og de mulighetene dette byr på for realiseringen av ett felles digitalt marked innenfor EU. Forordningen bygger på mange av de samme prinsipper som dagens regelverk, men stiller bl.a. større krav til dokumentasjon som viser at de nødvendige vurderinger og forholdsmessighetsvurderinger for en spesiell behandling av personopplysninger foretatt. Det innføres også bestemmelser som skal øke bruken av personvernfremmende teknologi for å sikre at personvernhensyn blir tatt i betraktning på et tidlig stadium ved utvikling og valg av IT-løsninger, og at det lagres så få personopplysninger som mulig (minimumsprinsippet). Det legges opp til en ny institusjonell struktur på personvernområdet, og det vil bli opprettet en felles europeisk datatilsynsmyndighet (*European Data Protection Board*), som skal bestå av representanter fra de ulike medlemsstatenes tilsynsmyndigheter. Videre gis nasjonale personvernmyndigheter nye verktøy for å sanksjonere brudd på regelverket, herunder myndighet til å ilegge overtredelsesgebyr på inntil 20 millioner euro, eller, for næringsselskaper, inntil 4 % av selskapets brutto omsetning globalt.

7.7.3. OECDs retningslinjer

Norge er medlem i OECD, som ble grunnlagt i 1961 og har cirka 200 komiteer og arbeidsgrupper. Medlemslandene, partnere og inviterte organisasjoner arbeider sammen med OECDs sekretariat med studier, anbefalinger og retningslinjer til støtte for medlemslandenes policyutvikling. OECDs anbefalinger og retningslinjer er ikke juridisk bindende, men veiledende. De blir fulgt i stor grad.

OECD har retningslinjer for beskyttelse av personopplysninger ved overføring og datalagring.[72] Retningslinjene omhandler bl.a. ulovlig lagring av personopplysninger, oppbevaring av uaktuelle opplysninger og utlevering av sensitive opplysninger. Myndigheters bruk av data er også omfattet. Retningslinjene omfatter åtte forskjellige prinsipper med krav til mengden innsamlede personopplysninger, datakvalitet, formålet med å behandle dataene, behandlingen (det vil si håndtering og bruk), sikkerhet, åpenhet om bruken, individets rettigheter, samt det å definere hvem som har ansvaret for databehandlingen. Disse prinsippene ligger til grunn også for dagens personvern.

7.7.4. FNs generalforsamlings tredje komité

FNs generalforsamlings tredje komité behandler menneskerettighetsspørsmål. Vestlige land, herunder Norge, legger til grunn at menneskerettighetene gjelder i det digitale rom på lik linje med samfunnet for øvrig. Diskusjonen om balansen mellom sikkerhet og frihet og mellom privatliv og overvåking er krevende. Brasil og Tyskland fremmet en resolusjon om overvåking og privatliv i 2013 som Norge og en rekke andre land, herunder USA, sluttet seg til. FNs generalforsamling har avgitt to resolusjoner om retten til et privatliv i den digitale tidsalder. Resolusjonene er ikke rettslig bindende, men anses for å angi visse minstestandarder. Resolusjon 68/167 av 18. desember 2013 hadde først og fremst betydning ved at den innledet en internasjonal dialog om personvern i det digitale rom. Resolusjonen ga FNs høykommissær for menneskerettigheter i mandat å utarbeide en rapport om temaet. Rapporten forelå 30. juni 2014.[73] Høykommissærens rapport dannet så utgangspunktet for forhandlingene om en ny resolusjon på området, som ble vedtatt av FNs generalforsamling 18. desember 2014. Som en oppfølging av generalforsamlingens sistnevnte resolusjon vedtok FNs menneskerettsråd 24. mars 2015 å oppnevne en spesialrapportør for personvern.

7.7.5. FNs råd for menneskerettigheter

I FNs råd for menneskerettigheter i Genève ble det i 2012 vedtatt en resolusjon med konsensus som for første gang bekrefter at de samme rettighetene som finnes offline, også gjelder online. En oppfølgingsresolusjon ble vedtatt i 2014, der også spørsmål om retten til utdanning og styringsspørsmål ble tatt opp. Høykommissærens rapport *The right to privacy in the digital age* ble diskutert i et panel i september 2014 og presentert i FNs generalforsamlings tredje komité i oktober samme år. Debatten tok blant annet opp menneskerettighetenes ekstraterritorielle anvendelse.

7.8. Praksis fra andre land og internasjonale domstoler av særlig interesse

7.8.1. Innledning

Statens behov for å innhente informasjon til ivaretakelse av egen sikkerhet, reiser en rekke viktige problemstillinger sett fra et menneskeretts- og personvernperspektiv. Det er derfor etter utvalgets syn av relevans å se noe nærmere på hvordan dette har blitt håndtert i andre rettssystemer, også systemer som ikke er direkte rettslig bindende i Norge eller for norsk lovgivning.

Utvalget finner særlig grunn til å trekke frem EU-domstolens dom i saken *Digital Rights Ireland* om datalagringsdirektivet (DLD)[74] og *Privacy Shield*-avtalen mellom EU og USA.

7.8.2. EU-domstolens dom i *Digital Rights Ireland* (DLD-dommen)

Datalagringsdirektivet [75] (DLD) vekket stor samfunnsdebatt og direktivet ble til slutt kjent ugyldig av EU-domstolen den 8. april 2014. Utvalget mener man ikke kan drøfte DGF uten å se hen til hva som skjedde med DLD.

EU-domstolen kom til at DLD var i strid med EU-charteret artikkel 7 og 8 om retten til privatliv og retten til personvern, og gikk lenger enn unntaksadgangen i artikkel 52 åpner for. Det betyr i korte trekk at DLD ble ansett mer inngripende i retten til privatliv og personvern enn det som er nødvendig for å ivareta allmenne interesser eller andres rettigheter.

Det sentrale i dommen er etter utvalgets vurdering:

- Domstolen slo for det første fast at DLD tilfredsstilte vilkåret i artikkel 52 om mål av allmenn interesse (avsnitt 44). Selv om det i dag er mulig å benytte andre kommunikasjonsformer som ikke er lagringspliktige, betyr ikke det at tiltaket ikke

[72] *Guidelines governing the protection of privacy and transborder flows of personal data*. Retningslinjene ble opprinnelig fastsatt 23. september 1980, men ble revidert 11. juli 2013.

[73] http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

[74] Sak C-293/12 og C-594-12).

[75] Direktiv 2006/24/EF.

er formålstjenlig. Formålet om å bekjempe kriminalitet er reelt. Retten pekte særlig på behovet for å bekjempe organisert kriminalitet og terrorisme. Retten syntes å oppfatte det slik at DLDs regler har en negativ innvirkning, men ikke grunnleggende negativ innvirkning, på personvernet. Retten fant likevel at inngrepet i retten til privatliv og personvern gikk lenger enn hva som er nødvendig for å ivareta allmenne interesser eller andres rettigheter (avsnitt 69). Og fordi det i denne saken var et alvorlig inngrep i en viktig rettighet, foretok domstolen en inngående vurdering (avsnitt 48).

- Domstolen fremholdt at kampen mot alvorlig kriminalitet er viktig, men ikke slik at den kan berettige lagring slik DLD legger opp til. Inngrep i personvernet må begrenses til hva som er strengt nødvendig og følge av klare og presise regler. Reglene må gi personer som har fått sine kommunikasjonsdata lagret en minimumssikkerhet og tilstrekkelig garanti for en effektiv beskyttelse av dataene. Behovene er generelt større som følge av automatisk lagring og der det er reelle muligheter for ureglementert tilgang til dataene.

- Retten konstaterte at lagringsplikten er meget omfattende og gjelder hele befolkningen uten unntak (avsnitt 57-59). Lagringsplikten gjør ingen unntak for grupper som er underlagt lovpålagt taushetsplikt (advokater, leger etc.), og er ikke betinget av at dataene kan knyttes til en straffbar handling, eller er generert i en bestemt periode, i et bestemt område eller av bestemte personer. Dette representerer et inngrep i fundamentale rettigheter til hele Europas befolkning.

- Domstolen viste til at DLD mangler objektive kriterier for å begrense tilgang til og påfølgende bruk av dataene for nasjonale myndigheter ifm. forhindring, avsløring og bekjempelse av kriminalitet (avsnitt 60-62). Eneste føring ligger i henvisningen til «alvorlig kriminalitet», og det er overlatt til medlemsstatene å definere dette nærmere. DLD mangler også en nærmere angivelse av vilkårene for bruk som sikrer at dataene kun brukes til å bekjempe nærmere definerte former for alvorlig kriminalitet. Retten fremhevet dessuten som en svakhet at det ikke kreves at adgangen til dataene skal være underlagt domstolskontroll eller kontroll av et uavhengig forvaltningsorgan.

- For det tredje kritiserte domstolen den generelt utformede lagringstiden på minimum seks måneder og maksimum 24 måneder (avsnitt 63-64). DLD skiller ikke mellom ulike kategorier data basert på nytteverdien, verken for så vidt gjelder adgangen til å fastsette en kortere lagringsperiode enn seks måneder for enkelte typer data, eller innenfor spennet fra seks måneder til 24 måneder.

- Domstolen pekte på manglende datasikkerhet (avsnitt 66-67). Direktivet stiller ikke strenge nok krav til datasikkerhet. Domstolen ga på dette punktet uttrykk for bekymring for at direktivet åpner for at ekomtilbydere kan ta økonomiske hensyn når de avgjør sikkerhetsnivået. DLD sikrer heller ikke sletting når lagringstiden er ute. Dernest er det etter domstolens syn også problematisk at ikke DLD krever at data skal lagres innen EU slik at datasikkerheten kan kontrolleres av en uavhengig myndighet (avsnitt 68).

Dommen er i en utredning[76] til Samferdselsdepartementet sammenfattet slik:

«Som det fremgår av gjennomgangen ovenfor, pekte domstolen på en rekke forhold før de konkluderte med at direktivet var i strid med de grunnleggende rettighetene i artikkel 7 og 8 i EU-charteret. Ettersom domstolens konklusjon baserer seg på en helhetlig vurdering av disse forholdene, er det vanskelig å trekke sikre slutninger om hva som var utslagsgivende for domstolen. Dette medfører at det er uklart hvilke konkrete justeringer direktivet måtte være underlagt for at kravet til proporsjonalitet skulle blitt ansett oppfylt. Et sentralt punkt i EU-domstolens vurdering var at direktivet verken gir prosessuelle eller materielle regler om tilgang til og bruk av data. Ei heller oppstiller direktivet objektive vilkår for å sikre at tilgang og bruk skjer i tråd med prinsippene om nødvendighet og forholdsmessighet. Denne oppgaven overlates til nasjonale myndigheter. Dermed oppstår spørsmålet om de nasjonale datalagringslovgivningene kan utformes på en måte som medfører

[76] Se Hans Petter Graver og Henning Harborg: «Datalagring og menneskerettighetene – Utredning til Justisdepartementet og Samferdselsdepartementet» av 1. oktober 2015, tilgjengelig på www.regjeringen.no.

at unntaksvilkårene i EU-charteret artikkel 7 og 8 blir oppfylt. I en rekke land har den nasjonale lovgivningen som gjennomførte direktivet blitt underkjent. Sverige og Danmark, utgjør, som vi skal komme tilbake til, unntak fra denne tendensen. Foreløpig har ikke EU-domstolen tatt stilling til om noen av de nasjonale lovgivningene medfører brudd på artikkel 7 eller 8.»

Rekkevidden av dommen er ikke på alle punkter klar. I forbindelse med et søksmål i Sverige fra Tele2 Sverige mot Post- og telestyrelsen, har Kammarrätten i Stockholm forelagt flere spørsmål for EU-domstolen knyttet til gjennomføringen av DLD i svensk lovgivning. Generaladvokaten har nylig avgitt sin uttalelse i saken.[77] Generaladvokatens forslag til konklusjoner er disse:

«263. In light of the foregoing, I propose that the Court's answer to the question referred for a preliminary ruling by the Kammarrätten I Stockholm (Administrative Court of Appeal, Stockholm, Sweden) and the Court of Appeal (Emgland & Wales) (Civil Division) should be as follows:

Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector ('Directive on privacy and electronic communications'), as amended by Directive 2009/136/EC of the European Parliament and the Council of 25 November 2009, and Articles 7, 8 and 15(1) of the Charter of Fundamental Rights of the European Union are to be interpreted as not precluding Member States from imposing on providers of electronic communications services an obligation to retain all data relating to communications effected by the users of their services where all of the following conditions are satisfied, which it is for the referring courts to determine in the light of all the relevant characteristics of the national regimes at issue in the main proceedings:

- *the obligation and the safeguards which accompany it must be provided for in legislative or regulatory measures possessing the characteristics of accessibility, foreseeability, and adequate protection against arbitrary interference;*

- *the obligation and the safeguards which accompany it must observe the essence of the rights recognized by Articles 7 and 8 of the Charter of Fundamental Rights;*

- *the obligation must be strictly necessary in the fight against serious crime, which means that no other measure or combination of measures could be as effective in the fight against serious crime while at the same time interfering to a lesser extent with the rights enshrined in Directive 2002/58 and Articles 7 and 8 of the Charter of Fundamental Rights;*

- *the obligation must be accompanied by all the safeguards described by the Court in paragraphs 60 to 68 of its judgement of (April 2014 in Digital Rights Ireland and Others (C-293/12 and C-594/12, EU:C:2014:238) concerning access to the data, the period of retention and the protection and security of the data, in order to limit the interference with the rights enshrined in Directive 2002/58 and Articles 7 and 8 of the Charter of Fundamental Rights to what is strictly necessary; and*

- *the obligation must be proportionate, within a democratic society, to the objective of fighting serious crime, which means that the serious risks engendered by the obligation, in a democratic society, must not be disproportionate to the advantages which it offers in the fight against serious crime."*

EUs datalagringsdirektiv (DLD) medførte en opprivende debatt om balansen mellom sikkerhet og personvern, både i EU og i Norge.

Stortinget vedtok 15. april 2011 norske regler om datalagring for bekjempelse av alvorlig kriminalitet, og at DLD skulle innlemmes i EØS-avtalen. Etter EU-domstolens avgjørelse 8. april 2014 hvor DLD ble kjent ugyldig, besluttet regjeringen at den planlagte lovproposisjonen ikke skulle fremmes i vårsesjonen 2014. Den norske regulering om datalagring er derfor ikke satt i kraft. Det ligger utenfor utvalgets mandat å ta stilling til den norske implementeringslovgivningen knyttet til DLD. En del av de svakhetene EU-domstolen påpekte for DLD, gjør seg ikke gjeldende på samme måte for den norske lagringsloven. Dermed er heller ikke EU-domstolens avgjørelse noe prejudikat for at den norske lagringsloven ville ha vært i strid med de personvernreglene som gjelder som del av EØS-avtalen.[78]

Utvalget finner det uansett klart at det ikke kan legges til grunn at EU-domstolens avgjørelse om DLD

[77] http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEC%3A62015CC0203.

[78] Personverndirektivet 1995/46/EF og kommunikasjonsdirektivet 2002/58/EF.

innebærer at datalagring som ledd i overvåkingsprogrammer for utenlandsetterretningsformål også vil stride mot europeiske fundamentale rettigheter. Domstolen gir uttrykk for at datalagring for de formål som begrunnet DLD i seg selv ikke går på tvers av essensen i de grunnleggende regler om privatliv og beskyttelse av persondata. Domstolen slår fast at kampen mot terrorisme og alvorlig kriminalitet er «an object of general interest» og «a valuable tool for criminal investigations», og at hensynet til offentlig sikkerhet kan begrunne å ta i bruk moderne tekniske overvåkingsmetoder. Det kreves imidlertid at inngrepet er saklig avgrenset og undergitt klare og avgrensede regler for anvendelse. Videre kreves rettssikkerhetsgarantier og garantier mot misbruk.

Etter utvalgets vurdering får EU-domstolens avgjørelse således ingen direkte konsekvenser for inngripen i personvern og kommunikasjonsfrihet begrunnet i rikets sikkerhet (utenlandsetterretningsformål). Men avgjørelsen illustrerer viktigheten av tilstrekkelige presise avgrensninger, adekvate begrensninger og tiltak for å hindre formålsglidning. Utvalget mener at de prinsipper som EU-domstolen bygger på, må ivaretas ved innrettingen av DGF dersom det skal innføres.

7.8.3. *Privacy Shield*-avtalen mellom EU og USA

EU-domstolen konkluderte i en avgjørelse 6. oktober 2015 (i den såkalte Max Schrems-saken) med at EU-kommisjonens *Safe Harbour*-avtale med USA om fri overføring av personopplysninger til USA, var ugyldig. Domstolens avgjørelse bygget på et premiss om at USA ikke behandler personopplysninger på en forsvarlig måte. Begrunnelsen viste i stor grad til at dokumenter knyttet til Snowden, dokumenterer en uønsket masseovervåking fra NSAs side. Fra domstolens pressemelding av 6. oktober 2015 om avgjørelsen hitsettes:

«*As regards a level of protection essentially equivalent to the fundamental rights and freedoms guaranteed within the EU, the Court finds* that under EU law, legislation is not limited to what is strictly necessary where it authorizes, on a generalised basis, storage of all of the personnel data of all the persons *whose data is transferred from the EU to the United States* without any differentiation, limitation or exception being made *in light of the objective pursued and without an objective criterion being laid down for determining the limits of the access of the public authorities to the data and of its subsequent use. The Court adds that legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as* compromising the essence of the fundamental right to respect for private life.

Likewise, the Court observes that legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, compromises the essence of the fundamental rights to effective judicial protection, *the existence of such a possibility being inherent in the existence of* the rule of law.»

Etter til dels kompliserte forhandlinger mellom EU-kommisjonen og amerikanske myndigheter, ble det i en pressemelding fra EU-kommisjonen 2. februar 2016 opplyst om at partene var enige om en ny avtale (benevnt *The EU-US Privacy Shield*) for transatlantisk dataoverføring, som ivaretar EU-domstolens vilkår («requirements»). Detaljene i avtalen[79] ble offentliggjort 29. februar 2016. Det nye rammeverket ble formelt vedtatt av EU-kommisjonen 12. juli 2016[80] etter at det våren 2016 på initiativ fra europeiske datatilsyn bl.a. ble fremforhandlet bedre kontrollmekanismer. *Privacy Shield* trådte i kraft samme dag. Rammeverket er EØS-relevant og vil også gjelde for Norge.

I det nye avtaleverket legges det blant annet opp til nye krav til virksomheters håndtering av personopplysninger, regler for amerikanske myndigheters innsyn, en særskilt ombudsmannsordning, og etablering av en ny klagemekanisme.

Av relevans for DGF er særlig de spesielle krav som EU har lagt til grunn overfor amerikanske myndig-

[79] Avtalen må sees i sammenheng med EUs reformpakke knyttet til personvern (*data protection*), som består både av en forordning og et direktiv, samt med paraplyavtalen av 8. september 2015 knyttet til databeskyttelse for rettshåndhevingsformål (*Agreement between the US and EU on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses*).

[80] Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield. Rammeverket har syv annekser, hvorav særlig anneks VI er relevant for bulkaksess (brev 22. februar 2016 fra ONI General Councel Robert Litt).

heter når det gjelder begrensninger, rettssikkerhetstiltak («safeguards») og kontroll i forbindelse med amerikanske etterretningsorganisasjoners aksess til data og kommunikasjon. Et sentralt element for EU har vært at "*the US government has given the European Commission explicit assurance that the U.S. Intelligence Community 'does not engage in indiscriminate surveillance of anyone, including ordinary European citizens'*".[81] Det understrekes også at i de tilfeller hvor bulkinnsamling anses nødvendig, vil søk i lagrede data foregå målrettet.[82] EU-kommisjonen konkluderer med at avtalen med – og lovgivningen og etterretningspraksis i – USA «*conforms with the standard set out by the Court of Justice in the* Schrems *judgment, [..]*."[8384]

EU-kommisjonen må gjennom dette anses å mene at bulkinnsamling i seg selv ikke er i strid med grunnleggende rettsprinsipper, selv om det legges vekt på at «*bulk collection will only be authorised exceptionally where targeted collection is not feasible*».[85]

EU-kommisjonen fremhever at grunnleggende menneskerettskrav må ivaretas. Disse kan oppsummeres dithen at ethvert inngrep i personvernet til enkeltpersoner må være basert på klare og tilgjengelige regler, være nødvendig og forholdsmessig, være underlagt upartisk og effektiv kontroll, og gi den som mener seg krenket tilgang til effektive rettsmidler. Utvalgets vurderinger av DGF opp mot forannevnte prinsipper fremgår av kap. 9.5, hvor utvalget også foretar en særskilt analyse av DGF opp mot de prinsipper EU har lagt til grunn i tilknytning til *Privacy Shield*-avtaleverket.

Avtalen er blitt kritisert, også av europeiske datatilsynsmyndigheter, og det synes klart at det vil komme revisjoner av ordningen som vil fokusere på om håndhevelsen av tilstrekkelig. Det er også varslet at ordningen vil bli rettslig prøvet. Det gjenstår å se om det nye rammeverket og EU-kommisjonens beslutning vil bli utfordret rettslig overfor EU-domstolen og EMD, eventuelt hvilke elementer som vil bli prøvet, og hva utfallet i så fall vil bli.[86] Det er vanskelig å slå fast hvorledes ordningen vil bli vurdert av EU-domstolen eller EMD. Men de prinsipper og krav som EU-kommisjonen har lagt til grunn, bygger på menneskerettighetenes krav. Det er i så fall ikke kravene som vil bli skjerpet ved en eventuell ny domstolsprøving. Utvalget mener likevel det er relevant å se hen til hvilke elementer EU-kommisjonen har vektlagt.

7.8.4. Annen praksis

Det finnes en rekke uttalelser fra enkeltpersoner, eksempelvis spesialrapportører i FN-systemet, samt uttalelser fra nasjonale og internasjonale organisasjoner, herunder uttalelser fra EU-parlamentet, som har pekt på innvendinger av menneskeretts- og personvernrettlig karakter mot myndighetenes tilgang til digital kommunikasjon. I den senere tid har imidlertid statenes syn, statlige offentlige utredninger og parlamentariske debatter kommet mer på banen. I hovedsak har disse konkludert med at bulkaksess har vært lovlig og bør fortsette, og at tilgang til store datamengder i seg selv ikke innebærer ulovlig masseovervåkning.

Som vist ovenfor verserer det rettssaker anlagt mot myndighetene i flere land. Det er etter utvalgets syn ikke grunnlag for å si at praksis generelt underbygger at bulk aksess er ulovlig eller i strid med sentrale rettsprinsipper, men de nærmere vilkårene for slik aksess må vurderes nøye.

---

[81] Commission Implementing Decision para. 82.

[82] Commission Implementing Decision para. 81.

[83] Commission Implementing Decision para. 90.

[84] *EU-US Privacy Shield* forutsetter ikke avvikling av noen pågående utenlandsetterretningsprogrammer i USA, og forutsetter heller ingen endringer i amerikansk lovgivning. Dette underbygges av avtalens ordlyd, herunder annex VI som viser til de tiltak som allerede forelå på tidspunktet for EU-domstolens avgjørelse, blant annet gjennom det amerikanske SIGINT-direktivet (Presidential Policy Directive 28 av 17. januar 2014).

[85] Commission Implementing Decision para. 89.

[86] Utvalget har merket seg at EU-landenes nasjonale datatilsyn har avgitt en rådgivende uttalelse 13. april 2016 om Privacy Shield-avtalen i rammen av WP29 (Article 29 Data Protection Working Party), jf. også pressemelding fra WP29 1. juli 2016. Basert på denne uttalelsen samt EU-parlamentets resolusjon av 26. mai 2016 tok imidlertid EU-kommisjonen opp igjen forhandlingene med USA, hvilket bl.a. resulterte i «additional clarifications on bulk collection of data» (iht pressemelding fra EU-kommisjonen av 12. juli 2016) uten at disse klargjøringene endrer substansen i forhold til avtaleenigheten fra februar 2016. WP29 har varslet at de vil gjennomføre en koordinert analyse av rammeverket og publisere en ny uttalelse så snart som mulig, men har samtidig i pressemelding 26. juli 2016 varslet at de ikke vil utfordre rammeverket før den har fått virke i et år.

8. TEKNISKE LØSNINGER OG BEGRENSNINGER

8.1. Ekomnett og ekomtjenester i Norge

Norge har en godt utbygget telekommunikasjonsinfrastruktur bestående av tre kommersielt drevne mobilnettverk (Telenor, Telia og ICE), en rekke regionale netteiere, samt Telenor sitt landsdekkende kjernenett som bærer det alt vesentligste av den datatrafikken som går på tvers av regionene.[87] Alle andre leverandører av nettjenester til det sivile samfunn, slik som Nødnettet, Helsenettet og de mobiloperatørene som ikke eier egne basestasjoner, bruker denne generelle telekom-infrastrukturen som en plattform for å kunne levere sine egne tjenester.

For at vi i Norge skal kunne kommunisere med resten av verden, er vår struktur koblet sammen med utenlandske nettstrukturer på flere steder. Disse sammenkoblingene kan være kabelbasert, eller gå trådløst via satellitt. Den trafikken som går via satellitt utgjør en liten og minkende andel av den totale kommunikasjonen mellom Norge og utlandet. Dette er en av begrunnelsene E-tjenesten oppgir når de ber om at det legges til rette for at de får tilgang til kabelbasert kommunikasjon som krysser våre landegrenser.

Det finnes i størrelsesorden ett dusin veier for kabelbasert kommunikasjon inn i og ut av Norge. Det er tallmessig overvekt av landkabler, men det er også flere kabler som ligger i sjøbunnen. DGF, slik begrepet brukes i denne rapporten, består i å gi E-tjenesten mulighet til å lese datastrømmer som overføres på disse grensekryssende kablene.

I skrivende stund går mesteparten av kommunikasjonen med utlandet gjennom landkabler til Sverige.[88] Videre er det på nåværende tidspunkt svært lite datatrafikk som går igjennom Norge på sin vei mellom to andre land, slik at mesteparten av de datastrømmene som krysser vår yttergrense vil enten ha sitt opphav eller sitt endepunkt i Norge. Det foreligger flere initiativer for legging av ytterligere sjøkabler fra Norge til utlandet. Det er derfor grunn til å tro at vi får flere forbindelser mellom utenlandsk og norsk infrastruktur i løpet av noen år. Den beskrivelsen av grensekryssende trafikk som vi har gitt over, kan derfor gjennomgå betydelige endringer i løpet av kort tid.

8.2. Hvilken informasjon passerer gjennom innsamlingspunktene?

Et sentralt spørsmål i diskusjonen om DGF er knyttet til hvilken informasjon som sendes gjennom de kablene som krysser landegrensen, og som derfor vil kunne leses av de som har tilgang til etterretningsutstyret. Som nevnt over er det i øyeblikket lite datatrafikk som bruker Norge som transittland, slik at mesteparten av datatrafikken vil enten ha sin avsender eller sin mottaker i Norge, eller begge deler.

Telefonsamtaler, meldinger og e-poster som eksplisitt sendes mellom Norge og utlandet vil opplagt måtte krysse disse kablene. Likeledes vil de fleste forstå at svært mye av det man foretar seg på nettet også vil krysse landegrensene. Bruk av de fleste nettjenester som er eid og drevet av aktører som ikke er norske, vil derfor passere de samme kablene. Dette gjelder alle de vanligste søketjenestene, og de vanligste sosiale mediene.

Mindre intuitivt er det at svært mange kommunikasjonstjenester er laget på en slik måte at metadata, kommunikasjonsinnholdet eller begge deler går ut av landet og inn igjen selv om både avsender og mottaker av kommunikasjonen befinner seg i Norge. Dette gjelder epost dersom en av partene benytter en leverandør med mailserver i utlandet, det gjelder mobiltelefoni dersom en av partene har abonnement på noe annet enn Telenor sitt mobilnett, og det gjelder samtaletjenester som Skype, meldingstjenester som WhatsApp og bildedelingstjenester som Instagram.

I tillegg må nevnes at informasjon kan krysse landegrensen uten at en bruker naturlig vil oppfatte at hun eller han bedriver kommunikasjon. Bruk av skytjenester for backup av telefoner, og tjenester som gir brukeren samtidig tilgang til bilder og dokumenter på flere maskiner, blir stadig vanligere. Disse tjenestene vil svært ofte føre til at mye informasjon som ikke er tenkt kommunisert med noen, likevel vil krysse landegrensen.

[87] Dette bildet er i endring. Det finnes to andre nettoperatører, Broadnet og Altibox, som kontrollerer landsdekkende nettverk med mye av de samme kapasitetene som Telenor, men som ikke har den samme nasjonale viktighet. Se NOU 2015:13 *Digital sårbarhet – sikkert samfunn*.

[88] http://www.tu.no/artikler/80-prosent-av-norsk-nett-trafikk-gar-gjennom-svenske-kabler/233824

Andelen av digital aktivitet som kun gjelder personer som befinner seg i Norge, men som likevel krysser landegrensen er derfor høy og økende. Det er to trender som påvirker dette:

- Globale tjenesteleverandører produserer oftest tjenestene sine utenfor Norge. Noen av disse har økende betydning for kommunikasjon innad i Norge gjennom en økende markedsandel her i landet. Denne markedsandelen vinner de enten ved å tilby en egen proprietær tjeneste (slik som Skype, iMessage eller skytjenester for lagring og backup), eller ved at de tilbyr en standardisert tjeneste, som f.eks. epost, i sin egen sky-infrastruktur utenfor Norges grenser.
- Nasjonale tjenesteleverandører legger deler av produksjonen sin til utlandet, bl.a. av kostnadsgrunner.

Det foreligger ingen tegn til at disse trendene vil snu. Utvalget legger derfor til grunn for arbeidet at en stor og økende andel av den elektroniske aktiviteten som kun er ment å involvere personer i Norge, likevel vil passere utstyret for DGF. Videre legger utvalget til grunn at det vil forbli vanskelig for den jevne borger å vurdere hvilke deler av den elektroniske kommunikasjonen de deltar i som vil gå igjennom det samme utstyret.

8.3. Konsekvenser av økende kryptering

Kryptografi brukes for å støtte opp under konfidensialitet, autentisitet og identitet. I diskusjonen knyttet til DGF er det den økende bruken av kryptering for konfidensialitet som er viktig.

Det er stor variasjon i hvilken grad forskjellige kommunikasjonstjenester benytter seg av kryptering. Den raske endringstakten innen kommunikasjonstjenester så vel som kryptobruk gjør det lite hensiktsmessig å gi en samlet oversikt. Alle kommunikasjonsstrømmer faller imidlertid i en av tre kategorier:

- Ukryptert kommunikasjon.
- Kommunikasjon som er kryptert med mekanismer som man vet lar seg forsere, og hvor metodene for å gjøre dette er tilgjengelig på nettet.
- Kommunikasjon som er kryptert med mekanismer for hvilke det ikke er offentlig kjent hvorvidt en ressurssterk etterretningstjeneste er i stand til å forsere dem. Slik forsering kan skje ved at tjenesten har tilgang til krypteringsnøkler, eller ved at koder knekkes med bruk av datamaskiner.

Etter Snowden-saken har det vært en markert reduksjon av tjenester som faller i de to første av disse kategoriene, og en tilsvarende økning i tjenester som ligger i den siste kategorien.

Flere offentlige diskusjoner, hendelser og dokumenter peker i retning av at bruk av moderne og sterke krypteringsmekanismer er utfordrende, selv for ressurssterke etterretningstjenester. Eksempler på dette er at sentrale politikere i NATO-land har tatt til orde for at bruk av sterk kryptering bør underlegges regulering[89], at FBI ber Apple om hjelp til å lese innholdet på en Iphone[90], samt innholdet i dokumenter knyttet til Snowden.[91] Vi må derfor anta at en betydelig andel utbredte krypteringsmetoder nå ikke kan forseres. DGF vil derfor ikke gi E-tjenesten tilgang til innholdet i all kommunikasjon som krysser grensen. Tilgangen vil variere med graden av kryptering som kommunikasjonstjenestene benytter, og med hvilken evne til kryptoforsering som E-tjenesten til enhver tid besitter. Det er grunn til å anta at den tiltagende bruken av sterk kryptering vil fortsette. Dette vil påvirke den verdien E-tjenesten har av å kunne avlytte kommunikasjonen ved riksgrensen.

I tillegg til økt kryptering i sluttbrukerutstyret, kan det forventes å bli mer vanlig at nettoperatørene selv krypterer all trafikk som krysser landegrensene. Dette omtales gjerne som linkkryptering eller kryptering på lag 2. Linkkryptering er positivt for nettenes sikkerhet, men vil langt på vei forhindre en effektiv bruk av DGF. Tilretteleggingsplikten for teletilbyderne må derfor omfatte leveranse av datastrøm uten linkkryptering dersom dette er implementert på den grensekryssende forbindelsen. Tilretteleggingsplikten bør imidlertid ikke inneholde krav om støtte til omgåelse av krypto utover dette. F.eks. vil brukergenerert kryptering ikke være omfattet av tilretteleggingsplikten. For øvrig viser utvalget til kap. 9.5.4 om tilretteleggingsplikten.

[89] http://www.theguardian.com/uk-news/2015/jan/15/david-cameron-ask-us-barack-obama-help-tracking-islamist-extremists-online.

[90] http://www.vox.com/2016/2/17/11037748/fbi-apple-san-bernardino.

[91] Glenn Greenwald: *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (2014)

8.4. Hvordan kan informasjonstilfanget i DGF begrenses?

8.4.1. Innledning

Volumet av informasjon som vil kunne plukkes opp av overvåkingsutstyr plassert på de kablene som krysser landegrensen er stor, og det er problematisk å gi E-tjenesten uregulert tilgang til hele trafikktilfanget. Dette er det tre grunner til:

- Det er en svært liten andel av datatrafikken som er relevant for E-tjenestens samfunnsoppdrag.
- Juridiske forholdsmessighetsvurderinger avgjør om tiltaket er i henhold til Grunnloven, internasjonale menneskerettigheter og personvernlovgivning. Disse vurderingene vil avhenge av hvilke datastrømmer E-tjenesten får tilgang til. Uregulert tilgang til hele trafikktilfanget vil vanskelig kunne anses som forholdsmessig.
- Det bør legges til rette for at offentligheten får en godt begrunnet tillit til at DGF ikke kan benyttes til masseovervåkning av norske borgere.

Dette tilsier at mye av trafikken bør filtreres ut før den gjøres tilgjengelig for etterretningsformål. Videre kan det tilsi at det bør ligge begrensninger på hvordan den trafikken som blir gjort tilgjengelig for E-tjenesten kan tillates benyttet. Det er to forskjellige former for teknologiske begrensninger man kunne tenke seg å legge inn:

- Det kan være begrensninger på hvilke data fra datastrømmene som skal kunne tas vare på i et lager. Dette blir gjerne implementert ved hjelp av et logisk filter.
- Det kan være begrensninger på hvordan, og av hvem, lagrede data kan benyttes.

8.4.2. Filtrering

Ideelt sett ville man ønske seg maskinell filtrering som kun ga E-tjenesten tilgang til relevant og forholdsmessig tilpasset informasjon. Forskjellige tilnærminger til dette diskuteres under. Som et gjennomgående eksempel tar vi for oss i hvilken grad man teknologisk vil kunne sikre at kommunikasjon mellom to norske borgere ikke kan gjøres til gjenstand for overvåkning. Dette er ikke den eneste filtreringsproblematikken som ligger i DGF, men det er et representativt og lett forståelig eksempel på informasjon som krysser grensen og som ligger utenfor E-tjenesten sitt arbeidsområde.

En metode for filtrering består i at man spesifiserer hva som filtreres vekk. Informasjon som ikke maskinelt gjenkjennes som noe som skal filtreres vekk vil gjøres tilgjengelig for bruk. Eksempelvis vil man i vårt tilfelle ønske å filtrere ut kommunikasjon mellom to norske statsborgere som begge befinner seg i Norge. For enkelte kommunikasjonstjenester – slik som standard telefoni og SMS – vil dette la seg gjøre. For de fremvoksende IP-baserte tjenestene vil dette være langt vanskeligere. Det vil i mange tilfeller kreve oppbygging av et register over brukernavn knyttet til norske borgere på hver av de forskjellige tjenestene. Styrken ved slik negativ filtrering er at det er lite etterretningspotensiale som går tapt selv ikke når nye kommunikasjonsplattformer dukker opp, Svakheten er at de grensene man setter for hvilken informasjon E-tjenesten skal ha tilgang til, vil bli utfordret av de samme nye kommunikasjonsplattformene. For hver ny tjeneste vil det måtte bygges opp nye registre over hvilke brukere som er norske borgere.

Ved positiv filtrering vil man på forhånd spesifisere hva som skal tillates benyttet til etterretningsformål. Alle datastrømmer som ikke maskinelt gjenkjennes som noe som skal tas vare på, blir da filtrert vekk. Positiv filtrering vil her bety at man måtte identifisere hvilke utvalgte utenlandske brukere som er av interesse. Dette vil redusere den etterretningsmessige nytten av DGF, da man mister muligheten til å gjennomgå historien til en person eller organisasjon som plutselig fremstår som etterretningsmessig viktig. Det begrenser for øvrig etterretning til kun kjente trusler og umuliggjør målutvikling og avdekking av nye trusler. Styrken til positiv filtrering er at de begrensningene man setter for DGF ikke blir utfordret av teknologisk utvikling. Til gjengjeld vil den etterretningsmessige verdien av DGF bli utfordret av den samme utviklingen.

Forskjellen i positiv og negativ filtrering kommer til syne når det er en del av datatilfanget som verken kan defineres som klart relevant eller klart irrelevant. For DGF ligger mye av det etterretningsmessige potensialet gjemt i informasjon som faller i denne ikke definerbare kategorien. Det er derfor ikke praktisk mulig å lage fullt automatiserte filtre som verken reduserer den etterretningsmessige verdien av DGF eller gir E-tjenesten tilgang på informasjon som ligger utenfor dens virkeområde.

8.4.3. Begrensninger på søk i innsamlet materiale

Av diskusjonen over følger det at filtrering alene ikke løser alle problemer knyttet til DGF. Dersom man bygger opp et datasett over historisk grensekryssende trafikk, vil dette datasettet uvegerlig in-

neholde en andel data som klart faller utenfor E-tjenesten sitt arbeidsområde. Teknologisk vil dette kunne løses ved å legge begrensninger på hvilke søk man kan gjøre i dette materialet. Selv om teknologiske hindre for uønskede søk er mulige, har de en svakere tillitsskapende effekt enn begrensninger på hva som lagres i utgangspunktet. Tilliten til begrensninger på søk i innsamlet materiale må derfor hvile på menneskelige kontrollmekanismer i kombinasjon med teknologiske begrensninger.

8.5. Forholdet mellom utstyrskapasitet og formålet med DGF

I senere tid har omfanget av elektronisk informasjon eksplodert. Samtidig har strukturen i telenettene endret seg, slik at man ved å avlytte noen få punkter får tilgang til svært mye av trafikken. Likeledes har utstyret for lagring og søk vært gjennom en rivende utvikling. Det er nå innenfor teknologisk og økonomisk rekkevidde å fortløpende lagre alle telefonsamtaler og all skrevet tekst i et land.

De fiberkablene som krysser landegrensene er et av de punktene som samler svært mye av den elektroniske kommunikasjonen i landet. Ovenfor er redegjort for at det bare er en liten andel av denne trafikken som er relevant for E-tjenesten. Likeledes diskuterte vi hvordan man kunne filtrere ut den trafikken som ikke faller inn under E-tjenesten sitt virkeområde. Den diskusjonen var i sin helhet begrunnet i ønsket om å begrense E-tjenesten sitt innsyn. Det er i liten grad teknologisk kapasitet for lagring og søk som legger begrensninger på hvilken informasjon som kan tas vare på i DGF. De teknologiske kapasitetsbegrensningene som fremdeles gjenstår, vil bli ytterligere redusert i løpet av noen år. Den eneste reelle teknologibegrensningen knyttet til overvåkning av kabler som krysser riksgrensen, ligger i E-tjenestens sin evne til kryptoforsering. Den evne de har eller ikke har til dette vil imidlertid alltid være gradert. Hvilke krypteringsmekanismer som kan eller ikke kan knekkes, er således lite egnet som en tillitsskapende grensedragning sett fra befolkningens side.

E-tjenesten har intet ønske om å drive masseovervåkning. En må likevel legge til grunn at det utstyret som eventuelt vil brukes til DGF, vil ha teknologisk kapasitet til å gjøre nettopp dette. Videre vil det relativt enkelt kunne tilpasses til en slik oppgave. De tillitsskapende hindre som må legges i veien for masseovervåkning, vil derfor ikke kunne være av ren teknologisk art. De vil måtte bestå av teknologiske filtreringsmekanismer som er underlagt menneskebasert, uavhengig og effektiv kontroll.

9. UTVALGETS VURDERINGER

9.1. Innledning

Utvalget har gjennom sitt arbeid fått forståelse for at DGF vil være nødvendig for at E-tjenesten fortsatt skal ivareta sitt samfunnsoppdrag. DGF kan utformes på mange ulike måter, både teknisk og juridisk. Utvalget anser samtidig at DGF i sin natur vil være sterkt personverninngripende og at et demokratisk samfunn som Norge må vektlegge en eventuell innføring på en måte som gjør at grunnleggende hensyn som at befolkningens tillit til myndighetene ikke svekkes, og at det i minst mulig grad oppstår noen nedkjølingseffekt på den offentlige debatt og informasjonssøken. I lys av slike grunnleggende hensyn har utvalget diskutert ulike innretninger av et mulig DGF med E-tjenesten. Det DGF som utvalget har vurdert er vesentlig annerledes enn hvordan DGF ville ha vært om man kun skulle ta etterretningsfaglige hensyn, og har bl.a. av personvernhensyn en sterk grad av tekniske og prosessuelle begrensninger, juridiske skranker og kontrollmekanismer.

Utvalget vurderer altså at en rekke tiltak og vilkår bør være på plass, dersom DGF skal iverksettes. Det er avgjørende at tiltakene samlet sett er troverdige, og at ordningene på en betryggende måte ivaretar både hensynet til E-tjenestens oppgaveløsning og hensynet til personvern og kommunikasjonsvern. Det er kun på den måten at folk flest kan ha tillit til at DGF ikke vil innebære at E-tjenesten, verken lovlig eller ulovlig (ved misbruk), vil lese sms'ene, e-postene eller facebookmeldingene deres eller hvilke nettsider de surfer på. Risiko for misbruk må innenfor rimelighetens grenser reduseres til det usannsynlige.

Fire sentrale prinsipper som utvalget legger til grunn i denne sammenheng, er formålsavgrensning, minimalisering, autorisasjon og kontroll. *Formålsavgrensning* innebærer at data samlet inn for ett formål ikke skal kunne anvendes for et helt annet formål. *Minimalisering* innebærer å samle inn tilstrekkelige og nødvendige data for det formål eller den oppgave som foreligger, og samtidig unnta, begrense tilgang til eller sortere bort eventuell ikke-relevant eller overskytende informasjon. *Autorisasjon* innebærer i denne sammenheng at bruk av inngripende metoder krever prøving og forhåndsgodkjenning fra (uavhengig) kompetent myndighet. *Kontroll* innebærer uavhengige og effektive mekanismer som etterprøver om de begrensninger som følger av de øvrige tre prinsippene etterleves i praksis. Kontrollen kan skje samtidig eller etterfølgende, eller begge deler.

Under beskrives først oppsett av et mulig DGF-system som ligger til grunn for utvalgets vurderinger (kap. 9.2-9.4). Dernest beskrives utvalgets vurderinger (kap. 9.5).

9.2. Et mulig DGF-system med kontrollmekanismer

9.2.1. Innledning

Her introduseres de viktigste begrepene knyttet til hvordan DGF-systemet konseptuelt kan implementeres. Disse begrepene knyttes til kontrollmekanismene så vel som de tekniske løsningene.

9.2.2. Kontrollmekanismer

Kontroll av hvordan den tekniske installasjonen tillates benyttet, består av tre hovedelementer:

- **DGF-domstol***:* Enkelte operasjonselementer for DGF er egnet for å legges inn under et regime med *forhåndsgodkjenninger*. Dette er elementer som typisk endrer seg med lav hyppighet, og som kan beskrives i termer som ikke krever dyp teknologisk innsikt. Disse forhåndsgodkjenningene foreslås å legges til en domstol.

- **DGF-tilsyn***:* De delene av DGF som ikke er egnet for forhåndsgodkjenninger, bør *kontinuerlig overvåkes* av et tilsynsregime. DGF-tilsynet skal ha en kontinuerlig tilstedeværelse i DGF-systemet, og de skal ha fullt innsyn i alt som skjer der. De skal føre tilsyn med at virksomheten drives i henhold til lov, avgjørelsene fra DGF-domstolen og E-tjenesten sine interne retningslinjer.

- **EOS-utvalget***: Etterhåndskontroll* av de hemmelige tjenestene foregår allerede i dag i regi av EOS-utvalget. Denne rollen vil EOS-utvalget ha også for bruk av DGF. De vil motta rapporter fra DGF-tilsynet, og ha oversyn med hvordan E-tjenesten utøver bruken av DGF samt hvorledes Forsvarsdepartementet styrer E-tjenesten sin bruk av DGF.

9.2.3. Overordnet beskrivelse av DGF

En overordnet skjematisk tegning av DGF-systemet er som tegnet under.

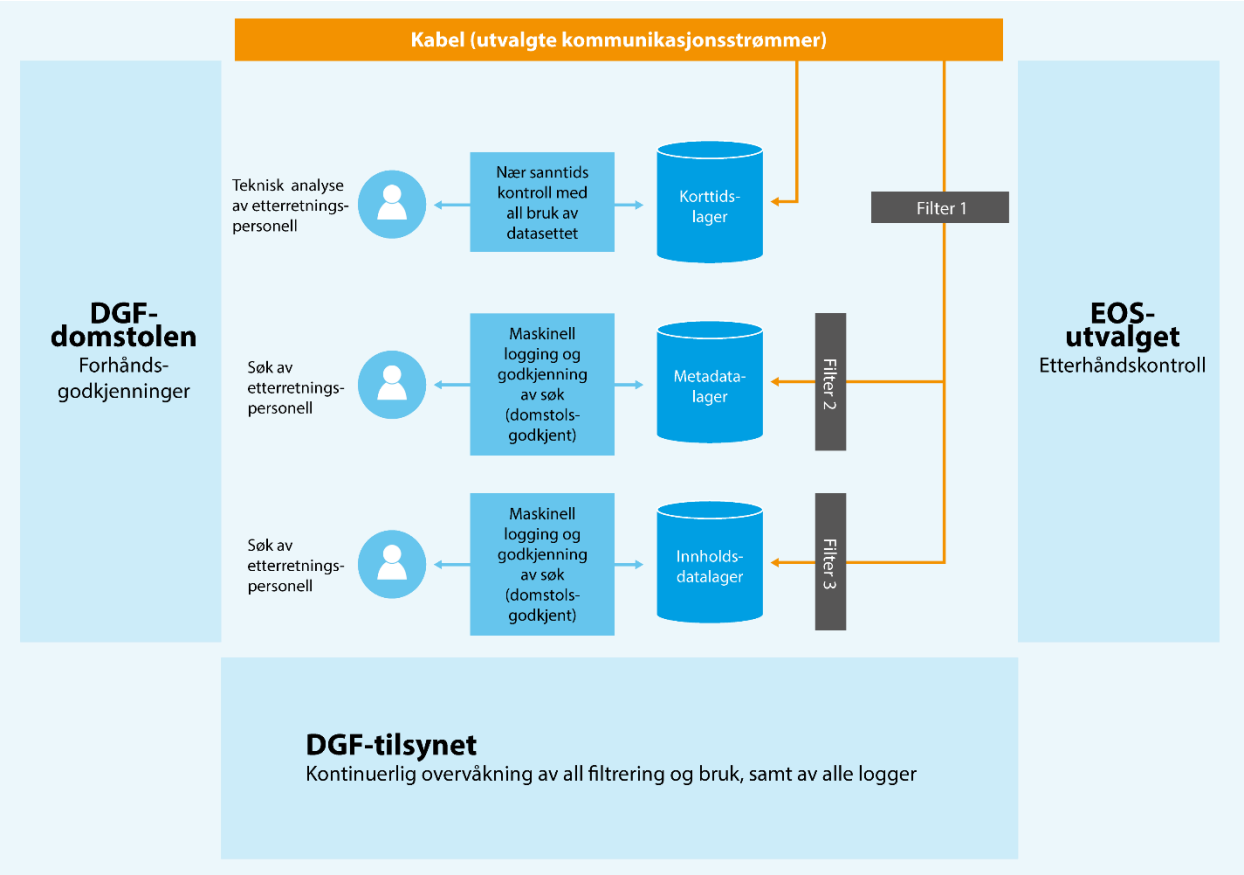

Fig. 2. Overordnet beskrivelse av DGF.

Som det fremgår av figuren, består systemet av tre forskjellige datasett som det kan gjøres søk i. Disse beskrives kort under og mer utfyllende i kap. 9.2.5.

- **Korttidslageret** inneholder et uttrekk av ufiltrert kommunikasjon som har gått over den fiberoptiske kabelen i løpet av den siste 14-dagers perioden. Dette er ikke et kontinuerlig bilde av all datatrafikk, men svært korte tidsintervaller som vil inneholde både metadata og innholdsdata. Dette lageret brukes utelukkende til teknisk vedlikeholdsarbeid av filtrene, og aldri til søk for etterretningsproduksjonsformål.

- **Metadatalageret** inneholder metadata fra utvalgte protokoller knyttet til utvalgte kommunikasjonstjenester. Så langt det er teknisk og praktisk mulig vil metadata som ikke er relevant for E-tjenestens samfunnsoppdrag, filtreres bort i Filter 1 og Filter 2. Man kan likevel ikke anta at alle irrelevante data lar seg filtrere bort. Søk i metadatalageret vil kun baseres på personselektorer knyttet til personer som DGF-domstolen har godkjent innhenting mot, eller modusselektorer knyttet til parametere som DGF-domstolen har forhåndsgodkjent.

- **Lageret med spesifiserte innholdsdata** vil inneholde fullstendige datastrømmer – også med innholdsdata – knyttet til kommunikasjon tilknyttet objekter (personselektorer) som er godkjent av DGF-domstolen. Disse datastrømmene plukkes ut av Filter 3.

9.2.4. Filtrene

De tre filtrene i figuren vil ha forskjellige oppgaver. Videre vil teknologiske egenskaper ved kommunikasjonsprotokollene sette begrensninger for hvor

effektive de vil kunne være. En kort sammenfatning av filtrenes oppgaver og i hvilken grad de fullt ut vil kunne oppfylle sine oppgaver, er som følger:

- **Filter 1** har som hovedoppgave å redusere mengden av data som flyter inn i systemet. Dette gjøres ved å dynamisk velge hvilke kabler/fibre/kommunikasjonsbærere man til enhver tid ser på, og ved å foreta filtrering av trafikk som enkelt lar seg identifisere som utenfor E-tjenestens oppdrag eller interesseområde. Oppgaven med å redusere den totale informasjonsmengden er teknologisk overkommelig. Filtrering av informasjon som ligger utenfor E-tjenestens samfunnsoppdrag er imidlertid komplekst, og vil i hovedsak bli overlatt til Filter 2. Filtrering i Filter 1 vil i stor grad skje gjennom negativ filtrering, ved at man identifiserer hva som filtreres bort. Nye kommunikasjonsformer som ikke tidligere er identifisert, vil derfor slippe gjennom dette filteret.

  Etter dialog med tjenestetilbydere velges det ut kun relevante kommunikasjonsbærere, basert på forutgående teknisk profilering av datatrafikk. Dette er bærere som formodes å inneholde en stor eller viktig andel utenlandstrafikk. Ingen fiber som kun inneholder norsk-norsk kommunikasjon velges ut. Hvor mye norsk-norsk trafikk som filtreres vekk i denne første fasen, avhenger av hvordan tjenestetilbyderen har organisert nettverket sitt.

  Filter 1 vil også kunne være et sted å plassere filtreringsfunksjoner som har til hensikt å filtrere ut kommunikasjon som opplagt ikke er innenfor E-tjenesten sitt virkeområde. Dette kan være norsk-norsk kommunikasjon som filtreres ut basert på et IP-adresse filter (f.eks. basert på geolokalisering av slike adresser), eller annen trafikk som ikke er relevant for E-tjenesten, som f.eks. trafikk fra store streamingtjenester. Slik filtrering bør gjøres så langt det er teknisk mulig. Det vises til kap. 8.4 for en nærmere diskusjon av tekniske utfordringer knyttet til dette.

- **Filter 2** har som oppgave å filtrere bort alle innholdsdata. Videre skal det i størst mulig grad filtrere ut metadata som ligger utenfor E-tjenesten sitt samfunnsoppdrag. Filtrering av innholdsdata er teknologisk overkommelig. Fullstendig filtrering av metadata fra kommunikasjon som ligger utenfor E-tjenesten sitt samfunnsoppdrag er imidlertid urealistisk. Først fordi det å definere hvilke kommunikasjoner som senere vil vise seg å ligge innenfor samfunnsoppdraget, er umulig. Dernest er det slik at selv kommunikasjon som opplagt ligger utenfor – slik som kommunikasjon mellom to nordmenn som begge befinner seg i Norge – for mange kommunikasjonsplattformer vil være teknisk og ressursmessig krevende å filtrere bort, som drøftet i kap. 8.4. Metadatalageret vil derfor inneholde betydelig informasjon om kommunikasjon mellom nordmenn som på kommunikasjonstidspunktet befant seg i Norge.

  Det kan i enkelte tilfeller være vanskelig å skille mellom hva som er metadata og hva som kan anses å være innholdsdata. Eksempelvis vil en epost, i tillegg til avsender, mottaker og tidspunkt, også inneholde et felt for emne eller «subject». Dette feltet vil kunne sammenlignes med overskriften i et brev, og vil finnes typisk på innsiden av konvolutten. Selv om dette er et felt som beskriver innholdet, så vil dette måtte betraktes som en del av innholdet. Et annet eksempel er en web-adresse eller en URL. Dette er en adresse og i utgangspunktet metadata. Samtidig vil en webadresse kunne si mye mer om innholdet enn en fysisk adresse. En URL vil også typisk kunne inneholde informasjon fra felter som brukeren har fylt ut på et nettsted, som for eksempel et søkefelt. I forbindelse med DGF vil det være behov for å identifisere og regulere slike tvilstilfeller, og vedlikeholde en liste over den type metadata som skal kunne lagres. Listen bør være gjenstand for periodisk etterhåndskontroll av EOS-utvalget, samt kontinuerlig tilsyn fra DGF-tilsynet.

- **Filter 3** har som oppgave å slippe gjennom kun innholdsdata fra kommunikasjonsstrømmer knyttet til objekter som er godkjent av DGF-domstolen. Dette kan gjøres med høy nøyaktighet, og med overkommelig ressursinnsats.

9.2.5. Datalagrene

Her går vi nærmere inn på hvordan selve datalagrene kan tenkes strukturert og benyttet.

Korttidslageret inneholder korte tidsintervaller med ufiltrert informasjon som har gått over den fiberoptiske kabelen. Intervallene bør normalt ikke være lengre enn ett minutt, det bør legges restriksjoner på hvor hyppig innsamlingsintervallene kommer, og ingen av dataene bør ligge lenger enn 14

dager. Dette lageret er helt nødvendig for å kunne drive kontinuerlig teknologisk oppdatering av filtrene i systemet. Uten dette lageret må man anta at kvaliteten på Filter 1 og Filter 2 vil bli vesentlig svekket. Det er derfor lite ønskelig å ha DGF uten dette korttidslageret. Det er nødvendig å mellomlagre data for i det hele tatt å kunne gjøre et fornuftig utvalg av kommunikasjonsbærere, herunder forstå hva slags kommunikasjon som går på bæreren, samt for å (videre)utvikle filtrerings- og seleksjonsmekanismen i DGF og etterfølgende re-prosessering.

Til gjengjeld må det legges meget sterke begrensninger på hvordan dette lageret kan benyttes. Det er viktig at det ikke åpnes for annen bruk av disse dataene enn til å studere hvordan filtrene kan optimaliseres. Korttidslageret vil måtte behandles av mennesker (ikke bare datamaskiner), og gruppen mennesker som har tilgang må være liten. Det må utvikles tydelige retningslinjer for hvordan datasettet kan samles inn og brukes, og DGF-tilsynet må ha som oppdrag å ettergå dette, herunder kontrollere i nær sanntid at all bruk av datasettet er i henhold til retningslinjene. I tillegg bør alle filteroppdateringer som kommer som et resultat av dette arbeidet gå til DGF-tilsynet. DGF-tilsynet bør rapportere periodisk til EOS-utvalget om hvordan korttidslageret er benyttet, og hvilke filteroppdateringer det har ført til. EOS-utvalget må ha god kompetanse til å forstå detaljene i søk og filtrering.

Representanter fra E-tjenesten har i møter med utvalget fremført at tjenesten ideelt sett ville ønske at korttidslageret kunne benyttes retrospektivt for etterretningsformål, særlig i etterkant av konkrete hendelser og trusler. Utvalget mener imidlertid at dette ikke bør tillates, fordi dette vil medføre lagring av større mengder ufiltrert informasjon i lageret enn det som er nødvendig for teknisk seleksjon og filtrering, samt risiko for omgåelse av de begrensninger og forhåndsautorisasjonsmekanismer som utvalget ellers foreslår.

Metadatalageret er prinsipielt sett en utfordrende del av DGF-konstruksjonen. Metadatalageret bærer en betydelig del av den etterretningsmessige verdien av hele DGF-konseptet. Samtidig er det vanskelig å gjøre fullgod filtrering av metadata som ikke er relevant for E-tjenesten sitt oppdrag. Effektiv kontroll med bruken av metadata må derfor bygge på begrensninger på søk i metadatalageret. Det vises til kap. 9.2.2 ovenfor samt nedenfor under kap. 9.3 om detaljene i hvordan slik kontroll kan bygges. Også for kontroll med bruken av metadatalageret er det en forutsetning at EOS-utvalget har god kompetanse til å forstå tekniske detaljer knyttet til søk og filtrering. Metadata vil bli lagret i så lang tid som anses nødvendig for å løse etterretningsoppdraget til E-tjenesten, og maksimalt i 18 måneder. En lagringstid på 18 måneder er av utvalget vurdert å være nødvendig og tilstrekkelig for å kunne gjennomføre en tilfredsstillende retrospektiv trafikkdataanalyse.

Lageret med spesifiserte innholdsdata (innholdsdatalageret) er det minst problematiske sett fra et personvern- og menneskerettighetsståsted. De kommunikasjonsstrømmene som ligger der er godkjent av en domstol, og det er teknologisk og ressursmessig overkommelig å sørge for at lageret ikke inneholder annet enn det som er godkjent av domstolen. Utvalget mener at DGF-tilsynet må ha innsyn i avgjørelsene fra domstolen og i utformingen av filteret. På den måten kan de kontrollere i hvilken grad lageret kun inneholder data innenfor den rammen som er gitt av domstolen. Videre må tilsynet ha innsyn i alle søk som gjøres her. Tilsynet rapporterer jevnlig til EOS-utvalget om hvordan innholdsdatabasen benyttes, og hvordan beslutningene i domstolen omsettes i filtreringsmekanismer. Igjen er det viktig at EOS-utvalget har god kompetanse til å forstå tekniske detaljer knyttet til søk og filtrering. Innholdsdata vil kun bli lagret i så lang tid som anses nødvendig for å løse etterretningsoppdraget til E-tjenesten.

9.2.6. Maskinell logging og godkjenning av søk i metadatalageret

Det fremgår over at lageret med metadata krever streng kontroll med hvilke søk som kan tillates. Utvalget vil anbefale at kontrollen med dette gjøres på en måte som er illustrert i følgende figur:

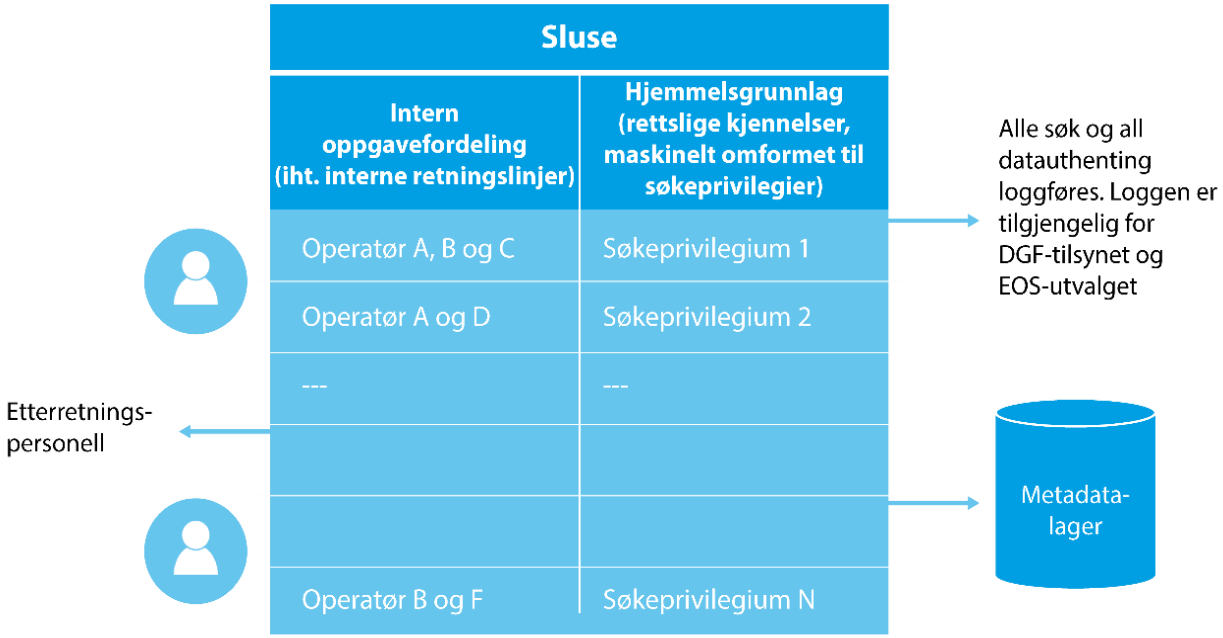

Fig 3. Maskinell logging og godkjenning av søk i metadatalageret.

Hvert søk i metadatalagret som gjøres av en DGF-operatør må gå igjennom en sluse. Denne slusen har to funksjoner. Den første er å logge søket og resultatet av søket, slik at søkene kan føres tilsyn med av DGF-tilsynet (og ved behov av EOS-utvalget). Den andre er å gjøre en maskinell sjekk på om søket er hjemlet i lov, rettsavgjørelse og retningslinjer. Dersom søket ikke er hjemlet, skal slusen avvise søket. Det må treffes nødvendige tiltak for å sikre loggens autentitet.

Rettsavgjørelsene oversettes til maskinelt definerte søkeprivilegier. Disse søkeprivilegiene skal føre til at ikke-hjemlede søk blir maskinelt avvist. Hvilken operatør som skal ha tilgang til hvilket søkekriterium bestemmes av E-tjenesten, og baserer seg på tjenesten sin eksisterende praksis med at informasjonstilgang er avhengig av hvilken oppgave hver enkelt operatør er satt til å arbeide med.

Spesielt for metadatalageret bør hvert søk være hjemlet i en rettsavgjørelse. Denne avgjørelsen baseres på en ny lovhjemmel for DGF og tilhørende søk, og må inneholde minst ett av følgende elementer:

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

Bruk av modusselektorer er aktuelt i målutviklingsøyemed. Prinsipielt sett kan målutvikling skje i forhold til både kjente og ukjente personer, med kjent og ukjent modus. Skjematisk kan dette fremstilles slik:

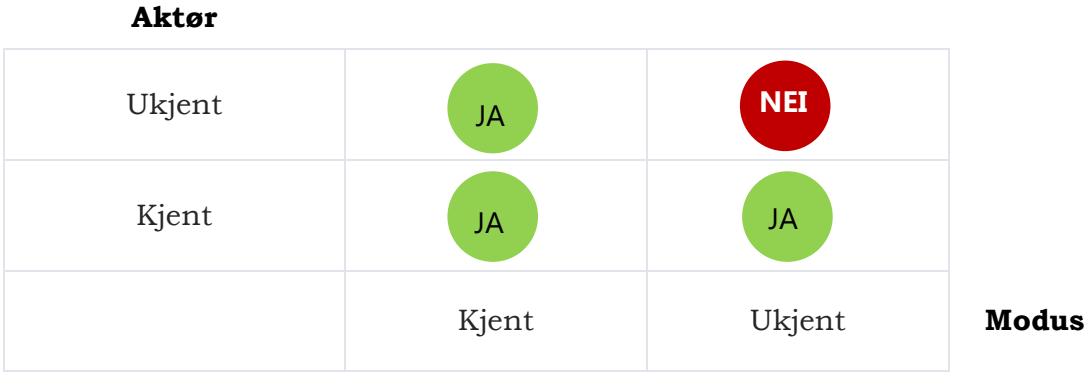

Fig. 4. Målutviklingskategorier.

Utvalget har kommet til at søk i metadatalageret bør ta utgangspunkt i enten en kjent aktør (f.eks. ansatte i en utenlandsk etterretningsorganisasjon) eller et kjent modus (f.eks. kommunikasjonsparametre som terrorister er kjent for å benytte). Søk i lageret basert på muligheten for å tilfeldig oppdage anomalier, hvor både aktør og modus er ukjent, fremstår for utvalget som grovkornet og grensende mot det vilkårlige. Kriteriene for en domstolsbehandling av slike søk blir svært vanskelig å utforme, og avgrensning av søk for å tilfredsstille forholdsmessighet blir vanskelig. Utvalget mener derfor at slike søk ikke bør tillates.

Kontrollen med hvilke søk som tillates, er mest kritisk for metadatalageret. Likevel mener utvalget at en tilsvarende funksjonalitet skal implementeres i alle lagrene. For korttidslageret og innholdsdatalageret er det ikke hensiktsmessig at søkeprivilegiene er hjemlet i selve rettsavgjørelsen. For disse lagrene bør privilegiene bygges i henhold til interne retningslinjer, og i størst mulig grad begrenses i henhold til hvilken funksjon disse lagrene er ment å understøtte. Kontroll med hvilke søk som foretas og med all bruk av datasettene skal imidlertid finne sted for alle lagrene.

9.3. Nærmere om styrkede kontrollmekanismer

9.3.1. Innledning

Fra beskrivelsen over kan vi avlede en mer utfyllende rollebeskrivelse for de tre kontrollinstansene. Informasjonsinnhentingen vil samlet sett være underlagt strenge, adekvate og effektive mekanismer mot misbruk. Utvalget mener at forslagene om styrkede kontrollmekanismer vil innebære en betydelig skjerpet uavhengig kontroll med E-tjenesten for denne delen av tjenestens kommunikasjonsetterretning.

Det vil etter utvalgets vurdering ikke være til å komme forbi at de kontrollmekanismer som foreslås, og særlig gjelder det opprettelse av en domstolsmekanisme for forhåndsautorisasjon, i noen grad vil redusere overordnede myndigheters mulighet til å styre og innrette E-tjenestens innhentingsvirksomhet for denne metodens/aksessens vedkommende. Etter utvalgets vurdering oppveies imidlertid eventuelle ulemper forbundet med dette av de fordeler som kontrollmekanismene vil tilføre DGF-systemet i form av en troverdig og uavhengig forsikring mot at søk og innsyn i data skjer i større grad enn strengt nødvendig.

Utvalget kan vanskelig se at nødvendighets- og forholdsmessighetsvurderingen i et menneskeretts- og personvernperspektiv vil stå seg dersom de foreslåtte kontrollmekanismer reduseres i særlig grad.

Utvalget fremhever at DGF delvis vil bestå av dataprogrammer og algoritmer. Det er sentralt at kontrollørene har nødvendig kompetanse til å kunne gjennomføre en effektiv kontroll.

9.3.2. DGF-domstolen

DGF-domstolen skal:

- Forhåndsgodkjenne hvilke objekter det skal samles inn innholdsdata fra. Disse godkjenningene implementeres teknisk i Filter 3. Dette filteret vil kunne plukke ut riktige innholdsdata med høy presisjon, basert på personselektorer.
- Forhåndsgodkjenne hvilke objekter og handlingsmønstre man kan gjøre søk på i metadatalageret (basert på personselektorer og/eller modusselektorer). Disse godkjenningene skal omsettes i søkeprivilegier som implementeres i metadatalageret sin søkesluse. Slike privilegier

vil kunne implementeres teknisk med høy presisjon.

Det må erkjennes at prøvingen for en domstol i det enkelte tilfelle vil bero på avveininger som ikke utelukkende er av rettslig karakter. Det vil derfor være viktig at domstolen har grunnleggende forståelse for etterretningsfaget og innsikt i etterretningsvurderinger og trusselbildet som ligger til grunn for anmodninger om søk. Av sikkerhetsmessige hensyn vil antallet dommere måtte være begrenset. De vil måtte inneha etterretningsfaglig kompetanse, teknisk og operativ innsikt i tjenestens virksomhet samt i overordnede myndigheters styrings- og prioriteringsvirksomhet. Videre vil godkjenningsmyndigheten måtte ta hensyn til at utenlandsetterretning ofte innebærer at man søker etter ukjente aktører basert på kjent modus, hvilket kan tilsi bred målutvikling før man gjennom analyse og videre tiltak kan skille ut den relevante informasjon for videre målrettet og presis innsamling. En forhåndsprøving som søker å «hoppe over» målutviklingsfasen, blir meningsløs.

Det vil alltid være en viss risiko for at dommerne etter hvert kan identifisere seg med tjenestens virke og oppgaver, grunnet deres operative medvirkning til tjenestens løpende oppdragsløsning. Det må derfor sikres mekanismer som også sørger for tilstrekkelig «avstand» mellom dommerne og tjenesten, for å unngå for tette bånd og at det utvikles en slik kultur.

Utvalget har ikke hatt anledning til å utrede mer detaljert hvordan slik domstolsbehandling skal legges opp, men vil likevel peke på enkelte sentrale forhold:

- Hovedreglene om domstolskontroll bør fremgå av E-loven selv. Det bør gjelde de grunnleggende vilkårene for å tillate søk, herunder terskelkrav («beviskrav»), varighet av søketillatelsen og kontroll med at tillatelse ikke vil være uforholdsmessig inngripende. Loven bør fastslå at domstolen ikke kan tillate søk når det vil fremstå som uforholdsmessig. Utfyllende regler om f.eks. utforming av begjæringer til domstolen mv. bør kunne fastsettes i forskrift.
- Utvalget antar at det et stykke på vei vil kunne søkes veiledning i utformingen av regelverket i politiloven kap. IIIa, som bl.a. gjelder PSTs forebyggende bruk av tvangsmidler. Regelverket bør så langt som mulig være åpent og offentlig tilgjengelig. Enkelte mer detaljerte spørsmål bør kunne overlates til regulering i forskrift eller interne retningslinjer i E-tjenesten. Det kan gjelde personell kompetanse til å be om rettens tillatelse, utforming av begjæringer mv.
- Rettens avgjørelser bør treffes ved kjennelse. Kjennelsen kan ikke meddeles de personer den gjelder, men den skal foruten til tjenesten selv, meddeles DGF-tilsynet og også være tilgjengelig for EOS-utvalget.
- Hovedvilkåret for å tillate søk må knyttes opp mot E-tjenestens formål, jf. E-loven § 3. Tillatelse til søk i registrene bør bare kunne gis dersom det er grunn til å tro at inngrepet vil gi opplysninger av betydning for dette formålet. Loven bør anvise – så langt det lar seg gjøre – hvor vide søketillatelser som kan gis. For søk basert på *personselektorer* knyttet til personer som domstolen har godkjent innhenting mot, antar utvalget at domstolens kjennelser i alle fall bør kunne inkludere to ledd ut i kommunikasjonskjeden. Dette vil for det første fasilitere bedre treff ved søk, og det vil i tillegg bidra til at antall rettsavgjørelser kan holdes på et håndterlig nivå.
- I alle fall for *modusselektorer* bør varigheten ikke være for kort for å ivareta muligheten til å detektere enkelte mer sjeldne signaturer. Politiloven kap. IIIa gir en lengste varighet på 6 måneder, jf. § 17e. For DGF kan dette i enkelte tilfeller synes for knapt, og utvalget antar derfor at lengstetiden bør kunne settes opp til ett år, i enkelte tilfeller muligens også lenger. Det innebærer ikke at dette nødvendigvis skal være den normale varigheten av en søketillatelse.

Det er sentralt at DGF-domstolen har kapasitet til å håndtere antall saker og at behandlingen kan skje raskt. Utvalget tar for sin del ikke stilling til om dette skal være en spesialdomstol eller om det f.eks. bør inngå som en del av porteføljen til Oslo tingrett. Av hensyn til gradering og sikkerhet vil det antagelig ikke være mulig å behandle sakene i Oslo tingretts vanlige lokaler. Skal sakene legges til Oslo tingrett, er det nok derfor mest nærliggende å se for seg en ordning der dommere med nødvendig sikkerhetsklarering, kan rullere på å behandle denne sakstypen i godkjente lokaler hos E-tjenesten.

I enkelte tilfeller kan det oppstå behov for å iverksette søk uten å avvente domstolens avgjørelse. Etter mønster av politiloven § 17d tredje ledd, bør regelverket antagelig åpne for det. Det må da stilles krav om etterfølgende foreleggelse for domstolen og sletting av søk dersom domstolen avslår godkjennelse.

9.3.3. DGF-tilsynet

DGF-tilsynet skal:

- I nær sanntid motta all informasjon om alle søk som gjøres i alle datasamlinger i DGF-systemet, motta alle avgjørelser fra DGF-domstolen, ha tilgang til all informasjon om hvordan filtrene er implementert og konfigurert, og ha tilgang til all informasjon om hvordan interne retningslinjer og avgjørelser fra domstolen er oversatt til søkeprivilegier.
- Rapportere avvik til EOS-utvalget og for øvrig rapportere regelmessig til EOS-utvalget, Forsvarsdepartementet og Samferdselsdepartementet. Avvik vil i denne sammenheng være bruk av DGF-systemet som ikke er hjemlet i E-loven, domstolens avgjørelser, eventuelle forskrifter og interne retningslinjer.
- Føre tilsyn[92] med at datasikkerheten i DGF-systemet er så høy som teknologisk og praktisk mulig.

Utvalgets anbefaling om opprettelse av DGF-tilsynet er særlig begrunnet i behovet for en tilnærmet kontinuerlig og uavhengig kontroll – i nær sanntid – knyttet til implementeringen av DGF-systemet. Dette vil trolig kreve kontinuerlig tilstedeværelse i E-tjenestens lokaler, og spesialisert teknologisk kompetanse. Etter utvalgets vurdering vil det antagelig være uhensiktsmessig – gitt EOS-utvalgets oppheng og lovregulerte oppdrag om etterfølgende kontroll – dersom EOS-utvalget skal tillegges denne oppgaven. Utvalget anbefaler derfor at DGF-tilsynet opprettes som et forvaltningsorgan. For å sikre uavhengighet av den statsråd som er konstitusjonelt ansvarlig for E-tjenestens virksomhet, anbefaler utvalget at DGF-tilsynet underlegges et annet departement enn Forsvarsdepartementet. I og med at DGF baserer seg på tilretteleggingsplikt for ekomindustrien i Norge og berører kommunikasjonsfriheten, foreslår utvalget at tilsynet underlegges Samferdselsdepartementet, som eventuelt kan vurdere å delegere det administrative forvaltningsansvaret for tilsynets virksomhet til Nkom.

DGF-tilsynet bør etter utvalgets syn ikke tillegges myndighet til å stanse virksomhet eller offentlig kritisere E-tjenesten for brudd på regelverket for DGF. Dette vil kreve oppbygging av juridisk kompetanse som vil dublere EOS-utvalgets kompetanse, og vil dessuten skape uhensiktsmessige ansvarslinjer i forhold til EOS-utvalgets mandat. Utvalget mener derfor at tilsynet, ved mistanke om avvik, skal rapportere dette umiddelbart til EOS-utvalget, som vil vurdere oppfølgingstiltak i tråd med de fullmakter som EOS-utvalget besitter, og rapportere til Stortinget i tråd med etablert praksis.

På samme måte som for domstolen, må det treffes tiltak (personellrotasjon, fysisk separasjon, eget lunchrom etc.) som sikrer at tilsynets medarbeidere ikke etter hvert kan identifisere seg med tjenestens virke og oppgaver. Særlig viktig vil dette være dersom representanter for tilsynet daglig skal oppholde seg sammen med E-tjenestens personell i E-tjenestens lokaler.

9.3.4. EOS-utvalget

EOS-utvalget skal:

- Utføre utvalgets kontrollvirksomhet etter lov og instruks for E-tjenestens DGF-virksomhet på samme måte som for E-tjenestens øvrige virksomhet.
- Motta rapporter fra DGF-tilsynet, og ha ubegrenset innsynsrett i DGF-systemet.
- Rapportere til Stortinget om hvordan E-tjenesten benytter seg av DGF, og om Forsvarsdepartementet sin styring med hvordan tjenesten bruker DGF-systemet.

Utvalget antar at etablering av DGF i seg selv ikke medfører behov for regelverksendringer for EOS-utvalgets virksomhet ut over de endringer som nå ligger til vurdering i Stortinget som følge av Evalueringsutvalgets innstilling. Utvalget har imidlertid pekt på viktigheten av at EOS-utvalget har god kompetanse til å forstå tekniske detaljer knyttet til søk og filtrering, samt til hvorledes DGF-systemet for øvrig fungerer og kan kontrolleres. Utvalget er kjent med at EOS-utvalgets sekretariat nylig er styrket med en medarbeider med teknologisk kompetanse, og at EOS-utvalget er utvidet med et medlem med teknologisk kompetanse. Ved eventuell innføring av DGF bør EOS-utvalget og Stortinget vurdere om dette er tilstrekkelig, samt vurdere om EOS-utvalget bør styrkes ytterligere med ressurser og kompetanse for å ivareta sitt kontrollansvar på dette området.[93] Det kan ikke utelukkes at innføring av DGF

[92] Uten å overta ansvaret som eventuelle andre offentlige myndigheter har for å føre lovpålagt tilsyn med sikkerhetsgraderte informasjonssystemer. F.eks. fører NSM et overordnet og systemrettet tilsyn med E-tjenesten.

[93] Se Evalueringsutvalgets tilrådning i Dok 16 (2015-2016) s. 145, hvor det heter at «Dersom tjenestens forslag om etablering av et digitalt grenseforsvar følges opp, vil det måtte får store konsekvenser for kontrollen med tjenesten generelt og EOS-utvalgets

også vil måtte medføre behov for inspeksjoner av leverandører av ekomnett og ekomtjenester.

9.4. Lovtiltak

9.4.1. Eksisterende grunnvilkår

Grunnvilkårene for innhenting av informasjon fremkommet gjennom DGF vil i utgangspunktet være som for E-tjenestens øvrige innsamlingsvirksomhet etter dagens regelverk, hvilket inkluderer følgende:

- Formålet med all informasjonsbehandling må utelukkende være rettet mot utenlandske forhold.

- Informasjonen som innhentes må ligge innenfor tjenestens lovbestemte oppgaver og de årlige politisk fastsatte prioriterte etterretningsbehov.

- Dersom innhentingen reiser politiske problemstillinger eller er av særlig viktighet eller prinsipiell karakter, skal politisk nivå forhåndssamtykke til innhentingen.

- Innhentingen kan ikke innebære fordekt innhenting på norsk territorium rettet mot norske fysiske eller juridiske personer.

- Tjenesten kan bare oppbevare informasjon som gjelder en norsk person dersom informasjonen har direkte tilknytning til ivaretakelsen av tjenesten oppgaver eller er direkte knyttet til en slik persons arbeid eller oppdrag for tjenesten.

9.4.2. Ny lovregulering

Etter utvalgets syn forutsetter DGF at det innføres en ny og tydelig lovgivning.

Utvalget legger til grunn at noen viktige prinsipper for informasjonsinnhenting og annen informasjonsbehandling bør lovfestes, hvorav noen allerede gjelder i dag og noen vil innebære et skjerpet regime for DGF sammenlignet med dagens rettstilstand:

- Data som skal lagres i E-tjenesten skal minimeres i størst mulig utstrekning, og slettes når informasjonen ikke lenger har etterretningsmessig verdi.

- Innhenting ved bruk av DGF skal kun benyttes dersom andre og mindre inngripende innhentingstiltak, for eksempel bruk av åpne kilder, ikke antas å fremskaffe den samme informasjonen.

- All overskuddsinformasjon [94] om norske eller utenlandske personer vil bli slettet. Overskuddsinformasjon som slettes i E-tjenesten, kan etter dagens regelverk overføres til andre offentlige myndigheter dersom opplysningene anses relevant for disse myndighetenes oppgaveløsning. Etter utvalgets syn bør dette ikke være mulig for informasjon fremkommet gjennom DGF. Utvalget vurderer at overskuddsinformasjon fra DGF bør slettes og ikke deles. Dette er viktig for å hindre formålsglidning. Utvalget anbefaler derfor at det for DGF lovfestes at all overskuddsinformasjon som ikke er relevant for E-tjenestens oppgaveløsning skal slettes. Klare instrukser og kontrollmekanismer må sikre at dette blir ivaretatt. Tiltaket vil sammen med øvrige tiltak bidra til at publikum vil ha tillit til at DGF ikke misbrukes for andre formål enn det informasjonstilgangen er ment for. I praksis vil dette si at dersom E-tjenesten – mot formodning og uten hensikt – skulle komme over informasjon om at en person har begått et drap, seksuelle overgrep mot barn eller deltatt i annen alvorlig kriminalitet som ikke er av relevans for E-tjenestens ansvarsområde, vil slik informasjon bli slettet uten videre oppfølging. Hensynet til rikets sikkerhet er viktigere enn å tillate bruk av denne overskuddsinformasjonen.

- Lovreguleringen av DGF må ikke bare omfatte tilretteleggingsplikt for ekom-aktørene, men også E-tjenestens rammer for bruk og lagring av DGF-fremskaffet informasjon, samt kontrolltiltakene som bør styrkes i den forbindelse. Terskelen for målrettet innsamling mot en eller flere bestemt(e) enkeltperson(er) bør lovfestes. Jf. kap. 9.5.2.

- Lovreguleringen bør være nasjonalitetsnøytral og uavhengig av hvor innhentingsmålet befinner seg på innhentingstidspunktet. Med andre ord bør lovgivningen legge til grunn at utenlandske borgere har samme krav på personvern

fokus på tjenesten spesielt.» Dette må antas også å omfatte de kompetansemessige konsekvenser.

[94] Med overskuddsinformasjon menes informasjon som ligger utenfor E-tjenestens ansvarsområde, men som tjenesten likevel kommer i besittelse av som følge av dens virksomhet rettet mot forhold innenfor ansvarsområdet.

som norske personer. Dette er en presisering av det som allerede fremgår av gjeldende rett, E-tjenesten vil være behandlingsansvarlig etter personopplysningsloven, uavhengig av om selve innhentingen av informasjon har funnet sted utenfor Norge. Personopplysningslovens regler kommer til anvendelse for personopplysninger om utenlandske personer, som E-tjenesten behandler.

- Det bør fastsettes i lov at DGF-innhentet informasjon ikke under noen omstendighet kan bli brukt som bevis mot tiltalte i straffesaker. Utvalget er klar over at dette av noen kan oppfattes å være i strid med prinsippet om fri bevisbedømmelse i straffeprosessretten, men mener like fullt at en slik formålsbegrensning i vesentlig grad vil styrke tilliten til at DGFs formålsbegrensninger etterleves. Omfattende databasert analyse kan i enkelte tilfeller føre til at bevisbyrden for å være uskyldig snus i praksis. Dette underbygger ytterligere denne begrensningen. Se også kap. 9.4.3.

- Det bør oppstilles et lovforbud mot å innrette DGF-innhenting annet enn gjennom de prioriterte nasjonale etterretningsbehov, som behandles årlig på politisk nivå med justeringer gjennom året ved oppdukkende informasjonsbehov.

- Det bør nedfelles i lov at E-tjenesten ikke skal innhente personopplysninger utelukkende på bakgrunn av hva som er kjent om en persons etnisitet eller nasjonale bakgrunn, politiske, religiøse eller filosofiske overbevisning, fagforeningstilhørighet eller opplysninger om helsemessige eller seksuelle forhold.

9.4.3. Særlig om formålsbegrensning for bruk av DGF

Utvalget har tidligere gjort rede for at svært mange av de digitale spor nordmenn etterlater seg i sine daglige liv vil passere de punktene hvor DGF samler inn data. Det betyr at DGF-installasjonen vil kunne være et svært kraftfullt virkemiddel også for nasjonale myndigheter som har ansvar for innenlandske forhold.

Utvalget vil sterkt advare mot en utvikling som går i retning av at DGF benyttes til annet enn utenlandsetterretningsformål. Brukt til overvåking av nordmenn i Norge har DGF et enormt potensial, og enhver formålsglidning i retning av annen bruk enn til utenlandsetterretningsformål vil raskt støte mot hensynet til personvern, mot juridiske skranker i folkeretten og virke svekkende på myndighetenes tillit i befolkningen.

Det er allerede i dag begrensninger på hvordan informasjon samlet inn av E-tjenesten kan benyttes til andre formål. E-tjenesten kan bare samarbeide med andre tjenester og myndigheter så lenge det ligger innenfor tjenestens rettsgrunnlag (det sees her bort fra ekstraordinære situasjoner/nødrettssituasjoner). Spesielt betyr dette at E-tjenesten ikke kan samle inn informasjon på anmodning fra andre myndigheter, uten at dette har et utenlandsetterretningsformål. Når informasjon E-tjenesten har samlet inn til utenlandsetterretningsformål inneholder elementer som er av relevans for andre myndigheter, kan denne informasjonen deles. Dersom dette er overskuddsinformasjon – dvs. informasjon som ligger utenfor E-tjenestens eget samfunnsoppdrag – skal denne informasjonen slettes hos E-tjenesten.

Utvalget anbefaler at de begrensningene E-tjenesten har i dag knyttet til samarbeid med andre nasjonale myndigheter videreføres også for DGF. DGF bør derfor kun benyttes til formål som er dekket av E-tjenestens samfunnsoppdrag. Det betyr i praksis at alle søk som godkjennes i metadatalageret, og alle kjennelser om innsamling av innholdsdata, skal ha utenlandsetterretning som begrunnelse.

Som nevnt i kap. 9.4.2 foran, anbefaler utvalget at det fastsettes i lovs form at informasjon innhentet gjennom DGF ikke under noen omstendighet skal kunne benyttes som bevis mot tiltalte i straffesaker. En slik formålsbegrensning vil i vesentlig grad styrke tilliten til at DGF ikke vil bli benyttet til andre formål enn forutsatt, og således hindre formålsglidning. Dette er imidlertid ikke til hinder for at informasjon innhentet gjennom DGF som ikke er å anse som overskuddsinformasjon, kan deles med PST – herunder gjennom Felles kontraterrorsenter (FKTS) – på vanlig måte, som kan bruke informasjonen som inngangsverdi for egen metodebruk/etterforskning basert på PSTs hjemmelsgrunnlag. Dersom en etterforskningssak leder til tiltale, vil imidlertid DGF-innhentet informasjon delt med PST ikke kunne benyttes som bevis.

9.5. Nødvendighet og forholdsmessighet

9.5.1. Overordnet vurdering

DGF vil benyttes til de fleste aspekter av E-tjenesten sitt samfunnsoppdrag slik det er beskrevet i kapittel kap. 3.3. De mest fremtredende effektene av en

eventuell innføring av DGF er imidlertid knyttet til håndtering av cyberhendelser og –angrep samt håndtering av potensielle trusler om terror på norsk jord. Det er derfor disse delene som er mest relevante i en diskusjon om hvorvidt DGF er nødvendig og forholdsmessig.

DGF vil i betydelig grad øke Norges kapasitet til å håndtere cybertrusler med utenlandsk utgangspunkt. Det vil styrke evnen til å oppdage at angrepene finner sted, til å identifisere hvilke punkter i Norge som blir angrepet, og til å identifisere gode mottiltak. Fordi cybertrusler først og fremst utspiller seg i det digitale rom, må de også oppdages og håndteres der. Det er derfor vanskelig å se for seg at en tilsvarende positiv effekt vil kunne oppnås på annen og mindre inngripende måte enn gjennom overvåking av landets digitale grenseoverganger, se kap. 5.8 ovenfor om dette.

Når det gjelder trusler knyttet til tradisjonell terrorisme vil DGF inngå som en av mange kapasiteter som E-tjenesten besitter. Innføring av DGF vil erstatte det etterretningsmessige tapet som følger av at kommunikasjon flytter fra kommunikasjonsbærere som kan overvåkes uten DGF og over i kabler som krysser landegrensen. I tillegg vil det gi E-tjenesten et innsyn i grensekryssende kommunikasjon som langt overstiger hva de tidligere har hatt. Dette vil være et kraftfullt verktøy. For motvirking av tradisjonell terror er det vanskelig å se for seg gode alternative kapasiteter til tilgang til grensekryssende kommunikasjonsstrømmer. Og dersom alternative tiltak skulle implementeres, kan disse på den annen side være vel så belastende som DGF, jf. kap. 5.8.

Forholdsmessighetsvurderingene avhenger av forholdet mellom de truslene vi utsettes for, og hvor inngripende tiltaket er. DGF er potensielt svært inngripende, og skadepotensialet er stort dersom det ikke legges tydelige føringer på hvordan det skal benyttes, og det ikke underlegges et sterkt kontrollregime som sørger for at det ikke blir misbrukt. I kap. 9.2 og 9.3 har vi i noen detalj beskrevet et kontrollregime som etter utvalgets syn reduserer skadepotensialet til et akseptabelt nivå. Så langt utvalget er kjent med vil dette tre-lags kontrollregimet være mer omfattende enn kontrollordningene for andre lands etterretningstjenester.

9.5.2. Er DGF forenlig med menneskerettighetene?

Utvalget har i kapittel 7 redegjort for de rammer for DGF som følger av Grunnloven og menneskerettskonvensjoner som Norge er bundet av. Herunder har utvalget redegjort for EU-domstolens dom om Datalagringsdirektivet (DLD-dommen) og avtalen mellom EU og USA om utveksling av personopplysninger (*Privacy Shield*-avtalen). Selv om EU-domstolens dom om DLD tar utgangspunktet i EU-charteret, som ikke gjelder for Norge, og til tross for at E-tjenesten ikke er rettslig avhengig av *Privacy Shield*-avtalen for å utveksle personopplysninger med amerikanske tjenester, mener utvalget dette er relevant fordi de gir uttrykk for gjeldende europeiske standarder for personvern og håndtering av personvernopplysninger.

I vedlegg 2 er det redegjort for forholdene i andre land. Både redegjørelsen i kapittel 7 og vedlegg 2 tilsier at det ikke kan være noe absolutt forbud mot DGF. Denne konklusjonen anser utvalget som sikker. På den annen side er det like klart at innretningen av DGF må ivareta de følgende kriteriene for ikke å komme på kant med det menneskerettslige vernet mot inngrep i privatliv eller ytringsfrihet:

i. DGF må ha tilstrekkelig klar lovhjemmel

Utvalget har i kap. 7.2 gitt en generell redegjørelse for legalitetsprinsippet. Utvalget er kjent med at EOS-utvalget i en særskilt melding til Stortinget 17. juni 2016 har stilt spørsmål ved om E-tjenesten har tilstrekkelig lovhjemmel for noe av den innhenting av informasjon som allerede i dag finner sted. Utvalget finner det for sin del ikke nødvendig å foreta en nærmere vurdering av om den eksisterende lovreguleringen kunne være tilstrekkelig som lovgrunnlag for DGF. Det er etter utvalgets syn slike særtrekk ved DGF sammenlignet med E-tjenestens nåværende metoder for informasjonsinnhenting at det tilsier en særskilt lovregulering. Reguleringen må bl.a. angi vilkårene for DGF og gi regler om kontroll. Det vil være lite tilfredsstillende å overlate dette til regulering i internt regelverk hos tjenesten. Regelverket bør så langt som mulig være offentlig kjent for å styrke tilliten til E-tjenestens virksomhet. Samtidig sier det seg selv at det kan være detaljer i reguleringen av DGF som vil kunne avdekke tjenestens kapasiteter mv., og som derfor ikke kan gjøres offentlig kjent.

DGF vil innebære at E-tjenesten gis tilgang til datatrafikk fra fiberoptiske kabler. Trafikken vil i hovedsak ha Norge som endepunkt eller komme fra Norge. Som følge av ruting av datatrafikk vil mye av trafikken gjelde kommunikasjon mellom norske borgere eller virksomheter. For å ramme inn hvilken

datatrafikk E-tjenesten skal ha tilgang til for å benytte i produksjon av etterretninger, må det stilles kvalifiserende vilkår. Hva slags vilkår som kan oppstilles, bør ses i sammenheng med hva slags kontrollmekanismer som kan etableres. Vilkårene må utformes slik at det er mulig å påse at de etterleves.

Utvalget vil anta at et grunnvilkår for E-tjenestens tilgang til datatrafikk, og det gjelder så vel metadata som innholdsdata, må være at det gjelder forhold som det er rimelig grunn til å undersøke om at berører de formål E-tjenesten skal ivareta etter loven § 1 og tjenestens oppgaver etter loven § 3.

ii. DGF må underlegges adekvate og uavhengige kontrollmekanismer

E-tjenesten er underlagt kontroll fra Forsvarsdepartementets side etter E-instruksen § 3. Denne kontrollen er viktig, men er ikke tilstrekkelig for å ivareta de menneskerettslige krav. Det trengs kontrollorganer som er helt uavhengige av tjenesten for å etablere nødvendig tillit til etterlevelse av regelverket.

Den kontrollen EOS-utvalget allerede fører med E-tjenesten må anses å være tilstrekkelig uavhengig. Etter utvalgets syn vil det likevel være behov for mer inngående og fortløpende/kontinuerlig kontroll med DGF. Slik kontroll bør være domstolskontroll med bruk av personrelaterte søkeprivilegier, se omtalen i kap. 9.3.2 foran. Videre bør det være løpende kontroll fra DGF-tilsynets side, se omtalen i kap. 9.3.3 foran. Den samlede effekten av disse tre kontrollmekanismene vil etter utvalgets syn ivareta kriteriet om adekvate kontrollmekanismer. Samtidig kan de innrettes på en måte som ikke vanskeliggjør E-tjenestens bruk av DGF i slik grad at nytteverdien blir vesentlig redusert.

iii. DGF må være nødvendig og forholdsmessig

Utvalget har i kapittel 5 og vedlegg 1 beskrevet nytten av DGF. Det vises også til vurderingen i kap. 9.5.1 foran. E-tjenesten skal etter E-loven §§ 1 og 3 ivareta sentrale og grunnleggende funksjoner for Norges selvstendighet, sikkerhet og andre viktige nasjonale interesser. Den teknologiske utviklingen innebærer at tjenestens mulighet til dette svekkes uten tilgang til DGF. Det gjelder i særlig grad for tjenestens oppgaver innenfor cyberforsvar. Det gjør seg imidlertid også gjeldende for tjenestens øvrige oppdrag, som kontraterror, selv om andre kompenserende tiltak delvis kan være mulige. Slike kompenserende tiltak vil kunne ha andre negative effekter for personvern, ha en mer usikker effekt og vil også kunne være vesentlig mer ressurs- og kostnadsdrivende for tjenesten. Utvalgets syn er derfor at DGF innenfor de rammer utvalget anbefaler, vil være nødvendig. Det er videre utvalgets syn at DGF innenfor disse rammene ikke vil innebære et uforholdsmessig inngrep i retten til privatliv. Den mulige nedkjølingseffekten (se kap. 6.3 foran) er usikker, men kan ikke sees bort fra. Etter utvalgets syn vil DGF likevel ikke innebære en innskrenkning i ytringsfriheten som går ut over det tillatte etter EMK artikkel 10 eller Grunnloven § 100.

Ut over dette vil utvalget legge til at det har vurdert om det må oppstilles særlige regler til vern om kommunikasjon med yrkesutøvere med streng taushetsplikt.[95] Kommunikasjon mellom en advokat og klient eller mellom en journalist og en kilde kan være viktige eksempler på det. Unnlatelsen av å vurdere dette nærmere ser ut til å være én av hovedinnvendingene i EU-domstolens avgjørelse om Datalagringsdirektivet. Utvalget har imidlertid ikke funnet å tilrå en slik begrensning for DGF. Det er flere grunner til det. En grunn er at det vil være teknisk vanskelig å gjennomføre filtrering uten en innrapporteringsordning på selektornivå. Slik innrapportering kan være lite realistisk og vil uansett vanskelig kunne etableres for personer i utlandet. Dernest vil filtrering kunne ha utilsiktede konsekvenser. Dersom tjenesten følger et legitimt mål i utlandet, antas filtreringsregelen å måtte medføre at kommunikasjon fra vedkommende til en «sperret» selektor i Norge ikke vil fremkomme. For det første vil dette være en omgåelsesmulighet for trusselaktører som ønsker å unngå tjenestens søkelys. For det annet vil manglende informasjon i enkelte tilfeller lede til at personer ikke «sjekkes ut» av et sakskompleks, med de negative konsekvenser dette kan ha for dem det gjelder. Endelig vil utvalget peke på at gruppen som skulle omfattes kan være uklar. Hva f.eks. med kommunikasjon med religiøse ledere i radikale trossamfunn – skal det likestilles med den taushetsplikt som gjelder for betroelse til prester? Hvem skal i så tilfelle treffe beslutning om at dette likestilles? Videre vil det være problematisk å legge til grunn at

[95] Et absolutt forbud mot innhenting av slike yrkesgruppers kommunikasjon kan ikke utledes av folkeretten, jf. Veneziakommisjonen (gruppe av folkerettseksperter oppnevnt av Europarådet, hvis fulle betegnelse er «European Commission for Democracy Through Law») sin rapport fra april 2015 (*Update of the 2007 Report on the Democratic Oversight of the Security Services and Report of the Democratic Oversight of Signals Intelligence Agencies* (CSL-AD(2015)006, Study No. 719/2013, Strasbourg, 7 April 2015), para. 106-108.

all kommunikasjon til eller fra f.eks. en advokat eller journalist er dekket av taushetsplikt og derfor skal filtreres ut. Det vil åpenbart legge til rette for å bruke stilling som skalkeskjul for dem som har interesse av det. Utvalgets syn er etter dette at en ikke bør legge inn bestemte begrensninger for yrkesgrupper med taushetplikt ved design og utforming av reglene for DGF. Behovet for slik sperre er dessuten mer begrenset ved at søk i metadatabasen og i innholdslagreret skal være forhåndsgodkjent av en domstol. Det vil måtte inngå i domstolens vurdering av om DGF i det konkrete tilfellet er forholdsmessig og skal tillates, om søk vil berøre personer hvis kommunikasjon for en anselig del må anses å være taushetsbelagt.

iv. Særskilt vurdering av DGF mot EU-domstolens avgjørelse om Datalagringsdirektivet (DLD)
Utvalget har redegjort for EU-domstolens avgjørelse i kap. 7.8 foran. Det er betydelige forskjeller mellom DLD og DGF, med den innretning utvalget foreslår. Det er imidlertid også en del likheter, og den mest fremtredende likheten er at myndighetene potensielt gis tilgang til store mengder datatrafikk om oss alle uten at det på forhånd bygger på en på forhånd identifisert mistanke eller konkret individualisert sikkerhetsbekymring.

Allerede formålet med DGF skiller det imidlertid fra DLD. DGF skal bidra til å ivareta rikets sikkerhet. Dette er et særdeles viktig formål. Som fremholdt foran, er DLD begrenset til bekjempelse av «alvorlig kriminalitet», men direktivet angir ikke selv noe nærmere om hvor strengt dette skal forstås. Det å kartlegge og motvirke trusler mot rikets sikkerhet gir en langt snevrere bruk enn politiets bekjempelse av alvorlig kriminalitet.

En annen viktig forskjell er at det tenkes lagt svært strenge begrensninger på hva dataene skal brukes til, og at fokus er rettet mot utlandet og ikke mot egen befolkning (personer i Norge). Videre er tilgangsmekanismene som foreslås svært strenge, og det legges opp til omfattende kontroll slik at eventuell misbruk eller formålsglidning avsløres raskt. Det tenkes også lagt inn legale barrierer for å hindre formålsglidning. Datasikkerheten hos E-tjenesten må for øvrig antas å være langt sikrere enn hos teletilbydere, og databasene skal kun lagres i Norge. Lagring hos tjenestetilbydere innebærer betydelig større datasikkerhetsmessige utfordringer enn lagring under kontroll av E-tjenesten.

Det er utvalgets vurdering at de prinsipper og synspunkter som EU-domstolen bygget på ved avgjørelsen om DLD, er godt ivaretatt gjennom utvalgets forslag til innretting av DGF-systemet med tilhørende lovregulerende og andre tiltak. Etter utvalgets syn støttes dette også av Generaladvokatens uttalelse i Tele2 Sverige-saken. Uttalelsen og de foreslåtte konklusjonspunktene er omtalt i kap. 7.8.2 foran.

Samlet sett mener utvalget at DGF, i lys av forskjellene beskrevet foran, i signifikant mindre grad enn DLD vil berøre det faktiske personvernet til vanlige norske borgere. DGF fremstår som mer forholdsmessig enn DLD.

v. Særskilt vurdering av DGF mot Privacy Shield-avtalen mellom EU og USA
Utvalget har redegjort for *Privacy Shield*-avtalen i kap. 7.8 foran. I det følgende vil utvalget vurdere DGF opp mot de de prinsipper EU-kommisjonen har lagt til grunn i tilknytning til *Privacy Shield*-avtaleverket.

EU-kommisjonen aksepterer at amerikanske etterretningstjenester samler inn datastrømmer/meng-dedata (*bulk collection*), men vektlegger samtidig de begrensninger som følger av presidentens SIGINT-direktiv. Direktivet begrenser formålet med slik innsamling til seks nærmere angitte kategorier knyttet til rikets sikkerhet. En av disse kategoriene er «*transnational criminal threats*». Til sammenligning vil DGF ha et mer begrenset formål, og vil ikke benyttes til å innhente informasjon om grenseoverskridende kriminalitet generelt.

Videre vektlegger EU-kommisjonen at amerikansk lovgivning fra 2015 (*US Freedom Act*) begrenser innsamling i bulk. Denne loven medførte imidlertid kun begrensninger knyttet til innsamling av innenlandske kommunikasjonsdata knyttet til amerikanske borgere. Til sammenligning vil DGF overhodet ikke kunne benyttes med formål å samle inn data knyttet til innenlandske forhold eller kommunikasjon innenlands.

EU-kommisjonen viser til det amerikanske presidentdirektivet for SIGINT, som man anser å ha spesiell viktighet for ikke-amerikanske borgere.

Følgende fremheves særskilt,, som i følge EU-kommisjonen «*captures the essence of the principles of necessity and proportionality*:"[96]

- Innsamling må skje i samsvar med lov. Dette vil også være tilfelle for DGF.
- Alle personer skal behandles med verdighet og respekt og nyte godt av «*appropriate safeguards*», uansett nasjonalitet eller geografisk oppholdssted. Dette vil gjelde tilsvarende for DGF, som også går lenger og sidestiller innhentingsvilkårene mot personer i utlandet uavhengig av om innhentingsmålet er norsk eller ikke-norsk. Se kap. 9.4.
- Alle personer har legitime personverninteresser knyttet til behandlingen av deres informasjon. Det samme vil gjelde for DGF.
- Personvernhensyn skal integreres i selve planleggingen av etterretningsaktivitet. Det vises her til fremstillingen i kap. 3.3.3 og 9.4, hvor det er nærmere redegjort for hvordan personopplysningsloven og ny lovgivning bør anvendes for DGF.
- Når det gjelder lagringstid for metadata innhentes i bulk, viser EU-kommmisjonen til at hovedregelen i USA vil være en lagringstid på maksimum 5 år. For DGF vil lagringstiden være betydelig kortere, jf. kap. 9.2.
- Innsamling skal alltid skje så målrettet som mulig, og etterretningstjenestene skal alltid vurdere om informasjon som skal innsamles er tilgjengelig ved andre og mindre inngripende metoder. Tilsvarende prinsipp vil gjelde for DGF, og dette prinsippet foreslår utvalget bør lovfestes, jf. kap. 9.4.

EU-kommisjonen har videre vektlagt at amerikanske etterretningstjenester er underlagt et omfattende kontrollregime, som inkluderer både den lovgivende, utøvende og dømmende makt, i tillegg til internkontrollregimer og rapporteringsregimer.[97] For DGF vises til kapittel 9.2 og 9.3 om hvilke kontrollmekanismer som bør etableres, i tillegg til eksisterende interne og uavhengige mekanismer. Så langt utvalget erfarer vil disse mekanismene gå både prinsipielt og praktisk lenger enn de mekanismer som for alle andre etterretningstjenester i Europa.[98] Eksempelvis vil utvalgets forslag til kontrollregime for DGF, til forskjell fra etterretningsprogrammet i USA som er hjemlet i Section 702 under FISA[99], kreve domstolskjennelse for både målutvikling og innhenting rettet mot utenlandske enkeltpersoner. Det anbefalte kontrollregimet for DGF er bygget på en blanding av kontroll fra både den lovgivende, utøvende og dømmende makt, etablerer tre uavhengige mekanismer, samt bygger på prinsippet om uavhengig kontroll forut for inngrepet i den enkeltes personvern, mens inngrepet skjer (i sanntid) og etterfølgende kontroll med søkemuligheter i E-tjenestens informasjonssystemer. Dette kontrollregimet, kombinert med maskinelle kontrollmekanismer, krav til logging og annen notoritet, samt øvrige tiltak, vil redusere risikoen for misbruk til det helt ubetydelige, og innebære et kontrollregime som går lenger enn de krav som EU-kommisjonen oppstiller eller som fremkommer av domstolspraksis fra EMD.

Vedrørende retten til individuell klageadgang og tilgang til effektivt rettsmiddel og domstolsbehandling, anser EU-kommisjonen at amerikansk lovgivning er tilfredsstillende, sett i lys av at avtalen også etablerer en ny klageordning knyttet til det amerikanske utenriksdepartementet (*Privacy Shield Ombudsperson*). Klageordningen kan benyttes av EØS-borgere for å undersøke klager på f.eks. ulovlig overvåking. Ombudsmannen er forutsatt å gi klagerne tilbakemelding om amerikansk lovgivning er blitt fulgt eller ikke, samt gi tilbakemelding – i saker om regelbrudd – om at korrigerende tiltak har blitt truffet. For DGF vil individuelle klager i utgangspunktet bli behandlet av EOS-utvalget, som kan gi tilsvarende tilbakemelding til klagerne uten å røpe sikkerhetsgradert informasjon. I tillegg kan personer som mener seg utsatt for urett i prinsippet bringe en sak inn for ordinær norsk domstol, selv om det kan være enkelte praktiske utfordringer knyttet til bevisførsel som gjelder sikkerhetsgraderte forhold. Det er noe uklart om EOS-utvalgets klageordning er åpen for ikke-norske borgere, selv om praksis viser at terskelen er lav for å ta klagesaker under behandling. Utvalget legger til grunn at dette spørsmålet avklares i forbindelse med Stortingets behandling av Evalueringsutvalgets rapport.[100]

[96] Communication fra EU-kommisjonen, COM(2016)117 Final av 29. februar 2016, pkt. 63.

[97] Commission Implementing Decision para. 92-110.

[98] En oversikt over situasjonen i EU-landene følger av en publikasjon fra EU Agency for Fundamental Rights (FRA) fra 2015 om «*Surveilllance by intelligence services: fundamental rights safeguards and remedies in the EU*».

[99] Foreign Intelligence Surveillance Act.

[100] Dok 16 (2015-2016) Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget). Det vises for øvrig til

Utvalget mener at kontroll- og rettssikkerhetsordningene for DGF i prinsippet må vurderes som adekvate i en norsk kontekst, uavhengig av *Privacy Shield*-avtalens videre skjebne. Utvalget konkluderer imidlertid med at de vilkår og løsninger utvalget anbefaler for DGF, uansett dekker de krav EU-kommisjonen har oppstilt overfor NSA og andre amerikanske etterretningsorganisasjoner i *Privacy Shield*-avtalen, og på flere punkter etablerer ordninger og lovbestemte begrensninger som går vesentlig lenger enn det EU-kommisjonen krever.

9.5.3. Er konsekvensene for personvernet akseptable?

Norge er på mange måter et trygt land, men også et åpent og globalisert samfunn. Norge er ikke mindre utsatt enn andre stater fra enkelte alvorlige trusler og utfordringer. Utvalget legger betydelig vekt på at digitaliseringen i Norge er kommet langt, og at vi derfor på enkelte samfunnsviktige områder er utsatt for cybertrusler. Potensialet for å skade vårt land gjennom digitale angrep er stort.[101]

I en viss forstand er usikkerhet noe vi må leve med; det risikofrie samfunn kan ikke etableres uten samtidig å ødelegge det frie samfunn og de verdier samfunnet bygger på. På den annen side kan myndighetene ikke motvirke cyberangrep eller andre alvorlige utfordringer uten evne til å innhente relevant informasjon i det digitale rom.

De norske verdier knyttet til åpenhet, demokrati, privatlivets fred, ytringsfrihet og toleranse, er verdier som staten samtidig må beskytte. For at folk skal kunne realisere sine liv i frihet, må de ha en beskyttet privatsfære.[102] Balansen mellom kontroll og frihet må bevares, og det er en kontinuerlig oppgave for den liberale rettsstaten å opprettholde en rimelig og forsvarlig likevekt. Spennet mellom åpenhet og sikkerhet er krevende. De dilemmaer som oppstår er av både politisk, juridisk og teknologisk art. Mer overvåking gir ikke automatisk mer sikkerhet. Men erfaring viser også at overvåking er helt nødvendig for å avdekke enkelte trusler.

Det er særlig viktig at man finner balansepunkter som beskytter og hensyntar minoriteter. Tesen om at den som ikke har noe å skjule, ikke har noe å frykte ved overvåking, er en for enkel situasjonsbeskrivelse.[103] Og spørsmålet om man er for eller mot overvåking, er en overforenkling. Samtidig gjelder at menneskerettighetene og personvernet er basert på enighet mellom statene som inkluderer innebyggede mekanismer for balanserte myndighetsinngrep i rettighetene.

Den digitale utviklingen både utfordrer etablerte personvernprinsipper og gir nye muligheter for et styrket personvern. [104] Overvåking bør kun skje målrettet og under strenge begrensninger, samtidig som myndighetene må ha tilgang til nødvendig informasjon og etterretning for å møte alvorlige trusler og utfordringer. Overvåking skal aldri rettes mot folk flest, «for sikkerhets skyld». Og overvåking må alltid rettes inn mot handlinger og planlegging av handlinger, ikke generelt mot tanker og ytringer. Dette ligger i rettsstatens kjerne.

Personvernet har fått en fremtredende plass i utvalgets mandat. Etter utvalgets syn er dette en riktig prioritering. Ethvert tiltak som griper inn i personvernet må ledsages av en integrert vurdering av tiltakets konsekvenser for personvernet. I utvalgets avveininger av ulike løsninger som ramme for DGF, har hensynet til personvernet for de personer som det vil bli lagret trafikkdata om selv om personene ikke er av interesse for E-tjenesten, veiet tungt. Dette har resultert i forslag om omfattende begrensninger i bruk og innsyn i lagrede data, krav om uavhengig forhåndsautorisasjon, og et stort kontrollapparat for å detektere eventuelle avvik. Utvalget har fått det inntrykk at anbefalingene avviker ganske vesentlig fra det E-tjenesten i utgangspunktet kunne ha ønsket.

En rekke andre land har implementert og anser DGF-lignende tiltak som nødvendige. Utvalget kan vanskelig vurdere merverdien i andre land, og har uansett ikke tillagt dette forhold avgjørende betyd-

---

rapportens vedlegg 4, utarbeidet av professor Erling Johannes Husabø, som konkluderer med at det er tvilsomt om EOS-utvalgets klagebehandling i seg selv er nok til å oppfylle kravene til effektivt rettsmiddel etter EMK art. 13.

[101] Se generelt om dette i NOU 2015:13.

[102] Dette er også utgangspunktet for regjeringens avveininger mellom personvern og kriminalitetsbekjempelse i Prop. 68 L (2015-2016) kapittel 3.

[103] Tesen synes heller ikke å ha støtte i befolkningen, se Teknologirådets og Datatilsynets publikasjon «Personvern – tilstand og trender 2014» (Oslo, januar 2014) s. 9-10.

[104] Se Meld. St. 37 (2015-2016) Årsmeldingane til Datatilsynet og Personvernnemnda for 2015.

ning. Det avgjørende for utvalget har vært situasjonen i Norge, og det presserende behovet for DGF i forhold til cyberutfordringene i vårt land. Etter hva utvalget er kjent med, er de kontrolltiltak og begrensninger som foreslås for et norsk DGF, strengere enn hva som er tilfellet i andre land. Utvalget fremhever at DGF vil innebære et inngrep i folks personvern. Sikkerhetshensyn kan på den annen side etter omstendighetene tilsi slike inngripende virkemidler. Særlig gjelder det når formålet er å beskytte Norge som selvstendig stat, samt beskytte befolkningen mot alvorlige og omfattende trusler. Behovet for DGF fremstår for utvalget som godt begrunnet, og utvalget har forsøkt å gi en grundig beskrivelse av hva som kan oppnås og konsekvensene dersom det ikke åpnes for DGF. I forhold til at detaljer i trusselbildet og opplysninger om E-tjenestens metodebruk er sikkerhetsgradert, mener utvalget at det i rapporten her utvises en åpenhet som for få år siden ville vært utenkelig. Dette bør også gjenspeiles i ny lovgivning.

Samlet sett har nytten av DGF i det digitale trusselbildet og formålsbegrensningene og kontrollmekanismene som foreslås, vært avgjørende for at proporsjonalitetsvurderingen har vippet i favør av å etablere et DGF. [105] Nødvendighetskriteriet i EMK art 8 er strengt, men i den digitale tidsalder er det vanskelig å tenke seg at noe annet virkemiddel skal kunne fungere. Tvert imot antar utvalget at DGF vil kunne minske behovet for andre digitale tiltak som i sum kan påføre et enda høyere og mer uregulert overvåkingsnivå med dårligere kontroll. Samtidig må det tas høyde for at teknologien stadig går fremover, og at man på et senere tidspunkt kan få mer ut av datastrømmene enn i dag. Formålsglidning må søkes forhindret så langt som mulig, og i et gitt presset politisk situasjon kan det være vanskelig å stanse en regulatorisk utvikling. Utvalget har derfor gjennom forslagene knyttet til filtrene og reguleringen av databasene vektlagt å bygge personvern inn i de tekniske løsninger for DGF-systemet («privacy by design» eller «innebygget personvern»). Tekniske søkemekanismer, tekniske godkjenninger og programmert lagringstid kan være forhold som kan være tyngre å endre, enn eventuelle lovforslag som utvider hva dataene kan brukes til. Slik «innebygget personvern» er mulig for et DGF fordi DGF-arkitekturen ennå ikke er anskaffet og bygget. Utvalget mener også at befolkningen, med de begrensninger og kontrolltiltak som er foreslått, vil kunne ha tillit til at dataene kun anvendes for E-tjenestens formål og at en eventuell nedkjølingseffekt derfor blir svært liten.

Behovet for DGF kan endre seg over tid, og dette bør man ta høyde for. Utvalget forutsetter at dersom DGF innføres, bør ordningen evalueres etter å ha virket en viss tid med sikte på å vurdere om DGF bør videreføres som et nødvendig og forholdsmessig tiltak i lys av situasjonen på evalueringstidspunktet. Etter utvalgets syn har Datatilsynet et viktig poeng når tilsynet understreker at det er svært sjelden inngripende fullmakter reverseres selv om behovet for fullmaktene reduseres. Dette bør uansett ikke hindre en evaluering, som første gang bør skje 5 år etter at DGF har virket operativt. Et grunnlag for evaluering vil inkludere ugraderte rapporter fra både DGF-domstolen, DGF-tilsynet og EOS-utvalget, som så langt mulig bør inkludere relevant statistikk. Dette vil gi borgerne grunnlag for tillit til systemet.

Totaliteten av ulike overvåkingstiltak i samfunnet er viktig. Samlet sett kan personvernet utfordres gjennom små skritt som hver for seg har gode intensjoner og er godt begrunnet, men som samlet sett kan ha utilsiktede konsekvenser. Man har gjennomført en rekke «terrorpakker» i Norge siden 2001. Man har flyttet grensene for det straffbare, introdusert flere inngripende metoder, og gitt disse anvendelse i det forebyggende sporet fremfor bare i etterforskningssporet. Utvalget mener at det er grunner som taler for en samlet gjennomgang av personvernets kår på dette området[106], men mener at det er enda viktigere at grundige personvernvurderinger innarbeides i de utredninger som ligger til grunn for de enkelte tiltak, slik at balansen mellom sikkerhet og personvern regelmessig gjøres til gjenstand for en bred offentlig debatt knyttet til konkrete problemstillinger, og ikke kun til generelle, teoretiske og verdibaserte betraktninger.

[105] Dette samsvarer med konklusjonen om signalspaning i Sverige i en delbetenkning fra den svenske personvernkommisjonen som ble oppnevnt av regjeringen i mai 2014 (Hur står det till med den personliga integriteten? – Delbetänkanda av Integritetskommittén, Stockholm 7. juni 2016). Kommisjonen anser risikoene for at signalspaning kan utfordre personvernet som «påtagliga», men ikke «allvarliga». Dette begrunnes med «att det finns tydliga regler om på vilket sätt denne spaning får bedrivas, att kontrollfunktionerna förefaller att fungera ockh att endast en ytterst liten del av den totala informationen blir granskad».

[106] Se f.eks. Representantforslag 94 S (2015-2016).

Utvalget mener DGF kan bygges på et entydig, klart og presist regelverk som hjemler inngrepet i personvernet. Utvalget mener at inngrepet er nødvendig og proporsjonalt. Utvalget anbefaler en effektiv kontroll for å hindre misbruk, og at det foreligger effektive rettsmidler for borgerne til å rette opp feil og ivareta sine interesser. Samlet sett mener utvalget at DGF, slik løsningen er skissert her, ikke utfordrer personvernet på en uakseptabel måte. Samtidig presiseres at konklusjonen kan bli motsatt dersom utvalgets løsninger endres i særlig grad.

9.5.4. Er konsekvensene for ekomindustrien i Norge akseptable?

Det er få holdepunkter for at innføring av DGF i Norge vil ha negative konsekvenser for norske IT-virksomheters konkurranseevne eller for internasjonale investeringer i Norge på dette feltet, f.eks. ut fra tankegangen om at en «overvåkingsfri sone» kan tiltrekke seg kommersielle aktører. Snarere tvert om: Et klart, åpent og presist rettslig rammeverk, og en klar evne og vilje fra myndighetenes side til å beskytte infrastruktur fra bl.a. ytre alvorlige cyberangrep, kan virke avklarende og kunne styrke konkurranseevne og investeringsvilje. En analyse foretatt av *Gearshiftgroup* for det finske forsvarsdepartementet om konsekvensene av svensk lovgivning (lag om signalspaning, også kalt FRA-lagen) for utenlandske investeringer i svensk IT-sektor, publisert i 2015 [107], understøtter dette. Analysen konkluderer slik:

"In conclusion, it is safe to say that no clear connection between the potential impact of the FRA Act on foreign investments in the IT sector following the enactment of the law or differences relative to equivalent investments in Finland could be established on the basis of the present study.

At the same time, the findings suggest that a precise piece of legislation may actually provide a more predictable operating environment for the IT sector. Investments rest on a more solid foundation when the common rules are clear. Large international corporations are today more aware of cybersecurity, an area where regulations issued by government to monitor content and defend against attack are welcomed."

Det må i denne sammenheng tas i betraktning at myndighetstilgang til kommunikasjon i fiberkabler er den dominerende praksis internasjonalt. Under henvisning til facebooks etablering i Sverige må det også erkjennes at andre faktorer som politisk stabilitet, samt billig strøm og kjøling, trolig teller mer enn eksistensen av en strengt regulert og forutsigbar myndighetstilgang. Utvalget mener derfor at etablering av DGF neppe vil ha nevneverdig betydning for næringsutviklingen på dette området, selv om det ikke kan utelukkes at etablering av DGF kan anses viktig for enkelte tilbydere.

Innføring av DGF innebærer intet pålegg til tjenesteleverandører om å lagre data. Det vil heller ikke innebære noen nevneverdige administrative eller økonomiske kostnader for tilbyderne. Det vises for øvrig til at utvalget har fått opplyst fra E-tjenesten at tjenesten i sine forslag har lagt til grunn at alle merkostnader for tilbyderne knyttet til tilretteleggingsplikten vil bli dekket av staten. Utvalget legger dette prinsippet til grunn.

DGF vil innebære en plikt for tjenesteleverandørene om å legge forholdene til rette for E-tjenestens aksess (tilretteleggingsplikten). Teleoperatører og andre tilbydere av nett og tjenester som opererer i andre land er vel kjent med tilsvarende ordninger i utlandet. Tilretteleggingsplikten bør inkludere tiltak som kan bidra til å effektivisere E-tjenestens testanalyser og ressursbruk, samt tilrettelegging for drift og vedlikehold av etablerte løsninger. Den nærmere utforming av tilretteleggingsplikten bør utredes nærmere, og tydeliggjøres i lovgrunnlaget for DGF.

Det er antatt at utviklingen innen sikkerhetsteknologi vil gjøre bruken av sterk kryptering av samband og tjenester mer vanlig i årene fremover. Dette er et positivt tiltak for kommunikasjonsfriheten og for generelt å hindre uvedkommende adgang til informasjon. Utviklingen vil samtidig kunne vanskeliggjøre E-tjenestens samfunnsoppdrag. Tjenestetilbydernes tilretteleggingsplikt må ta høyde for utviklingen innen kryptering. Tilretteleggingsplikten for teletilbyderne må derfor omfatte leveranse av datastrøm uten linkkryptering dersom dette er implementert på den grensekryssende forbindelsen. Tilretteleggingsplikten bør imidlertid ikke inneholde krav om støtte til omgåelse av krypto utover dette. F.eks. vil brukergenerert kryptering ikke være omfattet av til-

[107] Gearshiftgroup: *Foreign investments in the IT sector in Sweden and Finland during 2008-2013 and the potential impact of the Swedish 'FRA Act' on investments*, inntatt som vedlegg til en arbeidsgrupperapport, publisert her: http://www.defmin.fi/files/3144/GUIDELINES_FOR_DEVELOPING_FINNISH_INTELLIGENCE_LEGISLATION.pdf.

retteleggingsplikten For øvrig bør tilretteleggingsplikten følge de alminnelige bestemmelser etter ekomloven og ekomforskriften om tilrettelegging ifm. politiets kommunikasjonskontroll. Utvalget understreker at DGF ikke vil innebære at myndighetene vil presse tilbyderne til ikke å øke kommunikasjonssikkerheten.

En slik medvirknings- og tilretteleggingsplikt er nødvendig for å oppnå formålet med DGF, og for å unngå at hensynet til viktige nasjonale interesser overlates til den enkelte tilbyder å vurdere viktigheten av. En plikt til utlevering og medvirkning vil stille samtlige tilbydere likt, og man vil unngå at enkelte tilbydere unnviker et samarbeid ut fra konkurransemessige eller andre hensyn, herunder eventuelt press fra utenlandske eierinteresser som ikke har den samme motivasjon til å bidra til å trygge norske viktige interesser. På den annen side ligger det i sakens natur at formelle pålegg kun vil være et aktuelt middel dersom frivillig samarbeid ikke fører frem.

I utgangspunktet vil tilretteleggingsplikten gjelde for alle tilbydere som definert i ekomloven § 1-5. Det er på forhånd ikke gitt å identifisere hvilke tilbydere av kommunikasjonstjenester som vil bli mest berørt av lovforslaget. Dette vil bero på testvirksomhet og analyser av hvem som antas å ha best kontroll over utenlandsetterretningsrelevant kommunikasjon, og det må også tas høyde for raske og mer langsiktige endringer av dette bildet. I utgangspunktet vil enhver tilbyder kunne bli berørt, i den utstrekning de kan gi tilgang til elektronisk kommunikasjon som går over landegrensene.

Tilretteleggingsplikten antas i seg selv ikke å medføre at tilbyderne må gis innsyn i sikkerhetsgradert informasjon. Om nødvendig kan imidlertid sikkerhetslovens bestemmelser og ekomlovens taushetspliktregler gjøres gjeldende, på samme måte som i dag.

Nasjonal kommunikasjonsmyndighets (Nkom) tilsyns- og adgangsrett etter ekomloven kapittel 10 bør etter utvalgets vurdering ikke gjelde med hensyn til informasjon og områder som vil gi Nkom innsyn og myndighet i forhold til E-tjenesten og DGF-systemet, ut over det som eventuelt er nødvendig i forhold til å føre tilsyn med at tilretteleggingsplikten etterleves. Tilsyn og kontroll vil i stedet ivaretas av de særskilte kontrollregimer som utvalget anbefaler.

I enkelte tilfeller vil det foreligge gode grunner for å gripe inn i kommunikasjonsvernet (se kap. 6.5), og det finnes et handlingsrom for nasjonale tilpasninger. Vilkårene for inngripen er ikke vesensforskjellige fra inngripen i forhold til personvernet, selv om kommunikasjonsvernet også er underlagt særskilt regulering i internasjonale instrumenter (EUs kommunikasjonsdirektiv[108], Europarådets deklarasjon om kommunikasjonsvern på Internett[109], etc.). Utvalget viser derfor til vurderingene ovenfor i kap. 9.5.2 om forholdet mellom DGF og Norges menneskerettslige forpliktelser.

9.5.5. Er det en risiko for at uvedkommende får tilgang til overvåkingsutstyr og/eller innsamlet informasjon?

Hendelser har vist at det ikke er mulig å lage noen elektroniske systemer som er fullt ut sikre mot datainnbrudd. Reduksjon av risiko for at uvedkommende får tilgang til data og utstyr må derfor ha høy prioritet.

E-tjenesten besitter det som kanskje er Norges fremste ekspertisemiljø innen cybertrusler. Deres lokaler er fysisk godt skjermet, og oppmerksomheten rundt elektronisk sikkerhet og datasikkerhet er svært høy. Få om noen institusjoner i Norge er kompetansemessig bedre i stand til å ivareta sikkerheten rundt sine systemer. Grunnet DGF-systemets sensitivitet anbefaler utvalget at DGF-tilsynet har som en tilleggsoppgave å føre tilsyn med at datasikkerheten er så høy som teknologisk og praktisk mulig[110].

En særskilt problemstilling er knyttet til en potensiell fremtidig ikke-demokratisk maktovertakelse. Det bør utvikles mekanismer og rutiner for både sletting av all informasjon lagret i DGF, og for ødeleggelse av DGF-utstyret. Disse mekanismene og rutinene bør innrettes slik at det kan iverksettes ved ikke-demokratisk maktovertakelse.

[108] Direktivet er EØS-relevant og er nå under revisjon som følge av EUs nye personvernpakke. Direktivets artikkel 15 legger opp til en vurdering som ligger tett opp mot inngrepsvurderingen etter EMK artikkel 8.

[109] Freedom of communication on the Internet, Declaration adopted by the Committee of Ministers on 28 May 2003.

[110] Se note 92.

10. UTVALGETS KONKLUSJONER

Utvalget anbefaler at DGF etableres. Utvalget finner etter en samlet vurdering at DGF kan forsvares som nødvendig i et demokratisk samfunn. Under forutsetning av at kontrollregimet blir utformet slik som beskrevet i kapittel 9, vil vi også anse tiltaket som forholdsmessig i forhold til menneskerettighetene generelt, personvernet spesielt og konsekvensene for ekomindustrien i Norge, samt i lys av risiko for formålsglidning og uvedkommendes tilgang til informasjon. Marginene er imidlertid små. En svekkelse av de prinsipper vedrørende kontrollmekanismer og øvrige forutsetninger vi har beskrevet, vil kunne endre forholdsmessighetsvurderingen.

En eventuell innføring av DGF i Norge må tilfredsstille flere absolutte kriterier. Først må det gi en nødvendig etterretningsmessig merverdi. Dernest må det implementeres på en måte som både er juridisk gangbar og teknologisk gjennomførbar. Avslutningsvis må innføringen ikke svekke befolkningens tillit til de hemmelige tjenestene.

I kapittel 9 beskrives en innretning og implementasjon av DGF som er tydelig begrenset i forhold til hva E-tjenesten ideelt sett kunne ønske. Til tross for dette vil DGF være et godt verktøy i E-tjenesten sin verktøykasse, og potensialet for forbedret etterretning gjennom DGF er stort.

DGF vil bidra til at Norge evner å etablere og hevde suverenitet i det digitale rom. Spesielt i forhold til cybertruslene er det vanskelig å se for seg alternative virkemidler som vil gi tilsvarende kapasitetsheving som DGF kan gi. Økningen i cyberoperasjoner mot norske mål gjør at DGF på dette området kan anses som nødvendig. DGF vil også være et effektivt verktøy innen terrorbekjempelse, spesielt i arbeidet med å kartlegge utenlandske ekstremistmiljøer sine kontakter med Norge. For terrorbekjempelse alene er det tenkelig at fraværet av DGF i noen grad kan kompenseres med andre kapasiteter, men det er ikke gitt at slike kapasiteter vil innebære mindre overvåking/inngrep i personvernet enn DGF, antagelig snarere tvert om.

Både i folkeretten og i norsk lov finnes det begrensninger for hvordan DGF kan innrettes, og utvalget anbefaler ytterligere begrensninger i norsk lovgivning. Utvalget har vurdert det slik at den innretning og implementering vi foreslår for DGF vil tåle internasjonal rettslig prøving. Dette er imidlertid et juridisk område som frem til nå i liten grad har vært gjenstand for rettslig vurdering. EU-domstolens underkjennelse av Datalagringsdirektivet setter ned noen grensesteiner, men det er flere relevante saker som nå er under forberedelse. Avgjørelser i disse sakene kommer etter at utvalget har avsluttet sitt arbeid. Når de foreligger, vil DGF naturligvis også måtte vurderes i lys av disse.

Den viktigste teknologiske begrensningen ligger i at nøyaktig filtrering av data som ikke er relevant for E-tjenesten sitt samfunnsoppdrag langt på vei er umulig. Dersom man skal sikre at all ren innenlandstrafikk filtreres bort fra systemet, må man samtidig fjerne svært mye av den trafikken som gjør DGF verdifull. Klare rammer for bruken av data fra DGF er derfor helt påkrevet. Disse rammene må bestå både av teknologiske komponenter og av menneskelige kontrollmekanismer basert på rettslig grunnlag.

Befolkningens tillit til de hemmelige tjenestene er en mindre håndgripelig størrelse enn de juridiske, tekniske og etterretningsmessige aspektene vi har diskutert over. Utvalget mener at kontrollmekanismene som ivaretar de juridiske hensynene, langt på vei også vil virke befordrende på befolkningens tillit. Utvalget mener likevel at det i tillegg er viktig å sette klare grenser for å hindre at DGF skal kunne benyttes mot norske personer i Norge, nå og i fremtiden. Vi vil anbefale at det gjøres klart at DGF kun skal benyttes til utenlandsetterretningsformål, og at det ikke under noen omstendighet skal benyttes til straffeforfølgelsesformål. Spesielt bør DGF kun benyttes av E-tjenesten og til E-tjenesten sitt samfunnsoppdrag. Utvalget ser grunn til å advare om at en debatt i etterkant av fremtidige grove kriminalsaker vil kunne skape et betydelig trykk i retning av at også politiet bør ha tilgang til en DGF-installasjon. En slik tilgang vil utvalget sterkt fraråde.

Utvalget anser at DGF – implementert som beskrevet i kapittel 9 – vil tilfredsstille kravene til etterretningsmessig merverdi, juridisk holdbarhet, teknologisk realisme og tillit i befolkningen. Det er imidlertid etter utvalgets syn få frihetsgrader i hvordan DGF kan innrettes, og selv små endringer i oppsettet kan ha som resultat at etterretningmessig verdi, juridisk holdbarhet eller teknisk implementerbarhet tapes. Utvalget anbefaler også at DGF evalueres 5 år etter at DGF har virket operativt. Et grunnlag for evaluering bør inkludere ugraderte rapporter fra både

DGF-domstolen, DGF-tilsynet og EOS-utvalget, som så langt mulig bør inkludere relevant statistikk. Dette vil gi borgerne grunnlag for tillit til systemet.

Utvalget konkluderer slik:

- DGF kan utformes juridisk holdbart og forholdsmessig i et menneskeretts- og personvernperspektiv ved at filtrene, begrensninger på søk i dataene, formålsbegrensninger og kontrollmekanismene vi har beskrevet implementeres. Dette forutsetter at et tilstrekkelig klart lovgrunnlag vedtas.
- DGF er et potensielt svært personverninngripende virkemiddel, og utvalget kan ikke anbefale innføring av DGF med svakere kontrollmekanismer og tekniske filtre mv. enn det som er beskrevet i rapporten.
- DGF anses som nødvendig for nasjonens sikkerhet, særlig gjelder dette beskyttelse mot sabotasje og spionasje i det digitale rom.
- DGF slik utvalget anbefaler gir etterretningsmessig verdi og er teknologisk realiserbart.
- DGF vil kunne bidra til høyere grad av presisjon i nasjonalt sikkerhetsarbeid og vil derigjennom over tid også virke modererende på det samlede nasjonale overvåkingstrykket.
- DGF bør benyttes utelukkende til utenlandsetterretning. Ikke under noen omstendighet bør informasjon fremskaffet ved DGF kunne benyttes som bevis mot tiltalte i straffesaker.
- DGF slik det er beskrevet i rapporten anbefales innført.

VEDLEGG 1: SCENARIOER

Scenarioene i vedlegget her bygger på scenariobeskrivelser og utdypende forklaringer som utvalget har mottatt fra E-tjenesten.

Scenario - cyberspionasje
Scenarioet

Den sivile etterretningstjenesten ALFA i land X driver en målrettet og omfattende spionasjekampanje ved bruk av trojanere mot flere mål i Norge, inkludert mot departementer, politikere og næringsliv. ALFA er avansert og skjuler sin identitet gjennom mange hoppunkter i utlandet. Kampanjen har i lengre tid vært vellykket, inntil en sensor utplassert i en virksomhet gir alarm. En tid etter går alarmen i en annen virksomhet med lokal sensor. Den norske E-tjenesten var gjennom partnersamarbeid og egeninnhenting kjent med ALFAs særegne signatur, og signaturen var lagt inn i sensorene i de to virksomhetene som utløste alarmen.

Virksomhetene hvor alarmen gikk, fikk med bistand fra NSM ryddet opp i egne systemer. Intet videre skjedde, fordi det ikke var utplassert lokale sensorer hos de øvrige rammede virksomheter og personer. Man avdekket aldri at en rekke andre virksomheter også var rammet, og fortsatt var under angrep. Senere viste det seg at omfattende mengder myndighetssensitiv informasjon (politiske vurderinger, militære forhold og informasjon om sårbarheter i kritisk infrastruktur), forretningskonfidensiell informasjon og intellektuell eiendom var stjålet.

Konsekvensene av spionasjen ble vurdert å ha svært negative konsekvenser blant annet for landets forsvarsevne, særlig i forhold til evnen til å motstå digital sabotasje i krise og krig. Dette skyldes at uautorisert aksess til datasystemer tilknyttet kritisk infrastruktur, som i fredstid benyttes til etterretning, kan utnyttes til sabotasje i en eventuell krise/krig. Det ble videre anslått at spionasje-kampanjen for øvrig hadde kompromittert informasjon til en anslått verdi av 100 millioner kroner.

Verdien av DGF
Innledning
Med DGF hadde man kunnet detektere og stanse kampanjen på et langt tidligere tidspunkt og dermed forhindret tap av store mengder sensitiv informasjon, samt fått et mye bredere bilde av kampanjen og trusselaktøren. Med DGF kunne man fått mer og tidligere informasjon om samtlige rammede mål i Norge, kunnet oppdage andre mål i utlandet, og ervervet mer informasjon om trusselaktørens modus for å kunne detektere senere kampanjer fra samme aktør.

Mer detaljert beskrivelse av scenarioet
Trusselaktøren
Trusselaktøren (TA) er i scenarioet en statlig kapabel og utholdende aktør som har en kontinuerlig etterretningsaktivitet rettet mot Norge gjennom det digitale rom. TA benytter et eller flere hoppunkter i utlandet for å skjule sin identitet (K2 node på figuren nedenfor). Aktøren angriper flere mål i Norge. To av målene har en lokal sensor (stiplet grønn sirkel). Øvrige mål har ikke lokal sensor. Utplassering og drift av sensorer i hver enkelt virksomhet er svært ressurskrevende. Dette medfører at slike sensorer kun kan plasseres ut i et fåtall utvalgte virksomheter som er en del av, eller understøtter, nasjonal kritisk infrastruktur.

Initiell deteksjon og varsling
I dette eksempelet varsler de to lokale sensorene om aktivitet som kjennetegner metoder benyttet av en kjent statlig aktør (*behavior based detection*). Dette kan f.eks. være et bitmønster knyttet til en trojaner eller bruk av en spesiell kommunikasjonsprotokoll. Informasjon om trusselaktørens operasjonsmønster er ofte høyt gradert og har som regel fremkommet som et resultat av internasjonalt SIGINT-samarbeid. Dette fordrer i mange tilfeller at sensoren kan håndtere høygradert informasjon, og i flere tilfeller at sensoren håndteres av E-tjenesten. Alarm fra sensor fører i dette tilfellet til varsel til virksomhetene, som støttet av NSM rydder opp i systemene.

Manglende situasjonsforståelse
De to sensorene som observerte angrepet er kun i stand til å observere trafikk mellom seg selv og TA sin siste kommando- og kontrollnode (K2 node). Dette gir en dårlig oversikt over situasjonen og kan

sammenliknes med å observere TA gjennom et nøkkelhull. Denne begrensede deteksjonskapabiliteten vil etterlate mange spørsmål ubesvart:

- Hvilke andre virksomheter er berørt?
- Hvor mye data er eksfiltrert?
- Når var første kompromittering?
- Hva er intensjonen bak aktiviteten?
- På hvilke måter vil TA komme tilbake?
- etc.

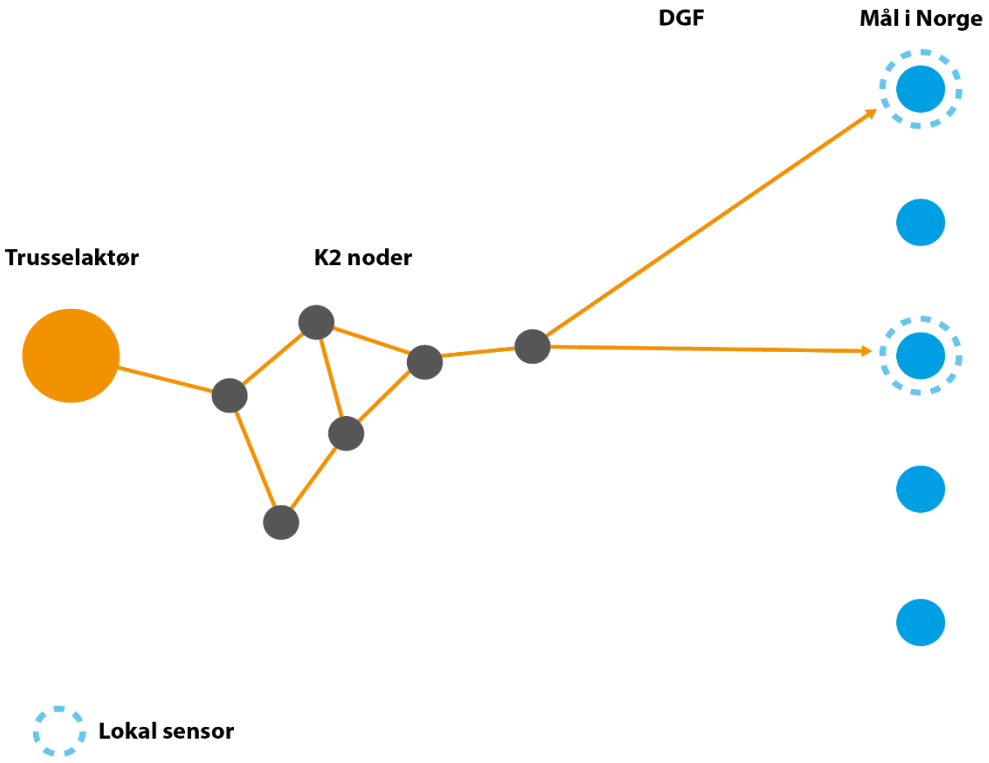

Fig. A. Situasjonsbilde som observert av de to lokale sensorene.

Retrospektiv metadataanalyse

Dersom sensorer ved Norges digitale landegrense lagret trafikkdata (metadata), ville søk og analyse av disse dataene kunne bidra til et mye bedre bilde av situasjonen. I dette eksempelet viser et søk etter IP-adressen til TA sin K2-node i utlandet at K2 noden kommuniserer med ytterligere to virksomheter i Norge. Videre trafikkmønsteranalyse gir i dette tilfellet grunn til å mistenke at også disse to er kompromittert.

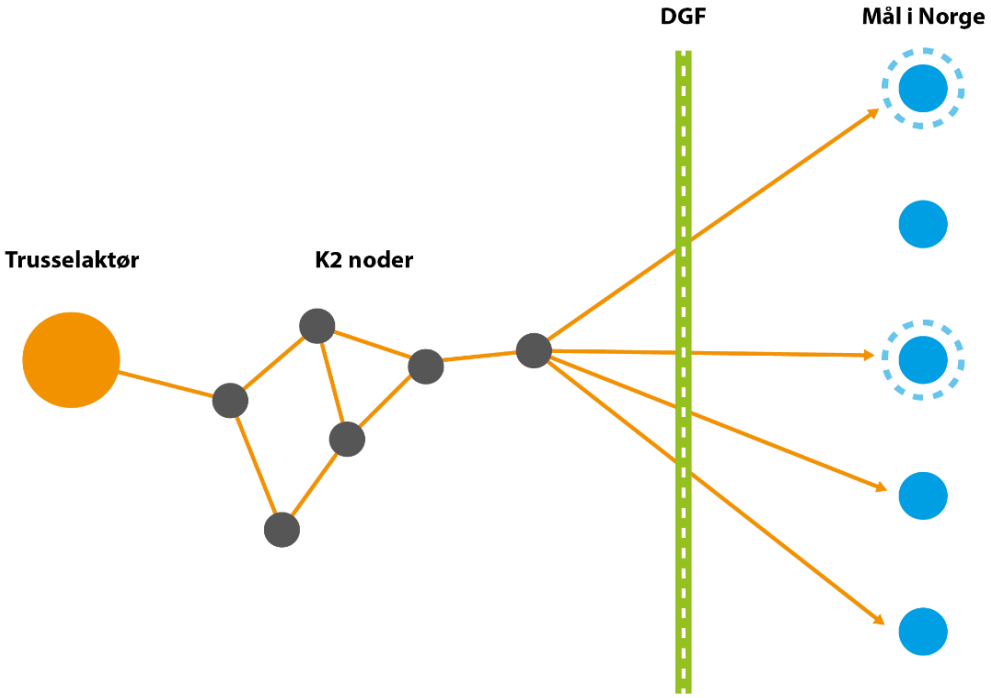

Fig B. Situasjonsbilde etter søk i DGF metadata på TA K2 node

Et søk i utgående trafikk fra de to nye målene viser at ett av målene kommuniserer ut til en rekke land. Dette skjer alltid like etter oppkobling fra den kjente K2 noden. Det gir grunn til å mistenke at en av de norske kompromitterte maskinene benyttes av TA som en K2-node eller til å angripe en tredjepart. Målet eller serveren som er kompromittert tilhører i dette eksempelet et lite firma, med dårlig konfigurerte servere. Firmaet antas ikke å besitte noe av etterretningsmessig verdi. Serveren er trolig valgt ut som mål med tanke på lav sikkerhet, høy båndbredde og svært lav sannsynlighet for tilstedeværelse av en statlig lokal sensor.

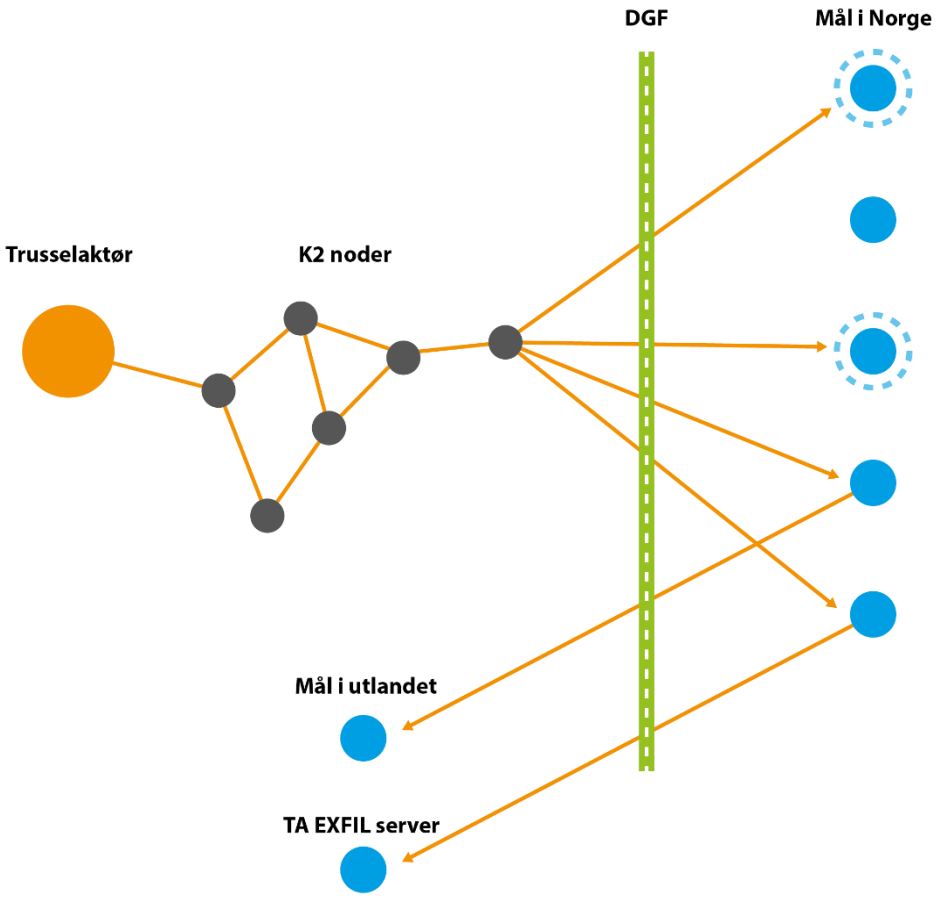

Fig. C. Situasjonsbilde etter søk i DGF metadata på utgående trafikk fra kompromitterte noder

Et av de andre målene sender store datamengder til en server i utlandet mot et portnummer som kan relateres TA. Den utgående trafikken observeres like i etterkant av oppkobling fra den kjente K2 noden. Det oppstår mistanke om at denne serveren er en del av TAs infrastruktur og benyttes for å motta eksfiltrerte dokumenter fra de kompromitterte maskinene. Som det fremgår av figurene vil DGF kunne observere alle grensekryssende kommunikasjonsstrømmer, og således gi en inngående forståelse av det totale omfanget av aktivitet fra TA. Analyse av trafikkdata fra DGF vil etter omstendighetene kunne gi informasjon om mengden data som har blitt eksfiltrert, og avhengig av lagringstid for trafikkdata, vil analysen vise det tidligste tidspunktet for aktivitet fra TAs K2 node.

Analyse av innholdsdata

All analyse av DGF-data har så langt, i dette eksempelet, vært basert på retrospektiv analyse av lagrede trafikkdata. For å bekrefte kompromitteringene fra trafikkdataanalysen, kan det være behov for å gå inn i innholdsdata. I dette eksempelet er TA fortsatt aktiv, og utvalgte IP-adresser som har fremkommet som et resultat av trafikkdataanalysen settes på innsamling, såkalt *tasking*, etter at tillatelse til dette er innhentet. Dette medfører en målrettet lagring med påfølgende manuell analyse av innholdsdata relatert til hendelsen. E-tjenesten vil også benytte sine øvrige kapabiliteter for å kartlegge TA i utlandet, og sammenstille dette med data fra DGF. I tillegg til å avkrefte eller bekrefte mistanke om kompromittering, vil den mer dyptgående analysen også kunne gi nye indikatorer, som det igjen kan gjøres søk på i trafikkdata for å få et enda bedre bilde av aktiviteten.

Etter en analyse av innholdsdata varsles nye berørte virksomheter. Dette skjer i samarbeid med de andre EOS-tjenestene. Videre oppdateres signatursett på

lokale sensorer. Basert på siste års utvikling i det sikkerhetspolitiske klimaet i Europa, sammenholdt med den betydelige økningen i etterretningstrusselen mot Norge, vil en avgjørende suksessfaktor for å bekjempe trusler mot Norge og norske interesser, ved siden av E-tjenestens kapasiteter, være et godt internasjonalt SIGINT samarbeid. Informasjon om trusselaktører i det digitale rom som E-tjenesten detekterer vil være av relevans for E-tjenestens partnere. Utveksling av slik informasjon vil gjøre E-tjenesten til en mer relevant partner for andre land slik at tjenesten blir bedre i stand til å beskytte norske borgere.

Nærmere om verdien av DGF
Dette scenarioet synliggjør merverdien av DGF, og samspillet mellom DGF og sensorer utplassert i virksomhetene. Den største merverdien av DGF vil være å kunne gjøre deteksjon i bredden basert på trafikkdata som kan knyttes til en kjent aktør. Dette kan sammenliknes med en radar ved den digitale landegrense. Ved utslag på indikatorer lagres og analyseres innholdsdata relatert til hendelsen for dypere analyse. Samspill med partnere og E-tjenestens øvrige sensorer og kapabiliteter blir viktig for å møte krypteringsutfordringen, men dette er uansett ikke en problemstilling i forhold til «radar-funksjonaliteten». DGF vil gi bedret evne til deteksjon, som ikke kan kompenseres gjennom utplassering av flere lokale sensorer. Gjennom samspill med andre kapabiliteter og nasjonale og internasjonale partnere, vil kapabiliteten gi en bedre forståelse av digitale trusler og dermed øke muligheten til forebygging og avverging.

Helt konkret bidrar DGF til følgende:
- Nasjonal suveren evne til å avdekke hendelser og angrep
- Bedre og tidligere deteksjon
- Hindre at norsk infrastruktur blir brukt for å understøtte angrep mot andre land
- Bedre forståelse av omfanget av en hendelse
- Bedre forståelse av trusselaktører
- Inngangsverdier til andre kapasiteter og sensorer
- Verdifull etterretningsinformasjon til partnere nasjonalt og internasjonalt
- Økt mulighet for rask håndtering ved mottiltak, samt evt. iverksettelse av nødvendige skadebegrensende tiltak.

Den mest åpenbare merverdien av DGF vil være å kunne observere alle inngående og utgående oppkoblinger mellom utlandet og Norge, og dermed ha potensial til å kunne se hele omfanget av en trusselaktørs aktivitet mot Norge. Dersom DGF-sensorene f.eks. mates med informasjon om kjente kommando- og kontrollnoder knyttet til en utenlandsk trusselaktørs infrastruktur, vil dette gi en unik mulighet til å detektere hele omfanget av aktiviteten fra aktøren.

Forholdet mellom DGF og lokale sensorer
Som eksempelet viser, vil lokale sensorer og en eventuell DGF virke utfyllende på hverandre. En lokal sensor vil, avhengig av avtale med virksomheten, kunne ha tilgang til intern trafikk i virksomheten og til en viss grad mulighet til å inspisere enkelte typer kryptert kommunikasjon (HTTPS o.a.). Dette betyr at en lokal sensor vil kunne gå noe mer i dybden ved en hendelse i virksomheten der sensoren er plassert, mens DGF vil kunne gi mer informasjon om trusselaktørens samlede aktivitet mot Norge. Indikatorer vil kunne utveksles begge veier for enda bedre deteksjon og forebygging. DGF kan sammenliknes med utplassering av sensorer på stammen i forhold til utplassering i hver av de ytterste grenene i en trestruktur. DGF og lokale sensorer vil være komplementære. Den oversikten som DGF vil gi, vil ikke være mulig å oppnå ved utplassering av sensorer i den enkelte virksomhet, både grunnet behov for samtykke og det massive omfanget av sensorer som da måtte plasseres ut for å få en god dekning.

Om lagring av metadata
Trafikkdata er teknisk informasjon om hvem som har kommunisert med hvem, hvor kommunikasjonen har funnet sted, når og hvordan. Eksempler på dette er IP-adresser, portnummer, protokoll og datamengde. Metadata (se kap. 4.3) vil være et paraplybegrep for trafikkdata, lokaliseringsdata og øvrig data som ikke kan anses som innholdsdata.

Selv om trafikkdata alene ikke kan si noe særlig om hvilket individ eller selskap kommunikasjonen omhandler, slik som en e-post adresse eller facebook ID gjerne gjør, er en IP-adresse likevel etter personopplysningsloven å anse som en personopplysning. Dette fordi en IP-adresse med relativt enkelte midler ofte kan knyttes til en enkeltperson. Behandlingen av denne type trafikkdata må derfor ivareta bestemmelser om oppbevaring, deling og sletting gitt i den alminnelige lovgivningen. Metadata knyttet til enkeltpersoner kan røpe betydelige mengder sensitiv informasjon, se kap. 4.3.

I tillegg til behovet for lagring av trafikkdata i form av en trafikklogg, som forklart over, kan det være

behov for å lagre utfyllende informasjon om tjenester på Internett. To relevante eksempler på slik informasjon er lagring av observerte digitale server-sertifikater og knytningen mellom IP-adresser og domener. Det samme gjelder informasjon om knytningen mellom domenenavn og IP-adresse, såkalt «passiv DNS» informasjon. Det er bare behov for å lagre den delen av informasjonen som angår serversiden av kommunikasjonen.

Lagringsbehovet for metadata, i forhold til oppdraget om å avdekke trusler i det digitale rom, kan dermed oppsummeres på følgende måte:

- Trafikkdata, som for eksempel IP-adresse, portnummer og protokoll
- Utfyllende informasjon om tjenester på Internett som for eksempel digitale sertifikater og passiv DNS (kun serverinformasjon)

Om lagring av innholdsdata
I eksemplet er det kun enkelte metadata (trafikkdata) som vil lagres for hele datastrømmen/aksessen. Innholdsdata lagres og analyseres bare for adresser relatert til en pågående hendelse eller trussel, såkalt *selekterte innholdsdata*. Dette fordrer at trusselaktøren fortsatt er aktiv på analysetidspunktet.

Fra et rent etterretningsperspektiv ville det være mer optimalt å mellomlagre alle innholdsdata i en periode (også innholdsdata i perioden mellom deteksjonstidspunktet og til beslutning om innhenting av innholdsdata er besluttet og utført), for å ha muligheten til å gå noe tilbake i tid for å kunne gjøre undersøkelser relatert til aktivitet forut for deteksjonstidspunktet. Gitt aksessens egenart ville dette også medføre mellomlagring av svært mye irrelevant informasjon.

Det er derfor kun aktuelt å lagre *selekterte* innholdsdata for produksjonsformål. Dette er målrettet lagring av innholdsdata basert på selektorer knyttet til en kjent utenlandsk trusselaktør, som for eksempel en IP-adresse. I tillegg har tjenesten behov for å gjennomføre analyse av datagrunnlaget, med formål om å kunne gjøre et relevant utvalg av trafikk, samt tilpasse innsamlingssystemene. Dette er såkalt survey aktivitet, og vil medføre behov for mellomlagring av uselekterte innholdsdata i en meget kort tidsperiode, jf. kap. 9.2 om dette.

Krypteringsutfordringen
DGFs merverdi på dette området vil i mindre grad enn på andre områder berøres av utviklingen innen kryptering. Det som refereres til som radarfunksjonaliteten (deteksjon av IP-adresser mv) i DGF, vil i mindre grad bli påvirket av kryptering, og det er nettopp denne funksjonaliteten som vil være DGFs viktigste funksjon. Erfaring tilsier at svært mye av den informasjonen som er nødvendig, også for dypere analyse av data, fortsatt går ukryptert. Grunnet krypteringsutviklingen er det imidlertid grunn til å anta et denne typen analyse vil bli mer utfordrende å gjennomføre med DGF-data alene i fremtiden. Det er derfor viktig å fremheve at slik analyse vil måtte kompletteres med data fra E-tjenestens øvrige sensorer og kapabiliteter. I tillegg vil analysen kunne støttes med informasjon fra eventuelle lokale sensorer og samarbeid med berørte virksomheter for å kompensere for noe av krypteringsutfordringen. I den utstrekning DGF vil bli påvirket av krypteringsutfordringer i fremtiden, vil dette således i stor grad kunne kompenseres med samspill med tjenestens øvrige kapabiliteter og data fra lokale sensorer, samt samarbeid med NSM, PST og den aktuelle virksomheten.

Scenario – internasjonal terrorisme
Scenarioet

En ekstrem islamistisk gruppering har tilholdssted i landet X i Midtøsten. Samfunnsstrukturer har brutt sammen, og landet X er i realiteten et konfliktområde og en «failed state». Gruppen uttaler et globalt fokus for sin virksomhet og truer vestlige interesser og Europa spesielt. Ved bruk av sosiale medier på internett driver gruppen både radikalisering og rekruttering av målgrupper i Europa. En betydelig andel av de som rekrutteres har skandinavisk bakgrunn. Som ledd i gruppens intensjon om å ramme Europa, planlegges det nå å utføre et terrorangrep i Norge. Det planlagte angrepet innebærer bruk av personer som over tid har trent i gruppens kjerneområder, i tillegg til en logistisk komponent som innebærer bruk av støttestrukturer i Norge. Støttestrukturen har som oppgave å skaffe til veie oppholdssted for angrepslaget, i tillegg til at den skal besørge våpen og eksplosiver for gjennomføring av selve angrepet. Det er et poeng at profilen på individene i støttestrukturen ikke er av en slik karakter at de tiltrekker seg politiets søkelys.

I kommunikasjon med gruppens ledelse i Midtøsten mottar støttestrukturen i Norge instruksjoner for forberedelser til angrepet. Detaljene i angreps-

planen holdes skjult. Parallelt med at støttestrukturen bringer til veie innkvartering, våpen og eksplosiver, starter angrepslaget fra Midtøsten på turen som skal ta dem til Norge. Angrepslaget bestående av fire personer utstyres med falske identitetspapirer, alle utstedt fra konfliktområdet. For å unngå europeiske etterretnings- og sikkerhetstjenesters søkelys følger de etablerte migrasjonsruter fra konfliktområdet til Europa, samt at de bevisst velger å ikke benytte fremmedkrigere fra Norge til å utføre angrepet.

Angrepslagets leder sender en e-post til støttestrukturen et par dager før ankomst for å gi støttestrukturen beskjed om nærmere tidspunkt for ankomst, da angrepslaget grunnet migrasjonskontroll lenger syd hadde blitt to dager forsinket. Gruppens ledelse i Midtøsten mottar etter fem uker en bekreftelse fra støtteapparatet i Norge om at angrepslaget har ankommet og at alt går etter planen.

Tre dager etter ankomst til Norge, en fredag ettermiddag, gjennomfører gruppen et koordinert angrep mot T-banenettet i Oslo. For å oppnå størst mulig effekt og kaos detoneres selvmordsvester mens t-banevognene er i fart i tunnelene. I tillegg har to fra angrepslaget stilt seg utenfor t-baneinngangene på stasjonene Nasjonalteateret og Stortinget, og skyter mot de menneskene som forsøker å flykte. 140 mennesker blir drept og 305 skades før terroristene er nedkjempet av politiet.

Verdien av DGF

E-tjenesten følger aktiviteten i konfliktområdet og bygger over tid opp kjennskap til individer og nettverk gjennom bl.a. innsamling av elektronisk kommunikasjon. Innsamlingen bidrar til å belyse gruppens kapasiteter og intensjoner om å ramme Europa, samtidig som den identifiserer individer og deres kommunikasjonsvaner.

Kommunikasjonen mellom gruppens ledelse i Midtøsten og støttestrukturen i Norge kunne ha blitt fanget opp på et tidlig tidspunkt, på den måten at innsamling av kommunikasjon i X ville blitt korrelert mot kommunikasjon inn og ut av Norge. Uten DGF vil det i praksis ikke være realistisk å avdekke at kommunikasjon samlet inn i Midtøsten faktisk har en norsk ende, fordi stadig mer kommunikasjon går via infrastruktur i andre deler av verden. Dersom man utelukkende har DGF som sensor, vil det på samme måte være vanskelig eller umulig å fange opp at den ene enden av kommunikasjonen stammer fra Midtøsten.

I scenarioet fanges den logiske kommunikasjonen mellom Midtøsten og Norge opp ved å sammenstille det som samles inn i Midtøsten og det som samles inn ved Norges digitale grense. Basert på kartlegging av kommunikasjonsform ved metadata, som igjen danner grunnlaget for å oppdage korrekt innholdsdata som beskriver den reelle trusselen mot Norge og norske interesser, vil E-tjenesten kunne varsle PST om at en ekstremistgruppe fra Midtøsten har kontakt med individer i Norge. PST gis dermed anledning til å iverksette nødvendige tiltak for å utrede og bidra til å avverge trusselen.

Angrepslaget fanges opp i det de starter reisen ut av konfliktområdet. Dette gjøres med den innsamlingen E-tjenesten har i konfliktområdet. Det er ikke kjent hvor gruppen er på vei når den forlater tjenestens dekningsområde. Ved å ha tilgang til DGF fanges disse opp igjen når de innpasserer i Norge eller om de under ferden til Norge kommuniserer inn til riket og aktivitet fra historisk kjente selektorer registreres aktive. E-tjenesten kan så varsle PST om at kommunikasjonsmidler knyttet til terrorvirksomhet i Midtøsten nå befinner seg i Norge. PST kan dermed få et grunnlag for metodebruk for å følge terroristenes bevegelser i Norge.

Terrorgruppen kommuniserer ved bruk av en rekke forskjellige kommunikasjonstjenester. Noen av disse tillater terroristene å kommunisere kryptert. Til tross for at kommunikasjonens innhold er kryptert, formidles som nevnt over enkelte eksterne parametere relatert til kommunikasjonen ukryptert. E-tjenestens mulighet til å sammenholde kommunikasjonens metadata, både på det tidspunktet det sendes fra konfliktområdet og på tidspunktet det passerer grensen til Norge, forteller i det minste at det er kommunikasjon mellom kjente individer i utlandet og individer i Norge. Videre er kunnskapen E-tjenesten besitter om individene i utlandet av en slik karakter at det faktum at kommunikasjon har funnet sted med en person i Norge, alene kan gi grunnlag for varsling til PST.

Den samlede kunnskapen om individene er i stor grad basert på gjennomgang av individenes kommunikasjon over tid, inkludert i de tilfellene der individene har kommunisert på en slik måte at innholdet i kommunikasjon har blitt fanget opp og er lesbar. Over tid har dette gitt E-tjenesten anledning til

å tegne et bilde av individenes og gruppens intensjon og kapasitet. I et dynamisk og flyktig signalmiljø vil det finnes muligheter for å tilegne seg relevante parametere, til tross for økt bruk av kryptert kommunikasjon.

En avgjørende faktor er tilgang på historiske metadata. Kravene til metadata er at de som et minimum inneholder de kommuniserende parters tekniske identifikatorer som for eksempel telefonnummer, epostadresser, brukernavn, osv. I tillegg forutsettes svært presis tidsangivelse for når og hvor kommunikasjonen har funnet sted. Når man ser på hvor en kommunikasjon har funnet sted, vil man se på ulike verdier avhengig av hva slags type kommunikasjon det er tale om.

På generell basis kan DGFs merverdi i kontraterrorsammenheng oppsummeres slik:

- Bedret deteksjonsmulighet av utenlandske trusler mot Norge, herunder avdekking av trusselaktørers intensjoner og kapasiteter
- Mulighet for å detektere om en trusselaktør passerer norske grenser
- Økt mulighet for å iverksette nødvendige nasjonale mottiltak for å avverge angrep
- Verdifull informasjon til partnere nasjonalt og internasjonalt

VEDLEGG 2: FORHOLDENE I ANDRE LAND

Innledning

I dag har de fleste land i verden, deriblant mange sammenlignbare stater som Sverige, Tyskland, Frankrike, Storbritannia, USA og Canada, i større eller mindre grad aksess for etterretningsformål til grenseoverskridende kommunikasjon som går i fiberoptiske kabler. Trenden er at stadig flere land ser dette som nødvendig. Nederland og Finland vurderer å etablere tilsvarende aksess. Sveits har nylig vedtatt lovgivning om det samme.

Det kan ikke gis en uttømmende liste over hvilke øvrige land som har slik aksess, fordi enkelte antas å ha aksess uten at de ønsker offentlig oppmerksomhet om dette. I det følgende gis det en oversikt over noen av landene som gir deres utenlandsetterretningstjenester tilgang til kommunikasjonsdata som transporteres i fiberoptiske kabler, og som er land Norge vanligvis trekker frem i andre sammenhenger for å få fram komparative argumenter og hensyn i en helhetlig fremstilling av en konkret tematikk. Utvalget understreker at fremstillingen utelukkende bygger på åpne kilder.[111] Det må derfor tas forbehold om at realiteten kan være noe annerledes i enkelte land enn det som fremkommer åpent.

En generell kommentar til fremstillingen er at selv om materielle vilkår for å kunne gjøre målrettede spørringer i innhentet kommunikasjonsdata fra kabel fremgår av de fleste lands lover og regelverk som er offentlige tilgjengelige, vil den reelle terskelen for bruken av tilgangen likevel vanskelig kunne fastlegges, da beslutningspraksis til beslutningstakeren samt interne prosedyrer for den enkelte tjenesten av åpenbare grunner ikke er kjent. I tillegg vil intern legalitetskontroll ikke være mulig å kartlegge basert utelukkende på åpne kilder.

Av de såkalte Five Eyes-landene (5EYES) omtales kun forholdene i Storbritannia og Canada. Forholdene i USA er alminnelig kjent gjennom dokumenter knyttet til Snowden og etterfølgende utredninger og regelendringstiltak. Om det amerikanske såkalte 702-programmet for bulk innsamling i medhold av FISA (Foreign Intelligence Surveillance Act) vises særlig til rapporten av 2. juli 2014 fra *Privacy and Civil Liberties Oversight Board*. Når det gjelder Australia og New Zealand har utvalget ikke prioritert å omtale disse landene.

Sverige (FRA)

FRA-loven (Lag om signalspaning i försvarsunderrättelseverksamhet, lag 2008:717), sammenholdt med lag om försvarsunderrättelseverksamhet (lag 2000:130) og lag om elektronisk kommunikation (lag 2003:389), gir Försvarets Radioanstalt (FRA) hjemmel for tilgang til kommunikasjonsdata som føres i alle former for fysiske kabler over Sveriges riksgrense, og oppstiller vilkår for å benytte denne tilgangen. Innenlandsk trafikk som ikke rutes over grensen vil imidlertid ikke omfattes av loven. En egen personopplysningslov gjelder for FRA.

FRA-loven krever at FRA[112] må søke om tillatelse til å benytte kabeladgangen (signalspaning), gjennom målrettede søk mv («søkbegrepp»), til Försvarsunderrättelsesdomstolen, som er en særdomstol utelukkende opprettet for dette formålet. Når en begjæring om tillatelse til signalspaning er kommet inn til domstolen, skal domstolen så snart som mulig utnevne et personvernombud i saken og holde rettsmøte. Ved rettsmøte skal begjærende myndighet og personvernombudet være til stede.

Det følger av loven at innhenting av informasjon bare kan iverksettes for nærmere oppstilte utenlandsetterretningsformål, og bare når hensynet til etterretningsformål veier klart tyngre enn hensynet til personlig integritet. Oppdragsgivere for signaletterretningsvirksomheten er regjeringen, Regjeringskansliet, Försvarsmakten, Säkerhetspolisen og NOA (Nationella operativa avdelningen innom polismyndigheten, tidligere Rikskriminalpolisen). Informasjon fremskaffet gjennom signalspaning kan ikke benyttes for straffeforfølgningsformål.

[111] Fremstillingen i kapittelet her bygger blant annet på en rapport fra november 2015 av European Union Agency for Fundamental Rights (FRA) om "*Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Mapping Member States' legal frameworks*".

[112] Försvarets Radioanstalt.

Gjennom det prosessuelle kravet om tillatelse fra domstolen før spørringer kan foretas i kommunikasjonsdata, vil FRA være underlagt uavhengig forhåndskontroll. Videre forestår Statens inspektion för försvarsunderrättelsesverksamheten (SIUN) uavhengig kontroll med FRA. SIUNs oppgave er i hovedsak å kontrollere at FRA utøver sin virksomhet innenfor gjeldende lovgivning, en kontroll av søkebegrepene som anvendes, og hvordan rapportering skjer. SIUN har også en rolle i å gi FRA praktisk aksess til de relevante kommunikasjonsbærere gjennom å koble opp disse til FRA fra såkalte «samverkanspunkt», dvs. at SIUN opptrer som kontrollsluse mellom tjenestetilbyderne og FRA. En annen uavhengig kontroll som utføres overfor FRA er det Datainspektionen som foretar. Deres primæroppgave er å kontrollere FRAs håndtering av personopplysninger.

Frankrike (DGSE)

Fransk utenlandsetterretningstjeneste (DGSE[113]) har hatt aksess til grenseoverskridende kommunikasjon i hvert fall siden 2008. Lovgivningen er metode- og teknologinøytral.

Statsministeren autoriserer bruk (målrettede spørringer i kommunikasjonsdata) av tilgangen basert på en anmodning fra en minister. Autorisasjonen kan delegeres til en konkret minister. Autorisasjonen er kun gyldig for fire måneder av gangen, men kan fornyes. DGSE kan bare foreta søk basert på anmodning fra en av DGSEs seks oppdragsgivere. Statsministeren setter et tak på hvor mange mål DGSE kan innhente mot samtidig (1840 fysiske personer i 2009). Det kan kun gis autorisasjon basert på en anmodning som begrunner aksessen med at informasjonen er relevant for nasjonal sikkerhet eller andre sikkerhetsrelaterte utfordringer. Loven stiller strenge krav om sletting av informasjonen når den har tjent sitt formål. DGSE kan motta informasjon direkte fra ekomtilbydere begrunnet i hensynet til forebygging av terrorisme. Slik informasjon kan kun behandles i en begrenset tidsperiode.

Den relevante lovgivningen ble revidert i juli 2015. Formålet med revisjonen var å gi myndighetene bedre overvåkningsmuligheter, innenfor et omfattende juridisk rammeverk, særlig relatert til å forebygge terrorhandlinger. Den nye loven styrker ekomtilbydernes plikt til å samarbeide med DGSE, og gir DGSE en mulighet til å pålegge ekomtilbydere å gjennomføre nødvendige endringer i nettverket, herunder automatisering av databehandlingen, for å gi mulighet for bl.a. sanntids innsamling for å forebygge terrorisme.

Hovedkontrollen av DGSE forestås av *National Commission for Security Interceptions* (CNCIS). CNCIS får seg forelagt alle autorisasjoner statsministeren godkjenner for gjennomgang. Ut i fra 6396 autorisasjoner som ble gitt i 2011 var det kun 55 autorisasjoner CNCIS mente burde vært avslått. CNCIS utfører kun etterhåndskontroll, og har ingen instruksjonsmyndighet overfor DGSE. Det forestås ingen ekstern forhåndskontroll av DGSEs virksomhet.

Storbritannia (GCHQ)

GCHQ[114] har i lengre tid hatt bulk-aksess. Virksomheten er først og fremst regulert av *Intelligence Services Act* 1994 (ISA), *Human Rights Act* 1998 (HRA), og *Regulation of Investigatory Powers Act* 2000 (RIPA). Sistnevnt regulerer SIGINT-innhenting konkret. Alle de nevnte lover er metode- og teknologinøytrale.

Det er statsministeren som har det overordnede ansvaret for GCHQ, men tjenesten hører direkte under utenriksministeren. En autorisasjon om å benytte tilgangen til elektronisk kommunikasjon (electronic interception), er det en minister som må godkjenne. RIPA inneholder nærmere krav til varighet, opphør og fornyelse.

Det kan kun gis autorisasjon om tilgang, gjennom søk i kommunikasjonsdata, etter en anmodning som begrunner tilgangen som nødvendig av hensyn til rikets sikkerhet, «safeguarding the economic well-being of the United Kingdom» eller for å bekjempe alvorlig kriminalitet. Overvåking må videre være forholdsmessig i forhold til det som søkes oppnådd med overvåkingen. Det følger også av RIPA at anmodningen enten må inneholde et navn eller et lokale/sted som innhentingen skal rette seg mot. RIPA stiller krav om at tiltak for å minimere inngrepets art ved bruken av kommunikasjonsdata iverksettes. Fremskaffet informasjon kan som hovedregel ikke benyttes som bevis i straffesaker.

GCHQ er underlagt tre ulike etterhånds kontrollmekanismer. Hovedkontrollen forestås av *Intelligence*

[113] Direction Générale de la Sécurité Extérieure.

[114] UK Government Communications Headquarters.

and Security Committee of Parliament (ISC), som også kontrollerer MI5 og MI6. ISC har medlemmer fra alle partiene. To uavhengige kommisjonærer kontrollerer GCHQ, og skal bli forelagt all dokumentasjon de ber om. *Investigatory Powers Tribunal* behandler alle klager fra innbyggere rettet mot GCHQ vedrørende blant annet brudd på retten til privatliv.

Lovgivningen på dette området er under revisjon i Storbritannia, etter tre års utredninger. Forslag til *Investigatory Powers Bill* (av motstanderne døpt «Snooper's Charter») ble fremmet for parlamentet i november 2015 og er fortsatt under behandling der. Lovforslaget inneholder en tydeligere regulering av «bulk collection» enn det som fremgår av gjeldende lovgivning, samt styrker plikten for britiske tjenestetilbydere til å tilrettelegge for aksess og å yte annen relevant bistand. Det foreslås også å gi domstolene en rolle ift. forhåndsautorisasjon. Komiteen som behandler lovforslaget i parlamentet avga sin rapport 11. februar 2016, hvor det anbefales at lovforslaget justeres på en rekke punkter og begrunnes bedre på andre. Menneskerettighetsaspektet ved lovforslaget ble vurdert av parlamentets *Joint Committee on Human Rights* i en rapport av 25. mai 2016. En hovedkonklusjon i rapporten er følgende:

«On the current state of the ECHR case-law, we do not consider the **bulk powers** in the Bill to be inherently incompatible with the right to respect for private life, but capable of being justified if they have a sufficiently clear legal basis, are shown to be necessary, and are proportionate in that they are accompanied by adequate safeguards against arbitrariness."

Canada (CSE)

I følge åpne kilder har CSE[115] i hvert fall hatt kabelaksess siden 2010. SIGINT- innhenting, herunder tilgang til kommunikasjonsdata som transporteres i kabel, er regulert i loven *National Defence Act* (NDA). Loven er metode- og teknologinøytral. Vilkårene for å benytte adgangen til kommunikasjonsdata fra kabel er ikke annerledes enn de vilkårene som stilles for andre innhentingsdisipliner innenfor SIGINT.

Beslutningen om å innhente kommunikasjonsdata besluttes internt i CSE. Det følger av NDA at CSE kun kan innhente SIGINT-informasjon i overensstemmelse med myndighetenes prioriteringer, men kan ikke rette innhentingen mot aktiviteter utført av kanadiske borgere eller mot personer i Canada. Ut over å stille vilkår om at tiltak for å sikre personvernet så langt det er mulig skal iverksettes ved innhenting ved SIGINT, gir NDA eller annet offentlig tilgjengelig regelverk få føringer på hvordan og hvem CSE skal innhente mot. Dette følger av sikkerhetsgradert regelverk.

CSE er underlagt uavhengig kontroll av *the Office of the CSE Commissioner* (OCSEC), som har tilgang til CSEs ansatte og dokumenter. OCSECs kontroll er regulert i NDA. CSE er ikke underlagt noen ytterligere ekstern kontroll, og heller ingen form for forhåndskontroll.

Tyskland (BND)

Basert på åpne kilder tyder mye på at BND[116] i lengre tid har hatt adgang til kommunikasjon som transporteres i kabel.

BNDs virksomhet reguleres av *Gesetz zur Beschränkung des Brief-, Post und Fernmeldegeheimnisses* også kalt «G-10-gesetz». Loven regulerer myndighetenes adgang til å overvåke post og telekommunikasjon, og gir adgang til både individuell overvåkning av personer og såkalt bulkaksess. Mye tyder på at hjemmelen til å bruke slik tilgang allerede ble gitt i 1994, da adgangen til innhenting ble vesentlig utvidet. I avgjørelsen «Weber and Saravia v. Germany» fra 2006, som gjaldt påstand om masseovervåkning for strategiske etterretningsformål, avviste Den europeiske menneskerettsdomstolen at Tyskland hadde opptrådt i strid med Den europeiske menneskerettskonvensjonen.

Tillatelse til å innhente kommunikasjonsdata gis av ministeren som har sektoransvaret for den etaten som søker om overvåkning. En parlamentarisk spesialoppnevnt kommisjon, G10 kommisjonen, avholder månedlige møter der kommisjonen vurderer nødvendigheten og lovligheten på inngrep i personvernet. BND fremmer skriftlig anmodning om et inngrep til ministeren som har sektoransvaret for BND. Dersom anmodningen støttes, går den videre til behandling hos G10 kommisjonen. G10 gir tidsbegrensede tillatelser til å benytte målrettede spørringer i kommunikasjonsdata, dvs. at kommisjonen utøver en uavhengig forhåndskontroll.

[115] Communications Security Establishment Canada.

[116] Bundernachrichtendienst.

Det følger av G-10 loven § 5 at innhenting av informasjon bare kan iverksettes når det er nødvendig for å avverge væpnede angrep mot Tyskland eller for å forebygge og motvirke terroranslag, ulovlig våpenhandel, ulovlig innføring av større partier narkotika, destabilisering av pengevesenet på bakgrunn av pengeforfalskning i utlandet, og organisert hvitvasking av penger. Loven stiller også krav om hvilke søkebegrep BND kan benytte. BND har bare adgang til å bruke søkebegrep som er egnet til å avdekke informasjon om forholdene angitt i tillatelsen. Søkebegrepene skal fremgå av tillatelsen.

BND er underlagt parlamentarisk kontroll, herunder gjennom G 10 kommisjonen. *Parlamentarisches Kontrollgremium* utøver også parlamentarisk kontroll av BND. I tillegg utøver *The Federal Commissioner for Data Protection and Freedom of Information* (BfDI) kontroll i forhold til BNDs overholdelse av personvernloven og andre personvernforskrifter.

Lovgivningen som regulerer BNDs virksomhet er under revisjon, og ny lovgivning forventes fremlagt om kort tid.

Nederland (MIVD/AIVD)

MIVD[117] og AIVD[118] har i dag hjemmel til å foreta *målrettede* spørringer i kommunikasjonsdata, enten data transporteres i kabel eller over satellitt. Tjenestene har imidlertid ikke adgang til å foreta ikke-målrettede spørringer i kommunikasjonsdata som går i kabel, kun i satellitt. Regjeringen i Nederland ga i 2014 uttrykk for at man ønsket å revidere *Intelligence and Security Act* fra 2002, for å gjøre loven teknologinøytral. Dette var basert på at et utvalg i 2013 (Dessens Committee) konkluderte med at det i dag ikke er lenger grunnlag for å skille mellom kommunikasjon som går i kabel og ikke i kabel (satellittkommunikasjon mv). Revidert lovgivning har imidlertid møtt motstand politisk og fra menneskerettighetsgrupper, som også har anlagt søksmål i saken for nasjonale domstoler, og lovrevisjonens fremtid er derfor usikker. Dog konkluderte regjeringen i midten av april 2016 med å gi tilslutning til lovforslaget, herunder de delene som utvider fullmaktene til etterretnings- og sikkerhetstjenestene til å omfatte lagring av og søk i kabelbundet kommunikasjon. Målsettingen er opplyst å være å oversende et revidert lovforslag til parlamentet i løpet av året.

Det foreliggende lovutkastet legger opp til at det fortsatt skal være forsvarsministeren som beslutter om adgangen til kommunikasjonsdata innhentet ved kabel skal benyttes. Grunnvilkåret for at MIVD kan foreta spørringer i data som tjenesten har tilgang til, er at kommunikasjonen minst har en utenlandsk kilde tilknyttet seg eller en utenlandsk destinasjon, altså at spørringene har utenlandsfokus. I lovforslaget er det foreslått visse tiltak for å styrke kontrollen som dagens kontrollorganer (CTIVD og CIVD) utfører. Kontrollen var opprinnelig forutsatt å være en uavhengig etterhåndskontroll, men resultatet av regjeringens konklusjon i april 2016 var at innhenting også bør forhåndsgodkjennes av en ny uavhengig komité. I tillegg er bruken av innhentede data ledsaget av strenge regler for oppbevaring og sletting. Lovforslaget inneholder for øvrig en plikt for enhver til å bistå med å dekryptere data som tjenesten lovlig kan innhente.

Som ledd i lovutredningen ble det bl.a. foretatt begrepsmessige endringer slik som for eksempel en endring av begrepet "ongericht", som betyr uselektert/bulk/uspesifisert, til begrepet "doelgericht" som betyr målrettet. Det var ikke meningen at det nye begrepet skulle innebære et forbud om bulkinnhenting mot metadata fra kabel, men begrepet ble innført for å klargjøre og begrense bruken av tilgangen.

Sveits (NDB)

Per i dag har ikke NDB[119] kabelaksess. Ettersom innenlands- og utenlandsetterretningstjenestene fusjonerte i 2010, har lovgrunnlaget for de tidligere to tjenestene vært utdatert. Det ble derfor utarbeidet en ny lov, som åpner for tilgang til kommunikasjon i kabel for etterretningsformål. Poenget med den nye loven (*Nachrichtendienstgesetz*) var at den skulle utgjøre et samlet lovgrunnlag for den nye tjenesten NDB - og at den skulle legge lovgrunnlaget for kabelaksess.

Loven ble vedtatt av det sveitiske parlamentet i september 2015, men grunnet etterfølgende mobilisering ble det nødvendige antall underskrifter frembrakt som gjør det nødvendig å avholde en folkeavstemning om loven. Denne vil gjennomføres 25. september 2016. Dersom loven ikke settes til side som følge av folkeavstemningen vil den tidligst tre i kraft medio 2017.

[117] Militaire Inlichtingen- en Veiligheidsdienst.
[118] Algemene Inlichtingen- en Veiligheidsdienst.
[119] Nachrichtendienst des Bundes.

Loven legger opp til både forhåndskontrollmekanismer og etterfølgende kontroll. Søkebegrep skal innom tre instanser før de kan benyttes av NDB; *Bundesverfassungsgericht*, *Sicherheitsausschuss* i *Bundesrat* og en representant fra Forsvarsdepartementet. Tillatelser som gis vil ha en gyldighet på 6 måneder, og kan forlenges med ytterligere 3 måneder.

For å påse at NDB ikke får tilgang til data knyttet til sveitsiske borgere, skal *Zenter für elektronische Operationen (ZEO)* gjennomføre den faktiske tekniske innsamlingen og filtreringen. De vil oversende data til NDB dersom disse passer til godkjente søkebegrep eller det foreligger indikasjoner på trusler mot den indre eller ytre sikkerheten i Sveits.

Finland (FIRE)
FIRE[120], som er Finlands SIGINT-tjeneste, har ikke kabelaksess per i dag.

En interdepartemental arbeidsgruppe under ledelse av Försvarsministeriet i Finland avga innstilling i mars 2015. Gruppen hadde et bredt mandat knyttet til behovet for å reformere etterretningslovgivningen generelt. Datatrafikkspaning var imidlertid en vesentlig del av utredningen. Gruppen konkluderte slik: "*Finland bör överväga att utveckla befogenheter för spaning som riktas mot gränsöverskridande datakommunikation för att man ska kunna bemöta den förändring i den yttre säkerhetspolitiska omgivningen som beskrivs i betänkandet. Datatrafikspaningen ska bägrensas till att gälla inhämtning av information om hot som äventyrar den nationella säkerheten. Hoten är till sin art antingen militära eller civila och de kan realiseras antingen i den reella världen eller via datanäten.*" Gruppen anbefalte at myndigheten burde legges til utenlandsetterretningstjenesten (FIRE). Det er mulig at gruppens forslag krever grunnlovsendring i Finland.

I desember 2015 ble det oppnevnt en parlamentarisk oppfølgingsgruppe for reform av etterretningslovgivningen, med mandatperiode til 31. desember 2016. Lovutredning pågår i regi av regjeringen, hvor ulike departementer har ansvar for ulike deler av lovreformen.

[120] Finnish Intelligence Research Establishment.

VEDLEGG 3: UTTALELSE FRA NIM

Jeg takker for brev, datert 20 april då. hvor utvalget anmoder om en skriftlig uttalelse med synspunkter på de menneskerettslige spørsmål og problemstillinger som utvalgets mandat reiser.

Henvendelsen gjelder en sentral del av mandatet til Nasjonal institusjon for menneskerettigheter, nemlig å gi råd til bla. offentlige organer. Nasjonal institusjon er imidlertid i en etableringsfase og jeg er fortsatt den eneste her med norsk juridisk bakgrunn. På denne bakgrunn må NIM begrense seg til å gi en generell uttalelse om de delene av mandatet som vi anser som de viktigste menneskerettslige spørsmål ved utvalgets mandat.

Innsamling av informasjon om den enkelte er et slikt spørsmål og kan være et inngrep i retten til respekt for privatliv, familieliv, hjem og korrespondanse, som er beskyttet i artikkel 8 i den europeiske menneskerettskonvensjon (EMK) og artikkel 17 i FN-konvensjonen om sivile og politiske rettigheter (SP). I denne retten ligger det i første rekke et vern mot inngrep fra myndighetenes side. Staten har også en plikt til å sikre rettighetene, dvs. ta positive skritt for å gjøre dem effektive. Hvor langt dette rekker, må vurderes konkret.

Inngrep i rettighetene er regulert i hhv EMK art 8 para 2 og SP art 17 para 1. I det følgende tas utgangspunkt i artikkel 8, hvor inngrepshjemmelen er mer konkret utformet og hvor man har mest relevant praksis.

For at myndighetene skal kunne gjøre inngrep i disse rettighetene, kreves det hjemmel i lov, inngrepet må søke å nå noen av de formålene som listes opp i bestemmelsen, samt at inngrepet må være «nødvendig i et demokratisk samfunn».

Den europeiske menneskerettsdomstol har gitt ut et såkalt «Factsheet» som inneholder relevant rettspraksis om tolkning av inngrepshjemmelen, se lenke nedenfor:
http://www.echr.coe.int/Documents/FS_Data_ENG.pdf

Når det gjelder lovskravet, fremgår det av rettspraksis at begrepet «lov» dekker både skrevne og uskrevne rettsregler. Videre fremgår det at inngrepet må ha grunnlag i nasjonal rett («the interference in question must have some basis in domestic law»).

I tillegg kommer krav om at regelen må være tilgjengelig («adequately accessible»). Dette innebærer at individet må få en tilfredsstillende angivelse av hvilke regler som gjelder i den konkrete sak. For det annet kan ikke en regel anses som «lov» med mindre den er formulert tilstrekkelig presist til at individet kan avpasse sin adferd etter den. Man må kunne forutse i rimelig grad hvilke konsekvenser en gitt handling vil få. Erfaring viser likevel at absolutt presisjon er uoppnåelig. Mange lover må nødvendigvis formuleres mer eller mindre vagt. I sak nr. 52019/07, L.H. v. Latvia, som er omtalt i EMDs «factsheet», ble det funnet krenkelse bla. på grunn av at lovhjemmelen ikke i tilstrekkelig grad hadde angitt «the scope of discretion conferred on competent authorities and the manner of its exercise». Også sakene Cruslin v. Frankrike, Wisse v. Frankrike og Dragojevic v. Kroatia, gjelder manglende klarhet i loven.

Uttrykket «i samsvar med loven» viser ikke bare til nasjonal lovgivning, men gjelder lovens kvalitet («the quality of the law»), idet regelen må være i samsvar med kravet om rettssikkerhet («the rule of law»). Nasjonal rett må gi rettslig beskyttelse mot vilkårlige inngrep i rettighetene fra myndighetenes side.

En skjønnsmessig nasjonal regel er ikke i seg selv i strid med kravet om forutberegnelighet («foreseeability»), forutsatt at rammen for skjønnet og måten det skal utøves på er angitt med tilstrekkelig klarhet til å beskytte mot vilkårlige inngrep, hensett til det legitime formål som skal ivaretas.

Vilkåret om at inngrep må være «nødvendig i et demokratisk samfunn» har, ifølge praksis bla. følgende elementer:

Nødvendighetskriteriet innebærer at inngrepet må svare til et tvingende samfunnsmessig behov («a pressing social need»). I saken Peck v. the United Kingdom kom domstolen til at det forelå et uforholdsmessig og uberettiget inngrep i klagerens privatliv.

Det er i første rekke statene som har ansvaret for å sikre konvensjonsrettighetene. Her har de et skjønnsmessig spillerom («margin of appreciation»). Dette er imidlertid ikke ubegrenset, og domstolen må avgjøre om et inngrep er for vidtgående. Avgjørende i denne forbindelse blir om staten kan påvise at inngrepet tilsvarte et tvingende samfunnsmessig behov, om det stod i forhold til det legitime formål som skal ivaretas, og om de grunner som anføres av de nasjonale myndigheter er relevante og tilstrekkelige («relevant and sufficient»). For å ta standpunkt til om grunnene er tilstrekkelige, må man ta i betraktning offentlige interesser som er aktuelle i saken.

Overvåkning av enkeltpersoner kan lede til inngrep på alle de områdene som er opplistet i artikkel 8. Det foreligger omfattende praksis fra domstolen på dette området. Saken Klass and Others v. Germany, (1978), som har fått stor betydning for senere praksis, gjaldt overvåkning i form av post og telefon. Domstolen slo fast at overvåkningen hadde lovhjemmel og ivaretok et legitimt formål. Under drøftelsen av om inngrepet var nødvendig i et demokratisk samfunn, vurderte domstolen de garantier som var stilt opp for å hindre misbruk, mot den trusselen som bla. kriminalitet og spionasje utgjorde for et demokrati. Domstolen kom til at det ikke forelå brudd på artikkel 8. Telefonavlytting var også tema i saken Malone v. United Kingdom (1984). Her kom domstolen til at det forelå krenkelse. I forbindelse med en helerisak hadde klagers telefon blitt avlyttet og myndighetene hadde registrert informasjon om bla. hvilke numre som var ringt. Dette var et inngrep i hans korrespondanse. I vurderingen av om inngrepet kunne godtas etter annet ledd, konstaterte domstolen at lovskravet ikke var oppfylt, siden loven var upresis og lite tilgjengelig.

Av nyere praksis når det gjelder telefonavlytting og lagring av informasjon, kan nevnes Amann v. Sveits, 2006 (storkammersak). Også her konstaterte domstolen at lovhjemmelen for inngrepet ikke i tilstrekkelig grad avklarte grensene for myndighetenes skjønn.

Sak nr. 47143/06 Roman Zakharov v. Russland, gjaldt hemmelig telefonavlytting. I dommen, som ble avsagt av storkammer 4. desember 2015, konkluderte EMD enstemmig med at det forelå brudd på artikkel 8. Domstolen slo bla. fast at lovhjemmelen for dette inngrepet, ikke inneholdt «adequate and effective guarantees against arbitrariness and the risk of abuse which was inherent in any system of secret surveillance…..». I dommen fastslås det at russisk lovgivning har mangler i forhold til konvensjonens krav bla. når det gjelder vilkår for hemmelig overvåkning, varighet av slik overvåkning, prosedyren for å tillate telefonavlytting, samt reglene for lagring og destruksjon av informasjon innhentet. Dommen har også en rekke referanser til rettspraksis, herunder til Klass og Malone dommene. Domstolen kom også til at russisk rett ikke gir en effektiv prøvningsrett til personer som påstår at de er overvåket.

Dette er ikke på noen måte en uttømmende uttalelse om de menneskerettslige spørsmål som utvalgets mandat reiser. Jeg har imidlertid lagt hovedvekten på artikkel 8 i EMK, som etter min mening (sammen med SP artikkel 17), regulerer de viktigste menneskerettslige spørsmålene på de områdene som omfattes av mandatet. En del sentrale dommer er kommentert og domstolens «factsheet» som det er lenke til foran, omtaler flere dommer som bidrar til å klarlegge tolkningen av denne bestemmelsen. Dette er imidlertid bare noen eksempler fra den rikholdige praksisen om artikkel 8.

FNs menneskerettighetskomite har også behandlet en rekke individklager som gjelder artikkel 17. Også komiteen legger i sin praksis vekt på at lovhjemler for inngrep må være presise, og at selv inngrep som er i samsvar med loven må være i samsvar med: «..the provisions, aims and objectives of the Covenant….», jfr. sak nr. 488/1992 Toonan v. Australia. Videre har praksis fra komiteen vist at inngrepet ikke må være uforholdsmessig, sett hen til formålet som søkes oppnådd, jfr. sak nr. 903/1999 van Hulst v. Nederland, som gjaldt telefonavlytting.

Komiteen vedtok en generell kommentar om SP artikkel 17 i 1988 («general comment 16»). Nedenfor følger en lenke til kommentaren, som for øvrig er langt kortere og mindre detaljert enn komiteens nyere kommentarer:
http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en

Jeg kan også nevne at FNs Menneskerettighetsråd i 2015 oppnevnte en spesialrapportør for «The right to privacy». I sin første rapport til rådet redegjør han bla. for arbeidsmetoder og temaer som han ønsker å ta opp i fremtidige rapporter. Nedenfor følger en lenke til mer informasjon om spesialrapportøren, herunder til hans mandat:

http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx

FNs Høykommissær for menneskerettigheter presenterte i 2014 en rapport til Menneskerettighetsrådet med tittel «The right to privacy in the digital age».
Rapporten kan lastes ned på følgende lenke:
http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

Praksis og rapporter fra internasjonale organer viser at det som ofte er avgjørende for om et inngrep er i samsvar med menneskerettslige normer, er om inngrepet er forholdsmessig i forhold til de formål som søkes oppnådd og om det er «nødvendig i et demokratisk samfunn». Høykommissæren peker i sin rapport også på at overvåkning og innsamling av persondata berører andre rettigheter, herunder ytringsfriheten og foreningsfriheten.

Praksis viser også at statene har en skjønnsmargin, men at det stilles strenge krav til innholdet i lover som hjemler inngrep.

Etter NIMs oppfatning må det sentrale for utvalget være at retten til å innhente informasjon klart knyttes til et samfunnsmessig behov. Lovbestemmelsen må utformes klart, og - så langt mulig – bør det unngås skjønnsmessige bestemmelser som gjør eventuell senere domstolskontroll vanskelig. Videre bør det gis klare regler for hvordan "overskuddsinformasjon" skal behandles, herunder om sletting av slik informasjon.

Oslo 2. mai 2016
Petter Wille.

VEDLEGG 4: FORKORTELSER OG DEFINISJONER

Forkortelse/begrep	Forklaring/definisjon
Algoritme	En presis beskrivelse av en serie operasjoner som skal utføres for å løse et problem eller et sett med flere problemer.
Bit-mønster	All datakommunikasjon består av sekvenser av ett-tall og nuller. Disse sekvensene dekodes eller tolkes om til tegn og bokstaver av datamaskiner. Ett enkelt 1-tall eller null er det samme som 1 bit. En bestemt sekvens av slike 1-tall og nuller kan betegnes som et bit-mønster. Skadevare vil kunne gjenkjennes ved at en sensor «lytter» på en linje etter en bit-sekvens/-mønster som kjennetegner denne skadevaren, et slags digitalt fingeravtrykk.
COMINT	Communications Intelligence – kommunikasjonsetterretning. COMINT er en undergruppe av SIGINT.
Digitalt grenseforsvar/ DGF	E-tjenestens målrettede innhenting og analyse av utenlandsetterretningsrelevant informasjon, basert på aksess til elektronisk kommunikasjon som går inn og ut av Norge, i den hensikt å kartlegge og motvirke mulige ytre trusler mot rikets sikkerhet og selvstendighet og andre viktige nasjonale interesser
EMD	Den europeiske menneskerettsdomstolen
EMK	Den europeiske menneskerettskonvensjonen
Innholdsdata	Data som ikke er metadata – typisk innholdet i en sms, epost, facebook-melding og lignende.
Innsamling	Data som sensoren plukker ut av trafikkstrømmen, basert på målrettede og godkjente søkebegrep.
K2	Kommando og kontroll
Kjernenett	Kjernenett benyttes ofte for å betegne de delene av et tele- eller datanett som består av hovedsentraler koblet sammen via overføringssystemer med høy hastighet. Kjernenettene er dermed de tykkeste eller raskeste hovedfartsårene for data og telekommunikasjon, og som gjerne transporterer store mengder med data over lange avstander. En mindre leverandør av bredbånd kan ha bygget ut et nettverk i et begrenset geografisk område, men vil f.eks. benytte seg av Telenor sitt kjernenett for kommunikasjon med andre byer eller utlandet.
Kryptoforsering	Kryptoforsering er den metoden eller prosessen som gjennomføres for å omgå eller bryte kryptering på en kryptert fil eller kommunikasjonsstrøm, uten å i utgangspunktet være i besittelse av krypteringsnøkkelen.
Maskin-til-maskin-kommunikasjon (M2M)	Kommunikasjon mellom maskiner uten menneskelig interaksjon, eksempelvis når en trådløs dekkventil rapporterer lavt lufttrykk til datamaskinen i en bil.
Metadata	Data som beskriver annen data eller som inneholder ekstra informasjon knyttet til data. Dette kan for eksempel være data som beskriver typen eller formatet på innholdet, eller ekstra informasjon knyttet til innholdet, som for eksempel navn på forfatter/avsender, størrelse eller mottaker. I forhold til DGF vil lagring av metadata være begrenset til den type metadata som ikke avslører innholdet i dataene, og som ikke avslører handlinger foretatt av en bruker på nettsteder eller sosiale medier som for eksempel informasjon om hvilke søk brukeren har utført.
Modusselektor	Se "Selektor".
Node	Node blir i denne sammenheng benyttet som en generell betegnelse for et informasjonssystem knyttet til Internett. Dette kan for eksempel være en PC, mobiltelefon, nettbrett eller en stor server.
Personselektor	Se "Selektor".

Selektor	Betegnelse på en identifikator for en bruker på en kommunikasjonstjeneste, eller en søkealgoritme for å finne en bruker/identifikator av etterretningsmessig interesse. Dette kan være et telefonnummer, epostadresse eller brukernavn på en gitt tjeneste. Selektorer kan benyttes til å velge ut (selektere) relevant datatrafikk tilknyttet et godkjent mål, eller for målutviklingsformål. Personselektor er en selektor knyttet til et konkret enkeltindivid. Modusselektor er en selektor knyttet til et bestemt handlingsmønster, eksempelvis all kommunikasjon som originerer fra en nærmere avgrenset geografisk lokasjon.
SIGINT	SIGINT betyr signaletterretning. Dette er å avskjære eller lytte på kommunikasjon mellom mennesker (COMINT), eller elektriske signaler som ikke direkte benyttes til kommunikasjon (ELINT), for etterretningsformål.
Signatur	Signatur blir i denne sammenheng benyttet for å beskrive identifikatorer som kan benyttes som kjennetegn for en digital trussel. I praksis kan dette for eksempel være en bestemt bitsekvens som kan observeres når en trojaner kommuniserer «hjem» til trusselaktøren, eller en bitsekvens som kjennetegner utnyttelse av et bestemt sikkerhetshull. Signaturer kan også lages mer generelle, slik at systemer gir alarm dersom det observeres kommunikasjon med en kjent IP-adresse eller domene som er knyttet til en trusselaktør.
Stordata (eng. big data)	Begrep som refererer til den enorme økningen i tilgang til, og automatisert bruk av, opplysninger, særlig til gigantiske mengder data som er kontrollert av selskaper, myndigheter og andre store organisasjoner, og som kan gjøres til gjenstand for omfattende analyse ved hjelp av algoritmer.
TA	Trusselaktør
Tasking	Ekvivalent med "Innsamling", se dette.
Tilgang	All datatrafikk som flyter forbi Etterretningstjenestens sensorer ved den digitale landegrensen.
Tingenes internett (IoT)	Det forventes at «tingene» i langt større grad enn i dag vil kommunisere med hverandre. Milliarder av enheter, for eksempel sensorer, maskiner og fysiske objekter, vil koples til nettene, enten trådløst eller gjennom fast tilknytning, og kommunisere seg imellom, ofte uten menneskelig interaksjon. For å kunne spore, fjernovervåke og styre alle disse enhetene og terminalene, må de være knyttet til et nettverk. Denne utviklingen benevnes ofte som tingenes internett (*Internet of Things/IoT* eller *Internet of Everything/IoE* på engelsk), og inkluderer smarte løsninger innen en rekke samfunnssektorer, som f. eks. e-helse, smarte hjem og bedrifter, smarte byer, intelligent trafikkstyring og smart miljø.
Trojaner	Trojaner er i denne sammenheng uønsket programvare, som gjerne gir seg ut for å være noe annet enn det er, og som gir en trusselaktør uautorisert tilgang til å utføre kommandoer på en datamaskin eller mobil/nettbrett. En trojaner har typisk ikke funksjonalitet for å spre seg selv som et datavirus, men er avhengig av at angriperen på en eller annen måte lurer brukeren til å installere den.
VDI	Varslingssystem for Digital Infrastruktur

***