Norges nasjonale institusjon
for menneskerettigheter

Forsvarsdepartementet
postmottak@fd.dep.no

**Dato:**
20. januar 2017

**Deres referanse:**
2016/2699-1/FD II 5/SIH

## Høringsuttalelse til forsvarsdepartementet om Lysne II-utvalgets utredning *Digitalt grenseforsvar (DGF)*

### 1. Innledning og konklusjon

Norges nasjonale institusjon for menneskerettigheter («Nasjonal institusjon») har som hovedoppgave å fremme og beskytte menneskerettighetene i tråd med Grunnloven, menneskerettsloven og den øvrige lovgivning, internasjonale traktater og folkeretten for øvrig.[1] Nasjonal institusjon skal blant annet gi råd til Stortinget, regjeringen og andre offentlige organer om gjennomføringen av menneskerettighetene. I dette ligger det særlig at Nasjonal institusjon skal komme med innspill i lovgivningsprosesser som berører menneskerettighetene.[2]

I e-post fra seniorrådgiver i forsvarsdepartementet Siri Horgen Hinze, 6. januar 2017, har Nasjonal institusjon fått **utsatt høringsfrist til 20. januar 2017.**

DGF berører kjernen i det politiske og rettslige spenningsforholdet mellom beskyttelse av nasjonale sikkerhetsinteresser og den enkeltes frihet fra myndighetsinngrep og rett til privatliv. DGF tar sikte på å ivareta nasjonale sikkerhetsinteresser ved å gi effektiv tilgang på utenlandsetterretning særlig for å motvirke cyberangrep og terrorisme. Samtidig favner DGF svært vidt i den forstand at det potensielt kan innebære innhenting og lagring av innholds- og metadata fra enhver, uten at det foreligger en identifisert og konkret begrunnelse.

Nasjonal institusjon har ingen mening om hvilke dataovervåkingskapasiteter e-tjenesten *bør* ha. Vårt anliggende er at et eventuelt dataovervåkingssystem er i samsvar med gjeldende konstitusjonelle og menneskerettslige regler, som legger rettslig bindende begrensninger for hvilke inngrep etterretningstjenesten kan foreta overfor borgerne. Vår høringsuttalelse vil derfor kun omhandle de konstitusjonelle og menneskerettslige aspektene ved DGF.

[1] Lov om Norges nasjonale institusjon for menneskerettigheter av 22. mai 2015 («NIM-loven») § 1, 2. ledd.
[2] NIM-loven § 3, 1 ledd, bokstav b; Innst. 216 L (2014-2015) s. 3.

Etter vårt syn er det springende punktet om den masselagring av datatrafikk som utgjør grunnfundamentet i DGF innebærer et forholdsmessig inngrep i retten til privatliv. Det er dette som er hovedtemaet for vårt høringsinnspill.

**Vår konklusjon er at datainnsamling til korttidslageret og metadatalageret trolig vil være i strid med EMK art. 8 og kommunikasjonsverndirektivet. Dette er nærmere begrunnet under punkt 3-6, hvor vi særlig ser hen til nyere praksis fra EMD og EU-domstolen, som ikke er adressert i utredningen. Kortidslageret og metadatalageret utgjør helt sentrale og nødvendige komponenter i det samlede DGF-konseptet, og på bakgrunn av våre konklusjoner anbefaler vi derfor at DGF ikke implementeres.**

Foruten enkelte generelle kommentarer, vil vi i denne høringsuttalelsen ikke gå nærmere inn på spørsmål om krav til lovutforming og kontrollmekanismer. Dette er imidlertid noe vi vil komme tilbake til dersom det fremsettes konkrete lovforslag om et dataovervåkingssystem for etterretningstjenesten. Nasjonal institusjon stiller seg også til disposisjon for å gi råd til departementet om disse temaene i en eventuell videre utredningsprosess.[3]

I tillegg til det som er hovedtemaet for høringsinnspillet, har vi enkelte mer overordnede kommentarer til utredningen under påfølgende punkt 2.

## 2. Noen overordnede kommentarer til utredningen

Tidligere har det vært relativt lite offentlig debatt om etterretningstjenestens virkemidler for hemmelig overvåking. Nasjonal institusjon mener det er positivt at forslag om en ordning med såpass vidtrekkende implikasjoner for den enkeltes kommunikasjonsvern og privatliv tilgjengeliggjøres for åpen og offentlig diskurs allerede på et tidlig stadium i utredningsprosessen. Høringen bidrar også til å sette søkelys på etterretningstjenesten og dens oppgaver, herunder i hvilken grad og hvordan dens virksomhet berører norske borgere og personer på norsk territorium. Mer generelt aktualiserer også DGF-utredningen spørsmål om rettsgrunnlaget for etterretningstjenestens nåværende overvåkingsvirksomhet overfor norske borgere, deriblant gjennom lagring av datatrafikk, men dette skal vi ikke gå nærmere inn på her.[4]

Etter vårt syn må det være riktig å betegne utredningen som en foreløpig *konseptuell* beskrivelse av et dataovervåkingssystem til etterretningsformål. Det rettslige og faktiske abstraksjonsnivået i utredningen medfører at det etterlates et relativt vidt rom for den nærmere rettslige og tekniske utformingen av DGF.

Utredningen inneholder ikke et lovforslag, og naturlig nok blir da enkelte aspekter ved den rettslige utformingen av DGF uklare. Utvalget gir på s. 60-61 en grei oversikt over de sentrale temaene som bør inngå i lovgivning om DGF. Nasjonal institusjon er for øvrig enig med utvalget i at et eventuelt dataovervåkingssystem bør innføres som et helhetlig lovverk, separat fra kriteriene i e-tjenesteloven. Dette skriver seg særlig til de strenge krav til innholdet og utformingen av overvåkingslovgivning som

[3] NIM-loven § 3, første ledd, bokstav b.
[4] EOS-utvalget, *Særskilt melding til Stortinget og rettsgrunnlaget for Etterretningstjenestens overvåkingsvirksomhet,* Oslo 2016.

særlig følger av EMDs praksis.[5] Vi viser også til de problematiske sidene ved e-tjenesteloven som rettsgrunnlag for dataovervåking.[6] Et sentralt tema som burde vært presisert ytterligere er det nærmere bestemte formålet med DGF. Foruten at DGF tar sikte på å gi tilgang på utenlandsetterretning for å håndtere nasjonale sikkerhetstrusler i form av cyberangrep og terrorisme, er det i liten grad angitt hvordan formålet skal avgrenses, blant annet med hensyn til nærmere kvalifikasjonskriterier, bruk og deling av informasjon, samt i hvilken grad ordningen også skal brukes på datatrafikk som har sender eller mottaker i Norge. For virkemidler som DGF gjelder strenge krav til formålsangivelse og –avgrensning, som gjeldende e-tjenestelov neppe oppfyller.

Den tekniske innretningen av DGF har avgjørende betydning for DGFs faktiske overvåkingspotensial og muligheten for at DGF reelt kan ivareta konstitusjonelle og menneskerettslige krav. Nasjonal institusjon har forståelse for at etterretningstjenesten har behov for å hemmeligholde detaljer om sine tekniske kapasiteter. Vi mener likevel at den faktiske beskrivelsen av DGF er i overkant generell og til dels utydelig på punkter som er av betydning for å kunne gi en faktisk og rettslig vurdering av ordningen. En uheldig side ved at det er tildels vanskelig å danne seg et konkret bilde av den faktiske ordningen er også at det kan gi grunnlag for spekulasjon og usikkerhet rundt hva DGF egentlig innebærer, noe som igjen er lite heldig for den offentlige debatten departementet ellers skal berømmes for å legge til rette for. En gjennomgang av allerede inngitte høringsuttalelser og medieomtale viser at det er ganske ulike oppfatninger om hva DGF rent faktisk er og hvordan det virker.

I utredningen gis en ganske utførlig beskrivelse av kontrollordninger for DGF. Nasjonal institusjon tilslutter seg høringsinnspill fra Borgarting lagmannsrett og Dommerforeningen, om at domstolkontrollen bør legges til de alminnelige domstoler. En «DGF-domstol» slik den er beskrevet i utredningen antageligvis kan innrettes på en måte som formelt oppfyller uavhengighetskravet. Når det gjelder myndighetenes dataovervåking er det særlig viktig at allmenheten har tillit til at det finner sted reell og uavhengig kontroll. Vi mener at dette hensynet ivaretas bedre ved at kontrollen legges til de alminnelige domstolene. Det fremstår uklart hvordan prosessordningen ved domstolkontrollen skal legges opp, herunder om sakene skal behandles i sivilrettslige eller straffeprosessuelle former, eller gjennom en egen prosessordning. Nasjonal institusjon vil understreke viktigheten av at prosessformen uansett ivaretar grunnleggende krav til en rettferdig rettergang, og vi vil særlig påpeke behovet for effektiv kontradiktorisk behandling, som innbefatter at ordningen bør innebære oppnevning av prosessfullmektig for å ivareta aktuelle privatlivsinteresser. De tekniske sidene ved DGF vil kunne ha avgjørende betydning for om dataovervåkingen generelt eller i konkrete tilfeller er i tråd med lovgivningen og menneskerettighetene. Nasjonal institusjon mener derfor at kontrollorganene må utstyres med teknisk kompetanse som muliggjør at de kan foreta selvstendige faktiske vurderinger. Dette er blant annet nødvendig for effektiv kontroll med at dataovervåkingen til enhver tid har integrert de virkemidler som sikrer best mulig målretting av datainnhentingen og utsiling av

[5] Se særlig Klass and others mot Tyskland, 6. september 1978, avsnitt 49, 50 og 59; Kruslin mot Frankrike, 24. april 1990, avsnitt 33; Kvasnica mot Slovakia, 9. september 2009, avsnitt 80; Kennedy mot UK, 18. mai 2010, avsnitt 153-154, Roman Zakharov mot Russland, 4. desember 2015, avsnitt 232, og Szabó og Vissy mot Ungarn, 6. juni 2016, avsnitt 57.

[6] EOS-utvalget, *Særskilt melding til Stortinget og rettsgrunnlaget for Etterretningstjenestens overvåkingsvirksomhet,* Oslo 2016, s. 23.

overskuddsinformasjon. Tilsvarende er det vanskelig å forestille seg at en domstol kan føre en effektiv forhåndskontroll med automatiserte søkekriterier uten å ha betydelig innsikt i hvordan disse teknisk virker i overvåkingssystemet, herunder i hvilket omfang søkekriterier kan fange opp private opplysninger som ikke er etterretningsrelevante, mv.

Nasjonal institusjon vil videre peke på at deling av lagret informasjon knyttet til en person også er et inngrep i privatlivet. Vi viser særlig til den forutsatte informasjonsdelingen med PST gjennom *Felles kontraterrorsenter*.[7] Informasjonsdelingen må ha et rettsgrunnlag, ivareta et legitimt formål og være forholdsmessig. I forholdsmessighetsvurderingen må det hensyntas hva informasjonen kan bli brukt til, særlig i lys av den relativt lave mistanketerskelen for å bruke skjulte tvangsmidler i forebyggingssporet i medhold av politiloven § 17d.

## 3. Generelle utgangspunkter for vår vurdering av adgangen til masseinnhenting av datatrafikk

I herværende og påfølgende punkt 4-6, skal vi behandle hovedtemaet i vårt høringsinnspill, som er om den masselagring av datatrafikk DGF gir adgang til innebærer et forholdsmessig inngrep i privatlivet ut fra formålet om å skaffe utenlandsetterretning for å kartlegge og motvirke trusler mot rikets sikkerhet, særlig cyberangrep og terrorisme.

Vår vurdering bygger på utvalgets faktiske beskrivelse av DGF i utredningen kapittel 2, 8 og 9.2. Vi har også sett hen til Datatilsynets høringsuttalelse, hvor det er gitt en mer forklarende beskrivelse av DGF.[8]

Det rettslige utgangspunktet for vurderingen er EMK art. 8 og direktiv 2002/58/EF av 12. juli 2002 («kommunikasjonsverndirektivet») art. 15(1), særlig i lys av henholdsvis EMDs dom Szabó og Vissy mot Ungarn, 6. juni 2016 og EU-domstolens dom i sak C-203/15 og C-698/15, 21. desember 2015 («Tele2»).

Innledningsvis ser vi grunn til å knytte enkelte kommentarer til den generelle rettskildeverdien av EU-domstolens dom i Tele2-saken. Avgjørelsen bygger på kommunikasjonsverndirektivet som er del av EØS-avtalen og er gjennomført i norsk rett.[9] EU-domstolens tolkning av kommunikasjonsverndirektivet art. 15(1) er i praksis bindende for norske myndigheter.[10] Selv om det formalrettslige utgangspunktet i Tele2-avgjørelsen er kommunikasjonsverndirektivet art. 15(1), bygger avgjørelsen i stor grad på rettslige premisser hentet fra EU charteret om fundamentale rettigheter, som ikke er bindende for Norge.[11] I den grad man skulle mene at dette reduserer Tele2-avgjørelsens rettskildeverdi i norsk rett, viser vi til at EMD i saken Szabó og Vissy mot Ungarn, 6. juni 2016, legger stor vekt på EU-domstolens dom i sak C-293/12 og 594/12 av 8. april 2014 *(«Digital rights»)* ved tolkningen av EMK art. 8.[12] Digital rights-avgjørelsen gjaldt lovligheten av datalagringsdirektivet og bygger på EU charteret om fundamentale rettigheter, særlig art. 7 og 8, som gjelder henholdsvis retten til privatliv og databeskyttelse. Føringene fra Digital rights-dommen fremstår videre som helt sentrale premisser i

[7] DGF s. 22 og 61.
[8] Datatilsynets høringsuttalelse 18. januar 2017, s. 7-12.
[9] St.prp. 59 (2003-2004); Innst. S. nr. 233 (2003-2004). Se også http://europalov.no/rettsakt/kommunikasjonsverndirektivet-e-databeskyttelsesdirektivet/id-2232
[10] Fredrik Sejersted, m.fl. EØS-rett, 3. utgave 2011, s. 223-224, med videre henvisninger.
[11] Tele2-saken, avsnitt 98-109.
[12] Szabó og Vissy v. Ungarn, 6. juni 2016, avsnitt 68-73.

Tele2-avgjørelsen.[13] I tillegg kommer det at rettssetningene EMD bygger på i Szabó og Vissy mot Ungarn fremstår substansielt tilsvarende som rettssetningene EU-domstolen bygger på i Tele2-avgjørelsen. På denne bakgrunn mener vi at rettskildeverdien av Tele2-avgjørelsen ikke kan anses svekket fordi den bygger på rettslige premisser fra EUs charter om fundamentale rettigheter. De samme premissene har grunnlag i EMDs praksis, både direkte og indirekte gjennom EMDs henvisninger til Digital rights-avgjørelsen.

Norske domstoler har frem til nå tolket Grunnloven § 102, første punktum, i samsvar med EMK art. 8. Det er imidlertid ikke gitt at praksis fra EMD etter grunnlovsreformen i 2014 vil ha samme betydning for tolkningen av Grunnloven som EMDs praksis fra før grunnlovsreformen.[14] Det fremstår likevel lite sannsynlig at norske domstoler vil tolke rettighetsvernet etter Grunnloven § 102, første punktum, snevrere enn det som kommer til uttrykk i EMDs praksis om EMK art. 8, fra grunnlovsrevisjonen og frem til i dag. Vi ser imidlertid ikke grunn til å gå nærmere inn på dette her. Antagelsen er likevel at Grunnloven § 102, første punktum, gir et minst like omfattende rettighetsvern som EMK art. 8.

## 4. DGF og terskelen for inngrep i privatlivet

Bruken av DGF vil utvilsomt innebære inngrep i retten til privatliv slik den er beskyttet i Grunnloven § 102, første punktum, EMK art. 8, SP art. 17, og kommunikasjonsverndirektivet. Ordningen innebærer potensielt en rekke separate inngrep i rettighetsvernet, først ved innsamling og lagring, deretter ved ulike former for bruk og deling, mv. Det som imidlertid ikke har blitt fremhevet i utredningen er at eksistensen av et DGF-system i seg selv innebærer et inngrep i privatlivet etter EMK art. 8, jf. Szabó og Vissy mot Ungarn, avsnitt 53, med videre henvisninger:

> *In the mere existence of the legislation itself there is involved, for all those to whom the legislation could be applied, a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an "interference by a public authority" with the exercise of the applicants' right to respect for private and family life and for correspondence (see Klass and Others, cited above, § 41). Given the technological advances since the Klass and Others case, the potential interferences with email, mobile phone and Internet services as well as those of mass surveillance attract the Convention protection of private life even more acutely (see Copland v. the United Kingdom, no. 62617/00, § 41, ECHR 2007-I).*

Inngrepet konstitueres av den latente overvåkingstrusselen som ligger i at ordningen i det hele tatt eksisterer. Det avgjørende er da det rettslige og faktiske overvåkingspotensialet ved ordningen, ikke hvilken overvåking som faktisk skjer. Selv om siktemålet med DGF er utenlandsetterretning, er det likevel på det rene at DGF vil fange opp betydelige mengder *intern datatrafikk* i Norge, som passerer via utenlandske servere. Enhver datatrafikk, intern eller ekstern, som passerer innsamlingspunktet kan bli fanget opp ufiltrert og lagret i DGF-systemets korttidslager i opptil 14 dager. Innsamlingen til

[13] Se avsnitt 98-109.
[14] Rt-2015-93, avsnitt 57.

metadatalageret filtreres, men filtreringsteknikken slik den er beskrevet, vil innebære at metadatalageret også vil inneholde store mengder *intern* metadata som ikke er relevant for utenlandsetterretningsformål. Metadata skal videre kunne oppbevares i 18 måneder. At dette potensialet for datainnsamling foreligger er nok til at implementeringen av DGF i seg selv vil innebære et privatlivsinngrep. Desto mer vil imidlertid dette gjelde for personer som etterretningstjenesten kan målrette søk mot, blant annet norske borgere i utlandet. EMD fremhever at teknologiutviklingen av masseovervåkingssystemer aktualiserer privatlivsbeskyttelsen etter konvensjonen i særlig grad.

Etter kommunikasjonsverndirektivet er det kanskje ikke like naturlig med betegnelsen *inngrep,* men etter art. 15 (1) må *«legislative measures»* som begrenser rekkevidden av forpliktelsene og rettighetene i kommunikasjonsverndirektivet art. 5, 6, 8 nr. 1,2,3 og 4, samt art. 9, være *«necessary, appropriate and proportionate measure within a democratic society»*, blant annet for å ivareta nasjonal sikkerhet, forsvar, offentlig sikkerhet, eller forebygging og avdekking av straffbare handlinger. Også her er det lovgivningstiltaket i seg selv som aktualiserer derogasjonsvurderingen, herunder spørsmålet om forholdsmessighet.

Forannevnte art. 5 gjelder statens plikt til å sikre fortrolighet for kommunikasjon som foregår via offentlige kommunikasjonsnett og offentlig tilgjengelige kommunikasjonstjenester, samt fortrolighet for metadata knyttet til slik kommunikasjon. I direktivets forstand er kommunikasjon enhver opplysning som utveksles eller overføres mellom et begrenset antall parter (innholdsdata).[15] Art. 6 gjelder plikten til å slette eller anonymisere metadata. Art. 9 gjelder lokaliseringsdata, og fastsetter blant annet at lokaliseringsdata kun kan behandles dersom brukeren anonymiseres eller samtykker.[16]

Det er på det rene at DGF, slik det er konseptuelt beskrevet, innebærer innhenting og lagring av innholdsdata og metadata. Et eventuelt DGF må derfor være i samsvar med vilkårene i direktivet art. 15(1).

## 5. Kravet om *«strict necessity»* og masseinnsamling av metadata og innholdsdata for utenlandsetterretningsformål

### *5.1. Utgangspunkter*

I Szabó og Vissy mot Ungarn avsnitt 71-73 oppstiller EMD krav om at hemmelig overvåking som blant annet innebærer innsamling av personlig data må oppfylle et krav om *«strict necessity»*. I Tele2-saken avsnitt 96 legger EU-domstolen til grunn et krav om at inngrep i beskyttelsen av personlig data må være *«strictly necessary»* (heretter samlebetegnelsen «strengt nødvendig», e.l.).

Nasjonal institusjon mener det er klart at kravet om streng nødvendighet gjelder ved innsamling av innholdsdata og metadata gjennom DGF. Anvendelsesområdet for normen EMD legger til grunn er blant annet *«massive monitoring of communications susceptible to containing indications of impending incidents», «automated and systemic data collection»* og *«surveillance methods resulting*

[15] Kommunikasjonsverndirektivet art. 2, bokstav d.

[16] Se St.prp. nr. 59 (2003-2004) for en generell redegjørelse for kommunikasjonsverndirektivet, samt norsk oversettelse av kommunikasjonsverndirektivet.

*in masses of data collected».*[17] Etter vårt syn er det klart at DGF faller innenfor det tematiske anvendelsesområdet EMD beskriver.

I Tele2-saken tar EU-domstolen et noe annet utgangspunkt, og legger til grunn at normen gjelder ved *«retention of traffic and location data».*[18] Strengere krav gjelder ved innsamling av *«communication»,* altså innholdsdata, som innebærer et inngrep i kjernen av retten til privatliv og databeskyttelse.[19] Det er klart at også dette anvendelsesområdet omfatter DGF.

I motsetningen til overvåkningsordningene som ble vurdert av EMD og EU-domstolen i de ovennevnte sakene, tar ikke DGF sikte på intern kriminalitetsbekjempelse, men utadrettet etterretningsvirksomhet blant annet for å motvirke eksterne cyberangrep og terrortrusler. Etter vårt syn må det avgjørende likevel være at ordningen rent faktisk innebærer innsamling og lagring av betydelige mengder *intern datatrafikk,* metadata så vel som innholdsdata, som enhver kan være avsender eller mottaker av. Så lenge dette er den faktiske virkningen av ordningen, er det heller ikke rettslige holdepunkter for at de alminnelige skrankene for inngrep ikke gjelder fordi ordningen har et *utenlandsetterretningsformål.* Gjennom den forutsatte informasjonsdelingen med PST, får også ordningen et formål som i realiteten retter seg mot interne forhold, som de forannevnte avgjørelsene direkte gjelder. Det er videre vanskelig eventuelt å begrunne hvorfor et formål om utenlandsetterretning som knytter seg til nasjonal sikkerhet, skal ha større gjennomslag i forholdsmessighetsvurderingen enn et formål om *intern etterretning* som også tar sikte på å beskytte nasjonal sikkerhet, særlig slik som i Szabó og Vissy mot Ungarn, men til dels også i Tele2-saken.

Nasjonal institusjon mener at de forannevnte krav om streng nødvendighet må legges til grunn ved vurderingen av om DGF er i tråd med EMK art. 8 og kommunikasjonsverndirektivet.

### *5.2. Nærmere om kravet til streng nødvendighet*

I kravet til streng nødvendighet ligger det at terskelen for adgangen til dataovervåking er svært høy. I flere saker har EMD litt slagordsmessig vist til at det er en iboende risiko ved overvåkingssystemer som skal ivareta nasjonal sikkerhet at de *«may undermine or even destroy democracy under the cloak of defending it».*[20] EU-domstolen har på sin side særlig vist til den usikkerheten i befolkningen som kan oppstå ved at det finnes vidtrekkende overvåkingsregimer, noe som også har en side mot den såkalte nedkjølingseffekten og ytringsfriheten.[21] Domstolene anser frihet fra overvåking som en helt sentral komponent i demokratiske samfunn. Dette har nok en sammenheng med felleseuropeiske erfaringer med masseovervåking, og tilliten til myndighetene, som i mange europeiske land er lavere enn i Norge. Dette er et viktig bakteppe for forståelsen av hvorfor de menneskerettslige skrankene for overvåking er såpass strenge som de er.

I Szabó og Vissy mot Ungarn avsnitt 73 utlegger EMD kravet om *«strict necessity»* slik:

[17] Szabó og Vissy mot Ungarn, avsnitt 68.
[18] Tele2-saken, avsnitt 103.
[19] Tele2-saken, avsnitt 101.
[20] Se blant annet Roman Zakharov mot Russland, 4. desember 2015, avsnitt 232 (storkammer)
[21] Tele2-saken, avsnitt 100 og 101, og Digital rights, avsnitt 28, 37 og 39.

> *However, given the particular character of the interference in question and the potential of cutting-edge surveillance technologies to invade citizens' privacy, the Court considers that the requirement "necessary in a democratic society" must be interpreted in this context as requiring "strict necessity" in two aspects. A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal.*

I dette ligger to kumulative hovedkriterier for lovligheten av blant annet overvåking av datatrafikk. Det første er at overvåkingstiltaket må være strengt nødvendig for å sikre statens demokratiske institusjoner. I den grad overvåkingen er strengt nødvendig for å oppnå dette må den konkrete overvåkingen i tillegg være strengt nødvendig for å få tilgang på *vital informasjon* i en individuell sak. Av særlig betydning for DGF er det at det må foreligge en klar tilknytning mellom overvåkingsbehovet og et konkret sakskompleks som *strengt* nødvendiggjør overvåkingen, ikke bare for å få informasjon, men informasjon av kvalifisert verdi.

Dette svarer i hovedsak til det EU-domstolen legger til grunn i Tele2-saken avsnitt 108-111, hvor følgende fremgår i det første og generelle avsnittet:

> *However, Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.*

Også her oppstilles krav om tilknytning mellom dataovervåkingen og en konkret og kvalifisert situasjon. Innholdet i dette kravet er videre presisert i avgjørelsens påfølgende avsnitt 109-111. Rettssetningen knytter seg spesifikt til metadata, og innebærer at innsamlingen av metadata må være målrettet og følgelig begrenset med hensyn til typer data, kommunikasjonsformer og hvem innsamlingen rettes mot.

I sammenheng oppstiller avgjørelsene fra EMD og EU-domstolen svært strenge krav til tilknytning til et konkret og kvalifisert saksforhold, og målretting av datainnsamlingen.

Selv om disse uttalelsene er informative i seg selv, blir innholdet klarere gjennom domstolenes videre angivelse av hvilke overvåkingstiltak som ikke vil være i tråd med konvensjonene.

Med henvising til Kennedy mot Storbritannia, 18. august 2010, fremholder EMD følgende i Szabó og Vissy mot Ungarn, avsnitt 69:

> *The Court recalls that in Kennedy, the impugned legislation did not allow for "indiscriminate capturing of vast amounts of communications" (see Kennedy, cited above, § 160) which was one of the elements enabling it not to find a violation of Article 8. However, in the present case, the Court considers that, in the absence of specific rules to that effect or any submissions to the contrary, it cannot be ruled out that the broad-based provisions of the National Security Act can be taken to enable so-called strategic, large-scale interception, which is a matter of serious concern.*

Som en motsetning til hva som skal til for at overvåking er strengt nødvendig viser EMD her til at en del av begrunnelsen for at domstolen kom til at det ikke forelå krenkelse i Kennedy-saken var at den aktuelle ordningen *ikke* åpnet for helt generell (*«indiscriminate»*) innsamling av kommunikasjon.

Betydningen av at ordningen gir adgang til generell datainnsamling er klarere angitt i Tele2-avgjørelsen, som omhandler metadata og lokasjonsdata. I Tele2 avgjørelsen avsnitt 103 fremgår følgende:

> *Further, while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 51)*

Her fremgår det utvetydig at selv ikke hensynet til bekjempelse av alvorlig kriminalitet, inkludert terrorisme, kan rettferdiggjøre generell innsamling av metadata. Dette bør leses i sammenheng med avsnitt 106 i dommen:

> *Such legislation does not require there to be any relationship between the data which must be retained and a threat to public security. In particular, it is not restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 59).*

Her går domstolen tilbake til normen om streng nødvendighet. Det følger av dette at en ordning som innebærer generell innsamling av datatrafikk, uten et konkret behov utledet fra en bestemt situasjon, og tilhørende målretting av overvåkingen, ikke er i samsvar med kravet om streng nødvendighet. Konklusjonen fremgår direkte i det påfølgende avsnittet, hvor det heter at den aktuelle ordningen *«(…) exceeds the limits of what is strictly necessary and cannot considered to be justified, within a democratic society (…)».*

Rettssetningen som kan deduseres fra denne gjennomgangen, som er særlig relevant for DGF, kan oppsummeres i følgende punkter:

(i) Dataovervåking er i utgangspunktet tillatt dersom det er strengt nødvendig for å sikre statens demokratiske institusjoner. Dette vil blant annet omfatte terrorbekjempelse og kvalifiserte trusler fra andre stater. Det kan nok også omfatte cyberangrep i den grad disse er egnet til å skade statens demokratiske institusjoner.

(ii) Dataovervåking kan kun skje i den utstrekning det er strengt nødvendig for å innhente *vitale* opplysninger i en konkret sak eller operasjon, for å sikre statens demokratiske institusjoner. Det må være en klar tilknytning mellom dataovervåkingen og informasjonsbehov i et konkret saksforhold.

(iii) Dataovervåkingen må være målrettet og avgrenset inn mot den konkrete saken eller operasjonen. Dette innebærer at overvåkingen må begrenses blant annet til type data, kommunikasjonsformat, geografisk område, personkrets og lagringsperiode, som er strengt nødvendig for å få vital informasjon i den konkrete saken eller operasjonen. Dataovervåkingen kan ikke finne sted ut over dette.

(iv) Det er ikke adgang til generell (*«indiscriminate»*) innhenting av enhver datatrafikk, herunder metadata, lokasjonsdata og innholdsdata.

Etter vårt syn oppsummerer disse fire punktene den relevante materielle skranken for dataovervåkingsregimer, slik som DGF. Punktene må selvsagt leses i lys av det som konkret fremgår i rettskildene.

### *5.3. Oppfyller DGF kravet til streng nødvendighet?*

#### 5.3.1. Overordnet

DGF innebærer tilgang til fiberoptiske kabler som krysser den norske landegrensen. Etterretningstjenesten skal kunne innhente datatrafikk som passerer i kablene gjennom såkalte *innsamlingspunkter.* Datatrafikken vil i det vesentlig ha avsender eller mottaker i Norge. Ofte vil imidlertid datatrafikken som krysser landegrensen ha både mottaker og avsender i Norge. Informasjon fra en dataenhet i Norge som ikke er ment kommunisert vil også i stor grad passere innsamlingspunktene. Årsaken til at intern datatrafikk kan passere innsamlingspunktene er at en rekke nettbaserte tjenester har servere i utlandet, f.eks. e-postleverandører og skytjenester. Dette medfører at kommunikasjonen via serveren vil passere frem og tilbake over landegrensen. Dermed kan datatrafikken fanges opp gjennom DGF-systemet. I utredningen heter det videre at *«Andelen av digital aktivitet som kun gjelder personer som befinner seg i Norge, men som likevel krysser landegrensen er (…) høy og økende.».*[22] Det er kun datatrafikk som utelukkende faktisk foregår innenfor landegrensene som ikke vil kunne fanges opp.

#### 5.3.2. Korttidslageret

I korte tidsintervaller vil det bli innhentet ufiltrert datatrafikk, som inneholder både metadata og innholdsdata, som vil bli lagret i det såkalte *korttidslageret* i opptil 14 dager. I og med at datastrømmen

[22] DGF s. 48-49.

til kortidslageret ikke filtreres vil det inneholde all metadata og innholdsdata om enhver, som tilfeldigvis passerer innsamlingspunktet i tidsintervallet innhentingen skjer. Isolert sett er dette den videste og mest inngripende datalagringsmekanismen i DGF. Formålet med kortidslageret er å kunne drive kontinuerlig teknologisk oppdatering av filtrene i det øvrige DGF systemet, som tar sikte på å sjalte ut datatrafikk til metadatalageret som ikke er relevant for etterretningstjenesten. Dataene i kortidslageret skal kun brukes for å *studere hvordan filtrene skal optimaliseres.* Kortidslageret skal behandles av mennesker, ikke kun maskinelt.

Nasjonal institusjon skjønner at kortidslageret er viktig for å optimalisere den tekniske funksjonaliteten av DGF. Dette forandrer likevel ikke at datainnhentingen til kortidslageret er helt generell (*«indiscriminate»*) og omfatter enhver datatrafikk som passerer innsamlingspunktene. På bakgrunn av det rettslige rammeverket som er utlagt ovenfor under punkt 5.2, mener Nasjonal institusjon at den masselagring av både metadata og innholdsdata som kortidslageret innebærer ikke er strengt nødvendig, uavhengig av formål. For øvrig medfører det konkrete formålet med kortidslageret antageligvis at også avgrenset datalagring vil være konvensjonsstridig. Så lenge kortidslageret har denne masselagringsfunksjonen har det for øvrig ikke betydning for vurderingen om man legger til grunn at formålet med kortidslageret er det samme som det overordnede formålet med DGF, eller om man foretar vurderingen ut fra det konkrete formålet med kortidslageret i DGF-systemet.

Det er vår vurdering at kortidslageret, slik det er beskrevet i utredningen, vil være i strid med EMK art. 8 og kommunikasjonsverndirektivet.

#### 5.3.3. Metadatalageret

Vi oppfatter at metadatalageret utgjør den mest sentrale delen av DGF-systemet. Det er dette datalageret som har størst verdi for etterretningsformålet. I metadatalageret skal det kun lagres metadata, og dataene skal kunne lagres i opptil 18 måneder.

I motsetning til kortidslageret skal datastrømmen til metadatalageret filtreres. Som utvalget skriver, legger vi til grunn at det er mulig å filtrere bort innholdsdata, selv om det kan by på enkelte utfordringer. Filtreringen av metadata som ikke er etterretningsrelevant er mer problematisk, og i utredningen heter det at *«Metadatalageret vil (…) inneholde betydelig informasjon om kommunikasjon mellom nordmenn som på kommunikasjonstidspunktet befant seg i Norge.».* Etter hva vi forstår vil det være særlig vanskelig å filtrere metadata fra IP-baserte kommunikasjonsplattformer. Ut fra beskrivelsen i utredningen oppfatter vi videre at metadata fra IP-baserte kommunikasjonsplattformer potensielt i ganske liten grad vil bli filtrert bort. Blant annet dette gir metadatalageret et betydelig generisk (*«indiscriminatory»*) preg. Metadatalageret vil inneholde betydelige mengder *intern* metadata som ikke har noen som helst tilknytning til trusler mot demokratiske institusjoner, og desto mindre har tilknytning til konkrete saksforhold som har sammenheng med dette. Selv om datastrømmen til metadatalageret filtreres vil metadatalageret innebære lagring av svært store mengder metadata fra kommunikasjon internt i Norge, og kommunikasjon hvor mottaker eller avsender er i Norge, i opptil 18 måneder. De lagrede dataene skal videre være søkbare, men med begrensninger.

Med henvisning til redegjørelsen for de rettslige rammene under foregående punkt 5.2, kan vi ikke se at metadatalageret oppfyller kravet om at datainnsamlingen må være strengt nødvendig i en konkret sak eller operasjon for å innhente vital informasjon. Vi kan heller ikke se at omfanget av den generiske datalagringen, som metadatalageret faktisk innebærer, er forenelig med de målrettingskriterier som skal sikre at dataovervåkingen kun skjer i den utstrekning det er strengt nødvendig i et avgrenset sakskompleks.

Vår vurdering er at det er mest nærliggende at metadatalageret, slik det er beskrevet, vil være i strid med EMK art. 8 og kommunikasjonsverndirektivet.

#### 5.3.4. Innholdsdatalageret

Innholdsdatalageret skiller seg vesentlig fra kortidslageret og metadatalageret ved at det er målrettet ut fra domstolsgodkjente personselektorer. Nasjonal institusjon antar at innholdsdatalageret, slik det er konseptuelt beskrevet, kan utformes i samsvar med de rettslige rammene som er redegjort for under punkt 5.2 ovenfor.

## 6. Konklusjon

Med forbehold om at utredningen gir en *konseptuell* beskrivelse av DGF, er det Nasjonal institusjons vurdering at sentrale sider ved den beskrevne ordningen, særlig datainnsamling til korttidslageret og metadatalageret, trolig vil være i strid med EMK art. 8 og kommunikasjonsverndirektivet. I og med at dette utgjør integrerte deler av det samlede DGF-konseptet, vil en implementering av DGF slik det er beskrevet i utredningen antageligvis være konvensjonsstridig og i strid med nasjonal rettslige rammer. I den grad Høyesterett ikke innsnevrer rettighetsvernet etter Grunnloven § 102, andre punktum, i forhold til EMK art. 8, vil DGF trolig også være grunnlovsstridig.

Vennlig hilsen

**Norges nasjonale institusjon for menneskerettigheter**

Petter F. Wille
Direktør

Kristian Reinert Haugland Nilsen
Seniorrådgiver