DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Forsvarsdepartementet
Postboks 8126 DEP
0032 OSLO

Deres ref.	Vår ref.	Dato
2016/2699	16/7421 - TJU	16.01.2017

Høring - rapport avgitt av Lysne II-utvalget om digitalt grenseforsvar

Vi viser Forsvarsdepartementets brev 5. oktober 2016 med vedlegg, som Justis- og beredskapsdepartementet først mottok 23. november 2016. Vi viser for øvrig til avtale om utsatt svarfrist til mandag 16. januar 2017.

Justis- og beredskapsdepartementet (JD) har følgende merknader:

1. Generelle bemerkninger

I likhet med samfunnsutviklingen for øvrig, digitaliseres og internasjonaliseres truslene i stadig større grad. Norges eneste utenlandsetterretning – Etterretningstjenesten (E-tjenesten) – bør ha mulighet til å innhente informasjon der relevant kommunikasjon foregår.

Etablering av digitalt grenseforsvar (DGF) synes godt begrunnet i behovet for å styrke samfunnets samlede evne til å avdekke og motvirke trusler mot Norge. DGF vil gjøre at E-tjenesten blir bedre i stand til å utføre sitt samfunnsoppdrag.

Vi viser særlig til de hensyn Lysne II-utvalget peker på i rapporten på side 28–30. Departementet har der særlig merket seg følgende utgangspunkt, jf. rapporten s. 28, at:

> [D]*e 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.*

Postadresse	Kontoradresse	Telefon - sentralbord	Departementsrådens	Saksbehandler
Postboks 8005 Dep	Gullhaug Torg 4A	22 24 90 90	sekretariat	Toril Juul
0030 Oslo	0484 Oslo	Org.nr.: 972 417 831		22245125
0030 Oslo				toril.juul@jd.dep.no

Videre taler også det som fremgår av rapportens punkt 5.7, om folkerettslige forpliktelser, for etablering av DGF, samt punkt 5.8, hvor det blant annet fremgår at:

> *«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».*

Rapporten peker imidlertid på prinsipielle utfordringer ved en eventuell etablering av DGF som vil være viktig for den videre debatten.

Det er viktig å sikre at hjemlene for informasjonsinnhenting i størst mulig grad er teknologinøytrale. Dette innebærer at teknologisk utvikling når det gjelder informasjonsbærere for kommunikasjon ikke må medføre reelle innskrenkninger i den mulighet til å innhente informasjon om og fra kommunikasjon som har vært hjemlet ved «gamle» metoder for kommunikasjon.

Det er videre viktig for hensynet til nasjonal selvstendighet og suverenitet – og for å sikre at informasjonsinnhentingen skjer ut fra nasjonale behov og ikke som biprodukt av andre nasjoners informasjonsinnhenting – at mest mulig informasjonsinnhenting skjer av norske organer; i dette tilfelle E-tjenesten. Dette er dessuten avgjørende for at overvåkningen kan kontrolleres av norske domstoler og EOS-utvalget.

Vi legger til grunn at formålet med DGF er å sikre E-tjenesten teknisk tilgang til en informasjonskilde som i dag ikke er tilgjengelig. Det er vår forståelse at Norge også i dag kan skaffe deler av den etterretningsinformasjon det er tale om, men at en i så fall er helt avhengig av hjelp fra samarbeidende tjenester i andre land. Utvalget har vist til at slik informasjon ofte kommer for sent, som biprodukt av andre tjenesters prioriterte oppgaver og dessuten i stor utstrekning stammer fra samarbeidspartnerens bruk av DGF, jf. rapporten side 27 og 29.

En sentral premiss for vår forståelse og vurdering av utvalgets vurdering er at DGF ikke utvider E-tjenestens oppgaver, ansvarsområde eller typen informasjon tjenesten skal ha tilgang til, jf. rapporten side 29. Vi legger dessuten til grunn at DGF ikke vil innebære at Politiets sikkerhetstjeneste eller Nasjonal sikkerhetsmyndighet får utvidet eller direkte tilgang til E-tjenestens informasjon, jf. rapporten side 29. Vi merker oss også at det i rapporten er pekt på at det lovmessige og prinsipielle forblir enten uforandret eller strengere, sistnevnte for eksempel ved ytterligere begrensninger på deling av overskuddsinformasjon, jf. side 29.

Informasjon innhentet ved hjelp av DGF og formidlet til PST, vil være nyttig for PSTs oppgaveløsning, innenfor PSTs samfunnsoppdrag. Og økt bruk av informasjon fra E-

tjenesten, istedenfor fra internasjonale samarbeidspartnere, vil sikre at en større andel av PSTs informasjonstilfang er underlagt norsk kontroll ved domstoler og EOS-utvalget.

Det er liten tvil om at DGF har flere rettslige og personvernmessige utfordringer. Hensynet til befolkningens tillit til E-tjenestens arbeid tilsier således klart at innføring av DGF som virkemiddel for de hemmelige tjenestene må skje innenfor de overordnede rammer som utvalget har trukket opp på side 6 i rapporten (særlig kulepunktene 1, 2 og 6) og videre at regelverket bygger på prinsippene om formålsavgrensning, minimalisering, autorisasjon og kontroll, jf. rapporten side 52. Etter vårt syn er det også klart, slik utvalget fremhever, at informasjon innhentet ved bruk av DGF ikke bør kunne benyttes som bevis i straffesaker, jf. rapporten side 6, 22 og 61.

2. Utformingen av regelverket

Lysne II-utvalget har trukket opp retningslinjer for utformingen av et regelverk om DGF, jf. rapporten side 60–61 om lovtiltak, og side 62–66 om de menneskerettslige rammene. Vi slutter oss til synspunktene som her fremholdes av utvalget, og vil for øvrig bemerke:

Utvalget fremhever at det må etableres klar lovhjemmel for DGF-løsningen, jf. blant annet rapporten side 62. Foruten en slik hjemmel må det utformes lett tilgjengelige bestemmelser om bruk av overskuddsinformasjon og om lagring og sletting av opplysninger. Vi legger til at dersom det er behov for å oppstille begrensninger i lovens hovedvilkår, tilsier risikoen for formålsutglidning at det ikke utformes unntaksregler med stort rom for skjønn.

Det er på det rene at etableringen av DGF innebærer et inngrep i retten til privatliv etter Grunnloven § 102 og EMK artikkel 8, og at den potensielle «nedkjølingseffekten» har en side til vernet av ytringsfriheten, jf. Grunnloven § 100 og EMK artikkel 10. Som utvalget mener vi at DGF ikke bør innrettes slik at løsningen balanserer på grensen av hva som er akseptabelt innenfor de rammer Grunnloven og menneskerettskonvensjonene oppstiller, se utredningen side 35. Det bør etableres så vidt strenge vilkår for bruken av DGF at løsningen er robust nok til å følge eventuelle skjerpede grenser for hva som anses å være et akseptabelt inngrep i den enkeltes rettigheter.

Utvalget avgrenser mot bruk av informasjon innhentet ved DGF som bevis mot tiltalte i straffesaker. Vi er enige i utvalgets syn på at en slik lovfestet formålsbegrensning antagelig er egnet til å styrke tilliten til bruken av DGF, jf. rapporten på side 61. Norsk straffeprosess bygger på prinsippet om fri bevisførsel. Unntak følger blant annet av bevisforbudene i straffeprosessloven §§ 117 flg. og reglene om bevisavskjæring i straffeprosessloven §§ 292 og 292 a. Etter vårt syn kan det være hensiktsmessig om en ved utformingen av et eventuelt regelverk om DGF vurderer om formålsbegrensningen bør suppleres med et eget bevisforbud eller en avskjæringshjemmel i straffeprosessloven.

Det fremgår av rapporten side 58 at utvalget ikke har hatt anledning til å utrede hvordan domstolsbehandlingen for kontroll av DGF-tiltak skal legges opp, og videre at utvalget ikke tar stilling til spørsmålet om forhåndskontroll av DGF skal foretas av en spesialdomstol. Vi peker her på at en i Norge tradisjonelt har benyttet spesialdomstoler i liten grad. Til fordel for bruk av spesialdomstoler taler synspunktet om at det er positivt at personene som skal ta stilling til bruk av DGF har kunnskap om etterretningsfaget og trusselbildet, slik utvalget viser til. Dette behovet kan etter vårt syn godt ivaretas ved at slike avgjørelser legges til én bestemt tingrett eller enkelte dommere eller en avdeling ved en tingrett. Det er dessuten liten tvil om at det vil kreve betydelige ressurser å opprette en særskilt domstol, og vi stiller spørsmål om det for DGF vil bli tale om et så vidt stort antall saker at en slik ressursbruk kan forsvares. Det kan også legges til at risikoen for at dommerne etter hvert identifiserer seg med E-tjenestens virke og oppgaver, jf. utvalgets synspunkter på side 58, trolig vil være mindre dersom dommerne befatter seg med ulike oppgaver og fagfelt, slik det i dag er ved de alminnelige domstoler.

Lysne II-utvalget viser til at det i enkelte tilfeller kan være behov for å iverksette søk i DGF uten å avvente forhåndsgodkjenning fra domstolene, jf. rapporten side 58. Utvalget foreslår at regelverket skal åpne for dette etter mønster av politiloven § 17 d. Vi påpeker her at forslaget om å etablere DGF for etterretningsformål ikke fullt ut kan sammenlignes med bruk av straffeprosessuelle tvangsmidler. Politiets sikkerhetstjeneste og E-tjenesten har ulike roller, oppgaver og rammer for sitt arbeid. Det fremgår ikke av rapporten om utvalget har sett nærmere på hvilken betydning slike ulikheter bør få for spørsmålet om å unnlate forhåndsgodkjenning, og i så fall på hvilke vilkår. Ettersom bruk av DGF er meget personverninngripende, bør dette spørsmålet vurderes nærmere.

3. Økonomiske- og administrative konsekvenser

For å kunne vurdere den reelle nytteverdi av forslaget sett opp mot de kostnader det vil medføre, sammenholdt med de personvernsmessige problemstillinger, foreslår JD at det foretas en kost-nytte-vurdering av DGF. Det bør her særlig tas hensyn til den merverdi DGF vil innebære når man tar i betraktning den økende bruk av kryptering ved digital kommunikasjon. Vurderingen bør omfatte hvorvidt det finnes alternative tiltak, som er mindre inngripende, men kan ha samme effekt for nasjonal sikkerhet.

Med vennlig hilsen

Harald Aass
fagdirektør

Toril Juul
seniorrådgiver

Dokumentet er godkjent og sendes uten signatur