DET NASJONALE STATSADVOKATEMBETET

FOR BEKJEMPELSE AV ORGANISERT OG ANNEN ALVORLIG KRIMINALITET

Forsvarsdepartementet
Postboks 8126 Dep.
0032 Oslo

Deres referanse	*Vår referanse*	*Dato*
2016/2699-1/FD II 5/SIH	2016/01692-2	17. januar 2017

HØRING – RAPPORT AVGITT AV LYSNE II-UTVALGET OM DIGITALT GRENSEFORSVAR

Det vises til Forsvarsdepartementets høringsbrev av 5. oktober 2016 vedrørende rapport avgitt av Lysne II-utvalget 26. august s.å. om digitalt grenseforsvar (DGF). I telefonsamtale med seniorrådgiver Siri Horgen Hinze 6. d.m. ble frist for å sende inn høringssvar forlenget til 17. januar 2017.

Utvalget anbefaler at DGF – innenfor de strenge rammer som beskrives i rapporten – etableres i Norge. Etter utvalgets oppfatning er DGF nødvendig for nasjonens sikkerhet, særlig med tanke på beskyttelse mot sabotasje og spionasje i det digitale rom, men også knyttet til håndtering av potensielle trusler om terror på norsk jord. Hva gjelder sistnevnte vil DGF ifølge utvalget "*være et effektivt verktøy innen terrorbekjempelse, spesielt i arbeidet med å kartlegge utenlandske ekstremistmiljøer sine kontakter med Norge*" (rapporten s 70).

Som utvalget gjør noye rede for er DGF et potensielt svært personverninngripende virkemiddel. I rapporten fremheves herunder at en DGF-installasjon ikke bare vil plukke opp kommunikasjon mellom Norge og utlandet. Som følge av ruting av datatrafikk vil mye av trafikken ifølge utvalget gjelde kommunikasjon mellom norske borgere som befinner seg i Norge, i tillegg til at mange elektroniske tjenester som benyttes av et individ kun for dettes formål innebærer kommunikasjon over landegrensene (eksempelvis skybaserte lagringstjenester), jfr. rapporten s 5. Etter utvalgets oppfatning må en eventuell innføring av DGF tilfredsstille flere absolutte kriterier. DGF må herunder underlegges strenge formålsbegrensninger – DGF skal kun benyttes til utenlandsetterretningsformål, og kan "ikke under noen omstendighet" brukes til straffeforfølgelsesformål (s 70) – datainnsamlingen skal minimaliseres og det må etableres et strengt tre-lags kontrollregime, alt beskrevet nærmere i kapittel 9 i rapporten.

Det nasjonale statsadvokatembetet er enig med utvalget i at det er gode grunner for å innføre DGF også i Norge, og antar i likhet med utvalget og E-tjenesten at DGF vil være et viktig tiltak både for å håndtere cybertrusler med utenlandsk utgangspunkt og for å møte trusselen fra internasjonal terrorisme. Som det fremgår av rapporten har de fleste land i verden, deriblant sammenlignbare stater som Sverige, Tyskland, Frankrike og Storbritannia, i større eller mindre grad etablert ordninger tilsvarende DGF for etterretningsformål. Slik bulkaksess til kommunikasjon skal ha "*bidratt til å redde liv og hindre alvorlige terroranslag, samt avverget eller redusert konsekvensene av svært skadelige*

Postadresse: Postboks 8044 Dep 0030 OSLO
Kontoradresse: Brynsalléen 4 0667 OSLO
Telefon: 23 17 42 00
Telefax: 23 17 42 10
Mail : Post.nasj.emb@statsadvokatene.no

cyberoperasjoner" (rapportens pkt. 5.6). En er videre enig med utvalget i at DGF må underlegges strenge begrensninger for å være juridisk holdbart og forholdsmessig i et menneskeretts- og personvernperspektiv.

Etter embetets oppfatning bør det imidlertid være en viss adgang til å bruke informasjon fra DGF til strafforfølgningsformål, iallfall hva gjelder de alvorligste formene for kriminalitet, jfr. nærmere nedenfor.

En går ikke nærmere inn på den foreslåtte innrettingen av en DGF-installasjon for øvrig (jfr. rapportens kapittel 9).

Bruk av overskuddsinformasjon

Etter utvalgets syn forutsetter DGF at all overskuddsinformasjon må slettes, for å hindre formålsglidning. Som eksempel nevner utvalget følgende situasjon: "*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 oppfølgning*" (pkt. 9.4.2). I eksempelet beskrives straffbare handlinger som allerede *er begått,* men slik en forstår rapporten gjøres heller ikke noe unntak fra sletteplikten hvis E-tjenesten skulle plukke opp informasjon om at noen er *i ferd med å begå* alvorlig kriminalitet.

Det er utvilsomt viktig å hindre misbruk av informasjon fra et eventuelt DGF, og embetet har heller ikke innvendinger til at alle søk i datalagrene skal ha utenlandsetterretning som begrunnelse. Et absolutt forbud mot bruk av overskuddsinformasjon for å avverge – samt etterforske - alvorlige straffbare handlinger, vil imidlertid være svært uheldig. Hensynet til å unngå formålsglidning veier heller ikke like tungt så lenge PST eller politiet er uten innflytelse på E-tjenestens informasjonsinnhenting.

I rapporten ses bort fra "ekstraordinære situasjoner/nødrettssituasjoner" (s 60). Nødrett kan eventuelt gi grunnlag for å dele informasjon med politiet, som for eksempel opplysninger om et planlagt drap eller et pågående seksuelt overgrep mot barn. Etter embetets syn vil alene et nødrettslig grunnlag for informasjonsdeling i straffesaker likevel ikke være tilstrekkelig.

Forholdet til straffeloven 2005 § 196 om plikten til å avverge et straffbart forhold ses ikke vurdert i utvalgets rapport. Avvergingsplikten er angitt slik i § 196 første ledd:

"Med bot eller fengsel inntil 1 år straffes den som unnlater gjennom anmeldelse eller på annen måte å søke å avverge en straffbar handling eller følgene av den, på et tidspunkt da dette fortsatt er mulig og det fremstår som sikkert eller mest sannsynlig at handlingen er eller vil bli begått."

Avvergingsplikten gjelder en rekke alvorlige straffbare handlinger, uttømmende oppregnet i første ledd annet punktum (herunder forbrytelser mot Norges selvstendighet, terrorrelaterte handlinger, grov kroppsskade, drap, de alvorligste seksuallovbruddene mv.). Det presiseres samme sted at plikten gjelder uavhengig av taushetsplikt, og det rettslige grunnlaget for taushetsplikten er uten betydning, jfr. Prop. 116 L (2009-2010) kap. 12.3 s 19. Sletting av overskuddsinformasjon uten videre oppfølgning slik utvalget foreslår kan derfor etter omstendighetene komme i konflikt med straffeloven 2005 § 196.

Utvalget drøfter heller ikke forholdet til straffeloven 2005 § 226 om plikten til å opplyse om uriktig tiltale eller domfellelse, som også gjelder uten hensyn til taushetsplikt.

I vedlegg 2 til rapporten om forholdene i andre land heter det at tilsvarende informasjon innhentet i Sverige ikke kan benyttes til straffeforfølgningsformål, mens situasjonen er annerledes i Storbritannia og Tyskland, der SIGINT-innhenting kan skje både av hensyn til rikets sikkerhet og for å bekjempe alvorlig kriminalitet.

Etter embetets syn må overskuddsinformasjon fra DGF i noen tilfeller kunne deles med politiet. I hvilke situasjoner samt hvordan dette skal skje må utredes nærmere i forkant av et eventuelt lovforslag om å implementere DGF i Norge. Det må primært være mulig å dele overskuddsinformasjon for å avverge alvorlig kriminalitet, men også en viss adgang til å dele slik informasjon med politiet for å etterforske de alvorligste straffesakene, herunder seksuelle overgrep mot barn. En begrenset adgang til å bruke opplysninger fra DGF i de alvorligste straffesakene behøver ikke å være uforenlig med det menneskerettslige vernet mot inngrep i privatliv eller ytringsfrihet. I tillegg må tas hensyn til "offerets personvern" og statens ansvar for å beskytte borgerne, jfr. blant annet Rt. 2013 s 588.

Bevisforbud for informasjon innhentet ved DGF?

Utvalget anbefaler at informasjon innhentet gjennom DGF ikke under noen omstendighet skal kunne benyttes som bevis mot tiltalte i straffesaker (pkt. 9.4.2). I rapporten presiseres at dette er "*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*" (pkt. 9.4.3).

En sentral målsetning ved innføring av DGF er som nevnt å møte trusselen fra internasjonal terrorisme. I rapportens vedlegg 1: Scenarioer gis en beskrivelse av et mulig terroranslag mot T-banenettet i Oslo. I et slikt scenario kan en se for seg at opplysninger innhentet gjennom DGF gir grunnlag for pågripelse, fengsling (jfr. Rt. 2004 s 411) og etterforsking av en eller flere terrorister. Satt på spissen kan det videre tenkes en situasjon der det etter endt etterforsking ved PST viser seg at det ikke er bevismessig grunnlag for å ta ut tiltale, uten å bruke opplysningene plukket opp gjennom DGF. I denne situasjonen må de siktede terroristene loslates og saken henlegges, dersom utvalgets anbefaling legges til grunn. Dette vil åpenbart være svært uheldig, både med tanke på faren for nye terrorhandlinger og tilliten til PST og rettssystemet.

Informasjon om en terrorhandling vil ikke være å anse som overskuddsinformasjon, og bør etter embetets oppfatning også kunne brukes som bevis under en hovedforhandling. Til sammenligning kan vises til politiloven § 17 f annet ledd bokstav c om bruk av opplysninger som PST i dag innhenter med forebyggende tvangsmidler. Det bør også utredes nærmere om opplysninger om andre alvorlige straffbare handlinger kan brukes som bevis, uten å komme på kant med våre konvensjonsforpliktelser. Av vedlegg 2 til rapporten fremgår at i Storbritannia kan fremskaffet informasjon "som hovedregel" ikke benyttes som bevis i straffesaker (s 81), og det hadde vært av interesse å vite mer om hvor langt bevisforbudet rekker i Storbritannia og andre land.

Med hilsen

Carl Fredrik Fari
statsadvokat