POLITIET
KRIPOS

Politidirektoratet
Postboks 8051 Dep.
0031 OSLO

NCIS NORWAY

pr e-post

Deres referanse:	Vår referanse:	Sted, Dato
201603847	201602071	Oslo, 13.1.2017

HØRINGSSVAR – LYSNE II-UTVALGET OM DIGITALT GRENSEFORSVAR

Det vises til skriv av 5. oktober 2016 fra Forsvarsdepartementet hvor Lysne II-utvalgets rapport av 26. august 2016 sendes på høring. Videre vises det til e-post fra Politidirektoratet av 2. november 2016 og etterfølgende kommunikasjon med direktoratet, hvor Kripos' frist for avgivelse av høringssvar er forlenget til 13. januar 2017.

Innledning

Innledningsvis vil Kripos bemerke at utvalget påviser gode grunner for å gi E-tjenesten innsyn i digitale datastrømmer og tilgang til relevant informasjon der. Imidlertid mener Kripos at det er sentrale problemstillinger som ikke er drøftet, og at rapporten således lider av vesentlige mangler.

Vi har forståelse for at det lå utenfor utvalgets mandat å utrede eller foreslå konkret lovgivning og at utvalget konsentrerer seg om de overordnede prinsipielle sider ved en eventuell innføring av digitalt grenseforsvar (DGF). Det hadde imidlertid vært lettere å ta stilling til de problemstillinger som reiser seg dersom utvalget hadde vært mer konkret og presist. Når utvalget foreslår innføring av DGF, men uttrykkelig forutsetter at det ikke kan anbefale slik innføring med svakere kontrollmekanismer enn det som er beskrevet i rapporten, blir det problematisk at utvalget tidvis behandler disse spørsmål noe overfladisk og upresist. Dette gjelder særlig i forhold til spørsmål rundt håndtering av overskuddsinformasjon og forholdet til politiet.

Utvalget foreslår innføring av DGF med det naturlige forbehold at dette må *"...gjøres på en måte som ikke strider mot folkeretten eller norsk lov.... og... forutsetter at et tilstrekkelig klart lovgrunnlag [må] vedtas."* Det er imidlertid vanskelig å ta stilling til utvalgets forslag uten at forslag til lovregulering skisseres noe mer konkret enn det utvalget gjør. Noen av utvalgets premisser synes lite forenlig med gjeldende nasjonal og internasjonal lovgivning.

Som eksempel på det Kripos oppfatter som upresise drøftelser kan det nevnes at utvalget på side 27 uttaler at «*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.*» På side 30 anføres det at «.. *de fleste toneangivende land, herunder de største*

Post: Pb. 8163 Dep., 0034 Oslo
Besøk: Brynsalléen 6, 0667 Oslo
www.politi.no/kripos
Telefon: (+47) 23 20 80 00
Telefaks: (+47) 23 20 88 80
E-post: kripos@politiet.no
Org. nr: 974 760 827

landene i NATO, har etablert ordninger tilsvarende DGF for utenlandsetterretningsformål.» Det er mer enn en nyanseforskjell mellom disse utsagn, og hvilke kriterier som ligger til grunn for at land anses som «*sammenlignbare*» eller «*toneangivende*» er for oss uklart. Vi har for vår del svært vanskelig for å tro at "*de fleste*" av de omlag 200 land som finnes i verden har slike ordninger.

Et annet eksempel følger på side 61 hvor utvalget sier at «*Det bør fastsettes i lov av 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 som å være i strid med prinsippet om fri bevisbedømmelse i straffeprosessretten...*». Prinsippet om fri bevisbedømmelse relaterer seg til hvorledes domstolene skal vurdere og vektlegge de i retten fremlagte bevis og har ingen relevans her. Viktigere er kanskje at formuleringen *"...ikke..... kan bli brukt som bevis mot tiltalte i straffesaker....."* kan tolkes som om dette kun gjelder spørsmålet om å anvende informasjonen som bevis under hovedforhandling. Andre uttalelser tyder imidlertid på at adgangen til å dele informasjon med politiet skal være langt snevrere enn som så.

Utvalgets beskrivelse av forholdene i andre land, herunder kontrollmekanismer, bruk av overskuddsinformasjon og forholdet til øvrige myndigheter er også mangelfull.

Kripos vil i denne høringsuttalelsen fokusere på det som er særskilt viktig for oss. Det er politiets rolle i forhold til de spørsmål som reises og særlig spørsmålet om håndtering av overskuddsinformasjon. Vi vil likevel kort tilkjennegi noen generelle prinsipielle merknader

Generelle prinsipielle merknader
På et generelt grunnlag mener Kripos at det bør utvises tilbakeholdenhet med å gi særregler for det digitale området. Mange spørsmål som diskuteres i forhold til "Cyber-området" er allerede løst i forhold til tilsvarende analoge problemstillinger. Utgangspunktet bør være mest mulig allmenne og teknologinøytrale regler med konkrete særbestemmelser etter behov.

På denne bakgrunn er Kripos skeptisk til utvalgets forslag om særlige tilsyns og domstolsordninger. Ved en eventuell innføring av DGF bør EOS utvalget tilføres den styrking av kompetanse og ressurser som måtte være nødvendig og domstolskontrollen skje ved de ordinære domstoler.

Når det gjelder de folkerettslige rammer synes utvalgets fokus i for stor grad å ha vært knyttet til det tradisjonelle synet på personvern, uten å ta hensyn til "offerets personvern" – og statens ansvar for å beskytte borgerne.

Det er selvsagt viktig at de begrensninger som folkeretten og menneskerettighetene setter for myndighetene respekteres. Det er imidlertid også slik at folkeretten og menneskerettighetene setter positive krav til at myndighetene sikrer borgernes integritet og rettigheter. Slike plikter fremgår blant annet av Grunnlovens kapittel E og FN's barnekonvensjon.

I denne sammenheng vil vi vise til EMK artikkel 1 som pålegger staten å sikre konvensjonens rettigheter for alle innenfor statens jurisdiksjon. Dette er i Rt. 2013 s. 588 beskrevet som at det *"innebærer blant annet at staten har en plikt til, etter forholdene, å ta aktive skritt for å hindre at private krenker hverandre - konvensjonen har i denne forstand også horisontal virkning."*

Dette vil kunne innebære at om man, f.eks. gjennom DGF, får kunnskap om at noen blir, eller er i ferd med å bli utsatt for alvorlige integritetskrenkelser, så vil staten ha en plikt til å beskytte den/de som utsettes. Jo alvorligere krenkelse det er snakk om – jo større plikt til vil staten ha til å gjøre å gjøre tiltak.

Offerets personvern er anerkjent gjennom flere avgjørelser i EMD. I dommen K.U. v Finland[1] (2. desember 2008) kom EMD til at Finland hadde brutt sin plikt til effektiv beskyttelse av retten til privatliv etter artikkel 8, ved ikke å ha hjemmel for utlevering av opplysninger som var nødvendige for etterforskning og oppklaring av den aktuelle saken.

Særlig om forholdet til politiets rolle og oppgaveutførelse
Utvalget fremhever særlig den kraftige eskalering av cybertrusler og økt fare for terrorisme som begrunnelse for å innføre DGF. Terrorbekjempelse er primært et polisiært ansvar, og håndtering og bekjempelse av cybertrusler vil også i stor grad involvere politiet. På denne bakgrunn mener vi at utvalgets redegjørelse for politiets oppgaver og samfunnsrolle er svært mangelfull.

I rapportens side 20 uttaler utvalget:

"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 på 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."

Uttalelsen er lite dekkende. Det er få, om noen, politiorganer som kun driver reaktiv etterforskning. De aller fleste, antagelig alle, har også oppgaver knyttet til etterretning, forebygging, avverging og krisehåndtering.

Det sentrale i denne sammenheng er imidlertid forholdet til politiet i Norge. Når utvalget viser til at: "*Politiets virksomhet retter seg mot enkeltpersoner som det er rimelig grunn til å etterforske/skjellig grunn til å mistenke om har begått visse straffbare handlinger eller forbereder slike*.", overser utvalget totalt politiets rolle, ansvar og myndighet for forebygging, avverging, opprettholdelse av sikkerhet og krisehåndtering.

Utvalgets manglende forståelse for politiets rolle og oppgaver viser seg også tydelig når det hevdes at det er: "*Grunnleggende rettslige og prinsipielle forskjeller mellom polisiære og straffeprosessuelle tvangsmidler på den ene siden, som blant annet bygger på strafferammevilkår som grunnvilkår for å ta i bruk de de ulike tvangsmidler, og E-tjenestens metodebruk for å innhente informasjon på den andre siden.*"

Politiets oppgaver følger av politiloven § 2. Politiet skal blant annet: opprettholde den offentlige orden og sikkerhet og alene eller sammen med andre myndigheter verne mot alt som truer den alminnelige tryggheten i samfunnet. Videre skal politiet forebygge kriminalitet

[1] http://www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/KU%20v%20Finland%20en%20presse.pdf

og andre krenkelser av den offentlige orden og sikkerhet. Til disse formål er politiet gitt eksklusive fullmakter. Fullmakter som også er relevante i forhold til å håndtere de trusler utvalget viser til for å begrunne DGF.

Utvalgets mangelfulle beskrivelse av politiets virksomhet generelt, og særlig i forhold til de oppgaver politiet har når det gjelder forebygging og etterretning, gir et svakt grunnlag for å drøfte politiets tilgang til informasjon innhentet gjennom DGF. *"Bruk av etterretning for å redusere usikkerhet hos beslutningstakere, med et særlig fokus på å predikere fremtiden"*, synes av utvalget å være antatt forbeholdt etterretningsorganisasjoner, men dette gjøres på tilsvarende måte hos politiet.

Mange av politiets oppgaver løses utenfor det straffeprosessuelle sporet. Vi kan her vise til politiets etterretningsdoktrine. I doktrinen fremkommer så vel både arbeidsmetoder og politiets rettslige rammer for etterretningsarbeidet. Samtidig er det viktig å påpeke at det også under etterforskning foreligger flere straffeprosessuelle hjemler som kan benyttes for å beskytte sensitiv informasjon.

Særlig om restriksjoner på bruk av overskuddsinformasjon og deling av informasjon med politiet

En eventuell opprettelse av DGF forutsetter et adekvat regelverk som beskytter personopplysninger og reduserer risiko for misbruk. Adgangen til å gi politiet og andre tilgang til opplysninger fra DGF må naturlig nok reduseres. Vårt prinsipielle utgangspunkt er imidlertid at kunnskap medfører ansvar. Formålsbetraktninger og hensyn til personvern vil gi begrensninger i hvorledes innhentet informasjon kan anvendes, herunder deles med andre, men like fullt må det alltid vurderes om tilgjengelig informasjon utløser en aktivitetsplikt.

De kryssende hensyn som gjør seg gjeldende nå det man skal vurdere om betydningen av å anvende informasjonen er viktigere enn de hensyn som taler for å beskytte informasjonen er på ingen måte særegent for dette området. Tilsvarende problemstillinger melder seg typisk for informasjon som i utgangspunktet er taushetsbelagt eller endog gradert av hensyn til rikets sikkerhet. Fra politiets virksomhet er et illustrerende eksempel håndteringen av overskuddsinformasjon som fremkommer ved kommunikasjonskontroll.

Vi vil vise til tre typetilfeller hvor besittelse av informasjon typisk vil kunne utløse en aktivitetsplikt.

For det første fastsetter straffeloven § 196 en plikt til å anmelde eller på annen måte søke å avverge bestemte alvorlige straffbare handlinger, eller følgene av disse. Dernest gir straffeloven § 226 en plikt til å opplyse om omstendigheter som godtgjør at en som er tiltalt eller domfelt er uskyldig. For det tredje pålegger barnevernloven § 6-4 offentlig myndighet til, av eget tiltak, å gi opplysninger til barnevernet når det er grunn til å tro at barn blir mishandlet. Alle disse bestemmelsene gjelder uten hensyn til taushetsplikt.

Utvalgets rapport drøfter ikke konkret problemstillingene knyttet til avvergings- og handleplikt, og sier således intet om hvordan nødvendig deling av informasjon for å ivareta statens plikt til å beskytte borgerne skal skje.

På side 60 i rapporten uttales det at *"All overskuddsinformasjon om norske eller utenlandske personer vil bli slettet."* Videre sies det at: *"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.".

Vi er litt usikre på hvilke begrensninger utvalget egentlig ser for seg i forhold til bruk av overskuddsinformasjon. Overnevnte sitat om at noen "*har begått*" kan tyde på at det ikke gjelder slike begrensinger for forhold som ennå kan avverges. Andre uttalelser i rapporten, som "*Ikke under noen omstendighet bør informasjon fremskaffet ved DGF brukes som bevis mot tiltalte i straffesaker.*" indikerer imidlertid ganske klart at utvalget ser for seg sterke begrensinger i adgangen til å dele informasjon med politiet eller andre myndigheter.

Kryssende hensyn mellom ønske om hemmelighold på grunn av ulike typer av sensitivitet og de samme opplysningers potensielle nytteverdi er som nevnt ikke særegent for det digitale området. Et av de spørsmål vi har rundt utvalgets vurderinger er hvorfor det skal være en særregel som vektlegger rikets sikkerhet på bekostning av enkeltindividets krav på beskyttelse på det dette området. Straffelovens §§ 196 og 296, samt barnevernloven § 6-4 vil fortsatt gjelde på de øvrige deler av E-tjenestens virksomhet som vi formoder kan være vel så sensitive.

Kripos mener at opplysninger fremkommet ved DGF i noen tilfeller må deles med andre og benyttes. Når dette skal skje, og i hvilke form opplysningene skal brukes, må utredes nærmere og reguleres. Det er ikke tilstrekkelig å besvare disse problemstillingene ved å si at informasjonen skal slettes og vise til at "*det sees her bort fra ekstraordinære situasjoner/nødrettssituasjoner*" (pkt. 9.4.3).

Hva hvis opplysningene om at noen har begått et drap gjelder en sak hvor en annen feilaktig er dømt? Straffeloven § 226 gir en plikt til å opplyse om slike omstendigheter, og en stat kan neppe lovregulere seg bort fra en plikt til å reagere når den blir kjent med at noen er uriktig dømt.

At offentlige tjenestemenn som kommer til kjennskap om seksuelt misbruk av barn skal kunne slette dette uten videre oppfølging finner vi helt uholdbart. Barn skal beskyttes. Grunnloven kapittel E, menneskerettsloven og EMK pålegger staten et ansvar for å beskytte barn mot misbruk som man heller ikke kan lovregulere seg bort fra.

Spørsmålet må da ikke være om videre oppfølging skal skje, men hvordan. Her som er ellers er avverging og skadereduksjon viktigere enn straffeforfølgning. På noen områder kan man tenke seg at opplysningene kan og skal benyttes i avvergende, reddende øyemed, men ikke tillates brukt som bevis for å straffeforfølge begåtte forhold. Når det gjelder seksuelle overgrep mot barn er imidlertid vår klare oppfatning gjentagelsesfaren er så åpenbar at det vil gi liten mening i å skille mellom behovet for følge opp pågående og avsluttede forhold.

Det må heller ikke glemmes at hovedbegrunnelsen for straff er individuell og allmenn prevensjon. Straffeforfølgning kan noen ganger være det beste virkemiddel for å beskytte samfunnet mot de farer som utvalget mener begrunner behovet for DGF.

Dette illustreres klart med dommer på forvaring. Hele poenget med forvaring er å beskytte allmennheten mot fremtidig fare. Det ville være særdeles uheldig dersom DGF skulle fremskaffe informasjon som ville kunne gi grunnlag for forvaringsdom for terrorister, men at

dette ikke ble tillatt benyttet som bevis, med den følge at det ikke var mulig å få dom på forvaring og det deretter finner sted en terrorhandling.

Formodentlig vil politiet behandle det meste av den informasjon som kommer fra DGF utenfor straffesak. Vårt prinsipielle utgangspunkt er imidlertid at informasjon fra DGF og delt med politiet også bør kunne benyttes som bevis i straffesak. Vi kan heller ikke se at dette vil innebære noen formålsglidning så lenge politiet ikke har hatt noen innvirkning på om eller hvordan E-tjenesten kom over informasjonen. Under enhver omstendighet må informasjonen kunne tillates brukt som bevis i de alvorligste sakene.

Oppsummering og avsluttende bemerkninger

Kripos ser at det er grunner for å innføre en DGF-ordning, men vi mener rammene rundt dette krever ytterligere utredning. Hvilke mothensyn som måtte foreligge og hvilke reguleringer som eventuelt kan oppveie eller kompensere for dette er i for liten grad omtalt og de dilemma som vil kunne oppstå i forhold til varslings- og avvergingsplikt er ikke tilstrekkelig utredet.

Kripos mener det forut for en eventuell innføring av DGF må foretas en langt grundigere gjennomgang av de kryssende hensyn som vil gjøre seg gjeldene når man gjennom DGF får tilgang til informasjon som politiet eller andre myndigheter har behov for. I denne sammenheng er det viktig å avklare hvilke rettslige skranker som settes av menneskerettighetene og Grunnloven.

Disse problemstillingene er ikke særegne på det digitale området og Kripos mener prinsipielt at man i minst mulig grad skal ha særregler på dette området. Av denne grunn er vi skeptiske til en ordning med egne tilsyns- og domstolsordning for DGF.

Utvalgets uttalelse om at overskuddsinformasjon om at det er begått seksuelle overgep mot barn skal slettes uten videre oppfølging, er oppsiktsvekkende og kan etter vår vurdering ikke begrunnes verken juridisk eller moralsk. For oss er det åpenbart at slike opplysninger må følges opp. Av hvem og hvordan er et annet spørsmål. En grundigere vurdering av hvorledes disse spørsmål er vurdert og håndteres i andre land ville være interessant.

Med hilsen

Ketil Haukaas

Kopi:
Det nasjonale statsadvokatembetet