Forsvarsdepartementet
postmottak@fd.dep.no

5. januar 2017

Høringsuttalelse – høring om rapport avgitt av Lysne II-utvalget om digitalt grenseforsvar

1. Innledning

Den internasjonale juristkommisjon – norsk avdeling (ICJ-Norge) viser til Forsvarsdepartementets høring om Lysne II-utvalgets rapport om digitalt grenseforsvar (DGF), idet vi ønsker å inngi denne høringsuttalelsen.

ICJ-Norge anser at Lysne II-utvalget har avgitt en i hovedsak grundig rapport, men mener likevel at dens forslag om DGF inneholder flere rettslig sett grunnleggende problematiske sider, som gjør at det ikke kan gjennomføres i den foreslåtte form innenfor rammene av gjeldede krav til person- og kommunikasjonsvern.

En grunnleggende premiss i den sammenheng, som også utvalget erkjenner, er at DGF vil innebære filtrering og lagring av vesentlige deler av hele den norske befolkningens elektroniske kommunikasjon, herunder kommunikasjon som foregår mellom norske borgere i Norge. Det er – særlig med hensyn til kommunikasjon via Internett, men også med hensyn til telekommunikasjon – langt på vei tilfeldig om innenlandsk kommunikasjon passerer Norges geografiske grenser. Store deler av befolkningens bruk av Internett (herunder vanlig "surfing", bruk av kommunikasjonstjenester som Skype, sosiale medier og lagring i skytjenester) innebærer kommunikasjon med servere som ligger utenfor Norge. Eventuelle forestillinger om at DGF bare omfatter "utenlandsk" kommunikasjon er derfor feilslåtte. DGF vil nødvendigvis hovedsakelig omfatte norske borgeres daglige bruk av digitale kommunikasjonstjenester.

På den bakgrunn representerer forslaget en utglidning i synet på, og en vesentlig undergraving av, kommunikasjonsvernet til den norske befolkningen. Som det vil fremgå i det videre, er det ICJ-Norges oppfatning at det foreliggende forslaget ikke kan gjennomføres i den form som foreslått av utvalget uten å bryte med de grunnleggende krav til person-/kommunikasjonsvern som gjelder i Norge og Europa for øvrig.

ICJ-Norge
Postadresse: c/o advokat Jon Wessel-Aas, postboks 775 Sentrum, 0106 Oslo
E-post: jwa@binghodneland.no **Nettside:** www.icj.no

2. Noen hovedbetraktninger

Under dette punktet vil vi gjengi noen hovedbetraktninger, hvorav enkelte vil utdypes i egne punkter senere i vår uttalelse.

ICJ-Norge mener at rapporten er uklar på et avgjørende punkt, nemlig hvilke formål DGF skal tjene.

Utvalget definerer allerede på side 10 i sin rapport "Digitalt grenseforsvar" på en bestemt måte, som tilsynelatende også innbefatter formålet med ordningen som diskuteres:

> *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*

Det vises ellers i rapporten til etterretningstjenesteloven § 3, som definerer Etterretningstjenestens (E-tjenesten) oppgaver. Vi kan ikke se at utvalgets mandat, eller utvalgets øvrige vurderinger, støtter opp om at et tiltak som DGF nødvendigvis må ha samme vide formål som E-tjenesten har for øvrig.

Tvert imot må hvert enkelt formål vurderes for seg, opp mot både menneskerettslige skranker og mot hva som vi som samfunn aksepterer som akseptable inngrep i person-/kommunikasjonvern. Her er det grunn til å minne om vurderingsmomentene fra Den europeiske menneskerettskonvensjon (EMK) og tilhørende praksis fra Den europeiske menneskerettsdomstol (EMD), hvor ethvert inngrep må være nødvendig i et demokratisk samfunn - av EMD nærmere presisert til et krav om tvingende samfunnsmessig behov ("pressing social need"). Hva gjelder inngrep i kommunikasjonsvernet, har EU-domstolen i flere avgjørelser klargjort terskelen for et slikt tiltak; det må ikke gripe inn i "kjernen i individets rettigheter", og for øvrig må det være "strengt nødvendig", jf. nærmere om dette nedenfor.

I denne sammenheng kan det bemerkes at én metode for innhenting av opplysninger, for eksempel menneskebasert innhenting eller bruk av åpne kilder godt kan være forholdsmessig for å ivareta visse av E-tjenestens oppgaver, mens det neppe vil være forholdsmessig å aksessere og lagre store datamengder om utenforstående, sivile tredjepersoner for å ivareta samtlige av de formål som E-tjenesten er satt til å fremme.

ICJ-Norge mener at utvalget har argumentert godt for hvorfor E-tjenesten i fremtiden vil måtte ha *en eller annen form for* tilgang til grenseoverskridende elektronisk kommunikasjon for å effektivt kunne beskytte mot cyberspionasje og -sabotasje mot Norge og vitale norske interesser. Med cyberspionasje og -sabotasje mener vi i denne sammenheng angrep og infiltrasjon som skjer *via elektroniske kommunikasjonssystemer,* rettet mot samfunnskritisk IKT-infrastruktur – det vil si der

hvor både den skadegjørende handlingen og dens mål skjer/befinner seg i IKT-infrastrukturen.

Derimot anser vi at utvalgets tilrådning om oppretting og bruk av DGF for også andre utenlandsetterretningsformål, herunder terrorbekjempelse, som til dels betydelig svakere begrunnet, både fra et nytte- og mer generelt forholdsmessighetsperspektiv. Det er i den sammenheng også viktig å understreke at bekjempelse av terror i Norge hovedsakelig er en politioppgave, der bruk av kommunikasjonskontroll og andre tilsvarende tvangsmidler overfor borgernes kommunikasjon er regulert i straffeprosessloven og (for PSTs forebyggende virksomhet) i politiloven.

I realiteten innebærer utvalgets forslag på dette punkt langt på vei at man vil omgå de begrensningene som gjelder for PSTs forebyggende virksomhet, ved å gi E-tjenesten adgang til å foreta en lagring av den norske befolkningens kommunikasjon, som det verken rettslig eller politisk er aktuelt å gi til PST – og som etter vår vurdering dessuten vil være klart i strid med etterretningsloven § 4, som inneholder forbud mot at E-tjenesten norsk territorium overvåker eller på annen fordekt måte innhenter informasjon om norske fysiske eller juridiske personer.

Det ligger i dette at ICJ-Norge, basert på den foreliggende dokumentasjonen fra utvalget, vil fraråde tilgang til kabelbåren kommunikasjon inn og ut av Norge for andre formål enn å beskytte norsk IKT-infrastruktur og -systemer mot spionasje og sabotasje fra fremmede aktører.

ICJ-Norge vil i den forbindelse særlig vise til EU-domstolens dom i Tele2 Sverige mot Post- og Telestyrelsen[1]. Som vi kommer nærmere inn på i punkt 3 nedenfor, anser ICJ-Norge at kommunikasjonsvernsdirektivet slik dette er fortolket i dommen setter strenge rammer for myndighetenes tilgang til data om borgernes kommunikasjon og deres lagring av slike data, også hvor formålet er nasjonal sikkerhet[2]. Utvalget har selv drøftet forholdet til den tidligere avgjørelsen fra EU-domstolen i saken *Digital Rights Ireland* (rapporten side 45-46 og 64), men som det fremgår der var Tele2 Sverige-saken fortsatt under behandling da utvalget avga sin rapport. Det er ICJ-Norges oppfatning at det endelige resultatet i Tele2-saken, vesentlig endrer de forutsetninger utvalget har bygget på hva gjelder de rettslige rammene for tiltaket, slik disse fremkommer på side 46 i rapporten.

3. Nærmere om den rettslige vurdering med hensyn til selve lagringen

Utvalget synes å overse og/eller undervurdere at både etter EMK og etter EU-lovgivningen, anses *selve lagringen av borgernes kommunikasjon/kommunikasjonsdata* som et inngrep i person-/kommunikasjonsvernet – som må begrunnes og vurderes uavhengig av spørsmålet om innsyn i de lagrede opplysningene.

[1] Joined cases C-203/15 and C-698-15

[2] Se særlig dommens avsnitt 73

I saken Digital Rights Ireland[3], som gjaldt gyldigheten av EUs datalagringsdirektiv opp mot EU-Charteret og kommunikasjonsvernsdirektivet, uttalte domstolen i avsnittene 38 og 39 at den typen lagring av metadata som direktivet la opp til utgjorde en "particularly serious interference" med personvernet. Det ble vektlagt at direktivet ikke omfattet lagring av selve innholdet i kommunikasjonen, som ville ha grepet inn i kjernen ("the essence") av person-/kommunikasjonsvernet.

Disse vurderingene er fulgt opp og utdypet i den nylig avsagte dommen i saken Tele2 Sverige, som omhandlet rent nasjonale regler for datalagring. På dette punktet, er det særlig EU-domstolens uttalelser i dommens avsnitt 100-107 som er av betydning:

> *100 The interference entailed by such legislation in the fundamental rights enshrined in Articles 7 and 8 of the Charter is very far-reaching and must be considered to be particularly serious. The fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 37).*
>
> *101 Even if such legislation does not permit retention of the content of a communication and is not, therefore, such as to affect adversely the essence of those rights (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 39), the retention of traffic and location data could nonetheless have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 28).*
>
> *102 Given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, only the objective of fighting serious crime is capable of justifying such a measure (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 60).*
>
> *103 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).*

[3] C-293-12

104 In that regard, it must be observed, first, that the effect of such legislation, in the light of its characteristic features as described in paragraph 97 of the present judgment, is that the retention of traffic and location data is the rule, whereas the system put in place by Directive 2002/58 requires the retention of data to be the exception.

105 Second, national legislation such as that at issue in the main proceedings, which covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data, provides for no differentiation, limitation or exception according to the objective pursued. It is comprehensive in that it affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious criminal offences. Further, it does not provide for any exception, and consequently it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraphs 57 and 58).

106 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).

107 National legislation such as that at issue in the main proceedings therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.

Basert på hva som sies blant annet i den ovenfor siterte del av EU-domstolens avgjørelse, er det ICJ-Norges syn at den lagringen av både innholdsdata og metadata som forutsettes i forslaget om DGF, vil være i strid med de grunnleggende krav til person-/kommunikasjonsvern som følger av EU-/EØS-retten (og EMK, som her må forutsettes å harmonere med EU-retten).

Etter utvalgets forslag vil DGF, både i *korttidslageret* og *innholdslageret*, omfatte lagring av innholdet i elektronisk kommunikasjon. For førstnevnte vil dette gjelde korte intervaller som omfatter i prinsippet *alles* kommunikasjon, helt uavhengig av om E-tjenesten kan artikulere noen mistanke eller individualisert behov. Det er derfor ICJ-

Norges syn at utvalgets forslag vil utgjøre nettopp et inngrep i *kjernen* av person-/kommunikasjonsvernet, som uansett ikke vil være tillatt etter kommunikasjonsvernsdirektivet artikkel 15 (avsnitt 105 i Tele2-dommen). Kommunikasjonsvernsdirektivet er som kjent EØS-relevant, og implementert i norsk lovgivning gjennom lov om elektronisk kommunikasjon.

I Tele2-dommen slår EU-domstolen fast at tiltak av denne type, selv om de "bare" omfatter metadata, uansett må være "strengt nødvendige" for å ivareta de spesifiserte formål som de skal fremme - her nasjonal sikkerhet. Om tiltaket faktisk *er* strengt nødvendig, vil være underlagt en streng og konkret prøving fra domstolene. Den lagringen som forslaget til DGF forutsetter, da særlig i det såkalte *metadatageret,* vil etter ICJ-Norges syn rammes av de samme betraktninger som EU-domstolen anførte i de ovenfor siterte avsnittene.

Tilsvarende ble også påpekt av Hans Petter Graver og Henning Harborg i deres utredning om norsk gjennomføring av datalagring[4], der de uttalte at "domstolene [vil] stille strenge krav til dokumentasjonen av nødvendigheten av å lagre kommunikasjonsdata (...)". Dette er nå bekreftet og konkretisert ved EU-domstolens dom i Tele2-saken. Gravers og Harborgs uttalelse om at "[i] det materialet som er lagt frem hittil finnes ikke en slik dokumentasjon ut over generelle påstander og anekdoter", vil for øvrig være treffende også for Lysne II-utvalgets vurderinger med hensyn til terrorbekjempelse som formål og begrunnelse for det foreslåtte DGF (jf. også punkt 6 nedenfor).

4. Lovfesting – domstolskontroll

Videre oppstiller EU-domstolen (som også EMD gjør i sin praksis) krav til presis lovgivning, både for omfanget av ("scope") og bruken av et inngripende tiltak (sml. avsnitt 117-119 i Tele2-dommen). Slik ICJ-Norge ser det, vil ikke en formålsbegrensning til det vage og ikke uttømmende begrepet "utenlandsetterretningsformål" tilfredstille et slik krav. Vi viser for øvrig til hva EOS-utvalget skriver i de to siste avsnitt i sin høringsuttalelse av 20. desember 2016, jf EOS-utvalgets særskilte melding av 17. Juni 2016 til Stortinget, om rettsgrunnlaget for Etterretningstjenestens overvåkningsvirksomhet.

Enkelte vil kanskje hevde at vurderingen av om kabeltilgangsbasert innhenting for et konkret utenlandsetterretningsformål er berettiget, vil måtte foretas av den forslåtte DGF-domstolen for det konkrete tilfellet, og at det derfor ikke er nødvendig å innskrenke DGFs formål ytterligere gjennom lovgiving.

Til dette vil ICJ-Norge for det første si at de menneskerettslige og konstitusjonelle krav til forutberegnelighet og tilgjengelighet tilsier at slike vurderinger så langt som mulig bør foretas av lovgiver og komme til uttrykk i den aktuelle lovbestemmelsen.

---

[4] Henning Harborg og Hans Petter Graver, Datalagring og menneskerettighetene – utredning til Justisdepartementet og Samferdselsdepartementet, 1. Oktober 2015

For det andre er det en kjensgjerning at kvaliteten på avgjørelsene fra en domstol vil bero på hvilke kriterier den skal anvende, og hvor spesifikke disse er. Forholdsmessighetsbetraktninger kan nok tjene som viktige "sikkerhetsventiler" for rettssikkerheten, men vi vil advare mot å skyve vanskelige vurderinger foran seg ved å overlate til domstolen å foreta brede skjønnsmessige vurderinger basert på mer eller mindre vage formålsangivelser (jf. blant annet Tele2-dommen avsnitt 117-119).

Domstolsprøvingens kvalitet vil også bero på om det har vært kontradiksjon i saken. ICJ-Norge kan ikke se at utvalget har vurdert dette, men anser det som en forutsetning at en offentlig oppnevnt, uavhengig advokat vil måtte forsvare de berørtes interesser i hver sak for DGF-domstolen.

5. Nødrett og avvergingsplikt

Utvalget ser for seg en lovgivning som avskjærer bruk av informasjon innhentet fra DGF til straffeforfølgning. Slik ICJ-Norge ser det må dette være en absolutt forutsetning for at et tiltak som DGF overhodet kan innføres, siden dette ellers i realiteten kunne snudd bevisbyrden – slik at vi alle, basert på beskyldninger fremmet på bakgrunn av fragmenter av kommunikasjon, i realiteten vil måtte bevise vår uskyld.

ICJ-Norge er likevel skeptisk til at noe slikt vil la seg gjøre innenfor rammen av norsk lovgivning for øvrig. For det første brukes nødrett som "hjemmelsgrunnlag" for tvangsmiddelbruk allerede[5], og flere av de situasjoner som utvalget nevner hvor bruk av informasjon fra DGF må utelukkes ligger nært opp til hva som tradisjonelt ville blitt ansett som nødrettssituasjoner.

Videre vil enhver norsk borger ha plikt, uten hinder av eventuell taushetsplikt, til å avverge en rekke straffbare handlinger, jf. straffeloven § 196. Slik avverging vil normal involvere varsling til politiet i de fleste tilfeller. Vi stiller derfor spørsmål ved om E-tjenestens personale skal unntas fra denne plikten, eller på hvilken annen måte et slikt forbud er tenkt å gjøres effektivt.

6. Terrorbekjempelse og DGF – empiri og nødvendighet

Ved siden av cybertrusler er det E-tjenestens arbeid med kontraterror som vies mest plass i utvalgets rapport. Empirien som utvalget presenterer på dette området synes langt svakere enn for førstnevnte formål. Basert på rapporten og andre åpne kilder alene synes det godtgjort klart at den foreslåtte form for masselagring og kabelaksess hverken vil være særlig effektivt eller forholdsmessig for dette formålet.

For eksempel synes scenariobeskrivelsen for bruk av DGF (rapporten side 77 flg.) å hvile på en rekke usikre forutsetninger:

1. Det finner sted kommunikasjon mellom angrepslag og støttestruktur som lar seg fange opp av DGF

[5] Se for eksempel Årsrapporten fra Kontrollutvalget for Kommunikasjonskontroll for 2015 på side 4

2. E-tjenesten har forutgående kjennskap til relevante selektorer for gruppens ledelse
3. E-tjenesten har samlet inn relevant informasjon med andre sensorer
4. Det er mulig å korrelere kommunikasjon ut av konfliktområdet med kommunikasjon i Norge
5. At innsamlingen rettet mot personer i Norge går klar av forbudet i lov om etterretningstjenesten § 4

Det kan selvfølgelig ikke utelukkes at alle disse forutsetningene vil kunne være til stede i enkeltsaker, men ICJ-Norge har vanskelig for å anse kabelaksess og lagring av metadata for nær sagt hele befolkningens kommunikasjon som et "strengt nødvendig" tiltak for terrorbekjempelse under slike forutsetninger. Dette må, som for kommunikasjon som gjøres av norske borgere for øvrig, løses gjennom PSTs mandat og hjemler i gjeldende lovgivning.

***

Oppsummert er det ICJ-Norges syn at det foreslåtte DGF ikke lovlig kan gjennomføres innenfor de rettslige rammer for person- og kommunikasjonsvern som gelder i Norge etter Grunnloven, EMK og EØS-/EU-retten. En modifisert form for DGF kan eventuelt kun forsvares for å forebygge cyberspionasje og -sabotasje (som nærmere definert ovenfor under punkt 1). Hvordan et slik system eventuelt skal innrettes må i så fall undergis ytterligere utredning, der det er essensielt at man trekker inn både juridisk og teknologisk kompetanse.

For ICJ-Norge

Jon Wessel-Aas
styrets leder

Erlend Balsvik
fagutvalgsleder

ICJ-Norge
Postadresse: c/o advokat Jon Wessel-Aas, postboks 775 Sentrum, 0106 Oslo
E-post: jwa@binghodneland.no **Nettside:** www.icj.no