FORSVARSMINISTERIET
DANISH MINISTRY OF DEFENCE

Folketingets Forsvarsudvalg
Christiansborg

FORSVARSMINISTEREN
23. maj 2014

Folketingets Forsvarsudvalg har den 14. maj 2014 stillet følgende spørgsmål 6 vedrørende L 192 til forsvarsministeren, som hermed besvares. Spørgsmålet er stillet efter ønske fra Nikolaj Villumsen (EL).

Spørgsmål 6:
"Ministeren bedes kommentere de bekymringer over lovforslaget, der blev fremført af oplægsholderne under høringen i Retsudvalget den 8. maj 2014 om lovforslaget, jf. oplæggene fra Rådet for Digital Sikkerhed, C-cure, IT-Politisk Forening og Dansk IT, omdelt på L 192 – bilag 2."

Svar:
Oplægsholdernes bekymringer er i betydeligt omfang kommenteret i lovforslagets bemærkninger, høringsoversigten og de øvrige besvarelser af spørgsmål vedrørende lovforslaget.

Dette gælder således spørgsmål vedrørende:

- Lovforslagets § 21, stk. 3 – se besvarelsen af spørgsmål 1.
- EU-domstolens dom af 8. april 2014 om logningsdirektivet og proportionalitet – se besvarelsen af spørgsmål 2 og 10 b.
- Definitionen af sikkerhedshændelser – se besvarelsen af spørgsmål 3 a og 10 a.
- Skærpelse af nødvendighedskravet – se besvarelsen af spørgsmål 3 c.
- Logning – se besvarelsen af spørgsmål 3 d.
- Opbevaring og sletning af data – se besvarelsen af spørgsmål 3 e og f og spørgsmål 10 c.
- Retskendelse ved afkryptering – se besvarelsen af spørgsmål 3 i.
- Placeringen af Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste – se besvarelsen af spørgsmål 7.

HOLMENS KANAL 42
1060 KØBENHAVN K
TELEFON: 33 92 33 20
TELEFAX: 33 32 06 55
MAIL: FMN@FMN.DK
WEB: www.FMN.DK
CVR: 25-77-56-35
EAN: 5798000201200

- Tilsynet med Center for Cybersikkerhed – se besvarelsen af spørgsmål 8.
- Revision af loven – se besvarelsen af spørgsmål 9.

I oplægget fra C-cure kritiseres lovforslagets § 9, stk. 1, 2. pkt. Hertil bemærkes, at bestemmelsen svarer til persondatalovens § 5, stk. 2, 2. pkt.

I oplægget fra C-cure anføres, at Center for Cybersikkerheds aktiviteter skal tilrettelægges således, at netsikkerhedstjenesten i mindst muligt omfang konkurrerer med private udbydere af sammenlignelige services. Der henvises herom til følgende afsnit i lovforslagets almindelige bemærkninger afsnit 3.1.3:

> *"Den foreslåede udvidelse af kredsen af virksomheder, der kan tilsluttes netsikkerhedstjenesten, vurderes ikke at ville påvirke det private marked for it-sikkerhedsydelser negativt. Netsikkerhedstjenestens brede dækningsområde samt tjenestens adgang til oplysninger fra andre netsikkerhedstjenester og den øvrige del af Forsvarets Efterretningstjeneste indebærer, at der ikke på det private marked findes sammenlignelige sikkerhedsydelser, som virksomhederne kan benytte. Samtidig kan netsikkerhedstjenestens ydelser ikke træde i stedet for virksomhedernes øvrige it-sikkerhedsforanstaltninger, men skal alene betragtes som et ekstra lag af sikkerhed.*
>
> *Imidlertid vurderes det, at den foreslåede ordning i et vist omfang vil kunne påvirke det private marked for it-sikkerhedsydelser positivt. Således vil de anbefalinger, som monitoreringen typisk resulterer i, kunne medføre et behov for at styrke informationssikkerhedsniveauet hos de tilsluttede virksomheder – og dermed en efterspørgsel efter it-sikkerhedsydelser, der normalt vil blive leveret af private leverandører."*

I oplægget fra Dansk-IT anføres, at lovforslaget overordnet set er elastik i metermål, at der ingen begrænsninger er i, hvad centeret vil kunne, og at lovteksten er meget bredt og løst formuleret. Hertil kan bemærkes, at en sådan beskrivelse af lovforslagets restriktive bestemmelser om behandling, analyse og videregivelse af data efter min opfattelse må anses for ganske misvisende.

I oplægget fra Dansk-IT anbefales, at der indføres en procedure, hvor "chefen for centeret hver gang skal give tilladelse til behandlingen". Hertil kan bemærkes, at Center for Cybersikkerhed lægger stor vægt på ledelseskontrol i forhold til behandlingen af personoplysninger. For at sikre den bedst mulige kontrol med behandlingen af personoplysninger fører GovCERT's ledelse således i dag den daglige kontrol med behandlingen af personoplysninger. Herudover foretager centerets jurister også et internt tilsyn med, at behandlingen af personoplysninger sker i overensstemmelse med de juridiske rammer for centerets arbejde.

Endelig kan nævnes, at det nuværende GovCERT-tilsyn i sin årsredegørelse har tilkendegivet, at sikkerheden for korrekt behandling af personoplysninger er behørigt forankret på øverste ledelsesniveau i Center for Cybersikkerhed.

I oplægget fra IT-Politisk Forening anføres, at det bør præciseres i loven, at kun trafikdata vedrørende sikkerhedshændelsen kan videregives. Hertil kan bemærkes, at det udtrykkeligt fremgår af lovforslagets § 16, nr. 2, at videregivelse af trafikdata kun kan ske ved begrundet mistanke om en sikkerhedshændelse. Trafikdata, der ikke er knyttet til sikkerhedshændelser, vil således ikke kunne videregives.

I oplægget fra IT-Politisk Forening anføres, at det ikke er klart, om de i de almindelige bemærkninger afsnit 3.5.3. omtalte retningslinjer om udveksling af oplysninger internt i FE er en hensigtserklæring eller et lovkrav. Hertil bemærkes, at der efter lovforslagets bemærkninger (selvsagt) er en pligt for Forsvarsministeriet til at udstede sådanne retningslinjer, der – som det fremgår af bemærkningerne – vil blive offentliggjort på Center for Cybersikkerheds hjemmeside.

Med venlig hilsen

Nicolai Wammen