Bilag 2

En henvendelse til udvalget og justitsministerens kommentar hertil

Henvendelsen fra Telekommunikationsindustrien i Danmark jf. L 55 – bilag 6, og justitsministerens kommentarer hertil, jf. L 55 – bilag 12, er optrykt efter ønske fra udvalget.

Henvendelsen fra Telekommunikationsindustrien, Danmark (modtaget 26. november 2003):

TI henviser til branchens bemærkninger til det oprindelige lovudkast (TI's høringssvar af 30. april 2003 til Justitsministeriet).

Det fremsatte lovforslag er ændret i forhold til det oprindelige udkast på en række punkter. TI finder dog, at lovforslaget på visse punkter fortsat er problematisk for telebranchen. TI vil i det følgende redegøre for, på hvilke punkter der efter TI's opfattelse er behov for justeringer/ændringer af lovteksten og/eller de tilhørende bemærkninger.

1. Typer af data, som kan omfattes af et pålæg

Et pålæg om hastesikring kan omfatte alle typer data, som er i teleudbyderens besiddelse på tidspunktet for meddelelsen af pålægget. Også data, som alene opbevares ganske midlertidigt kan således være omfattet af et pålæg. Som eksempel nævnes på s. 54 i bemærkningerne til lovforslaget E-mails, som kun opbevares i udbyderens system indtil kunden henter dem ned på sin computer.

TI finder det problematisk, at teleudbyderne skal være i stand til at sikre (og siden udlevere) data, som kun opbevares ganske flygtigt i udbydernes systemer, dels fordi systemerne ikke er indrettet hertil, og dels fordi det formentlig vil være af tvivlsom værdi for politiet at sikre adgangen til de normalt meget få data, der tilfældigvis er tilgængelige i systemerne netop på det tidspunkt, hvor pålægget meddeles (det vil i praksis sige når pålægget efterkommes hos udbyderen).

Dette kan illustreres med følgende eksempel: Kunden kan via sin mobiltelefon sende/modtage SMS og MMS-beskeder (tekst- og billedbeskeder). Indholdet af en SMS/MMS-besked opbevares kun i udbyderens systemer indtil den pågældende besked er afleveret på modtagerens mobiltelefon, dvs. normalt kun få sekunder. Det betyder, at en hastesikring af indholdet af SMS/MMS typisk kun vil omfatte én enkelt eller ganske få SMS/MMS.

På den baggrund består der efter TI's opfattelse et misforhold mellem den gevinst der opnås ved sikring af disse få SMS/MMS og de omkostninger, der er forbundet med at indrette systemerne, så det er muligt at imødekomme et konkret pålæg, hvis det skulle forekomme.

Det kan i den forbindelse oplyses, at udbyderne vil skulle investere store beløb i nyt software for at kunne foretage hastesikring af SMS/MMS på udbyderens centraler. På centraler leveret af Nokia er det på nuværende tidspunkt slet ikke muligt at skaffe software, der muliggør sikring af indholdet af MMS.

Samme synspunkter gør sig for så vidt gældende for sikring af E-mails, der kun opbevares på internetudbyderens server indtil kunden vælger at slette dem, idet det dog kan anføres, at E-mails typisk vil være i udbyderens system i en lidt længere periode end SMS/MMS, idet de fleste kunder typisk ikke henter (dvs. åbner) deres E-mails løbende, men f.eks. kun gør det én gang dagligt.

TI's skal med henvisning til branchens høringssvar fastholde, at data som kun opbevares ganske midlertidigt i udbydernes systemer, ikke bør kunne omfattes af et pålæg om hastesikring.

I er således uenig med Justitsministeriet, som på side 54 i bemærkningerne til lovforslaget anfører, at det afgørende efter ministeriets opfattelse må være, om de pågældende data er i udbyderens besiddelse på det tidspunkt, hvor pålægget gives, uanset om opbevaringen alene er af midlertidig karakter.

En så vidtgående fortolkning af bestemmelsen har efter TI's opfattelse ikke støtte i den bagvedliggende regel i konventionen om IT-kriminalitet (konventionens artikel 16).

I den forklarende rapport til konventionen forudsættes således, at et pålæg om hastesikring alene kan rettes mod allerede eksisterende data,