

Betænkning afgivet af Retsudvalget den 29. april 2004

Betænkning

over

Forslag til lov om ændring af straffeloven, retsplejeloven, markedsføringsloven og ophavsretsloven (It-kriminalitet m.v.)

[Af justitsministeren (Lene Espersen)]

1. Udvalgsarbejdet

Lovforslaget blev fremsat den 5. november 2003 og var til 1. behandling den 18. november 2003. Lovforslaget blev efter 1. behandling henvist til behandling i Retsudvalget.

Møder

Udvalget har behandlet lovforslaget i 5 møder.

Høring

Et udkast til lovforslaget har inden fremsættelsen været sendt i høring, og justitsministeren sendte den 20. december 2002 dette udkast til udvalget, jf. alm. del – bilag 467, 2002-03. Den 13. november 2003 sendte justitsministeren de indkomne høringssvar samt et notat herom til udvalget.

Teknisk gennemgang

Justitsministeren og embedsmænd fra Justitsministeriet har den 4. december 2003 foretaget en teknisk gennemgang af lovforslaget over for udvalget.

Skriftlige henvendelser

Udvalget har i forbindelse med udvalgsarbejdet modtaget skriftlige henvendelser fra:

Brancheorganisationen ForbrugerElektronik,
DR JURA,
Henning Petersen, København,
ITEK,
Scandinavian TV Organisation against Piracy – STOP,

Telekommunikationsindustrien i Danmark,
TDC Kabel TV og
Unispeed a/s.

Justitsministeren har over for udvalget kommenteret de skriftlige henvendelser til udvalget med undtagelse af 3 henvendelser, som forventes kommenteret inden 2. behandling. En af henvendelserne til udvalget og justitsministerens kommentar hertil er optrykt som bilag til betænkningen.

Deputationer

Endvidere har Telekommunikationsindustrien i Danmark og Unispeed a/s mundtligt over for udvalget redegjort for deres holdning til lovforslaget.

Spørgsmål

Udvalget har stillet 28 spørgsmål til justitsministeren til skriftlig besvarelse, som denne har besvaret med undtagelse af 3, som forventes besvaret inden 2. behandling.

2. Indstillinger og politiske bemærkninger

Et *flertal* i udvalget (udvalget med undtagelse af EL) indstiller lovforslaget til *vedtagelse uændret*.

Et mindretal i udvalget (S, SF og RV) bemærker, at dette mindretal kan støtte forslaget, da det strafferetlige værn hermed fremrykkes ved it-kriminalitet, og der herved opnås øget parallelitet til anden sammenlignelig kriminalitet.

Under udvalgsarbejdet har S, SF og RV hæftet sig ved, at piratdekodere ikke er omfattet sammen med øvrige adgangsmidler under henvisning til, at der ikke er noget grundlag for at vurdere nødvendigheden heraf. S, SF og RV finder, at der logisk bør være overensstemmelse mellem misbrug af adgangsmidler og disses strafferetlige værn. Samtidig er Retsudvalget blevet gjort opmærksom på, at der eksisterer misbrug af ikke uvæsentligt omfang. Derfor er ministeren i spørgsmål 22 blevet bedt om at udarbejde samt kommentere et ændringsforslag, som inkluderer piratdekodere i lovforslaget. I ministerens svar anføres, at dette vil kræve juridiske overvejelser, hvilket S, SF og RV accepterer, hvorfor S, SF og RV undlader at fremsætte et sådant ændringsforslag i klar forventning om, at justitsministeren vil foretage disse juridiske overvejelser og vende tilbage til Folketinget med en løsning af problemstillingen.

Et *mindretal* i udvalget (EL) indstiller lovforslaget til *forkastelse* ved 3. behandling.

Tjóðveldisflokkurin, Inuit Ataqatigiit og Siumut var på tidspunktet for betænkningens afgivelse ikke repræsenteret med medlemmer i udvalget og havde dermed ikke adgang til at komme med indstillinger eller politiske udtalelser i betænkningen.

En oversigt over Folketingets sammensætning er optrykt i betænkningen.

Inge Dahl-Sørensen (V) Birthe Rønn Hornbech (V) nfm. Karsten Nonbo (V) Freddy Dam (V) Per

Dalgaard (DF) Peter Skaarup (DF) Helge Adam Møller (KF) Lars Barfoed (KF) Jann Sjursen (KD)

Frode Sørensen (S) Lissa Mathiasen (S) Morten Bødskov (S) Per Kaalund (S) Sandy Brinck (S)

Anne Baastrup (SF) fmd. Elisabeth Arnold (RV) Line Barfod (EL)

Tjóðveldisflokkurin, Inuit Ataqatigiit og Siumut havde ikke medlemmer i udvalget.

Folketingets sammensætning

Venstre, Danmarks Liberale Parti (V)	55 *	Enhedslisten (EL)	4
Socialdemokratiet (S)	52	Kristendemokraterne (KD)	4
Dansk Folkeparti (DF)	22	Tjóðveldisflokkurin (TF)	1
Det Konservative Folkeparti (KF)	16	Inuit Ataqatigiit (IA)	1
Socialistisk Folkeparti (SF)	12	Siumut (SIU)	1
Det Radikale Venstre (RV)	9	Uden for folketingsgrupperne (UFG)	2

* Heraf 1 medlem valgt på Færøerne

Bilag 1

Oversigt over bilag vedrørende L 55

Bilagsnr.	Titel
1	Høringssvar samt høringsnotat fra justitsministeren
2	Henvendelse af 13/11-03 fra Henning Petersen, København N
3	Spm. 1 om kommentar til henvendelsen af 13/11-03 fra Henning Petersen, København N, til justitsministeren
4	Udkast til tidsplan over udvalgets behandling af lovforslaget
5	Spm. 2 om oversendelse af en samlet oversigt over de i forslaget foreslåede ændringer i strafferammer, til justitsministeren
6	Henvendelse af 26/11-03 fra Telekommunikationsindustrien i Danmark
7	Spm. 3 om kommentar til henvendelse af 26/11-03 fra Telekommunikationsindustrien i Danmark, til justitsministeren
8	Svar på spm. 2 om oversendelse af en samlet oversigt over de i forslaget foreslåede ændringer i strafferammer, fra justitsministeren
9	Tidsplan for udvalgets behandling af lovforslaget
10	Spm. 4 om den foreslåede ændring af markedsføringslovens § 10 (industrispionage), til justitsministeren
	Spm. 5 om anvendelsesområdet for § 293, stk. 2 (beskyttelse af it-systemer mod angreb), til justitsministeren

- 11 Svar på spm. 1 om kommentar til henvendelsen af 13/11-03 fra Henning Petersen, København N, fra justitsministeren
- 12 Svar på spm. 3 om kommentar til henvendelse af 26/11-03 fra Telekommunikationsindustrien i Danmark, fra justitsministeren
- 13 Spm. 6 om status for udmøntning af bemyndigelsen i terrorloven om registrering og opbevaring af oplysninger om teletrafik, til justitsministeren
- 14 Svar på spm. 4 om den foreslåede ændring af markedsføringslovens § 10 (industrispionage), fra justitsministeren
- Svar på spm. 5 om anvendelsesområdet for § 293, stk. 2 (beskyttelse af it-systemer mod angreb), fra justitsministeren
- 15 Spm. 7 om, i hvilket omfang man kan pålægge mindre udbydere, der slet ikke har faciliteter, der kan gemme de pågældende oplysninger, at indføre nye it-systemer, til justitsministeren
- Spm. 8 om, i hvilket omfang man kan pålægge mindre udbydere, der slet ikke har faciliteter, der kan gemme de pågældende oplysninger, at få faciliteterne hos en større udbyder, til justitsministeren
- Spm. 9 om, i hvilket omfang man kan pålægge større udbydere, der skal foretage programændringer for at gennemføre strakssikring, at foretage disse, til justitsministeren
- Spm. 10, om der også er større systemer, der ikke har mulighed for at udvikle muligheden for at foretage strakssikring af flygtige e-mails eller sms'er, til justitsministeren
- Spm. 11, om der vil blive indført minimumsregler, så en meget lille udbyder, f.eks. en rockerforening, ikke kan pålægges strakssikring, til justitsministeren
- Spm. 12 om, hvilke regelsæt der gælder for videregivelse af oplysninger fra små udbydere til store udbydere, til justitsministeren
- 16 Spm. 13 om ministerkommentar til artikel i Computerworld af 16/1-04: »E-mailovervågning gælder ikke webmail«, til justitsministeren
- 17 Svar på spm. 6 om status for udmøntning af bemyndigelsen i terrorloven om registrering og opbevaring af oplysninger om teletrafik, fra justitsministeren

- 18 Spm. 14 om kommentarer til udkast til ændringsforslag vedrørende forslaget om hastesikring, til justitsministeren
Spm. 15 om, hvordan ministeren forholder sig til hovedindholdet af udkastet til ændringsforslag, nemlig at der fastsættes nærmere regler om indholdet af udbydernes forpligtelser, for så vidt angår hastesikring, til justitsministeren
Spm. 16, om ministeren vil være indstillet på med et betækningsbidrag eller på anden tilsvarende vis at præcisere indholdet af den foreslåede bestemmelse om hastesikring, til justitsministeren
- 19 Svar på spm. 11, om der vil blive indført minimumsregler, så en meget lille udbyder, f.eks. en rockerforening, ikke kan pålægges strakssikring, fra justitsministeren
Svar på spm. 13 om ministerkommentar til artikel i Computerworld af 16/1-04: »E-mailovervågning gælder ikke webmail«, fra justitsministeren
- 20 Svar på spm. 7 om, i hvilket omfang man kan pålægge mindre udbydere, der slet ikke har faciliteter, der kan gemme de pågældende oplysninger, at indføre nye it-systemer, fra justitsministeren
Svar på spm. 8 om, i hvilket omfang man kan pålægge mindre udbydere, der slet ikke har faciliteter, der kan gemme de pågældende oplysninger, at få faciliteterne hos en større udbyder, fra justitsministeren
Svar på spm. 9 om, i hvilket omfang man kan pålægge større udbydere, der skal foretage programændringer for at gennemføre strakssikring, at foretage disse, fra justitsministeren
Svar på spm. 10, om der også er større systemer, der ikke har mulighed for at udvikle muligheden for at foretage strakssikring af flygtige e-mails eller sms'er, fra justitsministeren
Svar på spm. 12, om hvilke regelsæt der gælder for videregivelse af oplysninger fra små udbydere til store udbydere, fra justitsministeren
Svar på spm. 14 om kommentarer til udkast til ændringsforslag vedrørende forslaget om hastesikring, fra justitsministeren
Svar på spm. 15 om, hvordan ministeren forholder sig til hovedindholdet af udkastet til ændringsforslag, nemlig at der fastsættes nærmere regler om indholdet af udbydernes forpligtelser, for så vidt angår hastesikring, fra justitsministeren
Svar på spm. 16, om ministeren vil være indstillet på med et betækningsbidrag eller på anden tilsvarende vis at præcisere indholdet af den foreslåede bestemmelse om hastesikring, fra justitsministeren
- 21 1. udkast til betækning
- 22 Henvendelse af 4/2-04 fra Unispeed a/s

- 23 Henvendelse af 6/2-04 fra Unispeed a/s
- 24 Spm. 17 om kommentar til henvendelse af 6/2-04 fra Unispeed a/s, til
justitsministeren
- 25 Meddelelse om eventuel afholdelse af et fællesmøde
- 26 Henvendelse af 19/2-04 fra Unispeed a/s
- 27 Svar på spm. 17 om kommentar til henvendelse af 6/2-04 fra Unispeed
a/s, fra justitsministeren
- 28 Spm. 18 om kommentar til henvendelse af 19/2-04 fra Unispeed a/s,
til justitsministeren
- 29 Svar på spm. 18 om kommentar til henvendelse af 19/2-04 fra
Unispeed a/s, fra justitsministeren
- 30 Henvendelse af 18/3-04 fra Scandinavian TV Organisation against
Piracy – Stop
- 31 Spm. 19 om kommentar til henvendelse af 18/3-04 fra Scandinavian
TV Organisation against Piracy – Stop, til justitsministeren
- 32 Spm. 20, om piratdekodere er omfattet af lovforslaget, til
justitsministeren
- 33 Brev af 12/3-04 fra justitsministeren
- 34 Materiale fra foretræde fra Scandinavian TV Organisation against
Piracy – Stop den 31/3-04
- 35 Spm. 21 om kommentar til materiale modtaget i forbindelse med et
foretræde fra Scandinavian TV Organisation against Piracy – Stop den
31/3-04, til justitsministeren
- Spm. 22, om ministeren vil yde teknisk bistand til et ændringsforslag,
som indebærer, at piratdekodere bliver omfattet af lovforslaget, til
justitsministeren
- 36 Tidsplan for den videre behandling af forslaget
- 37 Spm. 23 om afgrænsningen af udbydere af teletjenester, til
justitsministeren
- 38 Svar på spm. 19 om kommentar til henvendelse af 18/3-04 fra
Scandinavian TV Organisation against Piracy – Stop, fra
justitsministeren
- Svar på spm. 20, om piratdekodere er omfattet af lovforslaget, fra
justitsministeren
- 39 Henvendelse af 2/4-04 fra Brancheorganisationen
ForbrugerElektronik
- 40 Spm. 24 om kommentar til henvendelse af 2/4-04 fra
Brancheorganisationen ForbrugerElektronik, til justitsministeren
- 41 Henvendelse af 15/4-04 fra Scandinavian TV Organisation against
Piracy – Stop
- 42 Spm. 25 om kommentar til henvendelse af 15/4-04 fra Scandinavian
TV Organisation against Piracy – Stop, til justitsministeren
- 43 Bilaget (spm. 26) tilbagetaget

- 44 Svar på spm. 21 om kommentar til materiale modtaget i forbindelse med et foretræde fra Scandinavian TV Organisation against Piracy – Stop den 31/3-04, fra justitsministeren
Svar på spm. 22, om ministeren vil yde teknisk bistand til et ændringsforslag, som indebærer, at piratdekodere bliver omfattet af lovforslaget, fra justitsministeren
Svar på spm. 23 om afgrænsningen af udbydere af teletjenester, fra justitsministeren
Svar på spm. 24 om kommentar til henvendelse af 2/4-04 fra Brancheorganisationen ForbrugerElektronik, fra justitsministeren
- 45 Svar på spm. 25 om kommentar til henvendelse af 15/4-04 fra Scandinavian TV Organisation against Piracy – Stop, fra justitsministeren
- 46 Henvendelse af 26/4-04 fra ITEK
- 47 Spm. 27 om kommentar til henvendelse af 26/4-04 fra ITEK, til justitsministeren
- 48 2. udkast til betænkning
- 49 Henvendelse af 26/4-04 fra TDC Kabel TV
- 50 Spm. 28 om kommentar til henvendelse af 26/4-04 fra TDC Kabel TV, til justitsministeren
- 51 Henvendelse af 27/4-04 fra DR JURA
- 52 Spm. 29 om kommentar til henvendelse af 27/4-04 fra DR JURA, til justitsministeren

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, som opbevares i et computersystem hos den dataansvarlige (se bl.a. rapportens pkt. 152, 159 og 161). Desuden forudsættes det, at bestemmelsen ikke kan forpligte udbyderen til at gemme sådanne flygtige data, som opbevares så kortvarigt, at de ikke med rimelighed

kan forventes sikret i henhold til et pålæg (rapportens pkt. 153). Af sidstnævnte pkt. 153 fremgår det samtidig tydeligt, at bestemmelsen om hastesikring generelt ikke kan forpligte udbyderne til at implementere nye tekniske systemer.

TI skal på baggrund af ovenstående opfordre til, at det præciseres i bemærkningerne til lovforslaget, at bestemmelsen ikke forpligter udbyderne til at sikre muligheden for hastesikring af data, som alene opbevares kortvarigt i udbyderens systemer.

2. Afgrænsning af pålægget om hastesikring

TI noterer sig med tilfredshed, at det i forhold til det oprindelige udkast nu fremgår af selve lovteksten, at politiet skal anføre præcist, hvilke data der skal sikres og i hvilket tidsrum de skal sikres (sikringsperioden). TI forudsætter, at dette skal forstås således, at politiet skal udpege den eller de bestemte kunder, pålægget rettes mod.

TI forudsatte i sit høringssvar, at en anmodning om hastesikring af data fremsættes skriftligt. Dette kommenteres hverken i ministeriets høringsnotat eller i bemærkningerne til lovforslaget.

Efter TI's opfattelse er bør det være en formel betingelse, at et pålæg om hastesikring meddeles skriftligt.

Dels udgør politiets skriftlige anmodning selve det juridiske grundlag for den behandling af data, som hastesikringen i sig selv er udtryk for, dels vil et skriftlighedskrav mindske risikoen for en efterfølgende tvist mellem udbyderen og politiet om, hvad pålægget om hastesikring nøjagtig omfattede. En anden væsentlig begrundelse for at kræve skriftlighed er, at udbyderen efter § 786a, stk. 3 kan straffes for ikke at opfylde et pålæg om hastesikring.

TI skal opfordre til, at der indsættes et krav i lovteksten om at et pålæg om hastesikring skal meddeles skriftligt.

3. Hvor gamle data kan være omfattet af et pålæg om hastesikring?

Det fremgår af bemærkningerne til lovforslaget, at et pålæg om hastesikring af data kan omfatte alle elektroniske data i udbyderens besiddelse, uanset hvor gamle disse data måtte være.

I forhold til det oprindelige lovudkast er det nu tilføjet i lovteksten, at politiet er forpligtet til at afgrænse pålægget til alene at omfatte de data, der er nødvendige for den konkrete efterforskning (proportionalitetskrav). Tidligere fremgik kravet alene af bemærkningerne.

Proportionalitetskravet er ikke et entydigt krav og udbyderne har ingen mulighed for at kontrollere, om politiet i en konkret sag har overholdt kravet. TI's frygt for, at politiet vil rette pålægget mod alle tilgængelige data i udbyderens systemer består for så vidt fortsat. Det skal i den forbindelse dog bemærkes, at udbyderne efter lovforslaget kan kræve betaling for at gennemføre et pålæg om hastesikring, hvilket må ventes at ville begrænse denne tendens.

Som anført i TI's høringssvar er konsekvensen af, at der ikke gælder nogen øvre grænse for hvor gamle data, som skal kunne sikres, at udbyderne vil være forpligtede til at ændre deres systemer, så det bliver muligt at sikre/opbevare alle data, som findes i udbydernes systemer i ekstra 90 dage.

Som eksempel kan nævnes trafikdata, som normalt opbevares i 5 år. Med den nuværende formulering af bestemmelsen skal udbydere være i stand til at gemme trafikdata i 5 år og 90 dage.

Justitsministeriet oplyser i høringsnotatet s. 15, at det netop er formålet med bestemmelsen at give mulighed for at sikre bevaringen af relevante data, som ellers stod for at skulle slettes. Ministeriet forholder sig ikke direkte til TI's forslag om indsættelse af en øvre grænse for hvor gamle data, som skal kunne hastesikres.

TI er enig med Justitsministeriet i, at det netop er formålet med bestemmelsen at sikre bevarelsen af data, der netop stod for at skulle slettes. TI finder imidlertid, at det vil være uforholdsmæssigt omkostningsfuldt og helt unødvendigt, hvis udbydere skal forpligtes til at investere i software/systemer, der sætter dem i stand til at sikre/gemme data i alle systemer i ekstra 90 dage, uanset alder. Det er TI's erfaring, at politiet i praksis meget sjældent har behov for data, der er flere år gamle.

TI henviser i den forbindelse til, at hastesikring efter ordlyden af konventionens artikel 16, stk. 1 fortrinsvis tænkes anvendt i tilfælde, hvor der er grund til at antage, at dataene er særligt udsat for at gå tabt eller blive ændret. I pkt. 161 i den forklarende rapport til konventionen nævnes som eksempel situationer, hvor dataene gemmes i en meget kort periode, f.eks. som følge af en firmapolitik eller fordi det medie, hvorpå dataene opbevares løbende overskrives med nye data.

Efter TI's opfattelse taler meget således for, at udbydere ikke forpligtes til at være i stand til at sikre (opbevare) data af en vis alder i yderligere 90 dage. Som minimum bør det sikres, at data aldrig vil skulle opbevares i mere end 5 år og at udbydere dermed ikke forpligtes til at indføre systemer, der understøtter et sådant krav.

4. Videregivelse af trafikdata om andre udbydere

Forpligtelsen til at videregive trafikdata om andre udbydere, hvis net/tjenester har været anvendt i forbindelse med den elektroniske kommunikation, som er omfattet af hastesikring, er uændret i forhold til lovudkastet.

Trods TI's opfordring hertil er der hverken i lovforslaget eller i de tilhørende bemærkninger givet nogen form for anvisning på, hvordan udbydere i praksis skal sørge for videregivelse af trafikdata om andre udbydere. Det står således fortsat åbent, om den udbyder pålægget retter sig mod, er forpligtet til at gennemgå alle de data, der skal sikres i medfør af pålægget. Som det fremgår af pkt. 3 kan et pålæg omfatte store mængder data.

TI henviser i den forbindelse til, at det fremgår af pkt. 169 i den forklarende rapport, at den kompetente myndighed (dvs. politiet) nærmere skal angive den type trafikdata, der skal videregives af udbyderen. Dette ses ikke være afspejlet i det danske lovforslag.

TI savner således fortsat en anvisning på, hvorledes denne del af bestemmelsen i praksis skal efterleves. Det er i den forbindelse væsentligt, at overtrædelse af bestemmelsen straffes med bøde.

TI skal opfordre til, at det i bemærkningerne til lovforslaget anføres, hvorledes videregivelse af trafikdata vedrørende andre udbydere, i praksis skal finde sted.

5. Implementeringsperiode

TI kan konstatere, at bestemmelsen efter forslaget skal træde i kraft dagen efter offentliggørelsen i Lovtidende.

Den nuværende udformning af lovforslaget indebærer som nævnt bl.a. et krav om at udbydernes systemer skal understøtte muligheden for sikring/opbevaring i yderligere 90 dage af alle former for data, som aktuelt opbevares hos udbyderen. Situationen vil typisk være den, at der foretages løbende automatisk sletning af alle data over en vis alder, og at et pålæg om hastesikring af data reelt indebærer krav om beskyttelse mod den rutinemæssige sletning.

Efter TI's opfattelse er der behov for, at loven først træder i kraft efter en vis passende implementeringsperiode, så udbyderne får mulighed for at gennemføre de nødvendige ændringer i systemer og administrative procedurer forud for ikrafttrædelsen.

Justitsministeren kommentarer af 22. december 2003 til henvendelsen fra Telekommunikations-industrien

Spørgsmål nr. 3:

Ministeren bedes kommentere henvendelsen modtaget den 26. november 2003 fra Telekommunikationsindustrien, jf. L 55 – bilag 6.

Svar:

I sin henvendelse til Retsudvalget anfører Telekommunikationsindustrien (herefter »TI«), at lovforslaget – uanset de ændringer, som er foretaget i forhold til det lovudkast, der har været i høring – efter TI's opfattelse vil give anledning til problemer for telebranchen.

De synspunkter, TI fremkommer med i henvendelsen, omhandler lovforslagets § 2, nr. 2. Med denne bestemmelse foreslås indsat en ny § 786 a i retsplejeloven, hvorefter politiet som led i en efterforskning, hvor elektronisk bevismateriale kan være af betydning, kan pålægge udbydere af telenet eller teletjenester at foretage såkaldt hastesikring af elektroniske data.

Bestemmelsen har til formål at hindre, at elektroniske data, der kan have betydning for efterforskningen, slettes som led i den normale drift hos teleudbydere mv. Bestemmelsen omhandler derimod ikke spørgsmålet om, hvorvidt de pågældende data kan udleveres til politiet til brug i forbindelse med efterforskningen. Dette vil fortsat skulle afgøres efter retsplejelovens kapitel om indgreb i meddelelshemmeligheden, og der ændres ikke herpå med lovforslaget.

1. TI finder det for det første problematisk, at et pålæg om hastesikring efter lovforslaget kan omfatte alle typer data, som er i teleudbyderens besiddelse på det tidspunkt, hvor pålægget meddeles. TI har i den forbindelse anført, at eksempelvis indholdet af SMS- eller MMS-beskeder kun opbevares i udbyderens systemer ganske kortvarigt, indtil den pågældende besked er afleveret på modtagerens mobiltelefon. TI fremfører samme synspunkter for så vidt angår e-mails, der kun opbevares på udbyderens server, indtil kunden vælger at slette dem. For e-mails vil der dog typisk være tale om opbevaring i en længere periode, end tilfældet er ved SMS- og MMS-beskeder.

På den baggrund finder TI, at det i lovforslaget bør præciseres, at bestemmelsen ikke forpligter

udbyderne til at kunne foretage hastesikring af data, der alene opbevares i udbyderens systemer i en kortvarig periode.

Justitsministeriet har til brug for besvarelsen vedrørende de dele af TI's bemærkninger, der er af mere teknisk karakter, indhentet en udtalelse fra Rigspolicehøveden, Politiets Efterretningstjeneste (PET).

I relation til spørgsmålet om, hvilke typer data der kan omfattes af et pålæg om hastesikring, har Rigspolicehøveden i sin udtalelse anført følgende:

»I den anledning skal PET bemærke, at PET ikke har konkret viden om, i hvor lang tid en SMS/MMS opbevares i de forskellige udbyderes net. Dette vil formentlig variere fra udbyder til udbyder, herunder kan det have betydning om SMS/MMS beskeden afsendes fra en mobiltelefon eller via internettet.

Det skal endvidere bemærkes, at SMS og MMS beskeder alene vil opbevares i få sekunder i udbyderens system, hvis modtageren er koblet til mobiltelefonnettet. Hvis modtagerens mobiltelefon ikke er koblet til mobiltelefonnettet, vil SMS/MMS beskeder typisk blive opbevaret i udbyderens system til de kan leveres, dvs. til modtageren kobles til mobiltelefonnettet.

Den periode som udbyderen opbevarer en SMS/MMS i med henblik på levering til en modtager, vil formentlig variere fra udbyder til udbyder.

For så vidt angår e-mails bemærkes, at det i høj grad er kunden, der bestemmer, hvornår en e-mail ikke længere skal opbevares hos udbyderen. En e-mail opbevares hos udbyderen i en periode indtil kunden henter sine e-mails. Det forhold, at en kunde har hentet sine e-mails, er imidlertid ikke ensbetydende med, at e-mailen ikke længere opbevares hos udbyderen. Dette vil bero på de enkelte udbyderes tekniske opsætning. En række udbydere giver eksempelvis mulighed for, at man kan hente sine e-mails fra forskellige computere, men at e-mailen først slettes hos udbyderen, når e-mailen hentes til en bestemt computer.

Man kan derfor ikke efter PET's opfattelse lægge til grund, at SMS/MMS beskeder generelt opbevares i meget kort tid hos udbyderne, ligesom man ikke kan lægge til grund, at e-mails opbevares i meget kort tid hos udbyderne.«

Justitsministeriet kan henholdes sig til det, Rigspolicehøveden har anført.

Justitsministeriet skal endvidere henvise til lovforslagets almindelige bemærkninger, pkt. 7.3, hvoraf det fremgår, at det er Justitsministeriets opfattelse, at både formålet med Cybercrime-konventionens bestemmelse om hastesikring, som den foreslåede § 786 a i retsplejeloven skal gennemføre, samt bemærkningerne i den forklarende rapport, der er knyttet til konventionen, taler for, at det afgørende i relation til, hvilke data der kan være genstand for et pålæg om hastesikring, er, om dataene er i udbyderens besiddelse på tidspunktet, hvor pålægget meddeles udbyderen. Efter den forklarende rapport er der således ikke tvivl om, at det er hensigten, at eksempelvis indholdet af e-mails skal kunne hastesikres, uanset at udbydernes besiddelse af sådanne data i praksis er af mere midlertidig karakter.

Justitsministeriet finder derfor ikke, at lovforslaget bør ændres som foreslået af TI.

Udbydere af telenet eller teletjenester er efter lovforslaget alene forpligtet til at sikre de oplysninger, der er i udbyderens besiddelse på det tidspunkt, hvor pålægget gives. Bestemmelsen indebærer således, at udbyderen straks efter pålæggets modtagelse skal "fiksere" de oplysninger, der måtte være til stede

på det pågældende tidspunkt.

Det afgørende for, om dataene skal hastesikres, er ikke, hvor længe dataene faktisk opbevares, men derimod om dataene rent faktisk er i udbyderens besiddelse i det øjeblik, hvor hastesikringen gennemføres.

En udbyder, der har gennemført et hastesikringspålæg i overensstemmelse med pålæg herom, har således iagttaget sine forpligtelser i henhold til den foreslåede § 786 a, stk. 1, i retsplejeloven, selv om det skulle forekomme, at udbyderen umiddelbart før sikringens faktiske gennemførelse havde yderligere SMS- eller MMS-beskeder opbevaret på sit system, men hvor disse når frem til modtageren, inden pålægget effektueres, og dermed forsvinder fra udbyderens besiddelse.

2. TI har i sin henvendelse endvidere anført, at det bør være en formel betingelse, at et pålæg om hastesikring meddeles skriftligt. TI har i den forbindelse anført, at et skriftlighedskrav vil mindske risikoen for efterfølgende uenighed om det nærmere indhold af pålægget, og at der bør stilles krav om skriftlighed, idet udbyderen efter § 786 a, stk. 4, kan straffes for ikke at opfylde et hastesikringspålæg.

Justitsministeriet er enig i, at risikoen for, at der opstår tvivl om indholdet af et pålæg om hastesikring, mindskes, når pålægges meddeles skriftligt. Politiet vil således have en naturlig interesse i at meddele pålæg om hastesikring ved en skriftlig henvendelse til den pågældende teleudbyder.

Som anført af TI, følger det af den foreslåede § 786 a, stk. 4, at en teleudbyders tilsidesættelse af sine forpligtelser i henhold til et pålæg om hastesikring kan straffes med bøde. Straf kommer imidlertid kun på tale, hvis anklagemyndigheden kan løfte bevisbyrden for, at den pågældende teleudbyder ikke har iagttaget et meddelt pålæg om hastesikring. Denne bevisbyrde vil efter omstændighederne kunne være vanskelig at løfte, hvis der ikke foreligger et skriftligt pålæg, der kan danne grundlag for en vurdering af, om teleudbyderen har begået en strafbar handling.

Rigspolitichefen har i den udtalelse, Justitsministeriet har indhentet til brug for besvarelsen, anført følgende herom:

»I den anledning skal PET bemærke, at et pålæg om hastesikring som udgangspunkt må forventes at blive meddelt skriftligt.

Der vil imidlertid være en række situationer, hvor det kan være nødvendigt at meddele pålægget mundtligt. Dette vil eksempelvis være tilfældet i de situationer, hvor behovet for at meddele pålægget opstår på et tidspunkt, hvor man ikke har adgang til politiets edb-systemer, eksempelvis i forbindelse med en ransagning hos en mistænkt, eller hvor man ved at afvente udarbejdelsen af det skriftlige pålæg risikerer at øjemedet forspildes.

Man skal endvidere være opmærksom på, at et krav om skriftlighed forudsætter, at alle udbydere uanset størrelse til en hver tid på døgnet er i stand til at modtage et skriftligt pålæg fra politiet. Dette er ikke tilfældet i dag.«

Justitsministeriet finder på den baggrund ikke anledning til at foreslå, at der indsættes et skriftlighedskrav som en formel betingelse for gyldigheden af et pålæg om hastesikring. Justitsministeriet finder det imidlertid naturligt, at politiet i de tilfælde, hvor pålæg om hastesikring er meddelt mundtligt, efterfølgende over for teleudbyderen skriftligt bekræfter indholdet af det meddelte

pålæg om hastesikring.

3. I henvendelsen til Retsudvalget har TI endvidere peget på, at der bør fastsættes en tidsmæssig grænse, således at data, der er mere end eksempelvis 5 år gamle, ikke kan omfattes af et pålæg om hastesikring. TI har henvist til, at udbyderen ikke har mulighed for at kontrollere, om politiet overholder det krav om proportionalitet, der er fremhævet i den foreslåede § 786 a, stk. 2. TI frygter således, at politiet vil rette et pålæg mod alle tilgængelige data med den konsekvens, at udbyderne vil skulle ændre deres systemer.

Justitsministeriet skal indledningsvis understrege, at det ikke indgår som en del af den foreslåede bestemmelse om hastesikring, at den enkelte udbyder skal foretage kontrol af, om politiet i den konkrete sag har afgrænset pålægget til alene at vedrøre de oplysninger, der er relevante for den pågældende efterforskning.

Politiet skal efter den foreslåede § 786 a, stk. 2, afgrænse et pålæg til alene at omfatte de data, der skønnes nødvendige for efterforskningen. Sikringsperioden skal endvidere være så kort som mulig og kan ikke overstige 90 dage. Politiet skal efter forslaget afholde de omkostninger, der er forbundet med udbyderens gennemførelse af et pålæg om hastesikring, og politiet vil ikke have nogen interesse i, som anført af TI, at gøre pålægget generelt, medmindre det konkret er nødvendigt.

Spørgsmålet om, hvilke data der er af betydning for politiets efterforskning, har ikke nødvendigvis sammenhæng med dataenes alder. "Gamle" data kan efter omstændighederne være lige så relevante for politiets efterforskning som nyere data. En bestemmelse, hvorefter data ikke kan være genstand for pålæg om hastesikring, alene fordi de pågældende data har en vis alder, stemmer således ikke overens med bestemmelsens formål om at sikre den fortsatte eksistens af data, der kan være af betydning for politiets efterforskning.

TI anfører, at det vil være bekesteligt, hvis udbyderne skal kunne gemme data i 5 år og 90 dage.

Justitsministeriet skal i den forbindelse fremhæve, at hastesikringen som nævnt kun kan omfatte data, der i forvejen opbevares af udbyderen. Med hastesikringen er der således alene tale om, at udbyderen vil skulle opretholde sin eksisterende opbevaring af de pågældende data i en periode, der højst kan udgøre 90 dage.

En situation som den TI omtaler, vil alene kunne forekomme, hvis politiet har fundet det nødvendigt at udstrække et hastesikringspålæg længst muligt (90 dage), og hvis pålægget samtidig omfatter data, der i forvejen har været gemt i 5 år hos udbyderen.

Det skal hertil bemærkes, at hastesikring ikke kun kan ske ved at gemme dataene i systemet, men også kan gennemføres ved at kopiere de pågældende data. Det afgørende er, at dataene ikke slettes eller ændres.

4. TI har videre anført, at der ikke i lovforslaget eller dets bemærkninger er givet anvisninger på, hvorledes udbyderne i praksis skal foretage den foreslåede videregivelse af trafikdata om andre udbydere til politiet.

TI's bemærkninger vedrører den foreslåede § 786 a, stk. 3, i retsplejeloven, hvorefter det påhviler udbydere af telenet eller teletjenester som led i hastesikring uden ugrundet ophold at videregive

trafikdata om andre telenet- eller teletjenesteudbydere, hvis net eller tjenester har været anvendt i forbindelse med den elektroniske kommunikation, som kan være af betydning for efterforskningen.

Som det fremgår af lovforslagets almindelige bemærkninger, pkt. 7.3., er formålet med denne bestemmelse at give politiet mulighed for at identificere og pålægge hver enkelt udbyder af telenet eller teletjenester at sikre trafikdata i tilfælde, hvor der anvendes flere udbydere. De oplysninger, som udbydere af telenet eller teletjenester efter forslaget skal videregive til politiet, er alene oplysninger om de såkaldte elektroniske stier, som føres fra den pågældende udbyder til en eller flere andre udbydere. Herved sikres, at politiet så hurtigt som muligt kan identificere samtlige udbydere, der har været involveret i den kommunikation, som efterforskningen angår, hvorved det undgås, at et elektronisk spor ender blindt hos en udbyder.

Rigspolitichefen har om dette spørgsmål anført følgende i sin udtalelse til Justitsministeriet:

»Det bemærkes hertil, at forslaget til retsplejelovens § 786 a, stk. 3, naturligt må forstås således, at det påhviler udbyderne at gennemgå alle data omfattet af hastesikringen med henblik på at identificere andre udbydere. Oplysningerne bør videregives til politiet i et elektronisk læsbart format.«

Justitsministeriet kan henholde sig til det, Rigspolitichefen har anført.

5. Endelig har TI i sin henvendelse bemærket, at lovforslaget kræver ændringer af teleudbydernes systemer og administrative procedurer, og at der derfor er behov for en vis implementeringsperiode forud for lovens ikrafttræden. TI har ikke nærmere anført, hvilke ændringer der er tale om.

Efter lovforslagets § 5 skal loven træde i kraft dagen efter bekendtgørelsen i Lovtidende.

Justitsministeriet finder ikke, at de bemærkninger, der er fremkommet i TI's henvendelse, giver anledning til at fravige den foreslåede ikrafttrædelsesdato. Begrundelsen herfor er, at et hastesikringspålæg efter sin karakter ligner de indgreb, der i medfør af retsplejelovens § 780 kan foretages i meddelelshemmeligheden, bortset fra at politiet ikke i medfør af et hastesikringspålæg kan få oplysningerne udleveret fra udbyderne. Ved indgreb i meddelelshemmeligheden skal udbyderne på politiets anmodning både kunne iværksætte en aflytning af telekommunikation samt give historiske (bagudrettede) oplysninger om telekommunikation. Ved hastesikring skal udbyderne på politiets anmodning sikre de oplysninger om f.eks. en konkret persons telekommunikation, som er i deres besiddelse, mod at blive slettet eller ændret. Der er i begge tilfælde tale om en konkret, afgrænset forpligtelse. Der er således ikke som ved logning i medfør af retsplejelovens § 786, stk. 4, tale om en løbende forpligtelse for udbyderne til at registrere og opbevare oplysninger om telekommunikation.

Det bemærkes i øvrigt, at Danmark først vil kunne ratificere konventionen om Cybercrime, når bestemmelsen om hastesikring er trådt i kraft.