der, og myndigheden i dette land, der skal påtale ulovlige forhold.«

Som det ses af ovenstående, har den eksisterende lovgivning således til formål at sikre forbrugeren klar besked, når spy- eller adware programmer downloades. Når en forbrugerudsendelse alligevel kan give et eksempel, hvor forbrugeren ikke har oplevet den fornødne klarhed, som ellers kræves i medfør af markedsføringslovens regler, kan det typisk hænge sammen med, at en dansk forbruger downloader et spywareprogram fra et andet land, hvorfor der således kan gælde et andet regelsæt end det danske. Dansk lovgivning kan ikke tilsidesætte andre staters lovgivning på området.

Derfor ser jeg ikke umiddelbart yderligere lovgivning som en metode, der i første omgang kan sikre borgerne bedre mod spyware og adware.

Videnskabsministeriet har i stedet iværksat en række oplysningstiltag for forbrugeren i forbindelse med spyware og adware. Således har IT- og Telestyrelsen udarbejdet en vejledning »Spyware – hvad er det? Og hvordan undgår jeg det?« som kan læses på borgerportalen *www.itborger.dk* sammen med en række gode råd og vejledning om it-sikkerhed generelt. Datatilsynet har også på sin web-side *(www.datatilsynet.dk)* offentliggjort information om, hvilke sikkerhedsforanstaltninger de dataansvarlige som minimum bør træffe for at leve op til persondatalovens krav også i forhold til spyware.

Vedrørende spørgsmålet om it-sikkerhed i det offentlige skal jeg gøre opmærksom på, at spy- og adware er rettet mod den enkelte bruger af en computer, og at det derfor er den enkelte medarbejder i det offentlige, der er »målet« og ikke de data, som behandles af den offentlige forvaltning.

Såfremt der er tale om angreb, som retter sig mod de data, som det offentlige behandler, er der ikke længere tale om spy- og adware men om egentlige forsøg på »hacking«, som er en overtrædelse af straffeloven.

Alle offentlige institutioner har selv ansvaret for, at data er tilstrækkeligt sikrede, og at it-sikkerheden er tilfredsstillende. Dette gælder for statens institutioner, for kommunerne og for amterne.

For at styrke den generelle it-sikkerhed i staten og opnå en større grad af ensartethed i it-sikkerhedstiltagene har regeringens økonomiudvalg den 12. januar 2004 tiltrådt, at det gøres obligatorisk for statens institutioner over en 3-årig periode at følge en fælles standard for it-sikkerhedsprocesser. Videnskabsministeriet er – i tæt samspil med ministerområderne – ved at udvikle et hjælpeprogram, der kan støtte de enkelte statslige institutioner med implementeringen af den fælles standard for it-sikkerhedsprocesser.

Til at følge implementeringen af den fælles standard for it-sikkerhedsprocesser har Statens it-råd nedsat en arbejdsgruppe med deltagelse af alle ministerier samt myndigheder, der har et særskilt ansvar for it-sikkerhed. Arbejdsgruppen har fået til opgave at sikre øget videndeling og koordinering bredt i staten, herunder bidrage til, at der skabes en fælles forståelse for og præcisering af almindelig god praksis for håndtering af it-sikkerhedsproblemstillinger.

KL, Amtsrådsforeningen, Rigsrevisionen samt Datatilsynet deltager som observatører i arbejdsgruppen.

Spm. nr. S 2950

Til skatteministeren (22/3 04) af:
Pernille Rosenkrantz-Theil (EL):
»Vil ministeren redegøre for, hvilke initiativer regeringen har taget i diverse internationale organisationer, herunder OECD, i forhold til at imødegå problemerne ved »double dip«?«

Svar (29/3 04)

Skatteministeren (Svend Erik Hovmand):
Som oplyst i svaret af 19. februar 2004 på spørgsmål 1933 har Danmark tidligere foreslået OECD at undersøge tilfælde med dobbelte fradrag som følge af forskellige kvalificering af begreber.

Som oplyst i samme svar vil Danmark igen foreslå en undersøgelse af mismatch som følge af forskellige kvalificering af begreber, når OECD-landene næste gang skal indsende forslag til emner til behandling i OECD's arbejdsgrupper om skat.
