

## Talepapir: Møde i Retsudvalget 26. august kl. 13.00-14.30

### Rådet for Digital Sikkerhed

Formand Birgitte Kofod Olsen

1. Det fælles initiativ fra Retsudvalget og Kulturudvalget er afgørende vigtigt for alle dele af det danske samfund. Vi er midt i en digital transformation, der er så dyb, at den ikke bare skaber en ny kultur, den ændrer også grundlæggende på vores opfattelse af retssikkerhed og demokrati. Vi er derfor nødt til at sætte fokus på digital tryghed.
2. I det globale perspektiv er de to udvalgs indsats ligeså vigtig. Danmark er helt i front med digitalisering – vi danner skole, og påtager os dermed også et ansvar. Og derfor er det så vigtigt, at vi viser, hvordan en digital kultur kan forankres i grundrettigheder og demokratiske principper. Hvis fx CPR-nummeret i dag skaber fuldstændig transparens for staten om borgernes forhold, så må vi spørge os selv, om vi ville synes, det var i orden, hvis det samme system blev anvendt i et land med et skrøbeligt demokrati.
3. Digital tryghed er ikke blot vigtigt for den enkelte borger og forbruger, men fremmer også aktiviteter, der bidrager til udvikling af Danmarks økonomi og indeholder potentiale til vækst, fx gennem effektiv udnyttelse af big data i danske virksomheder og myndigheder.
4. Vi kan opnå digital tryghed med et skarpt fokus på både it-sikkerhed og privatlivsbeskyttelse. Det er vigtigt at disse to komponenter går hånd i hånd og ses som integrerede frem for hinandens modsætninger. Med en sådan helhedsorienteret tilgang giver det god mening at tale om informationssikkerhed. Og med beretningen og den parlamentariske arbejdsgruppe er der skabt mulighed for at sætte informationssikkerhed på dagsordenen på en ny måde.
5. Mere konkret er Beretningen fra den 3. juni et vigtigt skridt i forhold til at få koordineret den strategiske, teknologiske og organisatoriske indsats, der skal til for at skabe digital tryghed i Danmark.
6. Strategi. Beretningen viser med tydelighed, at der er behov for en overordnet strategi for informationssikkerhed i DK. Med de emner, der er identificeret i beretningen, kunne et sådan mål om *digital tryghed* være en fin samlende vision for en fremadrettet indsats.

Et mål om digital tryghed afføder i hvert fald to spørgsmål, der må besvares indenfor en strategisk ramme:

*Hvad skal beskyttelsesniveauet være?*

Der er behov for et fælles sikkerhedskoncept, der kan sætte rammen og standarden for informationssikkerhed i både myndigheder og virksomheder. Det bør gøres på en måde, der kan tilpasse sikkerheden til det individuelle behov og den faktiske risiko.

*Hvordan opnår vi det?*

Det er Rådet for Digital Sikkerheds opfattelse, at vi med EU-forordningen vil vi få en retlig regulering, der samtænker den retlige beskyttelse af borgeren og hans eller hendes data, med de teknologiske muligheder, der kan omsætte den retlige beskyttelse til praksis i dagligdagen.

Forordningen stiller også krav om at integrere privacy i udvikling af it-løsninger og styrker dermed udbredelse af teknologier til at fremme informationssikkerhed.

Vi har i Danmark mange brancheorganisationer og interesseorganisationer med stor kompetence og praktisk erfaring inden for informationssikkerhed. De kan med fordel bidrage til udviklingen af anbefalinger til, hvordan it-sikkerheden højnes i de specifikke brancher, og hvordan de nye privacy fremmende teknologier integreres i deres udviklingsarbejde og daglige drift.

Derudover er der behov for instanser, der er proaktive i forhold til at rådgive om niveauet for informationssikkerhed, til at oplyse om god og sund digital adfærd hos borgere, virksomheder og myndigheder, og til at komme med anbefalinger om udforskning og udnyttelse af det potentiale, der ligger i de mange data, myndigheder og virksomheder ligger inde med, på en måde, der fremmer informationssikkerheden.

Endelig er der behov for et effektivt tilsyn med, at sikkerhedsniveauet er passende i den konkrete kontekst, og at internationale standarder for privatlivsbeskyttelse er overholdt.

7. Teknologier. Der findes allerede koncepter og systemer til at fremme privatlivsbeskyttelse i it-løsninger og projekter (bl.a. i Canada, UK og Tyskland), men vi mangler krav og anvendelse af dem i Danmark og anbefalinger til, hvordan det gøres bedst:

*Privacy Impact Assessment* - et dansk koncept er udviklet i digitaliseringsstyrelsen, men er i dag ikke obligatorisk. Det kan med fordel knyttes til ISO 27001 og den offentlige skabelon for projektstyring.

*Privacy by design* - er udviklet og kan implementeres gennem fx offentlige it-udbud som et krav til leverandører af offentlig it- og digitaliseringsløsninger

*Privacy by default* – er udviklet og langsomt under udbredelse. Det kan stilles som krav i designprincipper, brancheanbefalinger kravsspecifikationer mv.

8. Organisation. Organiseringen af de aktører, der skal bidrage til at sikre digital tryghed, er vigtig for borgernes og virksomhedernes tillid og for aktørernes troværdighed. Det opnår vi kun, hvis alle aspekter af det digital liv bliver håndteret af relevante, kompetente og effektive aktører. Billedet i dag ser sådan ud:

FE er vores nationale it-sikkerhedsmyndighed (indført med FE-loven – som en konsekvens af ressort-omlægningen i 2011). En del opgaver med at skabe sikkerhed i det civile rum er med det greb henlagt til en lukke tjeneste, der pga. af militære og sikkerhedsmæssige hensyn ikke er underlagt sædvanlige krav til retssikkerhed og transparens.

Center for Cybersikkerhed spiller en vigtig rolle i forhold til risikovurdering og overvågning af sikkerhedshændelser hos tilknyttede virksomheder og offentlig myndigheder. Rådet for Digital Sikkerhed har tidligere peget på, at netop den opgave gør, at placeringen af centeret i FE er problematisk.

Politiets Center for Cybercrime er nyetableret og skal efterforske it-kriminalitet. Et behov der er stort og stigende, og derfor vil kræve flere ressourcer i fremtiden.

Også Forbrugerombudsmanden er en vigtig aktør i forhold til at sikre, at kommerciel udnyttelse af persondata foregår i overensstemmelse med god markedsføringsskik.

Datatilsynet råder i dag hverken over de fornødne ressourcer, kompetencer eller det mandat, der er nødvendigt i dag for at koble juraen med teknisk indsigt og pålægge effektive sanktioner.

FE og PET tilsynet råder over juridisk og teknisk ekspertise, men er etableret i en retlig konstruktion, hvor almindelige regler for transparens og retssikkerhed ikke gælder.

Der er i dag ingen officiel aktør, der er ansvarlig for at holde borgere og virksomheder godt oplyst om god og sikker digital adfærd. I den analoge verden har vi en lang tradition for at forebygge og oplyse om skader og andre negative effekter af vores adfærd. Fx trafikikkerhed, seksuel sundhed, sikkerhed i vandet, tand- og anden hygiejne. Tidligere fungerede Teknologirådet som rådgiver for Folketinget i spørgsmål om anvendelse af ny teknologi.

I Rådet for Digital Sikkerhed forsøger vi at bidrage til den faglige og offentlige debat om sund digital adfærd for såvel borgere,

virksomheder og myndigheder og altså fra et perspektiv, der favner samfundets interesser bredt. Vi har vist, at det er muligt - på tværs af virksomheder, organisationer, forskere og myndigheder – at skabe en videns- og erfaringsplatform for en sådan indsats. Men vi har brug for midler for at kunne videreudvikle den faglige, oplysende og rådgivende indsats, der er nødvendig for at bidrage til digital tryghed.

9. Digitaliseringen er allerede sat i gang med motorvejshastighed. Men en sund digital kultur, der opfylder demokratiets principper for retssikkerhed og tilsyn, er ikke udviklet i samme tempo.

Vi står derfor som samfund over for en stor og vigtig udfordring – den har I taget fat på i Retsudvalget og Kulturudvalget. Rådet for Digital Sikkerhed vil meget gerne bidrage til dette vigtige arbejde med at sikre digital tryghed i Danmark.