JUSTITSMINISTERIET

Folketinget
Udvalget for Digitalisering og It
Christiansborg
1218 København K
DK Danmark

Dato: 6. oktober 2025
Kontor: Kontoret for EU-koordination og eksterne forhold
Sagsbeh: Ida Helene Bendtsen Høiberg
Sagsnr.: 2025-11182
Dok.: 3852673

Besvarelse af spørgsmål nr. 166 (Alm. del) fra Folketingets udvalg for Digitalisering og It

Hermed sendes besvarelse af spørgsmål nr. 166 (Alm. del), som Folketingets udvalg for Digitalisering og It har stillet til justitsministeren den 24. september 2025. Spørgsmålet er stillet efter ønske fra Dina Raabjerg (KF).

Peter Hummelgaard

/

Louise Black Mogensen

Slotsholmsgade 10
1216 København K.

T +45 7226 8400

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 166 (Alm. del) fra Folketingets udvalg for Digitalisering og It:

> ”Vil ministeren - i forlængelse af svaret på DIU alm. del – spørgsmål 160 - svare på, hvordan scanningen kan vurderes målrettet, når alle enheder pålægges at scanne indhold? Og hvordan vil man beskytte systemet mod misbrug fra hackere, når tekniske bagdøre først er bygget?”

Svar:

Forslaget til forordning om regler til forebyggelse og bekæmpelse af seksuelt misbrug af børn (CSA-forordningen), herunder det kompromisforslag det danske EU-formandskab har fremlagt, er fortsat genstand for forhandlinger i Rådet og kan derfor ændre sig.

Det danske kompromisforslag lægger op til, at opsporingspåbud kan udstedes som en sidste udvej, når der er dokumentation for, at der er en betydelig risiko for, at tjenesten anvendes med henblik på seksuelt misbrug af børn online, og når årsagerne til udstedelsen af opsporingspåbuddet opvejer de negative konsekvenser for alle berørte parters rettigheder og legitime interesser.

Opsporingspåbuddet skal være målrettet og indeholde en præcisering af påbuddet til, hvad der er strengt nødvendigt. Det indebærer eksempelvis, at opsporing om muligt skal begrænses til kun at finde sted på en identificerbar del eller komponent af en tjeneste, at der indføres effektive og forholdsmæssige garantier, og at anvendelsesperioden begrænses til, hvad der er strengt nødvendigt. Opsporingspåbuddet skal endvidere, i det omfang det er muligt, afgrænses til eksempelvis specifikke brugere, specifikke typer af brugere – f.eks. anonyme brugere – eller specifikke grupper på tjenesten.

Det følger desuden af det danske kompromisforslag, at opsporingspåbud alene kan udstedes til såkaldte højrisikotjenester eller højrisikodele af en tjeneste. Kategoriseringen af en tjeneste sker på baggrund af en vurdering af en række risikofaktorer, som fremgår af kompromisforslagets bilag XIV.

Det er forudsat i kompromisforslaget, at de teknologier, der anvendes til opsporing, ikke må underminere cybersikkerheden, herunder kryptering, eller den fortrolige kommunikation mellem brugere. I kompromisforslaget er opsporing på tjenester, der anvender end-to-end-kryptering konkret betinget af

brugerens forudgående samtykke. Der lægges således op til, at man som bruger vil kunne sige nej til scanning efter overgrebsmateriale og alene anvende kommunikationstjenesten til tekst- og lydbaseret kommunikation. I praksis vil tjenesteudbydere med end-to-end-krypterede tjenester kunne gennemføre opsporingen med såkaldt client-side-scanning, som fungerer ved, at visuelt materiale og links scannes forud for afsendelse.

Når tjenesteudbydere anvender teknologier til opsporing forpligtes de i medfør af forslaget til at identificere, analysere og vurdere mulige cybersikkerhedsrisici forbundet med teknologien og, hvis relevant, at indføre nødvendige foranstaltninger, der minimerer den identificerede risiko.