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.: 2025-11180
Dok.: 3852642

Besvarelse af spørgsmål nr. 164 (Alm. del) fra Folketingets udvalg for Digitalisering og It

Hermed sendes besvarelse af spørgsmål nr. 164 (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. 164 (Alm. del) fra Folketingets udvalg for Digitalisering- og It:

> ”Vil ministeren redegøre for, hvordan tilsynet med den overvågning, der er en konsekvens af CSA-forordningens pligt for digitale tjenester til at opspore seksuelt misbrug af børn, skal gennemføres? Og vil ministeren kommentere på, at vi med forslaget giver fremmede magter nemmere adgang til europæiske data?”

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 følger af kompromisforslaget, at tjenesteudbydere forpligtes til at indføre effektive interne procedurer til at forebygge og i nødvendigt omfang opspore og afhjælpe misbrug af de teknologier, indikatorer og data, der anvendes i opsporingen af overgrebsmateriale med børn på tjenesteudbyderens tjenester.

Tjenesteudbyderen skal derudover etablere og drive en tilgængelig, alderssvarende og brugervenlig mekanisme, der gør det muligt for brugerne inden for en rimelig frist at indgive klager over udbyderens påståede overtrædelser af sine forpligtelser

Som kompromisforslaget ligger nu, indebærer det, at udbyderne i visse tilfælde kan tildeles et opsporingspåbud. Sagsgangen vil som forslaget ligger nu være, at en koordinerende myndighed (udpeget i det enkelte medlemsland) skal kunne anmode (medlemslandets) kompetente retslige myndighed (f.eks. domstolene) eller en uafhængig administrativ myndighed om at udstede et opsporingspåbud til en konkret tjenesteudbyder, hvis der er dokumentation for, at der er en betydelig risiko for, at den pågældende tjeneste anvendes med henblik på seksuelt misbrug af børn online, og hvis årsagerne til udstedelsen af opsporingspåbuddet opvejer de negative konsekvenser for alle berørte parters rettigheder og legitime interesser. Det følger af forordningsforslaget, at det er tjenesteudbyderen og ikke myndighederne, der skal forestå opsporingen af overgrebsmateriale med børn. 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 forpligter tjenesteudbyderen til at installere og drive teknologier til opsporing af udbredelsen af kendt eller nyt materiale, der viser seksuelt misbrug af børn, og til at videresende oplysninger, der tyder på potentielt seksuelt misbrug af børn online på udbyderens tjenester, til et EU-center. Vurderer EU-centret, at oplysningerne kan danne grundlag for en strafferetlig efterforskning, videregiver EU-centret oplysningerne til de nationale retshåndhævende myndigheder. Opsporingspåbuddet omfatter fotos, videoer og links.

Tjenesteudbydere skal desuden føre logbog om den databehandling, der sker i medfør af udstedelse af et opsporingspåbud. Logbogen bruges til at verificere lovligheden af databehandlingen.

Forslaget lægger endvidere op til, at medlemslandene skal udpege en kompetent myndighed, som i medfør af forordningen bl.a. får kompetence til at gennemføre kontroller hos tjenesteudbyderne for at sikre, at forordningens regler efterleves.

I forhold til sikkerhedsrisici følger det af kompromisforslagets, at de teknologier, der anvendes af tjenesteudbyderne til opsporing af overgrebsmateriale, ikke skal introducere cybersikkerhedsrisici, som man ikke kan tage risikoafbødende tiltag imod. Teknologierne skal være i overensstemmelse med det aktuelle tekniske niveau i industrien og være mindst muligt indgribende over for brugernes ret til privatliv og familieliv, herunder til kommunikationshemmelighed og beskyttelsen af personoplysninger.

Kompromisforslaget er endelig baseret på en forudsætning om, at forordningen ikke må underminere cybersikkerhedstiltag såsom end-to-end-kryptering, og at forordningen ikke må tolkes sådan, at den indfører forpligtelser, der tvinger udbydere af onlinetjenester til at dekryptere data, skabe adgang til end-to-end-krypteret data eller forhindre udbydere af onlinetjenster i at tilbyde end-to-end-krypterede tjenester.