



JUSTITSMINISTERIET

Folketinget
Udvalget for Digitalisering og It
Christiansborg
1240 København K
DK Danmark

Dato: 31. oktober 2025
Kontor: Kontoret for EU-lovgivning
Sagsbeh: Ida Helene Bendtsen Højberg
Sagsnr.: 2025-11905
Dok.: 3870139

Besvarelse af spørgsmål nr. 169 (Alm. del) fra Folketingets Udvalg for Digitalisering og It

Hermed sendes besvarelse af spørgsmål nr. 169 (Alm. del), som Folketingets Udvalg for Digitalisering og It har stillet til justitsministeren den 2. oktober 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. 169 (Alm. del) fra Folketingets Udvalg for Digitalisering og It:

”Vil ministeren kommentere vedlagte notat, hvor forskere inden for datalogi, it og digital sikkerhed analyserer svaret på DIU alm. del, spørgsmål nr. 160 – og herunder konkret forholde sig til følgende:

- At den foreslåede client-side-scanning, jf. punkt A, B og C, bryder med ”end-to-kryptering”, da andre end modtager og afsender vil kunne se indholdet, idet der indføres scanning på klientsiden?
- At der – uagtet introduktionen af begrebet client-side-scanning – er tale om overvågning, jf. punkt C?
- At det vil være tjenesteudbyderen – og dermed techgiganterne – der i praksis skal foretage scanning af afsendt indhold, jf. punkt D, og at der dermed introduceres en mulighed for, at tjenesteudbyderen kan indsamle mere data end ønsket?
- At brugerne skal samtykke til scanning for at kunne anvende en tjeneste, jf. punkt E og F, og at man reelt må acceptere scanning for at kunne sende billeder?
- At der indirekte gives mulighed for at scanne tekst, og at scanningen vil kunne udvides til også at omfatte andre dele end URL’er i teksten, jf. punkt G?
- At det vil være muligt for borgere at vælge kommunikationstjenester, der ikke er placeret i EU og derfor ikke scannes – eller at der alternativt vil skulle indføres reel censur, jf. punkt H?
- Hvordan ministeren forholder sig til argumentationen om, at der ved indførelse af client-side-scanning sker en overtrædelse af brevhemmeligheden, jf. grundlovens § 72 og straffelovens § 263, da kommunikationen ikke længere vil være privat, jf. punkt I?
- Er det korrekt forstået, at ministeren i DR’s udsendelse Prompt har udtalt, at det helt generelt er en forkert opfattelse, at borgerne skal have ret til at kommunikere via en krypteret app, jf. punkt I?
- At det vil være tale om en meget ineffektiv og ressourcekrævende løsning at indføre client-side-scanning, jf. punkt J?
- At GDPR-materiale skal kunne kommunikeres krypteret via sikker digital post, som brydes ved client-side-scanning, jf. punkt K?
- At der introduceres en risiko for, at hackere kan udnytte scanningssoftware, jf. punkt L?
- At politiet vil blive overbebyrdet med flere digitale kriminalitetssager, end man har i forvejen, jf. punkt P?
- At forslaget ikke er proportionalt med den ønskede effekt, da der skal scannes ca. 290.000 billeder for at kunne finde

to billeder eller videoer af seksuelle overgreb mod børn, jf. punkt S?”

Svar:

CSA-forordningen er fortsat genstand for forhandlinger i Rådet, hvorfor forslaget og dets værktøjer kan ændre sig. Det gælder både i de videre forhandlinger i Rådet og i de efterfølgende interinstitutionelle forhandlinger med Europa-Kommissionen og Europa-Parlamentet.

Besvarelsen af spørgsmålet tager afsæt i det danske kompromisforslag, som blev præsenteret for medlemsstaterne i juli 2025. Det kompromisforslag, der er blevet fremlagt, er udarbejdet med henblik på at opnå tilstrækkelig opbakning i Rådet på baggrund af medlemsstaternes synspunkter. Det har imidlertid vist sig vanskeligt at skabe tilstrækkelig opbakning, og derfor forventer det danske formandskab at præsentere Rådet for en ny tilgang. Hvis formandskabet får opbakning til den ændrede tilgang, vil det betyde, at opsporingspåbuddet ikke vil være en del af et nyt kompromisforslag, og at det derfor fortsat vil være frivilligt for tech-giganterne at opspore materiale med seksuelt misbrug af børn. Forslaget vil indebære en række forpligtelser for udbydere af kommunikationstjenester til at bekæmpe udbredelse af materiale med seksuelt misbrug af børn via bl.a. tiltag, som kan begrænse risikoen for udbredelse såsom frivillig opsporing, rapporteringsforpligtelser og pligt til at fjerne sådan materiale på deres tjenester.

Der lægges med det danske kompromisforslag fra juli 2025 op til, at alle, der udbyder relevante tjenester i EU, er omfattet af forordningens anvendelsesområde. Det omfatter tjenester, som har en væsentlig tilknytning til EU. Det kan f.eks. være tjenester, der er etableret i EU, men det kan også være tjenester, der har et betydeligt antal brugere i en eller flere EU-medlemsstater, eller som målretter sin aktivitet mod én eller flere medlemsstater. At en tjenesteudbyder ikke er placeret i EU vil med andre ord ikke nødvendigvis medføre, at tjenesteudbyderen ikke vil skulle efterleve forordningen.

Forslaget lægger op til at indføre en række forpligtelser for udbydere af kommunikationstjenester i forhold til at forebygge misbrug af deres tjenester i form af deling af materiale, der viser seksuelt misbrug af børn. Hvis en udbyder ikke overholder forpligtelserne, indebærer forslaget, at myndighederne kan pålægge udbyderen et opsporingspåbud. Hvis en udbyder modtager et opsporingspåbud, skal udbyderen selv opspore spredning af over-

grebsmateriale med børn på tjenesten i en begrænset periode. Opsporingspåbuddet skal være målret og indeholde en præcisering af påbuddet til, hvad der er strengt nødvendigt. Det gælder endvidere, at den myndighed, der udsteder opsporingspåbuddet, forud for udstedelsen skal tage konkret stilling til, at påbuddet er nødvendigt og proportionalt i forhold til de grundlæggende rettigheder, herunder om opsporingspåbuddet kan gøres mindre indgribende i forhold til længden af påbuddet, de anvendte opsporingsteknologierne eller rækkevidden af påbuddet.

Det følger af kompromisforslaget, at opsporingspåbuddet afgrænses til billeder, videoer og URL'er. URL'er består af en streng af tegn, som til sammen udgør en "adresse", der angiver den præcise placering af en side eller fil på internettet. URL'er adskiller sig dermed rent teknisk fra ordinær tekst, hvorfor det er muligt for tjenester at sondre mellem tekstbeskeder og beskeder indeholdende links.

Det følger af det danske kompromisforslag, at EU-centeret, som oprettes med forslaget, skal kunne behandle personoplysninger i det omfang, det er nødvendigt for udførelsen af centerets opgaver. Centeret må kun behandle oplysninger i det omfang, det er strengt nødvendigt med henblik på at udføre en række specificerede opgaver, og centeret må ligeledes også kun opbevare dataen, så længe det er strengt nødvendigt. Centeret skal således slette oplysninger, så snart de ikke længere er strengt nødvendige for udførelsen af centerets opgaver. I det danske kompromisforslag er der endvidere indført et yderligere sikkerhedsværn i form af pseudonymisering, således at EU-centeret ikke får underretninger med personoplysninger i hænde, før centeret har vurderet, at underretningen ikke er åbenbart grundløs.

Der lægges op til at stille en række krav til de opsporingsteknologier, der anvendes til opsporing. Det er forudsat i kompromisforslaget, at teknologierne 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 i så fald alene at 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.

I forhold til, om teknologien, der skal anvendes, reelt findes, har online tjenester allerede i dag mulighed for på frivillig basis at foretage en vis scanning efter materiale, der viser overgreb mod børn. Det er en mulighed, der benyttes af flere tjenester, og som både tech-udbydere, børneorganisationer og vores myndigheder oplyser fungerer effektivt. Der er imidlertid en mulighed, som står til at bortfalde, når den gældende undtagelse fra e-privacy-direktivet udløbet i april 2026.

Forslaget indebærer, at der løbende skal udvikles teknologier til opfyldelse af forordningens formål. Det er således en integreret del af forslaget, at der stilles krav om udvikling af nye teknologier.

Det er et krav, at EU-Kommissionen tester og godkender den teknologi, der skal anvendes. Der vil således ikke kunne anvendes teknologier, som ikke på forhånd er blevet efterprøvet med hensyn til bl.a. sikkerhed og præcision.

Der lægges i forslaget vægt på, at opsporingsteknologierne vedvarende skal vurderes med henblik på at sikre, at de er tilstrækkeligt pålidelige. Det påhviler efter forslaget tjenesteudbydere at etablere menneskeligt eftersyn og, i nødvendigt omfang, menneskelig intervention for at undgå, at falske positive rapporteres og videreformidles til EU-centret.

Omfanget af ressourcer, der skal anvendes til at behandle eksempelvis indberetninger fra udbydere om opsporet materiale, afhænger af antallet af indberetninger og dermed af det endelige indhold af forordningen. I Kommissionens konsekvensanalyse blev det dog lagt til grund, at EU-centret vil skulle have mellem 75 og 85 ansatte til håndtering af opsporing, anmeldelse og fjernelse af materiale.

Det følger desuden af kompromisforslaget, at forordningen skal fortolkes i overensstemmelse med de grundlæggende rettigheder, navnlig retten til privat- og familieliv og retten til ytrings- og informationsfrihed.

NSK har tidligere oplyst, at den midlertidige frivillige ordning, som giver tjenesteudbydere lov til fortsat at detektere, rapportere og fjerne materiale med seksuelt misbrug af børn, generelt har fungeret tilfredsstillende siden 2021. Det blev samtidig påpeget, at den midlertidige ordning, der bygger på frivillighed, fører til en uensartet praksis, hvorfor der er behov for en retlig ramme for opsporing af misbrugsmateriale, som etablerer ensartede forpligtelser for alle platforme.

I forhold til spørgsmålet om min medvirken i podcasten ”Prompt” på DR kan jeg henvise til besvarelsen af 2. oktober 2024 af spørgsmål nr. 1425 (Alm. Del) fra Folketingets Retsudvalg som angår samme udtalelse til et andet medie.