



JUSTITSMINISTERIET

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

Dato: 7. oktober 2025
Kontor: Kontoret for EU-
lovgivning
Sagsbeh: Jakob Buchholt de Fønss
Sagsnr.: 2025-10545
Dok.: 3837141

UDKAST TIL TALE

Til brug for besvarelsen af samrådsspørgsmål I-L fra Folketingets Udvalg for Digitalisering og It

Samrådsspørgsmål I:

Vil ministrene redegøre for, hvorfor man fra regeringens side arbejder for at gennemføre en såkaldt "chatkontrol" via EU, som ifølge Dataetisk Råd og flere professorer i data og it vil medføre masseovervågning af almindelige borgeres private sms'er, mails og beskeder på sociale medier i et hidtil uset omfang?

Samrådsspørgsmål J:

Vil ministrene redegøre for, hvordan regeringen kan bakke op om et forslag, som vil medføre, at danske borgere risikerer at fremmede skal gennemgå private nøgenbilleder af deres børn, hvis de f.eks. sender billeder af deres børn, som er nøgne i badet eller på stranden til den anden forældre?

Samrådsspørgsmål K:

Vil ministrene redegøre for, hvordan man forholder sig til, at man vil gøre europæiske borgeres telefoner mere sårbare overfor hackerangreb i en tid, hvor omfanget af cyberkriminalitet og digital krigsførelse fra fremmedmagter som Rusland er voksende?

Samrådsspørgsmål L:

Hvorfor foreslår ministrene "chatkontrol", når tech-eksperter fraråder teknologien? Der henvises til artiklen "Chat Control 2.0? Experts urge the EU not to undermine encryption with new ProtectEU plan",

Slotsholmsgade 10
1216 København K.

T +45 7226 8400

www.justitsministeriet.dk
jm@jm.dk

www.techradar.com, 8. maj 2025, og hvordan vurderer ministrene "chatkontrol" i en dataetisk og it-sikkerhedsmæssig kontekst?

Spørgsmålet er stillet efter ønske fra Dina Raabjerg (KF), Helene Brydensholt (ALT), Kim Edberg Andersen (DD), Mette Thiesen (DF), Rosa Lund (EL), Jeppe Søe (UFG), Alexander Ryle (LA), Stinus Lindgreen (RV), Lisbeth Bech-Nielsen (SF).

Svar:

[Indledning]

Tak for ordet og tak for spørgsmålene.

Samrådet i dag handler om et meget vigtigt emne. Det angår nemlig spørgsmålet om, hvordan vi dæmmer op for de helt uhyrlige mængder af materiale med seksuelt misbrug af børn som deles og spredes på digitale kommunikationstjenester.

Bekæmpelse af seksuel udnyttelse af børn og den voldsomme udvikling i spredning af overgrebsmateriale med børn er en vigtig sag, og det er for mig helt afgørende, at vi som lovgiver tager de nødvendige skridt.

Derfor vil jeg også indlede med at sige, at jeg selvfølgelig hilser den store opmærksomhed på forslaget til CSA-forordning velkommen. Det er altid glædeligt, når man som minister kan konstatere, at der er livlig debat om et forslag, som man selv finder vigtigt.

Jeg har imidlertid også kunnet konstatere, at debatten blandt andet kredser omkring en række misforståelser, som også er indlagt i samrådsspørgsmålene.

Jeg er derfor meget glad for, at udvalget har givet mig mulighed for at forklare – og dermed forhåbentlig bane vejen for en konstruktiv dialog om forslaget, som ikke er baseret på de misforståelser, som jeg oplever kendetegner den aktuelle debat.

Det sagt, så ER der tale om et forslag, som indeholder vanskelige dilemmaer og afvejninger, og jeg lytter selvfølgelig til alle synspunkter og indvendinger.

Jeg er også med på, at der ligger nogle svære tekniske spørgsmål i forslaget, og at det stiller krav om udvikling af nye værktøjer, men det må være en udfordring, som vi kan overkomme.

Jeg har delt min taletid op således, at jeg vil sige lidt om, hvad selve CSA-forordningen egentlig indeholder, herunder hvad der ligger i det danske kompromisforslag. I tilknytning hertil vil jeg adressere nogle af de misforståelser, som jeg oplever, præger debatten om

forslaget. Til sidst vil jeg komme ind på den videre proces for forslaget.

[Baggrunden for CSA-forordningen]

Det helt overordnede formål med forslaget til CSA-forordningen er at sikre ensartede retlige rammer på tværs af medlemsstaterne og at pålægge udbydere pligt til at opspore, indberette og fjerne seksuelt misbrug af børn online.

I dag har udbydere af kommunikationstjenester mulighed for gennem en midlertidig ordning, som har været gældende siden 2021, at anvende opsporingsteknologi til at opspore materiale med seksuelt misbrug af børn på deres tjenester og indberette det. Ordningen er dog frivillig for udbydere og er i øvrigt ikke særligt målrettet udbydere med en særlig risikoprofil.

Den midlertidige ordning er blevet forlænget en gang og udløber i april 2026.

Tallene taler for sig selv. Vi har at gøre med en udfordring, som bare vokser i omfang, og de redskaber, vi har i dag, er ikke tilstrækkelige til at dæmme op for problemet.

Vi skal have skabt en retlig ramme, som forpligter tech-virksomhederne til at tage deres del af ansvaret her.

[Det danske kompromis]

Det danske kompromisforslag bygger videre på det kompromisforslag, som blev fremlagt af det tidligere belgiske formandskab i 2024.

Det indeholder således mulighed for, at myndighederne kan pålægge udbydere et såkaldt opsporingspåbud.

Opsporingspåbuddet medfører, at myndighederne som en sidste udvej kan pålægge udbydere af en online tjeneste at scanne deres egne tjenester efter tre ting. Og kun tre ting.

Til forskel fra Kommissionens oprindelige forslag omfatter det danske kompromisforslag nemlig ikke tekst, dvs. i praksis omfatter kompromisforslaget dermed ikke opsporing af grooming, men alene fotos, videoer og links der viser overgreb mod børn.

Det andet centrale spørgsmål i forhandlingerne drejer sig om scanningen af krypteret indhold, nærmere betegnet

som ”end-to-end-kryptering”. End-to-end-kryptering var omfattet af Kommissionens oprindelige forslag, mens Europa-Parlamentet i sit forhandlingsmandat har undtaget tjenester, der benytter end-to-end kryptering, fra forordningens anvendelsesområde.

I kompromisforslaget fra det danske EU-formandskab er der indarbejdet en forudsætning om, at forordningen ikke må forbyde, umuliggøre, svække, omgå eller på anden måde underminere cybersikkerhedstiltag, såsom den såkaldte end-to-end-kryptering.

I kompromisforslaget er opsporing på tjenester, der anvender end-to-end-kryptering således betinget af brugerens forudgående samtykke. Modellen lægger altså op til, at man som bruger vil kunne sige nej til scanning efter overgrebsmateriale og som følge deraf alene anvende kommunikationstjenesten til tekst- og lydbaseret kommunikation.

Det lyder alt sammen enormt teknisk. Men det danske kompromisforslag betyder altså, at man fortsat kan skrive med - og indtale beskeder til - hinanden krypteret. Men hvis du vil sende krypterede billeder, videoer eller links, må du finde dig i, at der fra tjenestens side kan ske

en scanning af materialet, men kun i det omfang, at tjenesten får et opsporingspåbud.

Tjenesteudbydere, som f.eks. [Signal eller WhatsApp], vil i praksis kunne gennemføre opsporingen med såkaldt client-side-scanning, som fungerer ved, at visuelt materiale og links scannes *forud* for afsendelse og krypteringen.

Jeg anerkender fuldt ud, at vi sideløbende har en diskussion om lovlig adgang til data, hvor der i EU-regi også pågår overvejelser. Og at dette spørgsmål – også – rejser bekymringer i forhold til kryptering. Den artikel, som spørgerne henviser til, angår netop det.

Men igen: det her vedrører ikke myndighedernes adgang til oplysninger.

Det handler om at få udbydere selv til at tage ansvar og forebygge delingen af overgrebsmateriale.

Lad os holde tingene adskilt.

[Gendrivelse af misforståelser]

Og det bringer mig til en af de mest udbredte misforståelser.

Den mest gængse misforståelse, jeg er stødt på, er, at CSA-forordningen grundlæggende handler om chatkontrol og omfatter scanning af borgeres e-mails, sms'er og beskeder på f.eks. Facebook, Instagram, Snapchat og krypterede tjenester som WhatsApp, Signal og Telegram.

Forslaget pålægger tjenesteudbydere en række forpligtelser i forhold til at forebygge misbrug af deres tjenester i form af deling af overgrebsmateriale med børn. Og som jeg tidligere har nævnt, kan myndighederne som en sidste udvej pålægge tjenesterne et opsporingspåbud, hvor *tjenesterne selv* skal bruge en forhåndsgodkendt teknologi til at scanne efter overgrebsmateriale med børn på deres tjeneste.

Og lad mig slå det fast en gang for alle.

Forslaget fjerner ikke borgernes mulighed for at skrive fortroligt sammen via eksempelvis chat eller e-mail, og myndighederne kan ikke kigge med i alle borgernes private kommunikation.

Forslaget giver ikke myndighederne adgang til at scanne borgernes kommunikation. Det er altså udbyderne selv og ikke myndighederne, som vil skulle stå for at scanne efter materiale med seksuelt misbrug af børn.

En anden misforståelse er spørgsmålet om, hvorvidt billederne fra stranden af ens egne nøgne børn, der løber rundt, pludselig vil figurere som overgrebsmateriale.

Det er en helt legitim bekymring, som jeg tager meget alvorligt.

Forordningsforslaget vil ikke medføre, at deling af ferie billeder bliver ulovligt. I forslaget sondres der mellem kendt og nyt materiale.

Kendt materiale defineres som materiale, der tidligere er blevet opsporet og identificeret af den nationale koordinerende myndighed, f.eks. politiet, som materiale, der viser seksuelt misbrug af børn.

Spørgsmålet om, hvorvidt ferie- og bade billeder kan blive fanget i en scanning som såkaldte ”falske positiver”, kan opstå, hvis der er udstedt et

opsporingspåbud for nyt materiale med seksuelt misbrug af børn.

Forslaget lægger op til, at opsporingspåbud for nyt materiale alene kan udstedes til tjenester, der tidligere har fået udstedt et opsporingspåbud for kendt materiale.

Det danske kompromisforslag har altså introduceret en række sikkerhedsgarantier, der har til formål at minimere risikoen for falske positive. Ligesom den teknologi, der anvendes til scanning, vil skulle forhåndsgodkendes af EU-Kommissionen med hensyn til bl.a. præcision og pålidelighed for at undgå falske positive.

[Regeringen står på børnenes side]

Det er klart, at forordningen vil pålægge onlinetjenesterne forpligtelser og dermed også byrder. Men det er i min optik helt rimeligt at forvente, at techgiganter og kommunikationsplatforme tager ansvar for, hvad der foregår på deres platforme.

I dag kan du sende og modtage materiale med overgreb mod børn på nogle tjenester, som måske/måske ikke foretager opsporing. Det er uholdbart.

Der er behov for en tydelig og klar ramme omkring bekæmpelse af spredning af materiale med seksuelt misbrug af børn, og der er behov for en erkendelse af, at udbyderne skal tage et mere proaktivt ansvar i den kamp.

Jeg hæfter mig ved, at en lang række børneorganisationer deler synspunktet og støtter forslaget. Og at de samme organisationer mener, at det vil være et katastrofalt svigt af børnene, hvis vi lader stå til.

[Den videre proces med forslaget]

Forslaget til forordningen blev fremlagt af Europa-Kommissionen tilbage i foråret 2022, og EU-Parlamentet vedtog sit forhandlingsmandat i november 2023.

Der har siden fremsættelsen været forhandlinger i Rådet om at nå frem til en generel indstilling, og der er i løbet af forhandlingerne fremlagt flere kompromisforslag, som har introduceret forskellige modeller og tilgang. Det danske kompromis er altså det seneste i rækken.

Forslaget er senest blevet drøftet på arbejdsgruppeniveau den 12. september 2025, og det er på den foreløbige dagsorden for RIA-rådsmødet i næste uge.

Først når kompromisforslaget opnår den fornødne opbakning i Rådet, kan man gå i gang med de forhandlinger mellem Rådet og Europa-Parlamentet som medlovgiver, som i sidste ende – når parterne er blevet enige – vil munde ud i, at forordningsforslaget endelig kan vedtages og træde i kraft.

Forslaget har allerede været længe undervejs, og det er selvfølgelig mit klare mål og ambition, at forslaget under dansk formandskab kommer nærmere en endelig vedtagelse.

[Afrunding]

Igen vil jeg sige mange tak for at bringe dette meget vigtige emne på dagsordenen og give mig mulighed for at sætte flere ord på forslaget.

Tak for ordet.