Faktaark: **11 myter og sandheder om CSA-forordningen**

JUSTITSMINISTERIET

Myte #1:

”CSA-forordningen handler grundlæggende om chatkontrol og omfatter scanning af borgeres e-mails, sms’er og beskeder på f.eks. Facebook Messenger, Instagram og Snapchat og krypterede tjenester som WhatsApp, Signal og Telegram”.

Fakta:

CSA-forordningen handler ikke om chatkontrol, men om at skabe en ensrettet ramme for forebyggelse og bekæmpelse af seksuelt misbrug af børn på nettet. Forslaget pålægger udbydere af online tjenester – f.eks. internetfora eller chatprogrammer – en række forpligtelser i forhold til at forebygge misbrug af deres tjenester i form af deling af materiale, der viser seksuelt misbrug af børn, og som en sidste udvej kan myndigheder pålægge en specifik tjeneste et opsporingspåbud, hvor tjenesten selv skal bruge en forhåndsgodkendt teknologi til selv at scanne efter materiale, der viser seksuelt misbrug af børn på deres tjeneste. Forslaget fjerner ikke borgernes mulighed for at skrive fortroligt sammen via eksempelvis chat eller e-mail, og myndighederne kan ikke kigge med i borgernes private kommunikation.

Myte #2:

”Den digitale kommunikation i EU vil potentielt kunne blive scannet af statsligt installeret overvågningssoftware”

Fakta:

Forslaget giver ikke myndighederne adgang til at scanne borgeres kommunikation. Som kompromisforslaget ligger nu, indebærer et opsporingspåbud, at en udbyder af en online tjeneste – på baggrund af en anmodning til en judiciel eller uafhængig myndighed, fx en domstol – som en sidste udvej og i en begrænset periode vil blive pålagt at scanne efter fotos, videoer eller links (og altså ikke eksempelvis tekst- eller lydbeskeder), der viser seksuelt misbrug af børn, hvis der er en særlig risiko for, at der findes materiale, der viser seksuelt misbrug af på tjenesten. Det er altså tjenesterne selv og ikke myndighederne, som vil skulle stå for at scanne efter materiale med seksuelt misbrug af børn. Identificerer tjenesten i den forbindelse materiale, der viser seksuelt misbrug af børn, vil tjenesten skulle videregive relevante oplysninger til et nyoprettet EU-center. Forordningen indebærer nemlig også etablering af et EU-center, der skal understøtte gennemførelse af forordningens formål og forenkle processen for modtagelse og videresendelse af indberetninger til myndighederne. EU-centeret skal bl.a. fungere som et center for indsamling og deling af viden og ekspertise, herunder i forhold til samarbejdet mellem myndigheder og tjenester.

Myte #3:

”Med forslaget lægges der op til permanent overvågning af din kommunikation”.

Fakta:

Forslaget giver myndighederne mulighed for – som en sidste udvej – at pålægge udbydere af onlinetjenester selv at opspore spredning af overgrebsmateriale med børn på deres tjenester i en tidsbegrænset periode. 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. Det indebærer, at opsporingspåbuddet – i det omfang det er muligt – vil skulle afgrænses til eksempelvis specifikke brugere, specifikke typer af brugere – f.eks. anonyme brugere – eller specifikke grupper på tjenesten. I øvrigt omfatter opsporingspåbuddet ikke tekst- eller lydbeskeder.

Myte #4:

”CSA-forordningen er et brud på brevhemmeligheden”

Fakta:

Forslaget skal selvfølgelig være foreneligt med grundloven. Forslagets forhold til grundlæggende rettigheder er et centralt tema for forhandlingerne i Rådet, og forslaget er løbende under forhandlingerne blevet tilpasset i denne henseende. Fra dansk side er der særligt fokus på, at forslaget rammer den rette balance mellem på den ene side respekten for brugernes grundlæggende rettigheder og på den anden side forebyggelse og bekæmpelse af seksuelt misbrug af børn online.

Myte #5:

”Politikere er undtaget det såkaldte opsporingspåbud, som man med forordningen lægger op til”

Fakta:

Der er ikke bestemte personer – f.eks. politikere eller ministre – der som gruppe er undtaget fra forslaget. Der lægges i det aktuelle kompromisforslag op til at undtage konti, der anvendes af staten til formål vedrørende den nationale sikkerhed, retshåndhævelse og militære formål, fra bestemmelserne om opsporing. Det handler om, at det er uhensigtsmæssigt, at f.eks. politiets konti, som bruges til at efterforske materiale, der viser seksuelt misbrug af børn, fanges af en scanning, som følger af et opsporingspåbud.

Myte #6:

”CSA-forordningen indebærer, at du ikke længere kan kommunikere anonymt. Hvis værktøjet skal virke, kræver det, at myndighederne ved, hvem afsenderen og modtageren af en besked er”

Fakta:

Det danske EU-formandskabs kompromistekst har **indført sikkerhedsværn, der betyder, at den kommunikation, der bliver identificeret som mulig deling af overgrebsmateriale videresendes af udbyderen af en onlinetjeneste til det foreslåede EU-center i anonymiseret form.** Først når EU-centeret vurderer, at oplysningerne kan danne grundlag for en strafferetlig efterforskning, gensendes oplysningerne fra tjenesten til EU-centeret uden anonymisering.

Myte #7:

”Der findes ikke dokumentation for, at det gør en forskel for politiet i efterforskningen og forebyggelsen af seksuelle overgreb mod børn”

Fakta:

Europa-Kommissionens konsekvensanalyse vurderer, at **den foreslåede ordning vil medføre en stærk forbedring af arbejdet med genkendelse, beskyttelse og støtte af ofre** for seksuelt misbrug, ligesom både **det forebyggende og efterforskningsmæssige spor vil blive styrket.** Red Barnet, Unicef, Digitalt Ansvar m.fl. har desuden kaldt digital scanning for et vigtigt teknisk værktøj, som allerede i dag opsporer store mængder overgrebsmateriale med børn.

Myte #8:

”Forslaget indebærer, at du ikke længere kan dele feriebilleder af dine børn på stranden”

Fakta:

Forordningsforslaget vil ikke medføre, at deling af feriebilleder 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 badebilleder 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 introduceret en række sikkerhedsgarantier, der har til formål at minimere risikoen for falske positiver, ligesom den teknologi, der anvendes til scanning, vil skulle forhåndsgodkendes af EU-Kommissionen med hensyn til bl.a. præcision og pålidelighed.

Myte #9:

”Forslaget er udarbejdet uden input fra eksperter”

Fakta:

Op til udarbejdelsen af forordningsforslaget har Kommissionen hørt relevante interessenter over to år for at identificere problemer og veje frem i kampen mod seksuelt misbrug af børn, både online og offline. Dette skete gennem undersøgelser, lige fra åbne offentlige høringer til målrettede undersøgelser af retshåndhævende myndigheder. **Der blev afholdt en række ekspertgruppemøder og bilaterale møder mellem Kommissionen og relevante interessenter** for at drøfte de potentielle virkninger af lovgivning på dette område, og **Kommissionen deltog i relevante workshopper, konferencer og arrangementer om børns rettigheder.**

Myte #10:

”Forslaget udgør en sikkerhedsrisiko, fordi det de facto bryder end-to-end krypteringen”

Fakta:

Forslaget tager højde for cybersikkerhedstiltag, herunder kryptering, og den teknologi, der skal benyttes til opsporing, bliver testet af Kommissionen.
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 end-to-end-kryptering. Det følger også af det danske kompromisforslag, 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.

Den teknologi, der skal anvendes til opsporing af overgrebsmateriale med børn, skal godkendes af EU-Kommissionen før implementering. Her efterser Kommissionen bl.a., at teknologien faktisk er egnet og effektiv til formålet, at den har den fornødne præcision, og at den ikke introducerer nye cybersikkerhedsrisici, som ikke kan afbødes.

Myte #11:

”Det er den danske regeringen og justitsministeren, der har fremlagt forslaget.”

Fakta:

Forslaget til CSA-forordningen blev **fremlagt af Europa-Kommissionen** den 11. maj 2022, der i overensstemmelse med den almindelige EU-lovgivningsproces har initiativretten og altså – ligesom regeringen kan fremlægge forslag til lovgivning i Danmark – kan fremsætte forslag til EU-regulering. Forslaget blev fremsat fordi, der sås at være et behov for at have ens retlige rammer på tværs af medlemsstaterne og for at pålægge udbydere pligt til at opspore, indberette og fjerne seksuelt misbrug af børn online.

Der har siden fremsættelsen af forslaget været forhandlinger i Rådet om at nå en generel indstilling. Det kompromisforslag, det danske formandskab har fremlagt, er således et forsøg på at finde en model, som kan opnå tilstrækkelig opbakning på tværs af EU’s medlemsstater. Det danske kompromisforslag er på en række parametre mindre indgribende og mere målrettet end Kommissionens oprindelige forslag.
Når et kompromisforslag opnår den fornødne opbakning i Rådet, indledes de interinstitutionelle forhandlinger mellem Rådet og Europa-Parlamentet som medlovgiver. Først når parterne er blevet enige, vil forordningsforslaget kunne vedtages endeligt og træde i kraft.
