Til Justitsminister Peter Hummelgaard

Cc: Medlemmerne af Folketingets It-udvalg, Europaudvalg og Retsudvalg

Kære Peter Hummelgaard København 4. oktober 2023

Vi retter henvendelse på baggrund af forslag til EU-forordning om forebyggelse og bekæmpelse af seksuelt misbrug af børn [KOM(2022) 0209], også kendt som CSA-forordningen. Som organisationer med praktisk erfaring og viden indenfor telekommunikation, jura, cybersikkerhed og dataetik er vi dybt bekymrede over forslaget og især den danske regerings hidtidige positive indstilling overfor forslaget. Vi opfordrer dig derfor til at lytte til den massive internationale kritik af forslaget.

Der er ingen tvivl om, at formålet med at forhindre seksuel udnyttelse af børn er et værdigt formål, som vi alle uden undtagelse kan bakke op om. Men metoden, der vil blive påbudt tjenesteudbydere af alle typer digital kommunikation fra sms og telefonopringninger til forskellige chatformer, er hverken gennemtænkt eller gennemtestet. Til gengæld er den ødelæggende for almindelige borgeres retssikkerhed samt retten til privat kommunikation, tilliden til digitalisering og ønsket om, at Danmark skal nå et højere niveau af cybersikkerhed.

De omfattende negative konsekvenser af forslaget er gået lidt under radaren hos mange, da forslaget umiddelbart kan ligne den nuværende midlertidige ordning, som gør det muligt for udbyderne af nummeruafhængige interpersonelle kommunikationstjenester at screene indhold på tjenesterne og opdage og rapportere materiale med seksuelt misbrug af børn. Den nye forordning er imidlertid i sin helhed langt mere vidtgående og omfatter overvågning af langt flere kommunikationstjenester, herunder også sms og telefonsamtaler, samt end-to-end krypterede kommunikationstjenester.

Retssikkerhed og retten til privat kommunikation

Metoden, der foreslås, indebærer en systematisk og generel overvågning af indholdet af kommunikation på tjenester, hvor der er risiko for, at de kan blive brugt til at dele materiale med seksuelle krænkelser af børn eller til grooming. Det kunne være f.eks. WhatsApp, Snapchat, Gmail, Signal, Proton, Teams, telefonsamtaler og sms'er. Det vil sige, at helt almindelige mennesker, der bruger de specifikke tjenester til at udveksle personlige beskeder, billeder og samtaler, bliver omfattet af påbuddet om scanning af indhold uden, at der behøver at være konkret mistanke mod den enkelte borger. Denne helt generelle masseovervågning er baggrunden for den massive kritik, der har været i de seneste måneder, ikke mindst fra EU's egne institutioner.

Rådets juridiske tjeneste har været ekstremt kritiske overfor forslaget[1]. Tjenestens analyse (rådsdokument 8787/23) konkluderer på grundlag af EU-Domstolens retspraksis, at der er en alvorlig risiko for, at forslaget de facto medfører en permanent overvågning af indholdet af al privat elektronisk kommunikation, og at denne overvågning vil være i strid med Charter om Grundlæggende Rettigheder.

Rådets juridiske tjeneste påpeger, at der er mangel på proportionalitet, da enhver, der kommunikerer digitalt, vil blive omfattet af overvågningen. Dette er kun acceptabelt i tidsbegrænsede situationer, hvor der er tale om, at statens sikkerhed er i fare. Rådets juridiske tjeneste anbefaler (pkt. 79), at opsporingspåbud bør begrænses til personer, hvor der er rimelig grund til at antage, at de er involveret i seksuelt misbrug af børn, det vil sige målrettet overvågning i stedet for det nuværende forslag om generel overvågning af alle brugere af kommunikationstjenesten.

The European Data Protection Board kritiserer[2] ligeledes forslaget for at være ude af proportioner og for at udviske grænsen mellem kriminelle, udbydere af tjenester og uskyldige brugere af sms, chat og mails.

For så vidt angår behovet for at styrke indsatsen i forhold til beskyttelse af børn og unge (som vi fuldt ud kan tilslutte os) henviser vi blandt andet til Digital Services Act, der pålægger online tjenester forpligtelser i forhold til risikovurdering og etablering af foranstaltninger mod spredning af krænkende og ulovligt materiale, navnlig på børne- og ungeområdet. Det er vores opfattelse, at Kommissionen og medlemslandene i tråd med Digital Service Act bør styrke det offentligt-private samarbejde i forhold til børnebeskyttelse på onlineplatforme og gamingtjenester, herunder for eksempel tilsynet med tjenesternes tryghedsindsats og sikre, at der tilgår forskningen og politimyndighederne oplysninger om brud med henblik på videnudvikling, forebyggelse og efterforskning. Digital Services Act træder i kraft i 2024 og dets virkemidler er derfor ikke afprøvet endnu.

Cybersikkerhed og tillid til digitalisering

Mange kommunikationstjenester gør i dag brug af end-to-end kryptering, som teknisk skal sikre at kun afsender og modtager kan læse beskeden. Kendte eksempler er tjenester som f.eks. Signal, der krypterer sms'er og samtaler, og Proton, der giver mulighed for krypterede mails. Begge dele fungerer som almindelige kommunikationstjenester og bruges af almindelige mennesker til hverdagsbrug. Krypterede tjenester er også den sikre løsning, hvis der skal udveksles følsomme

---

[1] https://www.euractiv.com/section/data-privacy/news/eu-councils-legal-opinion-gives-slap-to-anti-child-sex-abuse-law/ og juridisk vurdering af Kommissionens forslag fra Rådets Juridiske tjeneste i rådsdokument 8787/23 LIMITE https://www.statewatch.org/media/3901/eu-council-cls-opinion-csam-proposal-8787-23.pdf

[2] https://www.euractiv.com/section/law-enforcement/news/eu-watchdog-online-child-abuse-draft-law-creates-illusion-of-legality/ og https://edps.europa.eu/system/files/2022-07/22-07-28_edpb-edps-joint-opinion-csam_en.pdf

oplysninger, f.eks. mellem forældre og skole om en elevs diagnose, mellem en patient og en behandler eller mellem en fagforening og et medlem.

I en tid med stigende fokus på cybersikkerhed og almindelige borgeres muligheder for at forsvare sig mod cyberkriminalitet som identitetstyveri eller opringninger med det formål at få udleveret passwords eller få overført penge, er netop kryptering et væsentligt redskab for at undgå, at personfølsomme data er tilgængelige for andre end afsender og modtager. Det er her vigtigt at huske på, at når det handler om cybersikkerhed, så er det ikke nok, at statens institutioner har et højt sikkerhedsniveau. Et højt cybersikkerhedsniveau i Danmark er afhængigt af, at også borgere og erhvervsliv, uddannelsesinstitutioner, kommuner og sundhedssektoren er bedst muligt beskyttet og har de rigtige redskaber til at undgå hackerangreb, svindel, malware etc.

Et opsporingspåbud for end-to-end krypterede kommunikationstjenester kan i praksis kun implementeres ved, at tjenesteudbyderen indbygger bagdøre, for eksempel "client-side scanning" som er spyware på telefoner og computere. Uanset den konkrete udformning vil bagdøre altid undergrave sikkerheden ved kryptering, og bagdøre vil kunne misbruges af fjendtlige aktører. Det kan for eksempel være kriminelle hackere, der vil begå identitetstyveri. I et åbent brev i juli 2023 har mere end 400 forskere og eksperter i kryptering protesteret mod EU-forslaget og dets konsekvenser for cybersikkerhed og privatliv.[3]

Det er afgørende vigtigt for den fremtidige digitalisering af Danmark, at der er fuld tillid i befolkningen til, at man trygt kan bruge digitale kommunikationskanaler. Hvis det ikke længere er fuldt sikkert at sende følsomme oplysninger til f.eks. offentlige myndigheder eller banken, eller hvis det ikke er trygt at tale i telefon med familiemedlemmer om svære problemer, så risikerer vi et ønske om tilbagevenden til de analoge løsninger, som i mange tilfælde både er dyrere og mere tidskrævende og heller ikke altid længere en mulighed.

Opsamling

Flere af de underskrivende organisationer har i årevis arbejdet for at øge beskyttelsen af børn i det digitale univers. Men det er vigtigt at forstå, at dette forslag til forordning har omfattende negative konsekvenser for almindelige menneskers mulighed for privat kommunikation og går langt længere end den frivillige ordning, der fungerer i øjeblikket. Den nye forordning kan ikke bare ses som en permanentliggørelse af den hidtidige ordning. Vi opfatter den nye ordning som en markant udvidelse af overvågningen og som et voldsomt indgreb i meddelelseshemmeligheden, som både er beskyttet af grundloven, straffeloven, e-privacydirektivet og charteret.

I andre lande, herunder f.eks. i Tyskland, er der skabt bekymring for, om forordningen er proportional og potentielt i strid med charteret. Den voksende modstand og erkendelse af, at

---

[3] Computerworld 4. juli 2023, https://www.computerworld.dk/art/283530/300-kryptologer-verden-over-sender-aabent-brev-til-eu-i-protest-mod-ny-lov Ved udgangen af juli var der 465 underskrifter på brevet. https://docs.google.com/document/d/13Aeex72MtFBjKhExRTooVMWN9TC-pbH-5LEaAbMF91Y/preview?pli=1

forslaget er for vidtgående, har senest fået det spanske formandskab til at tage punktet af en rådsmødedagsorden.

Vi opfordrer dig derfor til at lytte til kritiske røster fra både internationale eksperter og den danske opposition og at regeringen holder fast i det strammede mandat, som blev givet i Europaudvalget, og som indebærer, at regeringen skal lægge "afgørende vægt" på, at forslaget ikke er i strid med Charteret. Det betyder for os at se, at regeringen vil være nødsaget til at stemme nej til forslaget, som det foreligger. Samtidig opfordrer vi til, at man undersøger, hvordan man kan styrke indsatsen mod misbrug og seksuelle krænkelser af børn med metoder, der er proportionelt forsvarlige med alle borgeres grundlæggende rettigheder til privatliv og privat kommunikation, og uden at man modarbejder en sikker og tillidsfuld digitalisering af Danmark.

Med venlig hilsen

Vibe Klarup	Generalsekretær, Amnesty International Danmark
Jens Myrup Pedersen	Professor, Aalborg Universitet, underskriver personligt
Ivan Damgård	Professor, Aarhus Universitet, underskriver personligt
Poul Noer	Fagchef for telepolitik, Dansk Erhverv
Jeanette Hartz	Adm. Dir., Dansk IT
Birgitte Kofod Olsen	Medstifter og forperson, DataEthics.eu
Andreas Holbak Espersen	Digitaliseringspolitisk chef, DI Digital
Thomas Hildebrandt	Professor, DIKU, underskriver personligt
Christian D. Jensen	Lektor, DTU, underskriver personligt
Grit Munk	It-politisk chefkonsulent, Ingeniørforeningen, IDA
Mette Lundberg	Politisk direktør, IT-Branchen
Jesper Lund	Formand, IT-Politisk Forening
Birgitte Arent Eiriksson	Direktør, Justitia Danmark
Niels Bertelsen	Formand, PROSA – forbundet af it-professionelle
Henning Mortensen	Formand, Rådet for Digital Sikkerhed
Jakob Willer	Direktør, Teleindustrien
Anders Kjærulff	Journalist og debattør