IT-Politisk Forening

Web: www.itpol.dk
Email: bestyrelsen@itpol.dk

5. september 2023

Til: Europaudvalget (EUU) og Retsudvalget (REU)

Henvendelse vedr. forordningsforslaget om forebyggelse og bekæmpelse af seksuelt misbrug af børn [KOM(2022) 0209] og RIA-rådsmødet den 28. september 2023

På rådsmødet for retlige og indre anliggender (RIA) den 28. september 2023 ønsker det spanske formandskab at vedtage en generel indstilling for forordningsforslaget om forebyggelse og bekæmpelse af seksuelt misbrug af børn [KOM(2022) 0209].

Ifølge de offentliggjorte dokumenter på Folketingets hjemmeside har Europaudvalget endnu ikke givet regeringen mandat i sagen.[1] I december 2022 afholdt Justitsministeriet en offentlig høring om forordningsforslaget, men regeringen har ikke oversendt eller kommenteret de modtagne høringssvar over for Europaudvalget. Høringssvaret fra IT-Politisk Forening er derfor vedlagt som bilag til denne henvendelse.

I denne henvendelse vil vi alene kommentere forordningsforslagets artikel 7-11 om opsporingspåbud for interpersonelle kommunikationstjenester. Disse tjenester kan blive pålagt at overvåge alle brugeres private kommunikation, uden krav om forudgående individuel mistanke, ved hjælp af algoritmer som stilles til rådighed af EU-Centeret. Alle juridiske vurderinger af forslaget, bortset fra Kommissionens egen vurdering, konkluderer, **at denne masseovervågning af privat kommunikation strider mod Charter om Grundlæggende Rettigheder.**[2]

1 EU-Oplysningens side for KOM(2022) 0209
https://www.eu.dk/samling/20221/kommissionsforslag/kom(2022)0209/index.htm

2 Fælles udtalelse fra EDPS og EDPB (juli 2022) https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_en,

Supplerende konsekvensanalyse fra Europa-Parlamentets Forskningstjeneste (EPRS) (april 2023) https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2023)740248 og

Juridisk vurdering af Kommissionens forslag fra Rådets Juridiske Tjeneste i rådsdokument 8787/23 LIMITE (tilgængelig her https://www.statewatch.org/media/3901/eu-council-cls-opinion-csam-proposal-8787-23.pdf).

Det er bemærkelsesværdigt, at de mest omfattende juridiske indvendinger kommer fra Rådets Juridiske Tjeneste. Deres juridiske analyse (rådsdokument 8787/23) på grundlag af EU-Domstolens retspraksis om bl.a. logning konkluderer, 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 (pkt. 79), at opsporingspåbud for at respektere Charteret bør begrænses til personer, hvor der er rimelig grund til at antage, at de er involveret i seksuelt misbrug af børn (dvs. målrettet overvågning i stedet for Kommissionens forslag om generel overvågning af alle brugere af kommunikationstjenesten).

Rådets arbejdsgruppe for forordningsforslaget, Law Enforcement Working Party (LEWP), har imidlertid valgt at ignorere den lange række af indvendinger om, at den generelle og udifferentierede overvågning af privat kommunikation strider mod Charter om Grundlæggende Rettigheder. I den senest offentliggjorte kompromistekst fra rådsarbejdsgruppen er der ingen ændringsforslag, som begrænser overvågningen (opsporingspåbud i artikel 7-11) til personer som konkret er under mistanke for at udbrede materiale med seksuelt misbrug af børn.[3]

Forslagets særdeles vidtgående konsekvenser for fortroligheden og sikkerheden af privat elektronisk kommunikation kan bedst illustreres ved, at rådsarbejdsgruppen har fundet det nødvendigt at indsætte en særlig undtagelse for interpersonelle kommunikationstjenester som anvendes af staten.[4]

Mange kommunikationstjenester gør i dag brug af end-to-end kryptering, som teknisk skal sikre at kun afsender og modtager kan læse beskeden. 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**, for eksempel kriminelle hackere der vil begå identitetstyveri. I et åbent brev i juli 2023 har flere hundrede forskere og eksperter i kryptering protesteret mod EU-forslaget og dets konsekvenser for cybersikkerhed og privatliv.[5]

3 Rådsdokument 11518/23 https://data.consilium.europa.eu/doc/document/ST-11518-2023-INIT/en/pdf

4 Præambelbetragtning 12a i kompromistekst 11518/23.

5 *300 kryptologer verden over sender åbent brev til EU i protest mod ny lov*, 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

På det foreliggende grundlag ser det altså ud til, at EU-regeringerne på RIA-rådsmødet den 28. september 2023 vil skulle tage stilling til en generel indstilling, som indeholder systematisk overvågning af borgernes private kommunikation, og som i væsentlig grad vil svække sikkerheden med bagdøre i end-to-end krypterede kommunikationstjenester.

IT-Politisk Forening vil derfor opfordre til, **at Danmark på rådsmødet den 28. september 2023 stemmer imod den generelle indstilling**, hvis den (som det p.t. ser ud til) indebærer masseovervågning af interpersonelle kommunikationstjenester og en alvorlig svækkelse af cybersikkerheden for end-to-end krypterede tjenester.

Forordningsforslaget om forebyggelse og bekæmpelse af seksuelt misbrug af børn er formentlig det mest kritiserede forslag fra EU-Kommissionen nogensinde. Det er konklusionen i en analyse fra European Digital Rights.[6]

IT-Politisk Forening håber, at den omfattende kritik af forordningsforslaget fra mange sider vil gøre indtryk på Europaudvalget og regeringen.

Indsatsen mod seksuelt misbrug af børn er naturligvis et vigtigt formål, men der er brug for helt andre, og reelt forebyggende, foranstaltninger end Kommissions forslag om masseovervågning af privat kommunikation. **Indsatsen mod seksuelt misbrug af børn bliver i øvrigt ikke reelt styrket, hvis den hovedsageligt baseres på en opsporingsforpligtelse, som efterfølgende underkendes af EU-Domstolen.**

Med venlig hilsen

Jesper Lund
Formand, IT-Politisk Forening

6 *Is this the most criticised draft EU law of all time*? European Digital Rights (EDRi), 29. august 2023 https://edri.org/our-work/most-criticised-eu-law-of-all-time/

IT-Politisk Forening

Web: www.itpol.dk
Email: bestyrelsen@itpol.dk

20. december 2022

Høringssvar vedr. EU-Kommissionens forslag til forordning om regler til forebyggelse og bekæmpelse af seksuelt misbrug af børn (Justitsministeriets j.nr. 2022-3050-0139)

Forordningsforslaget har bestemt et vigtigt formål, men bruger generelt de forkerte metoder, og forslaget vil derfor ikke opnå det erklærede mål om at beskytte børn. På flere punkter vil forslaget direkte skade børns rettigheder og digitale udfoldelsesmuligheder, foruden de stærkt negative konsekvenser for hele befolkningens grundlæggende rettigheder.

Opsporingsforpligtelsen, det centrale element i forslaget, må forventes at medføre en systematisk overvågning af privat kommunikation, der med rette kan sammenlignes med fortidens sorte kabinetter, hvor borgernes private breve på generel og udifferentieret basis blev åbnet, læst og kontrolleret af staten.[1] En sådan masseovervågning uden noget krav om forudgående individuel mistanke er i sagens natur endog meget vidtgående og næppe forenelig med retten til privatliv i Charter om Grundlæggende Rettigheder.

På en række punkter er forordningsforslaget udtryk for techno-solutionism, hvor sociale problemer som seksuelt misbrug af børn søges løst ved teknologiske foranstaltninger, herunder overvågning, i stedet for at tage hånd om de bagvedliggende årsager til disse alvorlige problemer. Opsporing af kendt misbrugsmateriale sker først efter at det seksuelle misbrug har fundet sted, og kan derfor ikke siges at forebygge seksuelt misbrug. I forhold til online misbrug som finder sted i realtid, eksempelvis grooming (hvervning af børn), er teknologierne i form af kunstig intelligens meget usikre. Brug af disse teknologier vil medføre et meget stort antal falsk-positive opsporinger, som vil være stærkt belastende for de personer som uretmæssigt beskyldes for seksuelt misbrug af børn, og som vil forstyrre og forsinke politiets arbejde med de virkelige sager om seksuelt misbrug af børn.

På flere punkter indeholder forordningsforslaget foranstaltninger, som reelt er teknisk umulige at implementere. Det gælder opsporingsforpligtelsen for end-to-end krypteret kommunikation og især påbud til internetudbydere om spærring af specifikke internetadresser (URL'er). I det omfang disse

1 Andreas Marklund, *Overvågningens historie: Fra sorte kabinetter til digital masseovervågning*, Gads Forlag 2020

foranstaltninger overhovedet kan gennemføres rent teknisk vil de have katastrofale konsekvenser for alle borgeres, herunder børnenes, informationssikkerhed på internettet.

Det er positivt, at der med forordningsforslaget oprettes et EU-center til forebyggelse og bekæmpelse af seksuelt misbrug af børn. Dette center får blandt andet til opgave at modtage indberetninger fra tjenesteudbydere, som får kendskab til potentielt seksuelt misbrug af børn. For de amerikanske tjenesteudbydere sendes disse indretninger i dag til NCMEC (National Center for Missing and Exploited Children) i USA, også for deres europæiske brugere, hvilket skaber en række problemer i forhold til EU's databeskyttelseslovgivning, herunder kravene til tredjelandsoverførsler.

IT-Politisk Forening vil anbefale, at Danmark i Rådet arbejder for at bestemmelserne om opsporing (artikel 7-11) helt udgår af forslaget. Der er tale om masseovervågning uden krav om forudgående mistanke, hvilket er uforeneligt med europæiske retsstatsprincipper. Indsatsen mod seksuelt misbrug af børn bliver ikke reelt styrket, hvis den baseres på en opsporingsforpligtelse, som efterfølgende underkendes af EU-Domstolen.

Disse vurderinger af forordningsforslaget uddybes i det følgende.

Risikovurdering og risikobegrænsning (artikel 3-6)

Artikel 3 pålægger udbydere af hostingtjenester og udbydere af interpersonelle kommunikationstjenester at vurdere risikoen for at tjenesten anvendes til seksuelt misbrug af børn. Artikel 4 pålægger i forlængelse heraf udbyderne at træffe rimelige afbødende foranstaltninger, som begrænser disse risici. Tjenesteudbyderens risikovurdering og beskrivelse af eventuelle afbødende foranstaltninger skal løbende indsendes til den koordinerende myndighed i etableringslandet, som kan pålægge udbyderen af foretage yderligere risikovurderinger eller implementere yderligere risikobegrænsende foranstaltninger.

Disse bestemmelser gælder for alle tjenesteudbydere uanset størrelse. Store platforme som Facebook/Meta, Twitter, Google, Microsoft og Tiktok har økonomiske ressourcer til at udføre disse opgaver. Det er ikke nødvendigvis tilfældet for mindre platforme, herunder platforme som drives af privatpersoner eller frivillige foreninger (for eksempel det hastig voksende antal Mastodon-instanser efter Elon Musk's overtagelse af Twitter). Hvis en række mindre tjenesteudbydere tvinges til at lukke eller væsentligt begrænse den funktionalitet, som de tilbyder deres brugere, vil borgerne ende med at få færre alternativer til de store platforme.

Forordningsforslaget risikerer dermed direkte at styrke den oligopolistiske position, som de store online platforme har i dag. Når der lovgives som om at alle platforme er Big Tech, bliver der kun plads til Big Tech i online økosystemet. Europas borgere, og ikke mindst børnene, har brug for flere alternativer, ikke færre, til de store (og ofte problematiske) platforme.

Bestemmelserne om risikovurdering og risikobegrænsning har en del lighedspunkter med de specifikke foranstaltninger i TCO-forordningen (EU) 2021/784. Der er imidlertid den væsentlige forskel, at kravene om specifikke foranstaltninger i TCO-forordningens artikel 5 kun gælder for tjenesteudbydere, som rent faktisk er eksponeret for terrorrelateret onlineindhold (objektivt defineret i TCO-forordningen). Forordningsforslaget er i stedet baseret på den abstrakte præmis, at alle onlinetjenester medfører risiko for seksuelt misbrug af børn.

Tidligere konstaterede tilfælde af seksuelt misbrug af børn indgår i risikovurderingen, men det er langt fra det eneste kriterium. Fraværet af alderskontrol og det forhold til at tjenesten bruges af børn er således defineret som en risiko i sig selv. Det kan via de risikobegrænsende foranstaltninger tvinge tjenesteudbydere til at indsamle oplysninger om brugerne, som ikke er nødvendige for udbud af selve tjenesten (for eksempel validerede aldersoplysninger via kopier af ID-dokumenter). En anden mulighed er at tjenesteudbyderne via deres brugerbetingelser direkte ”forbyder” børn at bruge deres tjenester, fordi forordningsforslaget meget ensidige kriterier for risikovurdering fører til en konklusion om, at risikoen ved at udbyde tjenesten til personer under 18 år er for stor.

For interpersonelle kommunikationstjenester er det i sig selv en risiko, at brugerne har mulighed for at etablere kontakt med andre brugere og dele billeder og videoer med hinanden. De nævnte kriterier er imidlertid selve formålet med en interpersonel kommunikationstjeneste (at brugerne kan kommunikere med hinanden), og dermed vil alle sådanne tjenester per definition udgøre en risiko for seksuelt misbrug af børn.

Specielt for interpersonelle kommunikationstjenester er det meget uklart hvordan udbyderen skal foretage den konkrete risikovurdering efter artikel 3 eller vurdere den potentielle resterende risiko efter risikobegrænsende foranstaltninger (artikel 4). Alle interpersonelle kommunikationstjenester er siden december 2020 omfattet af e-databeskyttelsesdirektivet 2002/58/EF, og udbyderen kan ikke lovligt foretage analyser af brugernes kommunikation eller tilhørende metadata. Forordningsforslagets artikel 3, stk. 3 nævner ”anonymiserede repræsentative data”, men det er i praksis ikke muligt at anonymisere kommunikationsdata.

Udbydere af interpersonelle kommunikationstjenester vil reelt blive tvunget til at indføre en form for alderskontrol, fordi de per definition (af forordningsforslaget) vil have en risiko for hvervning af børn. Det fremgår eksplicit af artikel 4, stk. 3. Det er muligt at alderskontrol kan undgås, hvis tjenesten ikke tilbydes til personer under 18 år (fordi det udelukker hvervning af børn), men selv med brugerbetingelser som kræver at brugeren skal være 18 år, kan tjenesteudbyderen reelt ikke vide, om der alligevel er børn blandt brugerne. Det er almindelig kendt, at en del børn under 13 år har oprettet profiler på sociale medier som Instagram og Tiktok ved at afgive forkerte oplysninger om deres fødselsdato.

Krav om alderskontrol vil tvinge tjenesteudbydere til at indsamle personoplysninger, som ikke er nødvendige for udbud af tjenesten. Det vil i praksis udelukke muligheden for anonym brug af kommunikationstjenester og sociale medier, hvilket i sig selv kan have en betydelig kølende effekt (chilling effect) på borgernes udøvelse af grundlæggende rettigheder som ytringsfriheden og forsamlingsfriheden. For personer, der ønsker at udforske deres seksuelle identitet (eksempelvis unge LBGTI+ personer) via online fællesskaber, kan muligheden for anonymitet være altafgørende for deres lyst til at gøre dette, fordi de frygter social udstødelse fra familie eller venner. Det gælder ikke mindst for unge personer, som er særligt sårbare i denne henseende. Forordningsforslaget ignorerer fuldstændigt denne problemstilling, fordi det nærmest per definition antages, at onlinetjenester med overvågning og alderskontrol er mere sikre for brugerne. Det er på ingen måde tilfældet, heller ikke for personer under 18 år.

For nærværende og i den overskuelige fremtid findes der reelt ingen gode metoder til alderskontrol på internettet. Eksisterende metoder er typisk baseret et usikkert estimat af brugerens alder via biometrisk analyse af brugerens ansigt (Instagram bruger teknologi fra Yoti til dette[2]), betaling af et mindre beløb via et kreditkort (som kun kan udstedes til personer over 18 år), eller indsendelse af digitale kopier af ID-dokumenter med fødselsdato. Specielt det sidste medfører en betydelig risiko for misbrug af personoplysninger, herunder risikoen for identitetstyveri i tilfælde af databrud hos tjenesteudbyderen. Personer med skumle hensigter vil i øvrigt relativt nemt kunne erhverve sig en ”valideret” falsk identitet via ID-oplysninger fra et sådant databrud. Aldersvurdering via biometriske ansigtsanalyser har betydelige problemer med usikkerhed og diskrimination, fordi usikkerheden afhænger af personens køn og hudfarve.[3]

2 *Videoselfies skal være med til at beskytte unge på Instagram*, Berlingske 7. november 2022 https://www.berlingske.dk/danmark/videoselfies-skal-vaere-med-til-at-beskytte-unge-paa-instagram

3 *Instagram is testing an AI tool that verifies your age by scanning your face*, The Verge, 23. juni 2022 https://www.theverge.com/2022/6/23/23179752/instagram-age-verification-ai-social-vouching-methods

Krav om alderskontrol vil generelt udelukke en række personer fra online fællesskaber og muligheden for digital kommunikation med andre, fordi de ikke er i besiddelse af ID-dokumenter eller kreditkort, eller ønsker at indsende sådanne oplysninger til Big Tech virksomheder, som i forvejen indsamler alt for mange personoplysninger om deres brugere. Den digitale eksklusion vil ramme børn uforholdsmæssigt hårdt. Alderskontrol via elektronisk ID (eID) vil på samme måde ekskludere en masse personer fra onlinetjenester, ikke mindst i de EU-lande hvor eID ikke er særligt udbredt.

Selv i Danmark, hvor MitID pga. tvangsdigitaliseringen officielt nærmer sig 100% udbredelse, vil krav om alderskontrol via eID virke ekskluderende, alene af den grund at 25% af befolkningen ifølge undersøgelser er udfordret af den offentlige digitalisering. Mange borgere vil formentlig også have ganske betydelig modstand mod at anvende MitID for at oprette en email konto eller bruge sociale medier, når de i årtier har kunnet oprette sådanne konti uden NemID/MitID. En så omfattende anvendelse af MitID på internettet vil i øvrigt være sikkerhedsmæssigt uforsvarligt på grund af den generelt mangelfulde sikkerhedsmodel i MitID.

Opsummering: forordningsforslaget er grundlæggende baseret på en falsk præmis om at alderskontrol og overvågning gør onlinetjenester mere sikre. I mange tilfælde vil denne overvågning faktisk gøre tjenesterne mere usikre, også for børn. Risikoen for at ekskludere en masse personer fra online fællesskaber ignoreres fuldstændigt. Det gælder ikke mindst for de unge personer, som forordningsforslaget søger at beskytte.

Opsporingsforpligtelser (artikel 7-11)

Under visse betingelser kan den nationale koordinerende myndighed få udstedt et opsporingspåbud til udbydere af hostingtjenester eller interpersonelle kommunikationstjenester. Det vil være muligt, hvis der er betydelig risiko for at tjenesten anvendes til seksuelt misbrug af børn. Artikel 7, stk. 5-7 definerer imidlertid ”betydelig risiko” på en sådan måde, at der ganske ofte vil være betydelig risiko. Der kan sågar være en betydelig risiko for helt nystartede tjenester uden konkrete eksempler på seksuelt misbrug af børn, fordi den koordinerende myndighed kan vælge at bruge indikationer fra en tilsvarende tjeneste.

Med den brede definition af ”betydelig risiko” vil et stort antal tjenesteudbydere kunne modtage et påbud om opsporing fra den koordinerende myndighed. Et påbud om opsporing indebærer jf. artikel 10, at tjenesteudbyderen skal installere og drive teknologier til overvågning, der stilles til rådighed

af EU-centret. Det er reelt et krav om installation af statslig spyware, som skal overvåge samtlige brugere på generel og udifferentieret basis (uden krav om forudgående individuel mistanke).

For interpersonelle kommunikationstjenester er det masseovervågning af privat kommunikation, svarende til fortidens sorte kabinetter (fra 1500-tallet), hvor staten åbnede og kontrollerede samtlige breve. For tjenester underlagt et påbud om opsporing er meddelelseshemmeligheden reelt ophævet. Det vil have uoverskuelige konsekvenser for borgernes grundlæggende rettigheder, når statslig spyware konstant undersøger deres private kommunikation. En direkte sammenligning af EU med Kina er helt på sin plads her.

For hostingtjenester kan der være tale om overvågning af private filer lagret i cloud-tjenester som Microsoft Onedrive eller uploadfiltre for sociale medier, hvor brugernes indlæg uden forudgående mistanke scannes for ulovligt indhold. Obligatoriske uploadfiltre indgik i Kommissionens forslag til TCO-forordningen, men på grund af indvendinger fra Europa-Parlamentet blev dette vidtgående element fjernet. På samme måde som overvågning af privat kommunikation i interpersonelle kommunikationstjenester vil uploadfiltre for sociale medier have en kølende effekt på udøvelsen af borgerne ytringsfrihed og andre grundlæggende rettigheder.

Påbud om opsporing kommer i tre forskellige udgaver: kendt materiale (med seksuelt misbrug), nyt materiale (ukendt seksuelt misbrug) og hvervning af børn (også kaldet grooming). Kendt materiale vil sige billeder m.v. som af kompetente myndigheder er identificeret som seksuelt misbrug af børn. Opsporing vil her indebære at tjenesteudbyderen skal sammenligne alle uploadede billeder m.v. med en database af kendt materiale, i praksis repræsenteret ved hashværdier (indikatorer). Sådanne sammenligninger kan i teorien gøres med en forholdsvis høj grad af præcision, omend der selv for den mest udbredte metode PhotoDNA ikke er lavet uafhængige analyser af teknologiens præcision. Konsekvensanalysen for forordningsforslaget [SWD(2022) 209 final] kan alene citere et tal for teknologiens præcision som stammer fra udvikleren af PhotoDNA, i øvrigt uden at nævne de statistiske forudsætninger for dette estimat.

Teknologierne til at opspore ukendt materiale og hvervning af børn er derimod langt mere usikre, og må reelt betegnes som decideret umodne teknologier. Hvor opsporing af kendt materiale sker ved at sammenligne hashværdier (et slags ”fingeraftryk” for materialet), er opsporing af ukendt materiale og hvervning af børn baseret på indholdsanalyse med kunstig intelligens. På grundlag af træningsdata prøver en algoritme at forudsige, om nyt ukendt materiale (billeder eller video) indeholder seksuelt misbrug af børn eller om en chat-samtale er forsøg på hvervning af børn.

Sådanne forudsigelser kommer med betydelig usikkerhed, blandt andet fordi kunstig intelligens typisk ikke er i stand til at forstå menneskelige intentioner. Der er talrige eksempler, hvor eksempelvis uskyldige billeder af nøgne børn på en badestrand (en ret almindelig situation) er blevet udpeget som potentielt seksuelt misbrug af børn af disse meget usikre teknologier.[4]

Som direkte konsekvens heraf vil der være en betydelig risiko for falsk-positive identifikationer, hvorved uskyldige personer udpeges som værende potentielt involveret i seksuelt misbrug af børn. De vil blive indberettet til EU-centret, som i mange tilfælde vil videresende indberetningen til politiet. Derudover vil de berørte personer næsten altid få lukket deres konto hos tjenesteudbyderen, og i mange tilfælde vil kontoen ikke blive genåbnet, selv hvis politiets efterforskning senere fuldstændigt frikender personen. En egentlig frikendelse fra politiets side forudsætter i øvrigt, at der er ressourcer til en politimæssig vurdering af de mange indberetninger, som politiet må forventes at modtage via EU-centret. Mange sager vil sikkert blot blive henlagt af politiet uden frikendelse af de mange uskyldige borgere, som vil blive berørt af falsk-positive opsporinger fra de usikre teknologier.

For hvervning af børn omtaler konsekvensanalysen et værktøj til opsporing, som er udviklet af Microsoft (Projekt Artemis), og som ifølge Microsoft selv har en præcision på 88%. Typisk overvurderer IT-virksomheder præcisionen når de markedsfører deres egne værktøjer, så den reelle præcision er sikkert lavere. Det er endvidere uklart hvad en præcision på 88% egentlig refererer til (der er flere forskellige mål for præcision, eksempelvis falsk-positive vs. falsk-negative matches), men hvis det refererer til riskoen for at en almindelig chat-samtale udpeges som mulig hvervning af børn, vil EU-centeret hver eneste dag bogstaveligt talt blive oversvømmet med millioner af forkerte indberetninger. Eftersom der er mange flere legitime chat-samtaler end forsøg på hvervning af børn, vil antallet af forkerte indberetninger være mange gange større end antallet af korrekte indberetninger (hvor der virkelig er tale om hvervning). Den problemstilling er kendt som base rate fallacy.[5]

Kommunikationstjenester med end-to-end kryptering

Antallet af interpersonelle kommunikationstjenester, som tilbyder brugerne end-to-end kryptering, vokser løbende. Formålet med end-to-end kryptering er at sikre, at kun afsender og modtager kan læse beskeden. Det beskytter brugerne mod overvågning, hvad enten der er tale om kommerciel

4 *A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal*, NY Times 21. august 2022 https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html

5 Se Wikipedias artikel om base rate fallacy (eksempel 3) https://en.wikipedia.org/wiki/Base_rate_fallacy

overvågning fra tjenesteudbyderen selv, kriminelle hackere med planer om afpresning eller identitetstyveri, eller statslige aktører som efterretningstjenester med adgang til tapning af kommunikationskabler. NSA's omfattende masseovervågning af privat kommunikation, som blev afsløret af whistlebloweren Edward Snowden i 2013, har givetvis bidraget til udbredelsen af end-to-end kryptering.

End-to-end kryptering er med andre ord en væsentlig sikkerhedsforanstaltning, som beskytter privat kommunikation og personoplysninger mod uautoriseret adgang og misbrug.

End-to-end kryptering betyder imidlertid også, at interpersonelle kommunikationstjenester ikke kan placere teknologier til opsporing på de centrale servere, som overfører brugernes kommunikation fra afsender til modtager. Når end-to-end kryptering beskytter mod tjenesteudbyderens kommercielle overvågning, beskytter teknologien selvsagt også mod udbyderens overvågning af andre årsager, herunder implementering af statsmagtens påbud om opsporing.

Selvom end-to-end kryptering altså reelt gør opsporing teknisk umuligt, er interpersonelle kommunikationstjenester med end-to-end kryptering alligevel omfattet af forordningsforslaget. Det fremgår direkte af præambelbetragtning nr. 26, som i øvrigt er det eneste sted i forordningsforslaget hvor kryptering nævnes. Under dække af at foranstaltninger i EU-lovgivning skal være teknologineutrale, vil påbud om opsporing blive udstedt uanset hvordan kommunikationstjenesten teknisk er indrettet. Hvis der bruges end-to-end kryptering, vil det være tjenesteudbyderens opgave at finde en måde hvorpå den private kommunikation alligevel kan overvåges trods end-to-end krypteringen, der ellers definitivt skulle beskytte mod en sådan overvågning.

Af Annex 9 i konsekvensanalysen kan man se hvordan Kommissionen forestiller sig, at tjenesteudbyderen skal "gøre det umulige" og overvåge end-to-end krypteret kommunikation: i stedet for at installere den statslige spyware på en central server, skal den installeres på brugernes telefoner eller computere, såkaldt client-side scanning.

Eksperter i kryptering og IT-sikkerhed betragter client-side scanning som en bagdør i kryptering på samme måde som de forslag om bagdøre, der var fremme i 1990'erne og som dengang blev opgivet efter voldsom offentlig kritik.[6] Eksperter i kryptering og IT-sikkerhed har fremsat en tilsvarende kritik af client-side scanning, blandt andet i artiklen *Bugs in our Pockets: The Risks of Client-Side Scanning* fra oktober 2021.[7] Selv om denne grundige analyse tager direkte udgangspunkt i Annex 9

6 Eksempelvis Key Escrow forslaget om nøgledeponering https://en.wikipedia.org/wiki/Key_escrow

7 Abelson et al, *Bugs in our Pockets: The Risks of Client-Side Scanning*, 14. oktober 2021 https://arxiv.org/abs/2110.07450

i konsekvensanalysen (som blev lækket at nyhedsmediet POLITICO i september 2020), har Kommissionen ikke fundet anledning til at kommentere kritikken. Annex 9 er ord-for-ord identisk med den version, som blev lækket af POLITICO i september 2020.

Det er også værd at fremhæve, at client side scanning alene eksisterer som et hypotetisk koncept i Kommissionens konsekvensanalyse (Annex 9). Ingen privat tjenesteudbyder har implementeret teknologi til client-side scanning. Apple lancerede i august 2021 planer om client-side scanning af billeder, der skulle uploades til iCloud med krypteret lagring. På grund af den voldsomme offentlige kritik fra eksperter i kryptering og IT-sikkerhed satte Apple planerne på hold efter blot en måned, og i december 2022 oplyste Apple, at planerne om client-side scanning var endegyldigt opgivet.[8]

Client-side scanning er en bagdør i krypteret kommunikation, som installeres direkte på brugernes telefoner eller computere. Client-side scanning opfylder også kriterierne for definitionen af spyware. Når denne spyware kan scanne kommunikation for kendt eller ukendt materiale med seksuelt misbrug af børn, eller analysere chat-samtaler for mulig hvervning af børn, kan den også senere udvides til at scanne for andre ting. Brugerne vil ikke have nogen mulighed for at opdage dette. De ved blot (i bedste fald) at deres kommunikation overvåges af private aktører på vegne af staten.

Denne risiko for ”mission creep” ignoreres fuldstændigt af forordningsforslaget. Dertil kommer den betydelige risiko for, at kriminelle hackere udnytter sårbarheder i den tvangsinstallerede software på brugernes telefoner til selv at skaffe sig adgang til brugernes private kommunikation. Det er i forvejen ganske svært at udvikle sikre IT-systemer, hvilket talrige eksempler på dårlig IT-sikkerhed dokumenterer. Hvis der samtidig er statslige krav om at indbygge sårbarheder som client-side scanning i IT-systemer, kan problemstillingen nemt gå fra ”svært” til ”helt umuligt”. Disse alvorlige konsekvenser for IT-sikkerheden ignoreres også fuldstændigt af Kommissionen.

Særlige konsekvenser for børns private kommunikation

Forordningsforslaget omfatter det indhold, som er defineret i artikel 2, litra c) og e) i direktiv 2011/93/EU om bekæmpelse af seksuelt misbrug og seksuel udnyttelse af børn og børnepornografi. Dette direktiv pålægger medlemsstaterne at kriminalisere navnlig fremstilling, anskaffelse, besiddelse og bevidst adgang til sådant materiale.

8 *Apple Kills Its Plan to Scan Your Photos for CSAM. Here's What's Next*, Wired 7. december 2022 https://www.wired.com/story/apple-photo-scanning-csam-communication-safety-messages/

Efter artikel 8 i direktivet kan medlemstaterne dog undlade kriminalisering for materiale, der involverer børn over den seksuelle lavalder, når dette materiale er fremstillet og besiddes med disse børns samtykke, og udelukkende anvendes til de involverede personers private brug, for så vidt handlingerne ikke involverer misbrug. Med denne undtagelse i direktivets artikel 8 kan børn over den seksuelle lavalder efter gensidigt samtykke lovligt besidde og udveksle seksuelle billeder med hinanden (f.eks. den udbredte praksis med "sexting"), uagtet at de samme billeder ville være kriminaliseret af direktivet, hvis de blev distribueret af andre personer.

Direktivets undtagelse for børn over den seksuelle lavalder, der varierer mellem 14 og 17 år i medlemsstaterne, er ikke medtaget i forordningsforslaget. Det betyder, at børns lovlige private kommunikation med seksuelle billeder er omfattet af forordningsforslaget bestemmelser, eksempelvis påbud om opsporing (artikel 7-11) og tjenesteudbydernes forpligtelse til at indberette materiale med seksuelt misbrug af børn (artikel 12). Indholdet af en chat-samtale mellem en 16-årig og en 17-årig kan eksempelvis opfylde kriterierne for at være "hvervning af børn", og den vil i så fald være omfattet af forordningsforslagets foranstaltninger (risikovurdering, risikobegrænsning, opsporing, indberetning, m.v.), uanset at der på ingen måde ikke er tale om seksuelt misbrug.

Opsporing vil medføre blokering af børns lovlige privat kommunikation og børnene vil blive indberettet til EU-centeret, som generelt vil videresende indberetningerne til Europol eller nationale politimyndigheder. Forordningsforslaget medfører naturligvis ikke kriminalisering af de nævnte aktiviteter (det hører fortsat under medlemsstaternes nationale lovgivning), men konsekvenserne for børn over den seksuelle lavalder kan alligevel blive ganske alvorlige på grund af indskrænkningen af rammerne for deres private kommunikation og deres udfoldelsesmuligheder på digitale tjenester.

Det er bemærkelsesværdigt, at børns private kommunikation i virkeligheden vil blive uforholdsmæssigt hårdt ramt af forordningsforslaget, når den erklærede hensigt med forslaget er at beskytte børn.

Forholdet til Charter om Grundlæggende Rettigheder

Den indledende begrundelse til forordningsforslaget indeholder en meget kortfattet og noget mangelfuld analyse af forholdet til Charter om Grundlæggende Rettigheder og EU-Domstolens retspraksis. Såvel begrundelsen som den 383-siders lange konsekvensanalyse omtaler alene præmis 126 i *La Quadrature du Net* dommen fra oktober 2020 (forenede sager C-511/18, C-512/18 og C-520/18). Ifølge præmis 126 kan der af Charteret udledes en vis positiv forpligtelse for bl.a. EU-lovgiver i forhold til bekæmpelse af strafbare handlinger mod mindreårige.

Kommissionen undlader derimod at nævne, at den samme dom i den efterfølgende præmis 127 kræver en afvejning mellem de omhandlede forskellige interesser og rettigheder. I besvarelsen af de præjudicielle spørgsmål i *La Quadrature du Net* dommen finder EU-Domstolen således, at formålet om bekæmpelse af seksuelt misbrug af børn ikke kan begrunde en generel og udifferentieret lagringspligt (”logning”) for alle trafikdata og lokaliseringsdata. Kun IP-adressen tildelt kilden til en kommunikation på internettet kan forlanges lagret på generel og udifferentieret basis (for alle brugere) med henblik på bekæmpelse af grov kriminalitet, herunder seksuelt misbrug af børn. På trods af dette bruger Kommissionen reelt *La Quadrature du Net* dommen som begrundelse for, at den generelle og udifferentierede overvågning af privat kommunikation ligger inden for rammerne af Charter om Grundlæggende Rettigheder.

La Quadrature du Net dommen behandler trafikdata og lokaliseringsdata, altså metadata for elektronisk kommunikation. Opsporing i forordningsforslagets artikel 7-11 er generel og udifferentieret overvågning af selve indholdet af kommunikationen. Ifølge præmis 94 i Schrems I dommen (C-362/14) skal ”*lovgivning, der gør det muligt for de offentlige myndigheder på generel vis at få adgang til indholdet af elektronisk kommunikation, anses for at udgøre et indgreb i det væsentligste indhold af den grundlæggende ret til respekt for privatlivet, således som denne er sikret ved chartrets artikel 7.*”

Efter Charteret artikel 52, stk. 1 skal alle indgreb i grundlæggende rettigheder respektere det væsentligste indhold af disse rettigheder. Det er stadig samme konklusion som med generel og udifferentieret overvågning af metadata, altså at det er i strid med Charteret.

Påvirkningen af det væsentligste indhold af den grundlæggende ret til privatliv fremhæves også i den fælles udtalelse fra EDPS og EDPB om forordningsforslaget.[9]

Påbud om spærring (artikel 16-18)

Artikel 16 giver mulighed for påbud, som pålægger en udbyder af internetadgangstjenester (”internetudbyder”) at spærre for adgangen til internetadresser med kendt materiale, der viser seksuelt misbrug af børn, identificeret via internetadresser registreret i EU-centrets database for indikatorer. Med formuleringen i artikel 36, stk. 1, litra b (”nøjagtige internetadresser med specifikt materiale”) må artikel 16 skulle forstås som en blokering på URL-niveau, altså specifikke undersider eller billeder i stedet for blokering af adgangen til hele websites.

9 EDPB-EDPS Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_en

Det er positivt, at muligheden for blokering af adgangen til indhold på internettet skal være målrettet specifikt indhold, som af kompetente myndigheder tidligere er vurderet til at være ulovligt, da det begrænser risikoen for overblokering af lovligt indhold (som ofte er et alvorligt problem, når adgangen til hele websites blokeres, eksempelvis med DNS-blokering). Det er også særdeles positivt, at adgangen til blokering via betingelsen i artikel 36, stk. 1, litra b kun gælder for indhold på websites som hostes uden for EU, og hvor udbyderen efter henvendelse fra myndigheder i EU nægter at fjerne indholdet (frivilligt).

Desværre ignorerer forordningsforslaget, at det vil være teknisk umuligt for internetudbydere at udføre blokering på URL-niveau, når adgangen til de pågældende websites sker via HTTPS. Det skyldes at den præcise internetadresse (URL'en) med HTTPS er krypteret i transmissionen mellem brugerens webbrowser og den webserver (website), som leverer indholdet. I den forbindelse skal det bemærkes, at stort set al web-trafik i dag bruger HTTPS, da det er best practice for sikkerhed på internettet.

For udbydere af interpersonelle kommunikationstjenester forestiller Kommissionen sig som bekendt, at udbyderen kan omgå tjenestens end-to-end kryptering med client-side scanning, jf. bemærkningerne ovenfor i dette høringssvar. Internetudbydere har ikke tekniske muligheder for at gøre noget tilsvarende, da adgangen til websites ikke sker via bestemte applikationer, som internetudbyderen kontrollerer og hypotetisk set kan forsyne med bagdøre til overvågning af besøgte URL'er på websites.

Som artikel 16, stk. 1 er formuleret kan adgangen til blokering ikke uden videre udstrækkes til blokering af hele websites, hvilket med end-to-end kryptering er den eneste tekniske mulighed for blokering hos internetudbydere. Påbuddet om blokering gælder for alle internetadresser registreret i EU-centrets database med indikatorer, hvis materialet vel at mærke hostes uden for EU. En blokering på domæne-niveau (hele websites) vil i hvert enkelt tilfælde som minimum forudsætte en proportionalitetsvurdering, der blandt andet inddrager omfanget af lovligt indhold som blokeres.