Elektronisk Forpost Norge
Medlem av EDRi, European Digital Rights

Justis- og beredskapsdepartementet
Via departementets høringsportal

10. februar 2023

Høringssvar - EU/EØS. Forslag til forordning for å forebygge og bekjempe seksuelle overgrep mot barn

Dette høringssvaret utgjør en mer sammenfattet versjon av det omfattende høringssvaret som er inngitt av EDRi - vår paraplyorganisasjon.

Med vennlig hilsen

Tom Fredrik Blenning
Daglig leder - EFN

Elektronisk Forpost Norge
Pb 27 Vålerenga, 0626 OSLO E-Post: horing@efn.no Tlf. 996 24 544

Elektronisk Forpost Norge

Et trygt internett for alle: Bevar privat og sikker kommunikasjon

Det er ikke bare voksne som har rett til privat kommunikasjon, men barn også. En bekymring som stort sett har blitt ignorert av Kommisjonens forslag.

I mars 2022, la EU-Kommisjonen frem et forslag til en lov som vil pålegge online tjenestetilbydere spesifikke mottiltak mot spredning av overgrepsmateriale mot barn (Child Sexual Abuse Material – CSAM) og online grooming.[1] Hvis loven blir vedtatt vil den ha virkning for nær sagt all digital kommunikasjon fra chattetjenester, sosiale medier, til skytjenester, app stores og til og med SMS, telefonsamtaler og infrastrukturtjenester på Internett. Noen regjeringer ønsker også å legge til søkemotorer.

Siden 2002, har det vært etablert EU-lov at disse online kommunikajons- og tjeneste-tilbyderne ikke kan tvinges til å vite innholdet i brukernes meldinger, samtaler, fotoopplastinger og annet personlig innhold. Dette er et bærende prinsipp i et demokratisk samfunn, at det personvernet vi er vant med offline også skal gjelde online. Akkurat som politiet ikke kan ransake huset ditt uten gå gjennom den digitale versjonen av ditt indre private liv, uten en spesifikk, individuell begrunnelse for å anta at du har gjort noe som tilsier det.

Personvern er ikke et abstrakt konsept eller en uønsket barriere, men en grunnleggende menneskerett. I hele verden er lover og verktøy som beskytter personvernet livsviktige for at journalister trygt kan rapportere om korrupsjon, menneskerettighetsaktivister kan holde makten til ansvar, at sivile kan flykter fra undertrykkende regimer, at LGBT+ kan uttrykke seg fritt, at mennesker fritt kan praktisere sin religion, ha adgang til helsehjelp og at demokratiet kan leve frem.

For å sitere European Data Protection Board and Supervisor, the proposed CSAR is likely to do great harm to regular people, with a very limited impact on stopping perpetrators of this terrible

1 ‘Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse’ (2022/0155 COD), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN

crime.[2] EFN har sammen med 118 (og flere kommer til hele tiden) andre organisasjoner bedt EU-kommisjonen om å trekke forslaget.[3] Vi ber om at EU-parlamentet og EUs medlemsstater forkaster forslaget, basert på vår analyse som har vist at:[4]

- Deteksjonsordrer kan ikke målrettes tilstrekkelig, og vil i stedet vanligvis kreve gjenomgripende skanning av privat digital kommunikasjon, noe som innebærer masseovervåking og kan i faretruende grad undergrave kryptering. Ingen mengde innovasjon eller teknologisk utvikling kan endre dette, da det er et grunnleggende trekk ved hvordan deteksjonsteknologier fungerer
- Det er sannsynlig at dersom de blir vedtatt, vil de inngripende skanningsforpliktelsene som følger av deteksjonsordre, anses som ulovlig generell overvåking av EU-domstolen
- Risikovurdering og avbøtende tiltak vil i stor grad stimulere til bruk av såkalte «opplastingsfiltre», som kan muliggjøre digital sensur og undertrykke ytringsfrihet
- Disse risikotiltakene vil også kreve utstrakt bruk av metoder for aldersverifisering som kan sette personopplysninger til barn og voksne i fare, forverre sosial ekskludering og eliminere muligheten for anonymitet på nettet
- Som et resultat vil CSAR sannsynligvis både undergrave og skape regulatorisk overlapp med Digital Services Act (DSA). Det er også sannsynlig at det vil krenke personvernet, databeskyttelsen og retten til ytringsfrihet for potensielt hele den europeiske befolkningen i uforholdsmessig grad, i strid med charteret om grunnleggende rettigheter
- Den foreslåtte modellen vil være tungvinn, mangler bevis for påstått effektivitet, og kan til og med virke mot sin hensikt når det gjelder å nå sine uttalte mål om å beskytte barn
- De teknologiske metodene som kreves for å implementere CSAR vil føre til store mengder falske alarmer, noe som gjør det vanskeligere å etterforske faktiske tilfeller av CSA, samtidig som enhetene som eies og brukes av ungdom og andre uskyldige internettbrukere utsettes for en økt risiko
- Et bærekraftig alternativ til CSAR er å fokusere på rask fjerning av CSAM fra internett. Dette ville være bedre oppnådd ved en kombinasjon av:
  - Sterk og effektiv implementering av DSA-varsel og handling
  - Oppretting av forpliktelser på plattformer og tjenester for å sikre at brukere alltid kan rapportere CSAM på måter som er både barnevennlige og effektive
  - Ved å gi et rettslig grunnlag til og øke investeringene i nasjonale barneverntelefoner, samt å dramatisk øke bevisstheten om deres eksistens og hvordan de kan få tilgang til dem

2 EDPB and EDPS Joint Opinion on the CSAR: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_hu

3 The call from civil society groups to withdraw the CSAR: https://edri.org/our-work/european-commission-must-uphold-privacy-security-and-free-expression-by-withdrawing-new-law/

4 EDRi's fulle position paper: https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-CSAR.pdf

- Slike tiltak må underbygges av meningsfulle samfunnsendringer, reformer av strafferettslige institusjoner, utdanning og en langt større investering i primær forebygging av CSA.

Innholdsfortegnelse

Elektronisk Forpost Norge

1. Hva ville endret seg sammenlignet med i dag som følge av CSAR?

Idag eksisterer det en midlertidig EU-lov i som tillater digitale kommunikasjonstjenester å skanne privat kommunikasjon mellom brukerne deres basert på deres tjenestevilkår.[5] Denne loven har blitt kritisert av sivilsamfunnet og lovgivere for sannsynligvis å være i konflikt med GDPR og for å oppmuntre til generell overvåking av folks kommunikasjon. Den har også blitt kritisert for å ikke oppfylle sentrale menneskerettighetsstandarder, for å være fullstendig ugjennomsiktig og for å gi for mye skjønn til private selskaper.

EU-kommisjonen har medgitt at det er nødvendig å erstatte denne problematiske midlertidige loven med en langsiktig lov. Til tross for offentlige påstander fra Kommisjonen om at hvis den nye loven ikke blir vedtatt innen 2024, vil barn stå uten beskyttelse, er dette rett og slett ikke sant. Det viktigste er at Digital Services Act (DSA) nå har trådt i kraft, og vil bli fullt operativ tidlig i 2024. Denne nye loven skaper et bredt spekter av metoder for å håndtere ulovlig innhold på nett, inkludert CSAM. Kommisjonen har også skriftlig bekreftet at hvis de måtte, kunne de forlenge den midlertidige loven. En kunstig følelse av at det haster, hjelper derfor ingen: barn er avhengige av at EU-lovgivere tar tilstrekkelig tid og omsorg for å finne måter å beskytte dem på som er trygge, effektive og lovlige. Det er lite sannsynlig at den foreslåtte CSAR oppfyller noen av disse tre kriteriene.

En av hovedendringene fra den midlertidige loven til CSAR er at den foreslåtte nye ordningen er obligatorisk. Risikovurdering og avbøtende tiltak vil i stor grad være universelle, mens krav til skanning vil gjelde først etter utstedelse av en deteksjonsordre.

Det betyr at mens leverandører tidligere kunne velge om de ville skanne innhold eller ikke, kunne de nå bli tvunget til å gjøre det, selv om det ville kreve at de nedgraderte sikkerheten til tjenesten deres for å gjøre dette mulig, samt bryte tilliten til brukerne deres. Som et resultat vil den største endringen fra i dag være at potensielt enhver tjeneste eller plattform som opererer i EU kan bli tvunget til å overvåke og skanne innholdet i hele brukernes digitale liv.

5 https://edri.org/our-work/a-beginners-guide-to-eu-rules-on-scanning-private-communications-part-1/

Elektronisk Forpost Norge

2. Hva er de viktigste nye reglene i CSAR?

Flere av de foreslåtte nye reglene i CSAR har dype implikasjoner for menneskerettighetene og den alle internettbrukeres digtale sikkerhet – ikke minst unge mennesker, som i økende grad stoler på internett for å kommunisere med venner, bygge fellesskap, koble til for aktivisme så vel som for utdanning og tilgang til mange ulike tjenester.

2.1 Risikovurdering og redusering (artikkel 3 og 4)

Artikkel 3 og 4 i CSAR krever at praktisk talt alle digitale eller nettbaserte plattformer eller tjenester identifiserer og reduserer risikoen for at CSAM blir utvekslet, eller at barn blir groomet, på deres plattform eller tjeneste. Dette betyr at leverandører må vite hva som blir sagt eller delt på deres plattform eller tjeneste til enhver tid, selv om det betyr systematisk overvåking av brukernes innhold. Dessuten vil plattformene eller tjenestene fortsatt anses som "betydelig" risikable med mindre de kan vise at utveksling av CSAM og forekomster av grooming er eliminert "utover isolerte og relativt sjeldne forekomster" (betraktning 21).

Disse tiltakene vil kreve at private selskaper tar en statslignende rolle i å avgjøre hvilket innhold som er akseptabelt og hva som ikke er det. Dette vil også sterkt motivere tilbydere til å treffe de mest inngripende tiltakene som er mulig for å unngå en deteksjonsordre. Skanning av offentlig kommunikasjon (noen ganger referert til som "opplastingsfiltre") og mange tilfeller av overfjerning av legitimt innhold vil derfor bli normen. Disse filtrene er notorisk defekte, noe som er et problem på grunn av hvor alvorlig en falsk påstand om CSA kan være. Opplastingsfiltre har også vært knyttet til en alvorlig innblanding i ytringsfriheten og tilgangen til kunnskap, og har en høy risiko for å bli brukt i sensur og undertrykkelse.

Dessuten kan tilgang til praktisk talt alle nettbaserte plattformer og tjenester bli betinget av å bevise alderen din. Dette kan ha store konsekvenser for ytringsfrihet og databeskyttelsesrettigheter, samt hindre tilgang til sosiale, økonomiske og politiske rettigheter. De tre hovedmetodene for aldersverifisering som for tiden eksisterer er:

- **Kreve at brukere laster opp et identitetsdokument, for eksempel en passkanning.** En slik ordning ville gjøre anonymitet på nett umulig, noe som kan sette alle fra journalister til varslere til sexarbeidere i fare, og ekskludere de uten formell ID
- **Implementere et omfattende digitalt identitetssystem.** Digitale identitetssystemer risikerer ytterligere å marginalisere mennesker som allerede står overfor høye nivåer av sosial ekskludering, som papirløse, hjemløse, romsamfunn og eldre. EU jobber for tiden med en digital identitetsordning (eID), og sivilsamfunnet har reist alvorlige bekymringer om

planene om å bruke dette systemet også for overvåkingsannonsering, det faktum at det foreløpig ikke er noen garantier for at dette systemet vil respektere personvernet, og det faktum at minst 20 % av EUs befolkning er spådd å bli ekskludert fra ordningen

- **Bruk av ansiktsgjenkjenning eller annen algoritmisk profilering for å forutsi brukernes alder.** Disse systemene er notorisk unøyaktige, spesielt for personer med farger og personer med ansiktsforskjeller. Per definisjon vil slike metoder også rutinemessig behandle de utrolig sensitive biometriske dataene til unge mennesker. Mange av disse systemene brukes allerede i kommersielle sammenhenger, og drar nytte av dataene de samler inn. Til tross for disse risikoene og overgrepene, blir det mer og mer vanlig at beslutningstakere oppmuntrer til bruk, uten å ta hensyn til den systemiske brudd på barns rettigheter som bruken medfører.

Elektronisk Forpost Norge

2.2 Deteksjonsordrer (artikkel 7–11)

Artikkel 7-11 i CSAR fastsetter reglene for hvordan nasjonale koordinatorer kan be om rettslig eller administrativ autorisasjon for å tvinge tilbydere til å skanne («oppdage») brukernes meldinger eller annet innhold. Det er tre typer innhold de kan bli bedt om å skanne etter:

- **Kjent CSAM**, vanligvis bilder eller videoer som tidligere er rapportert, gjennomgått og deretter lagt inn i en database. Dette blir noen ganger referert til som en 'hash-database' eller 'hash-matching' fordi skannet innhold sammenlignes med en referanse ('hash') til kjent CSAM. Selv om skaperne av disse databasene og skanneteknologiene hevder at de er svært nøyaktige, har det ikke vært noen uavhengig verifisering av dette, og forskning viser at hashen kan snus for å avsløre det originale misbruksbildet[6]
- **Ny CSAM**, altså bilder som ikke tidligere har blitt rapportert som CSAM eller lagt i en hash-database. Dette krever bruk av kunstig intelligens (AI)-baserte teknologier, som kan trenes til å se etter "indikatorer" (f.eks. forutsi om et bilde viser bar hud). Dette betyr at slike verktøy aldri vil flagge bare CSAM, men vil flagge alt materiale som passer søkekriteriene selv om det er aldri så uskyldig.
- **Grooming**, som betyr tekst, lyd eller atferd som kan indikere at noen groomer et barn. Igjen, dette krever bruk av AI-baserte teknologier for å se etter mønstre eller andre påståtte "indikatorer" på grooming.

Deteksjonsordrer er den elektroniske ekvivalenten til å plassere en opptaksenhet i hjem over hele EU, og deretter bruke AI-baserte verktøy for å forutsi om lyd- eller videoinnhold kan indikere seksuelle overgrep mot barn. Til tross for CSARs forsøk på å bruke deteksjonsordrer kun under spesifikke omstendigheter, er det umulig å målrette disse verktøyene kun mot mistenkte. Det er fordi når det gjelder privat kommunikasjon, kan du ikke vite hvem som er mistenkt før alles innhold først er skannet.

Den foreslåtte CSA-forordningen krever at disse ordrene skal være "målrettet" når det gjelder innhold og teknologier, men ikke i beskyttelsestiltak eller omfang. Dette betyr at deteksjonsordrer nesten alltid vil måtte skanne det legitime innholdet til lovlige internettbrukere, i stedet for å være spesifikt rettet mot kun de brukerne der det er skjellig grunn til å mistenke for ulovlig oppførsel. **Som et resultat er det sannsynlig at forslaget vil utgjøre en generell overvåkingsplikt, som EU-domstolen gjentatte ganger har slått fast er ulovlig.**[7]

6 https://gangw.cs.illinois.edu/PHashing.pdf

7 Forbudet mot generelle overvåkingsplikter er tydelig hevdet i ePrivcay-direktivet (2002) og loven om digitale tjenester (2022). Det har også blitt forsterket i dommer fra EU-domstolen, for eksempel La Quadrature du Net og andre (forenede saker C-511/18, C-512/18 og C-520/18), Schrems I (C -362/14), Digital Rights Ireland (forenede saker C-293/12 og C-594/12) og Polen mot parlamentet og råd (C-401/19)

Selv om en slik tilnærming til masseovervåking vil føre til at enkelte tilfeller av CSA blir flagget, blir den uakseptable invasjonen av folks privatliv gjort veldig tydelig av analogien på hjemmeopptaksenheten.

Dessuten vil det store flertallet av det disse skannesystemene fanger opp, være falske alarmer, spesielt for ukjent CSAM og stell. Dette er fordi ved mengden materiale som skannes, vil selv svært nøyaktige teknologier fange opp mye legitimt innhold i deres brede nett. Dette vil gjøre det å finne faktiske tilfeller av CSA som å finne nåla i høystakken, noe som gjør det sannsynlig at myndighetene – som allerede er overbelastet og lider under mangel på ressurser – vil ha mindre kapasitet til å beskytte ofre og straffe gjerningsmenn.

Det er også et problem her med hva som menes med ‘nøyaktighet’. Skanneteknologier kan justeres til å være svært nøyaktige når det gjelder å oppdage hud, for eksempel. Det betyr ikke at de er svært nøyaktige til å oppdage CSAM: bilder som inneholder hud kan være et bilde av en 20-åring i en badedrakt, eller et nærbilde av en tenårings arm. CSAR-forslaget hevder at en fremtredende skanneteknologi, 'PhotoDNA', er svært nøyaktig. Men når de ble brukt av nettverksplattformen LinkedIn, utgjorde bare 41 % av bildene som ble flagget av PhotoDNA i 2021 faktisk CSAM i henhold til EU-lovgivningen.[8]

Når det gjelder å oppdage ny CSAM og grooming , er dette avhengig av bruk av kunstig intelligens (AI) teknologier som maskinlæring. Det er ikke et spørsmål om at teknologien kan bli bedre over tid. Det er det faktum at hva som utgjør CSAM eller grooming kan være svært avhengig av kontekst. For eksempel avkriminaliserer flere EU-land deling av seksuelle bilder mellom samtykkende tenåringer, men et AI-basert verktøy kan ikke vite forskjellen mellom disse ulike nasjonale juridiske rammeverkene.

Kontekst er avgjørende for å skille mellom ulovlig CSA og legitimt uttrykk, og maskinlæringsteknologi kan ikke forstå kontekst, siden den ikke har noen sunn fornuft eller selvstendig vurderingsevne.

8 https://edri.org/our-work/internal-documents-revealed-the-worst-for-private-communications-in-the-eu-how-will-the-commissioners-respond/

Elektronisk Forpost Norge

2.3 Blokkeringsordre (artikkel 16–18)

Artikkel 16–18 i CSAR tillater myndighetene å tvinge internettilgangsleverandører til å blokkere tilgang til en URL (webside), for eksempel fordi et nettsted utenfor EU er vert for CSAM, noe som betyr at EU ikke har makt til å kreve innholdets fjerning. Et stort problem med blokkeringsordrer er at det rett og slett ikke er mulig for de fleste internettilgangsleverandører å blokkere en bestemt URL. De har ikke tilgang på URL-nivå, kun hele nettsiden (domenet).

Dette betyr at, for eksempel, hvis bare én side på et stort nettsted som Reddit ble funnet å inneholde CSAM, kan EU tvinge internettilgangsleverandører til å blokkere tilgang til hver enkelt Reddit-side, for hver person i EU. Dette vil representere en alvorlig og definitivt uforholdsmessig inngrep i ytringsfriheten og retten til tilgang til informasjon.

Elektronisk Forpost Norge

3. Hvordan vil kryptering bli påvirket?

CSAR er ikke et teknologinøytralt forslag. Selv om den ikke krever spesifikke teknologier som leverandører må bruke for å overholde loven (dette vil bli overlatt til en liste administrert av EU Center), er det visse teknologier som uunngåelig vil bli brukt eller påvirket.

Den mest fremtredende teknologien som vil bli påvirket er kryptering. Ved å ikke ha unntak fra deteksjonsordrer for ende-til-ende-krypterte (E2EE) tjenester, kan leverandører av sikre meldingstjenester bli tvunget til å skanne innholdet til brukerne sine, i strid med deres forpliktelse til å respektere brukernes personvern. Dette er teknisk veldig forskjellig fra eksisterende skanningspraksis for for eksempel "skadelig programvare", som ikke påvirker innholdet eller integriteten til disse E2EE-tjenestene. Det er derfor unøyaktig å sammenligne disse fremgangsmåtene med skanningen som ville kreves av en deteksjonsordre.

Angående, CSAR forklarer at kryptering av kommunikasjon er en av faktorene som mest sannsynlig gjør at en tjeneste anses som risikabel (og derfor sannsynligvis vil motta en deteksjonsordre). Det er forutsigbart at under CSAR vil de fleste E2EE-tjenester (som FNs høykommissær for menneskerettigheter minner oss om er et viktig menneskerettighetsverktøy)[9] enten måtte forlate EU, eller møte en deteksjonsordre.

Å overholde en deteksjonsordre er teknisk sett ikke mulig uten å undergrave sikkerheten og grunnleggende forutsetninger for en E2EE-tjeneste, noe som betyr at CSAR klart vil undergrave kryptering. Alle for tiden kjente metoder for å gjøre dette vil kreve enten å svekke krypteringen direkte, eller introdusere "Client-Side Scanning" (CSS), som har blitt kraftig kritisert av nettsikkerhets- og menneskerettighetssamfunnet for å gjøre folks enheter sårbare for ondsinnede aktører, som så vel som til manipulasjon.[10] EU-kommisjonens konsekvensutredning til CSAR anerkjenner at selv toppmoderne metoder har i beste fall lavt-middels nivå av personvern og sikkerhet, og aldri har vært vellykket implementert i stor skala.

Selv om en sikrere og sikrere teknikk enn CSS ble oppdaget i fremtiden, ville dette ikke overvinne det faktum at enhver deteksjonsmetode som er rullet ut i E2EE-miljøer, er fundamentalt uforenlig med poenget og formålet med E2EE. Dette er fordi det ville bringe en tredjepart inn i en kommunikasjon som er ment å være kun mellom avsender og mottaker. Denne forpliktelsen til personvern er det som sikrer at menneskerettighetsforkjempere, politikere, advokater, personer som

9 https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report

10 https://arxiv.org/abs/2110.07450; https://privacyinternational.org/sites/default/files/2022-09/SECURING%20PRIVACY%20-%20PI%20on%20End-to-End%20Encryption.pdf

søker reproduktiv helsetjenester, aktivister, mennesker som lever under autoritære regimer og mange andre kan stole på E2EE-tjenester for å være trygge.

Dessuten vil denne tredjeparten være forpliktet til å henvise ethvert innhold som gjenkjenningsverktøyene forutsier som CSAM eller grooming til politiet, inkludert uunngåelig store mengder lovlig og legitimt innhold.

Et sentralt aspekt er at det finnes ingen ingen måte å slå E2EE på og av for enkelte brukere. Som et resultat av en deteksjonsordre gitt til en ende-til-ende-kryptert tjeneste, vil alle som benytter og stoler på den aktuelle tjenesten få sitt personvern og sikkerhet kompromittert. Dette er uunngåelig da det er en teknisk funksjon for å sikre sikkerheten til E2EE. Dette vil derfor også ha en innvirkning på den plattformen eller tjenestens brukere utenfor EU.

En hver enhet som er underlagt CSS vil bli gjort teknisk mye mer sårbar for angrep og hacking av et bredt spektrum av ondsinnede aktører.

Elektronisk Forpost Norge

4. Forskjellen mellom effektivitet og effisiens.

Utover de teknologiske begrensningene til metodene som kreves for å oppfylle forpliktelser i henhold til CSAR, er det flere prosedyremessige årsaker til at det er usannsynlig at det er effektivt:

- Mesteparten av håndhevelsen av forslaget vil falle til Irland og Nederland, ettersom de fleste av EUs digitale tjenester er registrert i disse to territoriene. Med etterslep i GDPR-håndhevelsen som allerede strekker seg over flere år, vil det å opprette den samme prosessen for CSA skape alvorlige forsinkelser som vi ikke kan anse som akseptable når barns sikkerhet er i fare
- Desentraliserte modeller for fjerning av innhold – for eksempel av nasjonale hotlines eller av pålitelige varslere under DSAs fremtidige varsel- og handlingsmekanisme – anses som beste praksis for raskt å fjerne CSAM. Rask fjerning er allment akseptert som beste praksis for å forhindre CSA-overlevende fra å bli gjenopprettet av videre deling av bilder. Derimot viser en studie på sentraliserte modeller (som er hva EU-senteret ville være) at de kan legge til opptil 6 uker til tiden det tar å fjerne CSAM fra internett.[11] Dette betyr at CSAR med stor sannsynlighet ikke er den mest effektive måten å nå hovedmålet om å stoppe videre spredning av CSAM på nettet
- CSAR krever at hvert stykke mistenkt CSAM som ikke er "åpenbart ubegrunnet" (for eksempel et bilde av en kattunge som feilaktig har blitt flagget som CSAM) skal rapporteres til nasjonalt politi for etterforskning. Gitt den høye sannsynligheten for at mye av det rapporterte innholdet faktisk vil være lovlig og legitimt innhold, vil det være en enorm sløsing med allerede begrensede politiressurser å måtte etterforske hver gang en tenåring med samtykke sender en toppløs selfie eller en forelder sender et strandbilde til barnets besteforeldre
- Nederlands politikommisær har bekreftet at nederlandsk politi ikke vil være i stand til å håndtere mengden pleierapporter som de forventer å motta som følge av CSAR og en senior tysk politimann med ansvar for å etterforske CSA sa på samme måte at "chatkontroll" ikke vil hjelpe til med å finne flere gjerningsmenn, bare flere falske alarmer. Dette viser at selv rettsvesenets representanter i frontlinjene ikke ser at CSAR er sannsynlig å hjelpe i kampen mot CSA.[12]

11 https://www.lightbluetouchpaper.org/2022/05/11/european-commission-prefers-breaking-privacy-to-protecting-kids/

12 https://debatgemist.tweedekamer.nl/node/29579; https://www.deutschlandfunk.de/strafverfolgung-sexueller-kindesmissbrauch-datenschutz-100.html

5. Hvordan vil legitime internettbrukere bli påvirket?

De fleste bruker internett av legitime, lovlige og viktige grunner: arbeid, kommunikasjon med familie, lagring av kjære bilder, chatte med partneren, bygge fellesskap, rettferdighet, søke informasjon, holde kontakt med venner, gi eller få tilgang til helsetjenester, mobilisering for sosiale endre seg, uttrykke seg og mer.

Det faktum at et mindretall av brukere misbruker digitale kanaler til lovstridige og skadelige formål betyr ikke at enhver person rutinemessig skal behandles som mistenkelig, ettersom EU-lovgivningen i likhet med lovgivningen i alle «siviliserte» land fastslår at uskyldspresumpsjonen skal være et bærende prinsipp i rettsstaten.

Barnevernsgrupper forklarer at fremmede på nett ikke er den viktigste profilen til CSA-gjerningsmenn: «Selv om vanlige oppfatninger har en tendens til å ramme seksuelle overgrep både online og offline i form av 'fremmed fare', står barn i realiteten oftere overfor risikoen for skade fra mennesker innenfor deres nære relasjoner.»[13] CSARs foreslåtte generelle nettbaserte overvåkingsmodell er derfor ikke bare feiljustert i forhold til de viktigste måtene CSA er forpliktet på i virkeligheten, men vil også ha uforholdsmessige konsekvenser for allmennheten:

- Vi ser allerede at uskyldige mennesker blir utestengt fra sine digitale liv som et resultat av skanningsteknologier som feilaktig hevder at de har spredt CSAM. Det kommer flere og flere rapporter om at folk mister hvert eneste bilde de noen gang har lastet opp til skyen, og blir permanent utestengt fra e-postkontoene og passordbehandlerne deres, med stor innvirkning på deres evne til å jobbe, kommunisere og engasjere seg i det digitale livet. Anekdotiske rapporter antyder enda alvorligere konsekvenser for andre mennesker på grunnlag av falske anklager, inkludert tap av jobber, tap av familier og selvmord av de som er falskt anklaget
- Vår fullstendige rapport avslører at i Irland har hundrevis av mennesker fått dataene sine oppbevart av politiet (noe som sannsynligvis er ulovlig) til tross for at de har blitt konstatert fri for CSA-kriminalitet. Det disse menneskene hadde delt var faktisk legitimt innhold: dette inkluderte familiebilder av barna deres som lekte på stranden og seksuelle bilder mellom voksne.
- De alvorlige konsekvensene av generell overvåking blir ofte referert til som «nedkjølende effekt». Bare det å vite at samtalene, e-postene og opplastingene dine kan bli systematisk overvåket, kan undertrykke folks rettigheter til å uttrykke seg, til å søke informasjon og til å samles og assosiere fritt (for eksempel å delta i politiske aktiviteter eller aktivisme)

13 https://ecpat.org/wp-content/uploads/2022/01/05-01-2022_Project-Report_EN_FINAL.pdf

- I land som mangler en sterk rettsstat kan også risikoen for misbruk og såkalt «scope creep» være høy. For eksempel kan «opplastingsfiltre» brukes på nytt for å oppsøke legitimt innhold (som bevis på politisk dissidens, kritisk journalistikk eller folk som søker etter reproduktiv helsetjeneste)
- Internett er globalt. Ved å undergrave digitalt personvern, sikkerhet og sikkerhet i EU, kan CSAR oppmuntre tilbydere til også å svekke sikkerheten og øke overvåkingen for sine brukere over hele verden. Det er også et faktum at ved å gi et carte blanche til slike overvåkingsmetoder, gir EU et signal til land rundt om i verden om at disse tiltakene er akseptable.

Elektronisk Forpost Norge

6. Hva med barns rettigheter?

Internasjonal og europeisk lov pålegger stater forpliktelser til å beskytte barn mot seksuelle overgrep, en forferdelig forbrytelse som krenker flere av barns grunnleggende rettigheter. Lanzarote-konvensjonen krever at barns beste må være et primært hensyn. Dette betyr imidlertid ikke at ethvert tiltak for å beskytte barn automatisk vil være akseptabelt.

Mange av argumentene til fordel for CSAR har fremhevet alvorlighetsgraden av CSA. Alvorligheten av slike overgrep er et argument for at samfunnet må etabler mekanismer for å beskytte barn, men det betyr på ingen måte at CSAR nødvendigvis er en forholdsmessig, riktig eller effektiv strategi. Tiltak for å verne barn, også når de er sentrale for å minimalisere overgrep, må fortsatt være nødvendige og forholdsmessige tiltak i et demokratisk samfunn.[14]

Barnekonvensjonen krever også at regjeringer vurderer barns synspunkter og ønsker samt potensielle konsekvenser for deres rettigheter og friheter. FN, UNICEF og Child Rights International Network (CRIN) understreker alle at masseovervåking av barn kan være skadelig for deres utvikling og selvutfoldelse.[15] Vår analyse har vist at denne risikoen kan være spesielt høy for LHBTQI+-ungdom, som vil finne at den legitime utforskningen av deres seksuelle selvidentitet blir behandlet som om det er kriminell oppførsel.

CRIN legger til at den mest effektive nettsikkerhetsmekanismen er å sikre bemyndigede, motstandsdyktige unge mennesker som føler seg trygge på å si fra når noe gjør dem bekymret.[16] Flere overlevende fra CSA peker også på viktigheten av personvern på nettet for å søke hjelp og bygge en følelse av samfunn og håp.[17] Dette kan utryddes av CSAR, som risikerer å flagge overlevende som stoler på andre som CSAM, og fjerne enhver følelse av trygge rom takket være den konstante trusselen om overvåking. De utvilsomt meget store og alvorlige ringvirkninger av et høyt kontrollnivå hinsides forholdsmessighet vil svekke tryggheten og tilliten i samfunnet og hos individer, og dermed med til visshet grensende sannsynlighet øke sårbarheten overfor overgripere som bevisst jakter på usikre og sårbare individer. Usikkerhet og sårbarhet går hånd i hånd. Overvåkningssamfunnet der privatlivet undermineres av uforholdsmessige tiltak gir derfor dårlige kår for den individuelle robusthet som er en forutsetning for den sentrale grensesettingen.

---

14 Dette er spesielt tilfelle gitt at CSAR legger forpliktelser til private selskaper og enkeltpersoner. Dette betyr at forpliktelsene er "positive" forpliktelser for å beskytte barn mot skade, som ikke er absolutte (som betyr at staten ikke kan gjøre noe for enhver pris for å oppnå denne forpliktelsen), sammenlignet med "negative forpliktelser" som er absolutte (f.eks. staten kan aldri misbruk barn).

15 Se særlig https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC%2FC%2FGC%2F25&Lang=en

16 https://home.crin.org/issues/digital-rights/childrens-right-digital-age?rq=digital%20age

17 https://www.linkedin.com/pulse/why-i-dont-support-privacy-invasive-measures-tackle-child-hanff

Elektronisk Forpost Norge

7. Hva anbefaler vi i stedet?

Vi ber om at ressurser og tiltak rettes mot de individer som bruker noen metoder – digitale eller andre – for å utføre, tilrettelegge eller distribuere CSA. Dette kan inkludere genuint målrettede, lovlige tiltak for å etterforske minoriteten av brukere som misbruker krypterte tjenester for å begå CSA og andre alvorlige forbrytelser.[18] USAs hotline mot menneskehandel advarer om at kryptering ikke bør sees på som en "boogeyman" og at fokus i stedet må være på den underliggende praksisen der menneskehandlere og overgripere utnytter sårbare individer eller samfunn.[19]

Genuin, konstruktiv endring krever politisk forpliktelse til og investering i å etablere et samfunn som behandler overlevende med verdighet, som letter rask tilgang til rettferdighet, som nekter å se bort når det er mistanke om overgrep, som tilbyr psykisk helsestøtte til de som arbeider med CSA-saker og CSAM i enhver kapasitet, og som prioriterer forskning på forebygging for å øke bevisstgjøringen både hos potensielle ofre og potensielle overgripere. Slik kan CSA-kriminalitet reduseres til et minimum.

Langt mindre innvaderende, og sannsynligvis mer effektive og effektive metoder for å takle CSA både offline og online, inkluderer følgende (og kan også implementeres mye tidligere enn CSAR, og er derfor også i de overlevendes beste):

- Prioritere implementeringen av Digital Service Act (DSA) mekanismer for fjerning (varsel og handling) for ulovlig innhold, inkludert riktig utrustning av pålitelige flaggere
- Sikre at alle plattformer og tjenester i EU har en tydelig, tilgjengelig og barnevennlig måte for mistenkt CSAM å rapporteres på, og at responsteamene har tilstrekkelige ressurser til å kunne undersøke sakene på en rask og effektiv måte

18 Sitat fra Polaris (USAs nasjonale hotline mot menneskehandel): “The debate is not around whether or not encryption is good or bad. It’s about how are traffickers exploiting vulnerabilities of vulnerable communities, and where are they doing that, and how do we actually get ahead of that vulnerability and meet that need. I think there’s oftentimes a bit of a boogeyman made around emerging technologies. Technology is just a tool in which [crime] happens, but the underlying mechanisms need to be understood at its very core.” Rajan said that she believes encryption is part of a “human rights toolkit” that can protect and empower victims. She posed the question: “How do we prevent abuse of these technologies rather than passing a broad, sweeping critique of a tool?” Tilgjengelig på: https://www.cnbc.com/2022/06/10/wickr-amazons-encrypted-chat-app-has-a-child-sex-abuse-problem.html

19 Sitat fra Polaris (USAs nasjonale hotline mot menneskehandel): “The debate is not around whether or not encryption is good or bad. It’s about how are traffickers exploiting vulnerabilities of vulnerable communities, and where are they doing that, and how do we actually get ahead of that vulnerability and meet that need. I think there’s oftentimes a bit of a boogeyman made around emerging technologies. Technology is just a tool in which [crime] happens, but the underlying mechanisms need to be understood at its very core.” Rajan said that she believes encryption is part of a “human rights toolkit” that can protect and empower victims. She posed the question: “How do we prevent abuse of these technologies rather than passing a broad, sweeping critique of a tool?” Tilgjengelig på: https://www.cnbc.com/2022/06/10/wickr-amazons-encrypted-chat-app-has-a-child-sex-abuse-problem.html

- Investere i og gi et klart juridisk grunnlag til velprøvde tjenester som nasjonale telefonlinjer, samt sørge for at barn og unge er kjent med hva disse telefonnummerne er, hvordan de kan hjelpe dem og hvordan de kan ta kontakt
- Iverksette ambisiøse sosiale reformer, inkludert styrking av velferd, tiltak mot fattigdom, sosiale tjenester, politireform og rettsreform. Fokus på utdanning og styrking av unge mennesker til å bruke internett trygt.
- Benytte det fulle omfanget av eksisterende lov, inkludert direktivet om seksuelt misbruk av barn fra 2011 (som ikke er fullt ut implementert i mange medlemsland)
- Ta tak i de samfunnsmessige faktorene som senker terkskelen for CSA, inkludert skadelige kjønnsnormer for kvinner og jenter, og bredere spørsmål om sosial ulikhet
- Sørge for konsistens i kriminalregisterkontroller, opplæring og bevissthet om tegn på CSA for alle som jobber med barn og unge
- Øke forskningsmidler og kapasitet til forebygging, samt rask implementering av forebyggingsmetoder, for å forhindre CSA-kriminalitet før barn blir skadet. Potensialet for skadereduksjon ved å fokusere på forebygging er enormt, men vanligvis oversett.

I henhold til menneskerettighetene kan det være nødvendig og akseptabelt å begrense personvernet og databeskyttelsen til de som er mistenkt for alvorlige forbrytelser som seksuelle overgrep mot barn. Det finnes til og med teknologiske metoder for å støtte etterforskning i slike saker som – så lenge de følger regler for rettferdig prosess og respekterer menneskerettighetsprinsipper – kan være forenlig med rettsstaten.

Vi oppfordrer derfor lovgivere til å skille mellom intervensjoner og tiltak som er rettet mot individer som det er skjellig grunn til å mistenke, og som det derfor er forholdsmessig og legitimt å praktisere, og de tiltak som har en sterkt negativ innvirkning – enten den er bevisst eller utilsiktet – på en hel befolkning som f.eks. automatiserte opplastingsfiltre, mange former for aldersregistrering, samt generell innholdskontroll med verifisering og skanning av innhold i private meldinger. Vi mener at sistnevnte kategorier bør avvises av de ovennevnte grunner.

Den fullstendige juridiske og tekniske analysen som ligger til grunn for dette heftet er utført av våre europeiske samarbeidspartnere i EDRi og er tilgjengelig på:
https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-CSAR.pdf

Vi anbefaler også ytterligere ressurser om hvordan stater kan forfølge lovlige etterforskninger mot de som er mistenkt for alvorlig kriminalitet som CSA:

Elektronisk Forpost Norge

1. 10 Principles to Defend Children in the Digital Age (2022): https://edri.org/our-work/chat-control-10-principles-to-defend-children-in-the-digital-age/
2. Statlig tilgang til krypterte data (2022): https://edri.org/our-work/breaking-encryption-will-doom-our-freedoms-and-rights/