Oktober 2023

Notat om forslag til EU-forordning om regler til forebyggelse og bekæmpelse af seksuelt misbrug af børn (CSA)

EU-kommissionen har fremlagt et forslag til en forordning om regler til forebyggelse og bekæmpelse af seksuelt misbrug af børn.[1]

Forslaget er begrundet i ønsket om at beskytte børn mod at blive ofre for seksuelt misbrug online. Omfanget af deling af materiale, der viser seksuelt misbrug af børn online er nemlig stigende, ligesom børn i højere grad er eksponeret for grooming online.

I 2021 blev der rapporteret 85 millioner billeder og videoer af seksuelt misbrug af børn.[2] En global undersøgelse fra 2021 af WeProtect Global Alliance[3], viser at mere end én ud af tre respondenter var blevet bedt om at gøre noget seksuelt eksplicit online i deres barndom, og over halvdelen havde oplevet en form for seksuelt misbrug af børn online.[4] Det amerikanske National Centre for Missing and Exploited Children (NCMEC) modtog i 2020 over 21 millioner indberetninger, hvoraf over 1 millioner vedrørte EU-lande. Det seneste indberetningstal for 2021 viser en yderligere stigning, da antallet af indberetninger nærmer sig 30 millioner.[5]

I Danmark har politiet oplevet en årlig i stigning mellem 20-25 % af anmeldelser om grooming, overgreb og seksuel afpresning.[6] Red Barnets SletDet-rådgivning modtog i 2022 desuden 1.980 henvendelser, hvoraf 31 % drejede sig om seksualiserede digitale krænkelser (fx ufrivillig deling af et nøgenfoto).[7]

Forslaget har til formål at etablere en klar og ensartet retlig ramme til forebyggelse og bekæmpelse af seksuelt misbrug af børn online.[8] Forslaget indebærer bl.a., at udbydere af relevante informationssamfundstjenester skal risikovurdere samt minimere risikoen for at deres tjeneste anvendes med henblik på seksuelt misbrug af børn. Derudover kan udbydere af hostingtjenester og udbydere af interpersonelle tjenester i visse tilfælde forpligtes til at opspore og indberette materiale, der viser seksuelt misbrug af børn og grooming.[9]

Digitalt Ansvar støtter forordningsforslagets formål og finder det positivt, at der tages initiativ til regulering, der indeholder konkrete løsningsforslag til at forebygge og bekæmpe seksuelt misbrug af børn online. Det er

---

[1] https://www.eu.dk/samling/20221/kommissionsforslag/KOM(2022)0209/forslag/1883921/2607540.pdf
[2] https://home-affairs.ec.europa.eu/whats-new/communication-campaigns/legislation-prevent-and-combat-child-sexual-abuse_da
[3] Economist Impact survey offentliggjort i Global Threat Assessment, WeProtect Global Alliance, 2021
[4] Forslag til forordning om bekæmpelse af seksuelt misbrug af børn af 11. maj 2022, side 1, andet afsnit
[5] https://www.eu.dk/samling/20221/kommissionsforslag/KOM(2022)0209/forslag/1883921/2607540.pdf
[6] Grooming, overgreb og seksuel afpresning: Anmeldelser af digitale krænkelser er steget markant | Indland | DR
[7] Især piger søger hjælp efter digitale krænkelser (redbarnet.dk)
[8] Derudover har forordningen til formål at pålægge udbyder ansvar for at afsløre og indberette indhold med seksuelt misbrug af børn og grooming deres tjenester, og at sikre dette ved oprettelse af et europæisk center til forebyggelse og bekæmpelse af seksuelt misbrug af børn ("EU-centret")
[9] Hostingudbydere kan desuden pålægges at fjerne og/eller spærre materiale, der viser seksuelt misbrug af børn

nødvendigt, at der findes effektive og langsigtede løsninger på problemet. Derfor er det også positivt, at udbydere kan forpligtes til at anvende teknologi til opsporing af kendt eller nyt materiale, der viser seksuelt misbrug af børn samt grooming. Det er i den forbindelse essentielt, at der stilles præcise og klare krav til den teknologi, som udbyderne skal anvende Det er nødvendigt, at den anvendte teknologi er sikker at anvende, at der kan opnås indsigt og viden om den anvendte teknologi og at teknologien er nøjagtig.

Opsporingsforpligtelsen for udbydere rejser imidlertid en problematik i relation til retten til privatlivsbeskyttelse for brugere. Der skal derfor også findes en rimelig balance mellem hensynet til at beskytte børn mod seksuelt misbrug online og på den anden side brugere af digitale tjenesters ret til privatliv.

Status i dag: hvilke muligheder er der?

Eksisterende ordninger

Der er ikke dansk lovgivning, som forpligter udbydere til at opspore og fjerne materiale med seksuelt misbrug af børn. I Danmark findes "Netfilterordningen", hvor Rigspolitiet og Red Barnet sammen med størstedelen af internetudbyderne (som deltager på frivillig basis) samarbejder om at blokere internetsider med ulovligt materiale.[10] Politiet kan desuden få adgang til materiale på digitale tjenester, herunder krypterede tjenester, som led i deres efterforskning. Politiets adgang forudsætter, at en række betingelser er opfyldt. I praksis forudsætter det, at politiet har viden om at der deles overgrebsmateriale eller sker grooming, hvilken viden de sjældent har.

I EU anvender nogle tjenester i dag frivilligt teknologi til at opdage seksuelt misbrug af børn online i medfør af en midlertidig forordning, der udløber den 3. august 2024.[11] Forordningen gør det muligt for udbydere at anvende teknologi til at opdage og fjerne materiale, der viser seksuelt misbrug af børn. Opsporingen kan ske enten ved scanning af indhold (fx billeder og tekst) eller trafikdata for kommunikation. Efter den midlertidige forordnings udløb er der ikke EU-regulering, hvorefter udbydere (omend frivilligt) kan opspore og indberette materiale, der viser seksuelt misbrug af børn. Det betyder også, at mulighederne for at opdage og gribe ind over for de omfattende delinger af overgrebsmateriale og grooming fremover svækkes betydeligt. Konsekvensen er, at de mange millioner af delinger af overgrebsmateriale får lov til at florere, videredeles og fortsat udbredes, uden der kan gribes effektivt ind.

Amerikanske udbydere skal i henhold til amerikansk lovgivning indberette til amerikanske NCMEC, når de bliver opmærksomme på seksuelt misbrug af børn på deres tjenester. Størstedelen af de rapporteringer som europæiske myndigheder modtager om materiale, der viser seksuelt misbrug af børn, sker via NCMEC.[12]

---

[10] Samlenotat for sager på Justitsministeriets område, der forventes behandlet på rådsmødet (retlige og indre anliggender) den 28. september 2023, side 14

[11] Europa-Parlamentets og Rådets forordning (EU) 2021/1232 af 14. juli 2021 om en midlertidig undtagelse fra visse bestemmelser i direktiv 2002/58/EF, for så vidt angår den anvendelse af teknologier til behandling af personoplysninger og andre data, der foretages af udbydere af nummeruafhængige interpersonelle kommunikationstjenester med det formål at bekæmpe seksuelt misbrug af børn online

[12] Kommissionens konsekvensanalyse af 11. Maj 2022, side 21 (https://www.eu.dk/samling/20221/kommissionsforslag/KOM(2022)0209/forslag/1883924/2574753.pdf)

Oktober 2023

Teknologiske muligheder

I dag er det via såkaldt ”perceptual hashing-teknologi” muligt at detektere billede- og videomateriale, der viser seksuelt misbrug af børn.[13] Teknologien har vundet væsentlig udbredelse og har været anvendt i mere end 10 år, herunder af amerikanske NCMEC til at opspore materiale, der viser seksuelt misbrug af børn.

Ved ”perceptual hashing” omdannes et billede eller en video til et unikt fingeraftryk (”en hash-kode”). Det unikke fingeraftryk kan sammenlignes med fingeraftryk fra andre billeder eller videoer, som ligger i en database. Ved sammenligningen mellem to billeders fingeraftryk er det muligt at finde kopier. Nedenfor ses processen afbilledet. Et billede (nr. 1) omdannes til en ”hash-kode” (nr. 2), der kan sammenlignes med lignende ”hash-koder” (nr. 3). Hvis der identificeres et match (nr. 4) kan billedet (nr. 1) fjernes (nr. 5):

Kilde: *https://www.microsoft.com/en-us/photodna*

Perceptual hashing-teknologien gør det muligt at identificere billeder og videoer ved at sammenligne dem med materiale i en database, der f.eks. indeholder materiale, der viser seksuelt misbrug af børn. Identifikationen sker alene ved sammenligning af billeders unikke fingeraftryk (”hash-koden”) og således kun på kodeniveau. Der sker således ikke identifikation af personer eller analyse af den kontekst, som billedet eller videoen er identificeret i.[14]

Denne billedgenkendelsesteknologi har efter mange års brug og test har vist sig robust, pålidelig og særdeles præcis.[15] I konsekvensanalysen, der leder forordningsforslaget, er det anslået, at raten for falske positive (fejlvurdering af et billede) ved opsporing af kendt materiale er 1 til 50 milliard ved brug af programmet PhotoDNA fra Microsoft.[16] PhotoDNA er desuden modstandsdygtig over for manipulerede eller transformerede billeder og har en nøjagtighed på over 99 %.[17]

[13] Kommissionens konsekvensanalyse af 11. Maj 2022, side 71
[14] Kommissionens konsekvensanalyse af 11. Maj 2022, side 71
[15] Farid, Hany, Ph.D., Fostering a Healthier Internet to Protect Consumers, https://www.govinfo.gov/content/pkg/CHRG-116hhrg43533/pdf/CHRG-116hhrg43533.pdf
[16] Kommissionens konsekvensanalyse af 11. maj 2022, side 71
[17] Thoughts on Child Safety on Commodity Platforms, Dr Ian Levy Technical Director UK National Cyber Security Centre og Crispin Robinson Technical Director Cryptanalysis GCHQ, 21st July, 2022. https://arxiv.org/pdf/2207.09506.pdf

Oktober 2023

Forordningsforslagets hovedelementer

Forslaget består af to hovedelementer: **1)** udbydere kan blive pålagt forpligtelser til at opspore, indberette, fjerne og spærre kendt og nyt materiale, der viser seksuelt misbrug af børn samt grooming og **2)** der oprettes et EU-center for seksuelt misbrug af børn.

Udbyderne forpligtelser

Udbydere af informationssamfundstjenester[18] skal:

- vurdere risikoen for at deres tjeneste anvendes med henblik på seksuelt misbrug af børn (artikel 3)
- begrænse den konstaterede risiko ved afbødende foranstaltninger (artikel 4)
- rapportere om resultaterne af både risikovurderingen og indsatserne for at mindske risikoen for at tjenesten anvendes med henblik på seksuelt misbrug af børn (artikel 5)

Derudover kan udbydere af hostingtjenester eller interpersonelle kommunikationstjenester forpligtes til at:

- opspore materiale, der viser seksuelt misbrug af børn og grooming (artikel 7-11) og
- foretage indberetning hvis de får kendskab til oplysninger, der tyder på potentielt seksuelt misbrug af børn online (artikel 12-13)

En udbyder kan pålægges at anvende teknologi til at opspore materiale, der viser seksuelt misbrug af børn og grooming, hvis en række betingelser er opfyldt (artikel 7). Et påbud forudsætter dels, at der er dokumentation for, at der er en betydelig risiko for, at tjenesten anvendes med henblik på seksuelt misbrug af børn (artikel 7, stk. 4, litra a), dels at årsagerne til udstedelsen af opsporingspåbuddet opvejer de negative konsekvenser for alle berørte parters rettigheder og legitime interesser, navnlig under hensyntagen til behovet for at sikre en rimelig balance mellem disse parters grundlæggende rettigheder (artikel 7, stk. 4, litra b).

I vurderingen af om betingelserne er opfyldt skal der bl.a. tages hensyn til udbyderens risikovurdering og om de afbødende foranstaltninger, er tilstrækkelige til at begrænse risikoen for, at tjenesten med henblik på anvendelse af seksuelt misbrug af børn.

Hvis en udbyder opsporer potentielt seksuelt misbrug af børn skal udbyderen indberette det via EU-centeret (artikel 12). Det er uanset om opsporing er sket som led i et opsporingspåbud eller på anden vis.

Nedenfor er processen for udstedelse af et opsporingsopbud illustreret:

[18] Omfatter hostingtjenester, interpersonelle kommunikationstjenester, softwareapplikationsbutikker og internetadgangstjenester

Krav til den anvendte teknologi

En udbyder, der har fået et opsporingspåbud skal installere og drive teknologier, for at opspore seksuelt misbrug af børn online. Artikel 10 beskriver, hvordan udbyderne praktisk skal efterkomme et opsporingspåbud, herunder kravene til den teknologi der anvendes.[19] Kravene til teknologien er, at:

[19] EU-centeret stiller desuden gratis teknologi til rådighed for udbydere, men udbyderne er ikke forpligtet til at anvende en bestemt teknologi, herunder dem der stilles til rådighed af EU-centeret, jf. artikel 10, stk. 2

- den skal være *effektiv* med hensyn til at opspore udbredelsen af kendt eller nyt materiale eller grooming
- ikke må kunne udtrække andre oplysninger fra den pågældende kommunikation end de oplysninger, der er *strengt nødvendige* for at afdække mønstre for udbredelsen af kendt eller nyt materiale, der viser seksuelt misbrug af børn, eller for hvervning af børn
- være i *overensstemmelse med det aktuelle tekniske niveau* i industrien og *mindst muligt indgribende* over for brugernes ret til privatliv og familieliv, herunder til kommunikationshemmelighed og beskyttelsen af personoplysninger
- være *tilstrækkeligt pålidelige*, idet de i videst muligt omfang *begrænser fejlprocenten* i forbindelse med opsporingen

Artikel 10 oplister også krav til selve udbyderne, når de anvender teknologien. Udbyderne skal bl.a. træffe alle nødvendige foranstaltninger til at sikre, at teknologierne udelukkende anvendes til at opspore udbredelsen af kendt eller nyt materiale, der viser seksuelt misbrug af børn, eller grooming, i det omfang det er strengt nødvendigt for at efterkomme de opsporingspåbud. Derudover skal udbyderen indføre interne procedurer til at forebygge, opspore og afhjælpe misbrug af teknologien og sikre regelmæssigt menneskeligt tilsyn.

Derudover skal udbyderen orientere brugeren af tjenesten om, at der anvendes teknologi til opsporing, herunder hvordan teknologien anvendes. Brugeren skal også orienteres om, at udbyderen er forpligtet til at foretage indberetninger til EU-centeret og at brugeren har ret til domstolsprøvelse.

Hvilke muligheder giver forordningsforslaget?

Børns rettigheder nyder beskyttelse i bl.a. FNs konvention om barnets rettigheder og i EU-charterets artikel 24. Børns rettigheder skal beskyttes i et digitalt miljø – helt på samme måde som i den offline verden. Der er i dag dog store udfordringer med massiv og grænseoverskridende deling af materiale, der viser seksuelt misbrug af børn samt grooming. Derfor er det også kærkomment, at der tages initiativ til EU-regulering, for at komme problemet til livs. Forordningsforslaget indeholder en række gode takter, da det vil:

- sikre effektiv opsporing, indberetning og fjernelse af materiale, der viser seksuelt misbrug af børn online og grooming
- bidrage med fælles regulering af udbydernes forpligtelser til at forebygge og bekæmpe seksuelt misbrug af børn online
- tydeliggøre processerne for opsporing og indberetning, herunder fokus på brugeres rettigheder

Hvis udbyderne forpligtes til at opspore kendt materiale, der viser seksuelt misbrug af børn og grooming, vil det mindske recirkulationen af materiale og give grundlag for bedre at yde bistand til ofre i forbindelse med igangværende misbrug, da det materiale, der er omfattet af en sådan forpligtelse, kan have været i omløb i årevis.[20] Derudover vil opsporing af nyt materiale og grooming også kunne forebygge misbrug.

Der er behov for regulering

Det er nødvendigt, at der udarbejdes lovgivning, som giver effektiv mulighed for at forebygge og bekæmpe seksuelt misbrug af børn online. Der er ikke tilstrækkelige midler til at komme problemerne til livs i dag og da

[20] Forordningsforslaget, side 11, fjerde afsnit

der er tale om omfattende og grænseoverskridende udfordringer, er det nødvendigt med en målrettet og langsigtet indsats.

I dag sker opsporing og indberetning i medfør af midlertidige EU-regler, men denne regulering giver ikke mulighed for tilstrækkelig kontrol med processerne, sikring af brugeres rettigheder eller præcise nok krav til den teknologi, som udbydere skal anvende. Dertil kommer, at der er tale om frivillige ordninger for udbyderne, som således helt kan undgå ansvar.

Opsporings- og indberetningsforpligtelser for udbydere er ikke nyskabelser, men har hidtil været frivilligt for udbyderne, hvorfor der også er stor forskel på, hvor godt børn beskyttes på forskellige sociale medier og beskedtjenester. Når de midlertidige regler udløber i august 2024, vil det slet ikke være en mulighed for sociale medier og beskedtjenester at anvende opspore og indberette seksuelt misbrug af børn online.

Det er ikke tilstrækkeligt, at løsningerne fremover baserer sig på frivillighed eller midlertidig regulering. En frivillig ordning forpligter ikke udbyderne tilstrækkeligt og er heller ikke langtidsholdbar. Det er derfor positivt, at forslaget sikrer en overgang fra et frivilligt samarbejde til at udbydere kan pålægges obligatoriske forpligtelser. Hertil kommer, at forslaget vil medføre øget transparens om de processer, som udbyderne skal iværksætte og det skaber mere klarhed og sikkerhed for udbyderne. Derudover sikres klageadgang, ret til indsigt og information for både udbydere og berørte brugere, hvilket ikke er sikrede garantier i dag.

EU-regulering vil således medføre, at der sker ensretning af udbydernes forpligtelser og sikre at der sker opsporing og indberetning af det samme materiale og på samme måde. Det overlades ikke til udbyderne at vælge, om og hvad der indberettes. Hvis der på europæisk plan samles materiale, der er verificeret ulovligt i databaser, vil det være muligt kollektivt at sikre en effektiv opsporing og fjernelse af materiale, der viser seksuelt misbrug af børn.

Udbydere skal engageres

Det er positivt, at forslaget indeholder konkrete bud på, hvordan materiale, der viser seksuelt misbrug af børn og grooming kan hindres. I den forbindelse er det helt essentielt at udbyderne, som forslaget også lægger op til, pålægges forpligtelser. Udbyderne er nærmest til at konstatere om deres tjenester anvendes til seksuelt misbrug af børn og derfor bør de også spille en aktiv rolle i bekæmpelsen af problemet.

Det er positivt, at udbydere som forpligtes til at vurdere og mindske risikoen for seksuelt misbrug af børn online på deres tjenester. Samspillet mellem risikovurderingerne (artikel 3) og de afbødende foranstaltninger (artikel 4) er et dynamisk værktøj til effektivt til at mindske risikoen for deling af uønsket materiale. **Det er positivt, at forslaget lægger op til en risikobaseret tilgang, hvor udbydere en tidlig og præventiv indsats.** Et fokus på forebyggelse og risikominimering er en forudsætning for at komme udfordringerne til livs.

Det er desuden kun i tilfælde af, at udbyderens egne indsatser ikke er tilstrækkeligt effektive til at begrænse risikoen for at tjenesten anvendes med henblik på seksuelt misbrug af børn, at et opsporingspåbud kan komme på tale. **Forslagets udgangspunkt er derfor også, at der foretages risikovurdering og minimering, førend udbydere forpligtes til at opspore indhold.**

Oktober 2023

Teknologien gør præcis opsporing mulig

Det er er nødvendigt, at udbydere kan forpligtes til at foretage opsporing af kendt og nyt materiale, der viser seksuelt misbrug af børn og grooming. Der har længe været teknologi, der gør det muligt at sætte effektivt ind over for deling af overgrebsmateriale og grooming. Anvendelse af teknologi synes at være det mest effektive virkemiddel og derfor er det positivt, at udbydere forpligtes til at anvende teknologi til opsporing.

Et opsporingspåbud kan omfatte kendt eller nyt materiale, der viser seksuelt misbrug af børn og grooming. De teknologiske muligheder for opsporing afhængig af, hvad der er genstand for opsporingen.

Opsporing af kendt materiale

Kendt materiale er kopier af materiale, der tidligere er blevet pålideligt verificeret som materiale, der viser seksuelt misbrug af børn (fx dømt ulovligt af en domstol).

Ved opsporing af kendt materiale kan der anvendes den føromtalte perceptual hashing-teknologi. Hvis der deles et billede af kendt materiale, som således er svarer til et billede i en database, kan der ske billedgenkendelse, når kendt materiale figurerer på en tjeneste. Der sker således sammenligning af billeder eller videoer på kodeniveau med materiale, som allerede er verificeret som ulovligt.

Opsporing ved hjælp perceptual hashing-teknologi sikrer, at der sker effektiv og præcis identifikation med allerede verificeret materiale, der viser seksuelt misbrug af børn. Anvendelse af perceptual hashing-teknologi kan sammenlignes med scanning for virus eller spam. Der er tale om en maskinel, automatiseret proces, hvor der ikke bliver lyttet, læst eller set indhold i korrespondance. Der sker ikke identifikation af kontekst og sammenligningerne sker heller ikke sker på baggrund af personer på billederne, men alene via algoritmisk genkendelse. Teknologien sikrer derved anonymitet ved opsporing.

Ved anvendelse af teknologi til opsporing består der en risiko for, at der fremkommer falske positive ved at der fremkommer et ukorrekt match. Perceptual hashing-teknologien er imidlertid særdeles sikker og risikoen for falske positive er forsvindende lille, da fejlmarginen er 1 til 50 milliard. Som beskrevet ovenfor er teknologien særdeles nøjagtig – også når der er tale om manipulerede billeder eller billeder der på anden vis er transformeret.

Digitalt Ansvar har været i dialog med den førende ekspert på området for opsporing af overgrebsmateriale og grooming, Hany Farid, der er Ph.d. og professor ved Berkeley University. Han har specialiseret sig i analyse af digitale billeder og detektion af digitalt manipulerede billeder, såsom deepfakes. I en mail af 11. oktober 2023 har Digitalt Ansvar foreholdt ham dele af den fremsatte kritik af forslaget, og spurgt ind til hvor sikkert det er at anvende perceptual hashing teknologi. Han udtaler i den forbindelse, at han ikke er enig i, at digitale fingeraftryk (”hashes”) nemt kan omdannes og derved medføre fejlkvalifikationer og falske positive.

Opsporing af nyt materiale og grooming

Ved opsporing af nyt materiale eller grooming anvendes der kunstig intelligens, som ud fra indikatorer kan rangere nye billeders lighed med billeder, der allerede identificeret som materiale, der viser seksuelt misbrug af børn.

Oktober 2023

I dag findes der teknologi, der kan opspore nyt materiale med en nøjagtighed på over 90 %[21] og grooming med en nøjagtighed på omkring 90 %.[22] Grundet usikkerhedsmarginen på 10 % er det nødvendigt med en menneskelig gennemgang af det materiale, der vil blive identificeret.

Digitalt Ansvar har også foreholdt Hany Farid, at tekstgenkendelsesteknologi af grooming alene skulle være 88 % sikker, hvilket kritikere af forslaget har fremhævet. Hany Farid oplyser i en mail af 11. oktober 2023 til Digitalt Ansvar, at et pilotprojekt hos Microsoft havde en nøjagtighed på 85-90 %, men at testværktøjet var designet til interaktion mellem spillere på gaming-platforme. Han mener derfor ikke, at der i denne henseende er stor grund til bekymring, og at nyere sprogmodeller med sikkerhed vil have en forøget nøjagtighed.

Der er ingen effektive alternative løsninger

Det er nødvendigt, at der findes konkrete løsninger på deling af materiale, der viser seksuelt misbrug af børn online og grooming. Der ses ikke at være nogle alternative løsninger til anvendelse af teknologi til opsporing, der på samme præcise og effektive måde mitigerer problemet. Det taler betydeligt for, at opsporingsforpligtelser for udbydere ikke bør forkastes, men at det er en løsning, som skal betragtes på et seriøst bud. Hvis opsporing, indberetning og fjernelse baserer sig på frivillighed fra udbydernes side, skaber det en utilfredsstillende retstilstand for de børn, der får delt materiale og udsættes for grooming.

Hvis det alene overlades til politiet at efterforske delinger og grooming uden udbyderne deltager, er der også langt fra tale om en tilstrækkelig effektiv indsats. I dag er problemet bl.a., at de eksisterende juridiske samarbejder, er for langsommelige, og at samarbejdet mellem udbydere og myndigheder er upålideligt, inkonsekvent ligesom det mangler gennemsigtighed og klare definitioner af udbydere henholdsvis udbyderes og myndigheders ansvar. Derudover er EU-medlemsstater i dag afhængige af rapporteringer fra tredjelande, herunder fra NCMEC.[23] Det vil forslaget kunne ændre på, så der i EU effektivt kan sættes ind over for deling af materiale, der viser seksuelt misbrug og grooming.

[21] Kommissionens konsekvensanalyse af 11. maj 2022, side 79
[22] Kommissionens konsekvensanalyse af 11. maj 2022, side 81
[23] Kommissionens konsekvensanalyse af 11. maj 2022, side 33