POLITIET

ÅPEN

Distribusjonskode	H0 – Til kriminalitetsbekjempelse
Klassifisering	Åpen
Distribusjon	Åpen
Dato ferdigstilt	25.10.2024
Info cut off	30.09.2024
Kontaktpunkt	kripos@politiet.no
Antall sider	13 (inkl. forside og vedlegg)

Informasjon fra tjenestetilbydere: Seksuell utnyttelse av barn på digitale plattformer

Etterretningsrapport

1. Hovedpunkter

- Norsk politi har i over 10 år daglig mottatt informasjon fra National Center for Missing and Exploited Children (NCMEC). Informasjonen fra NCMEC stammer i hovedsak fra tilbydere lokalisert i USA, herunder Facebook, Instagram, Snapchat, Google og en rekke andre. I tillegg mottar politiet mer sporadisk informasjon fra en rekke andre tilbydere, enten direkte eller via Europol, Interpol eller utenlandske politimyndigheter.

- Tilbyderne varsler om en rekke forhold, men i all hovedsak er det ulike former for befatning med overgrepsmateriale, primært oppbevaring og deling. I tillegg varsler tilbyderne om seksualisert kontakt mellom voksne og barn, egenprodusert materiale, seksuell utpressing m.fl.

- Det er *sannsynlig* at mengden tips vil øke de tre neste årene. Det er *sannsynlig* at økningen vil treffe Kripos i større grad enn politidistriktene.

- Ved økt bruk av KI og maskinlæring i deteksjon av tidligere ukjent overgrepsmateriale er det *sannsynlig* at politiet vil få en økning i tips som prioriteres høyt, da det må avklares om overgrepsmaterialet som er delt indikerer at gjerningspersonen har begått egne overgrep.

2. Innhold

1. Hovedpunkter 2
2. Innhold 3
3. Bakgrunn og formål 4
3.1. Rapportens oppbygging og avgrensninger 4
4. Informasjon 4
4.1. Historisk utvikling og informasjon i dag 4
4.2. Hva mottar politiet? 7
4.3. Deteksjon og oppdagelse 7
4.4. Drivere som påvirker utvikling og omfang av informasjon 7
4.4.1. Oppmerksomhet mot personvern og sikkerhet: Krypterte kommunikasjonstjenester og anonymiseringstjenester 7
4.4.2. Tilbyderne tar større samfunnsansvar 8
4.4.3. Kunstig intelligens: Effektiv avdekking, men også produksjon av syntetisk overgrepsmateriale 9
4.4.4. Nasjonal og internasjonal lovgiving 10
4.4.5. Aktørenes endrede bruksmønster 10
4.4.6. Barn og unge: Bruk av teknologi og delingskultur 10
4.4.7. Nye tilbydere oppstår 11
5. Vurdering 11
5.1. Introduksjon til vurderinger og scenarioer 11
5.2. Scenarioer 11
5.2.1. Den mest sannsynlige utviklingen 11
5.2.2. Den alvorligste utviklingen 11
5.3. Vurderinger 12
6. Vedlegg 13
6.1. Sannsynlighetsord 13

3. Bakgrunn og formål

Kripos og deretter politidistriktene mottar årlig et stort antall tips fra ulike tjenestetilbydere på internett om nordmenn som begår seksuallovbrudd. Innholdet i slike tips varierer, fra relativt uskyldige videoer og bilder barn tar av seg selv, til dokumenterte voldtekter begått av norske gjerningspersoner. De fleste tipsene dreier seg allikevel om ulike former for befatning med overgrepsmateriale, herunder opp- og nedlasting, deling, besittelse eller annet.[1]

Omfanget av slike tips har økt jevnt siden Kripos først mottok slik informasjon tidlig på 2010-tallet. Primært sendes tipsene via National Center for Missing and Exploited Children (NCMEC), som er en amerikansk organisasjon. Amerikanske tilbydere er lovpålagt å varsle NCMEC dersom de avdekker forhold knyttet til seksuelle overgrep mot barn.[2] I tillegg sender en rekke andre tilbydere også tips gjennom organisasjonen. Kripos mottar også tips på vegne av norsk politi direkte fra noen tilbydere.

Bakgrunnen for rapporten mange henvendelser angående omfanget av tips og tipsenes videre utvikling i tilden framover. Rapporten skal gi beslutningsstøtte til alle nivåer i norsk politi og justissektor for å planlegge for framtidens utvikling og omfang av informasjon.

3.1. Rapportens oppbygging og avgrensninger

Rapporten har tre deler. Først beskrives noe historikk og nåsituasjonen i informasjonen som mottas fra tilbydere. Deretter gjennomgås ulike drivere som på hvert sitt vis vil ha påvirkning på den videre utviklingen av informasjonen og omfanget av den. Avslutningsvis beskrives to scenarioer, den mest sannsynlige utviklingen og den alvorligste utviklingen. Scenarioene blir etterfulgt av generelle vurderinger med en tidshorisont på tre år.

Begrepet *tips* brukes om all informasjon politiet mottar i ulike kanaler fra tjenestetilbydere på internett. Rapporten omtaler tips om seksuell utnyttelse av barn, primært på internett. Andre former for kriminalitet omtales ikke. Rapporten avgrenses derfor fra informasjon direkte fra publikum og informasjon fra politimyndigheter i andre land, for eksempel overskuddsinformasjon i straffesaker.

4. Informasjon

4.1. Historisk utvikling og informasjon i dag

Norsk politi har i over 10 år daglig mottatt informasjon fra NCMEC. Informasjonen fra NCMEC stammer i hovedsak fra tilbydere lokalisert i USA, herunder Facebook, Instagram, Snapchat, Google og en rekke andre. I tillegg mottar politiet mer sporadisk informasjon fra en rekke andre tilbydere, enten direkte eller via Europol, Interpol eller utenlandske politimyndigheter.

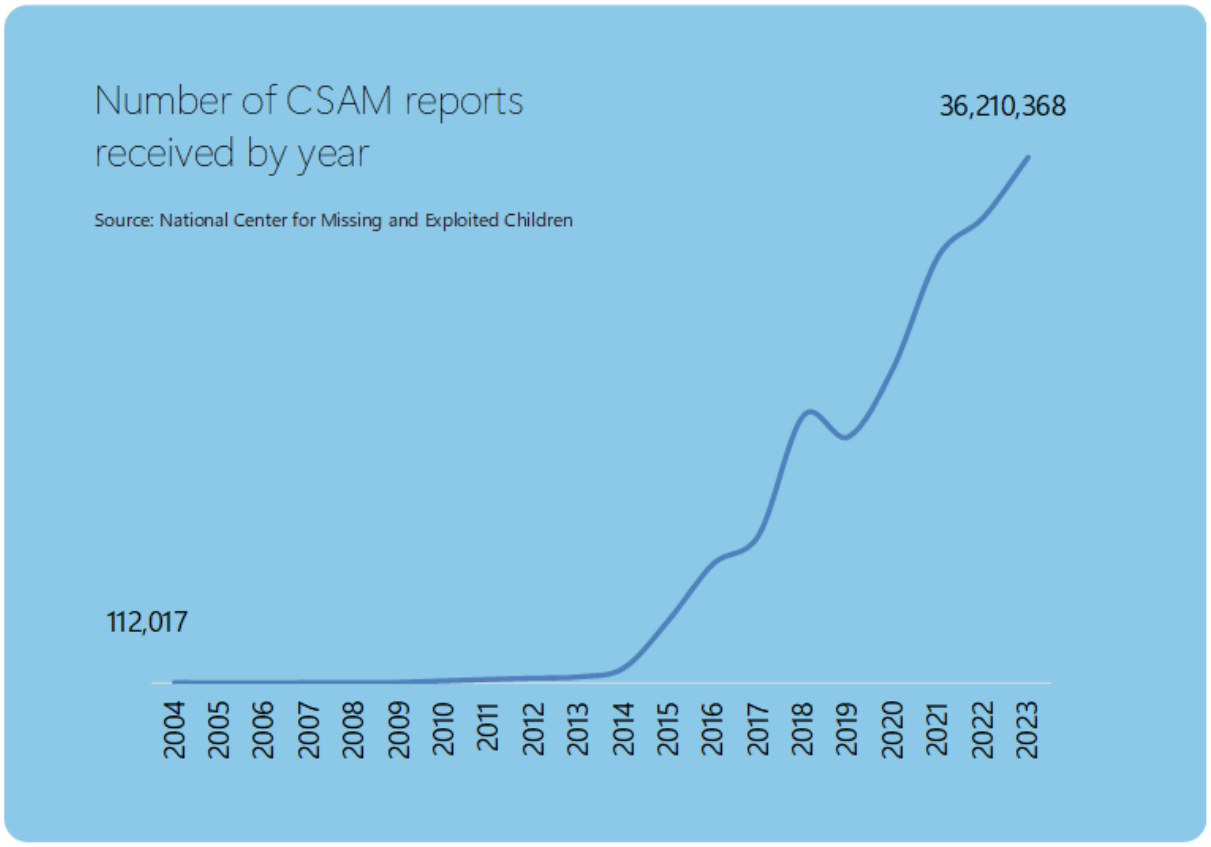
I noen land er slik informasjonsdeling/varsling lovpålagt. Et eksempel er USA, der alle tilbydere er forpliktet til å varsle om informasjon jf. 18 U.S. Code § 2258A - Reporting requirements of providers. I Norge gjelder ikke avvergingsplikten for

[1] Straffeloven § 311 straffer den som blant annet produserer, anskaffer, innfører, besitter, utgir, tilbyr, selger, overlater til en annen, gjør tilgjengelig eller på annen måte søker å utbre fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn eller forsettlig skaffer seg tilgang til slikt materiale. Med barn menes personer som er eller fremstår som under 18 år.

[2] 18 U.S. Code § 2258A - Reporting requirements of providers

overgrepsmaterialeog slike forhold krever derfor ikke lovpålagt varsling i Norge. [3] [4] Andre forhold som kan foregå på norske plattformer, kan allikevel være omfattet av avvergingsplikten, for eksempel voldtekt av barn på internett.[5]

Omfanget av cybertip-rapporter fra tilbydere til NCMEC har økt hvert år siden oppstart. Spesielt har omfanget økt de siste 10 årene og nå mottar NCMEC over 35 millioner tips hvert år, se figur under.



Figur 1: Antall rapporter NCMEC har mottatt siden 2004. Hentet fra Microsoft: Protecting the Public from AI-Generated Content.

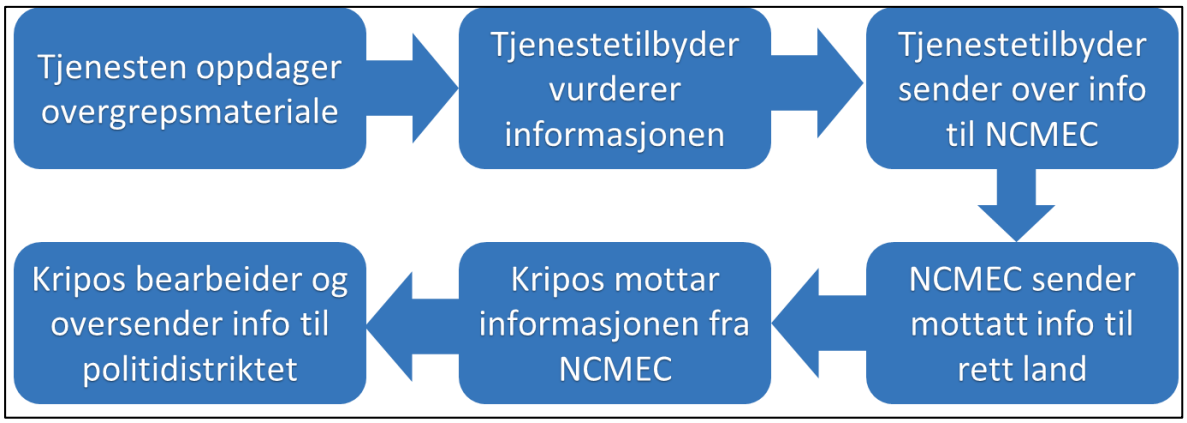
Tilbyderne varsler om en rekke forhold, men i all hovedsak er det ulike former for befatning med overgrepsmateriale, primært oppbevaring og deling. I tillegg varsler tilbyderne om seksualisert kontakt mellom voksne og barn, egenprodusert materiale, seksuell utpressing m.fl.

Figur 2 under er et enkelt flytskjema for behandling av tips fra NCMEC, fra den avdekkes av tilbyderen til den formidles videre til politidistriktene fra Kripos. Se ytterligere om deteksjon i kapittel 4.4. Kripos ved SOMB og avsnitt for innledende etterforskning (AIE)[6] mottar informasjonen som gjelder norske brukere. Oversendelsen fra NCMEC til Norge skjer med bakgrunn i geografiske opplysninger, gjerne geolokasjon[7] på IP-adresser. Videre formidles rapporter til politidistriktene etter en bearbeiding hos Kripos. Arbeidet

[3] Straffeloven § 311
[4] Straffeloven § 196
[5] Straffeloven § 299
[6] Avsnitt for innledende etterforskning (AIE) ved Seksjon for seksuelle overgrep mot barn (SOMB) er det nasjonale kontaktpunktet for all informasjon fra NCMEC og andre tilbydere på vegne av norsk politi. AIE foretar innledende undersøkelser før de oversender informasjonen til riktig politidistrikt.
[7] Geolokasjon for IP-adresser gir en indikasjon på hvilket geografisk område IP-adressen anvendes.

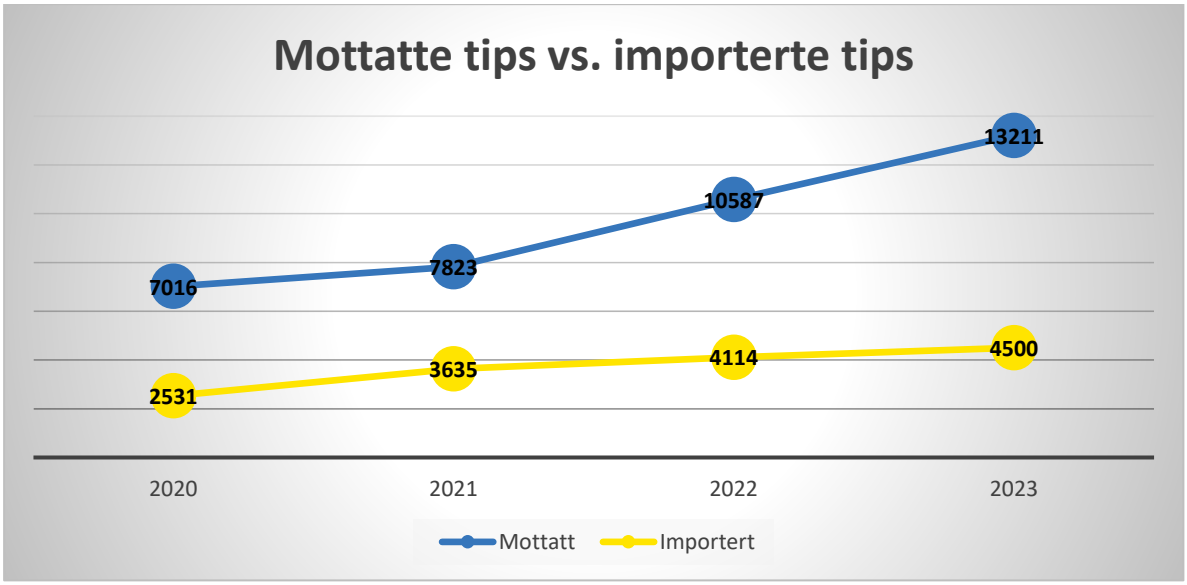
inkluderer prioritering/risikovurdering[8] og nødvendige sporinger for å fastslå hvilket politidistrikt som skal behandle tipset videre.

Figur 2 under er et enkelt flytskjema for behandling av tips fra NCMEC, fra den avdekkes av tilbyderen til den formidles videre til politidistriktene fra Kripos. I mange tilfeller skjer deteksjonen og oversendelse til NCMEC automatisk, slik at tilbyderen aldri vurderer informasjonen selv. Se ytterligere om deteksjon i kapittel 4.4.



Figur 2: Enkelt flytskjema for behandling av informasjon fra tilbydere som varsler gjennom NCMEC

Over tid har mengden tips fra tilbydere som sender informasjonen gjennom NCMEC økt. Tipsene AIE importerer for videre behandling har også økt, men ikke i samme takt som den totale informasjonsmengden, se figur 3 under. Siste steg i prosessen medfører derfor en betydelig reduksjon i tipsmengde, eksempelvis fra 13211 mottatte tips til 4500 importerte tips i 2023.



Figur 3: Figuren viser differansen mellom mottatte tips og importerte tips fra NCMEC i perioden 2020-2023

Import for videre arbeid med tipsene avhenger av flere kriterier. De vanligste årsakene til at tips avvises er at forholdet ikke er straffbart i Norge. I tillegg avvises en rekke tips som inneholder bilder og videoer som er straffbare, men som er under nedre terskel for hva politiet ønsker å iverksette tiltak mot.

[8] Tipsene prioriteres etter innhold i tipset og etter forhold knyttet til mistenkt bruker. Kriteriene for prioritering er delvis basert på KIRAT (Long, M., Alison, L., Tejeiro, R., Hendricks, E. & Giles, S. (2016). KIRAT: Law enforcement's prioritization tool for investigating indecent image offenders. *Psychology, public policy, and law*, *22*(1), 12-21. https://doi.org/10.1037/law0000069)

Andelen tips som importeres for videre behandling varierer svært mye mellom ulike tilbydere.

4.2. Hva mottar politiet?

Det varierer mellom tilbyderne hva tipsene/informasjonen inneholder. I de fleste tilfeller inneholder tipset en eller flere mediefiler, i form av bilder eller videoer. I tillegg til overgrepsmateriale kan også tipset inneholde profilbilder og andre bilder/videoer den rapporterte brukeren har delt eller lagret. I en del av tilfellene inneholder også tipset chat eller annen informasjon som gir kontekst til delingen, eksempelvis opplysninger om mottaker.

Tilbyderne sender både tidligere kjent overgrepsmateriale og nytt materiale, som regel egenprodusert av barn selv. Det er ikke kjent hvordan hver enkelt av tilbyderne fanger opp nytt materiale, men noen benytter manuell gjennomgang, noen benytter KI-verktøy og noen tips er basert på varslinger fra andre brukere.

Hvilke identifiserende opplysninger tilbyderne sender, varierer mellom de ulike tilbyderne. Noen tilbydere har omfattende opplysninger om sine brukere og legger følgelig også ved mange sporbare og identifiserende opplysninger.

4.3. Deteksjon og oppdagelse

Kripos har foretatt en gjennomgang av utvalgte tilbyderes "terms of service"/"community guidelines" eller tilsvarende. Det varierer i hvor stor grad tilbyderne er åpne om hvilke tiltak de iverksetter for å hindre seksuell utnyttelse av barn på egne plattformer og tjenester.

De fleste tilbyderne har regulert spesifikt i egne retningslinjer at seksualisert materiale av barn er uønsket på plattformene.

Google skriver at de benytter hash-matching for å oppdage kjent overgrepsmateriale. I tillegg skriver de at de benytter maskinlæring til å oppdage slik innhold som ikke er sett tidligere, noe som fører til avdekking av førstegenerasjons overgrepsmateriale. Ut over dette er det ikke avdekket at tilbyderne er åpne om hvilken metode de benytter for avdekking og deteksjon av overgrepsmateriale og andre straffbare forhold.

I tillegg til forhold tilbyderne avdekker selv, kan også tips fra politiet og tips fra andre brukere (publikum) danne grunnlag for tips fra tilbydere.

4.4. Drivere som påvirker utvikling og omfang av informasjon

I dette delkapittelet vil flere drivkrefter som kan påvirke utviklingen av tips fra tilbydere framover beskrives. Driverne vil deretter benyttes i scenarioene i neste kapittel. Hver driver har egne vurderinger.

4.4.1. Oppmerksomhet mot personvern og sikkerhet: Krypterte kommunikasjonstjenester og anonymiseringstjenester

Enkelte etablerte tilbydere har det siste året endret tjenestene sine slik at brukerne opplever økt personvern og sikkerhet. Som en konsekvens av dette vanskeliggjøres deteksjon av overgrepsmateriale, fordi kommunikasjon mellom brukerne krypteres. Når informasjonen i samtaler krypteres kan ikke innholdet skannes for kjent overgrepsmateriale. Et konkret eksempel er at Meta har gjort Messenger ende-til-ende-

kryptert og på den måten gjort en svært omfattende mengde med kommunikasjon og filutveksling usynlig for deteksjon.[9]

Meta argumenterer med at ende-til-ende kryptering fører til et ekstra lag sikkerhet og bedre personvern for brukeren.[10] En annen Meta-plattform som er ende-til-ende-kryptert er WhatsApp, og selv om Meta har iverksatt tiltak for å avdekke seksuell utnyttelse av barn på denne plattformen, er omfanget av tips fra WhatsApp marginalt sammenlignet med hva det historisk har vært for Facebook Messenger. Eksempelvis sendte Facebook 2752 tips via NCMEC til Norge i 2023, mens WhatsApp sendte 35 tips.

En annen måte å bevare anonymitet på er ved bruk av anonymiseringstjenester som VPN og proxy.[11] Dersom flere brukere i større grad bruker anonymiseringstjenester som VPN og proxy, kan det medføre et mindre tilfang av tips der gjerningspersonen framstår norsk, og på den måten redusere omfanget av tips til norsk politi. Bruk av slike anonymiseringstjenester kan derfor påvirke utviklingen framover.

Det har kommet flere politiske utspill den seneste tiden om å aldersregulere bruk av sosiale medier. Dersom slike aldersgrenser skal håndheves vil det medføre økt behov for legitimering på sosiale medier, for eksempel bruk av bankID ved innlogging, som er en av løsningene regjeringen vurderer.[12] [13]

Delvurdering

Det er *sannsynlig* at kryptering framover vil forekomme på flere og flere plattformer.

Økt anonymisering på internett vurderes som *sannsynlig* i framtiden. Samtidig er det også *mulig* at økt forekomst av anonymiseringstjenester vil føre til krav om mer legitimering på internett. Det samme gjelder eventuelle ønsker om å innføre strengere aldersgrenser på ulike plattformer på nett, da slike aldersgrenser må håndheves gjennom økt legitimering. Det er derfor vanskelig å avgjøre hvilken retning denne driveren vil ha i framtiden og det vurderes derfor som *mulig* at økt bruk av anonymiseringsverktøy vil føre til større mørketall og *mulig* at dette motvirkes av økt legitimering på nett, som vil føre til mindre mørketall.

4.4.2. Tilbyderne tar større samfunnsansvar

Selv om mange tilbydere gjennom nasjonal og internasjonal lovgiving er lovpålagt å varsle dersom de avdekker overgrepsmateriale er det også slik at tilbydere selv tar samfunnsansvar og velger å frivillig varsle politiet dersom de avdekker at tjenestene misbrukes til oppbevaring eller deling av overgrepsmateriale. Et konkret eksempel på dette er Telenor sitt samarbeid med politiet i avdekking av overgrepsmateriale på skytjenesten Min sky.

Slike initiativ kan føre til økt mengde tips gjennom økt omfang av tipsere. Samtidig kan slike tiltak virke avskrekkende ved at brukere som allerede misbruker, eller ønsker å misbruke, tjenesten flytter aktiviteten sin til andre tjenester som ikke varsler politiet. Dersom det skjer vil omfanget av tips reduseres, uten at aktiviteten reduseres. Allikevel

[9] https://about.fb.com/news/2024/03/end-to-end-encryption-on-messenger-explained/amp/

[10] https://about.fb.com/news/2024/03/end-to-end-encryption-on-messenger-explained/amp/

[11] Kripos: Cyberkriminalitet 2024

[12] https://www.nrk.no/norge/regjeringen-jobber-med-aldersgrense-pa-sosiale-medier-1.16831103

[13] https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Representantforslag/2022-2023/dok8-202223-247s/

tyder forskning på at fysisk forflytning etter forebyggende tiltak har en reduserende effekt på kriminaliteten ved at noen aktører opphører sin kriminelle aktivitet.[14]

Delvurdering

Det er *sannsynlig* at flere, nye tilbydere velger, eller pålegges, å tipse organisasjoner eller politiet, avhengig av hvilket land tilbyderen etableres i.

Det er *sannsynlig* at det oppstår nye tilbydere, som vil tipse politiet.

4.4.3. Kunstig intelligens: Effektiv avdekking, men også produksjon av syntetisk overgrepsmateriale

Produksjon av syntetisk overgrepsmateriale med kunstig intelligens vil være en aktuell drivkraft framover. Mengden overgrepsmateriale er allerede svært stor og med syntetisk overgrepsmateriale kan mengden øke i raskere takt enn tidligere, siden gjerningspersonene som produserer slikt materiale ikke trenger å ha tilgang til barn og kan produserer store mengder materiale på kort tid. I tillegg til å øke mengden, vil også arbeidsmengden for politiet øke med bakgrunn i at alt materiale må ekthetsvurderes av identifiseringsformål.[15] [16] Uansett vil syntetisk overgrepsmateriale generere arbeid, fordi slikt materiale er ulovlig i Norge på samme måte som ekte overgrepsmateriale.

I 2023 mottok NCMEC over 4700 tips om KI-generert syntetisk overgrepsmateriale, men få av disse ledet til Norge.[17]

Allerede nå har prisen på overgrepsmateriale på det mørke nettet sunket. En hypotese er at det skjer som følge av økt tilbud av syntetisk materiale og at det totale volumet av overgrepsmateriale derfor har økt.[18]

Tilbydere av KI-modeller som misbrukes til produksjon av syntetisk overgrepsmateriale vil i flere land være underlagt samme varslingsplikt som andre tilbydere. Det fører til at tips fra KI-tilbydere kommer i tillegg til tips fra øvrige tilbydere.

I tillegg kan kunstig intelligens på ulike måter brukes av tilbydere for å avdekke overgrepsmateriale på plattformer, også på nye og andre måter enn tidligere deteksjon. For eksempel kan KI anvendes til å detektere overgrepsmateriale som ikke allerede er kjent, som eksempelet fra Google over viser.

Delvurdering

Det er *meget sannsynlig* at forekomsten av syntetisk overgrepsmateriale vil øke i framtiden, og produksjon av syntetisk overgrepsmateriale vil øke forekomsten av overgrepsmateriale totalt.

Selv om tilbydere av KI-modeller tar grep for å forhindre misbruk av modellene, er det *meget sannsynlig* at forsøk på produksjon vil forekomme allikevel, og at slike forsøk vil generere tips til politiet.

Det er *sannsynlig* at KI vil medføre mer effektiv avdekking av nytt materiale som ikke tidligere er kjent og derfor ikke kan avdekkes med hash.

---

[14] Guerette, Rob T.: Analyzing Crime Displacement and Diffusion. Center for Problem-Oriented Policing. 2009.
[15] Europol: Internet Organized Crime Treat Assessment 2024
[16] Kripos: Cyberkriminalitet 2024
[17] Microsoft: Protecting the Public from AI-Generated Content.
[18] Chainalysis: The 2024 Crypto Crime Report. The latest trends in ransomware, scams, hacking, and more

Samlet vil derfor utviklingen innen KI føre med seg både økt omfang av materiale, nye former for ulovlig materiale, økt antall tilbydere som varsler og mer effektive avdekkingsmekanismer noe som *meget sannsynlig* vil føre til en stor økning av tips.

4.4.4. Nasjonal og internasjonal lovgiving

En annen driver som har potensiale til å endre omfanget av informasjon fra tjenestetilbydere i svært stor grad er nasjonal og internasjonal lovgiving. For Norges del er både nasjonal lovgiving i Norge, men også nasjonal lovgiving i andre land av betydning. I tillegg er regulering fra EU og andre overnasjonale organisasjoner av betydning.

I følge Internet Watch Foundation er EU den største "verten" for overgrepsmateriale globalt, omtrent 90 % i 2019. Nederland alene står for over 70 % av det tilgjengelige materialet i verden.[19] Etablering av strengere regulering og bedre rapporterings- og formidlingsrutiner innen EU har derfor potensiale til å øke omfanget av informasjon fra tjenestetilbydere betydelig. CSAM-forordningen behandles ikke ytterligere i denne rapporten.

Et annet eksempel er dersom Norge innfører avvergingsplikt som dekker strl. § 311. Dette kan medføre en økning i informasjon fra norske tilbydere, selv om det også kan ha en forebyggende effekt, jf. kap. 4.4.2.

Rapporten avgrenses fra å vekte sannsynligheten for endret lovgiving i Norge og internasjonalt.

4.4.5. Aktørenes endrede bruksmønster

I tillegg til slike villede endringer som følge av ulike reguleringer og endret rapporteringsvilje som beskrevet over, kan også brukernes bruksmønster endres uten at motivasjonen er å skjule seg bevisst. Aktørene kan også få økt teknisk kompetanse, som fører til at de tar mer bevisste valg knyttet til operasjonell sikkerhet.

Delvurdering

Det er *sannsynlig* at brukere i framtiden vil ha bedre teknisk kompetanse enn i dag og at det vil medføre at flere brukere benytter tekniske løsninger som sikrer anonymisering.

4.4.6. Barn og unge: Bruk av teknologi og delingskultur

Norske barn har høy tilgang til teknologi og sosiale medier. Blant annet viser årets Barn og medier-undersøkelse at omtrent alle barn over 9 år i Norge har tilgang til mobiltelefon og at over 90 % har tilgang til PC, enten i form av skole-PC eller privat PC.[20]

De senere årene har flere og flere barn delt seksualisert materiale av seg selv og andre, både mellom enkeltpersoner og i grupper på sosiale medier. Dette har blant annet blitt betegnet som en delingskultur.[21] Allikevel viste Barn og medier-undersøkelsen 2024[22] at andelen barn i alderen 13-18 år som sier de har delt nakenbilde av seg selv det siste året har sunket til 9 %, fra 15 % i tilsvarende undersøkelse i 2022[23].

[19] European Parliament: Curbing the surge in online child abuse. 2020.
[20] Medietilsynet: Barn og medier 2024. Delrapport: Barn og unges medievaner og tilgang til teknologi
[21] Politiets trusselvurdering 2024
[22] Medietilsynet: Barn og medier 2024. Delrapport: Skadelig innhold, seksuelle kommentarer og nakenbilder på nett.
[23] Medietilsynet: Barn og medier 2022

Som følge av barns høye digitale tilstedeværelse kan foreldre kan bli mer bevisste og oppmerksomme på barnas aktivitet på digitale plattformer. I tillegg kan det bli økt oppmerksomhet rundt digital sikkerhet i undervisning i skolen.

Delvurdering

Det er *sannsynlig* at norske barn får økt tilgang til digitale enheter i yngre alder. Samtidig er det *mulig* at denne effekten motvirkes av at foreldre setter strengere rammer for barnas bruk og/eller bidrar til bedre avdekking og at barn læres opp i digital trygghet i skolen.

4.4.7. Nye tilbydere oppstår

Tilbydere av elektroniske tjenester vil alltid oppstå og utvikle seg. I noen tilfeller er det snakk om en ny forretningsidé, andre tar opp en konkurranse med en etablert plattform.

Den senere tiden har særlig tilbydere av modeller for generativ KI etablert seg som egne tjenester. Noen av disse rapporterer også til NCMEC og representerer derfor helt nye tilbydere innenfor et nyoppstått område.[24]

Delvurdering

Det er *sannsynlig* at nye plattformer vil oppstå raskt og tiltrekke seg brukere som begår kriminalitet på disse plattformene. Utviklingen vil spesielt drives av teknologisk utvikling.

5. Vurdering

5.1. Introduksjon til vurderinger og scenarioer

Vurderingskapittelet inneholder både beskrivelsen av to scenarioer og overordnende, generelle vurderinger for hele rapporten. Vurderingene og scenarioene har en tidshorisont på tre år.

5.2. Scenarioer

Ved utforming av scenarioer er det tatt utgangspunkt i fire ulike scenarioer, to av dem presenteres under. Den best tenkelige utviklingen er ikke beskrevet i detalj, men idealsituasjonen er at størst mulig del av kriminaliteten avdekkes (få mørketall) og at kriminaliteten ikke øker. Det andre scenarioet som ikke er beskrevet ytterligere, er en situasjon der omfanget av tips til politiet øker, samtidig som at den alvorlige kriminaliteten skjules. Det kan derfor betegnes som "overlessing" av irrelevant informasjon, men med store mørketall.

5.2.1. Den mest sannsynlige utviklingen

Mengden tips øker og politiet må bruke en del ressurser på å følge opp og etterforske saker. Samtidig er tipsene i mindre grad om aktører som politiet er spesielt interessert i å rette oppmerksomheten mot, fordi ulike anonymiserings- og krypterings-verktøy gjør at aktørene som er bevisst mulighetene velger verktøy og plattformer der de kan skjule seg. Det vil være en økning i antall tips de nærmeste tre årene.

5.2.2. Den alvorligste utviklingen

Den alvorligste utviklingen er der kriminaliteten foregår i det skjulte og øker samtidig. I denne utviklingen er mørketallene store, og den mest alvorlige kriminaliteten foregår

[24] https://openai.com/index/child-safety-adopting-sbd-principles/

skjult. Politiet er ikke nødvendigvis nedlesset med arbeid, men ulike drivere fører til at de farligste gjerningspersonene går fri gjennom bruk av anonymiseringstjenester og økt bevissthet rundt operasjonell sikkerhet. Mye syntetisk overgrepsmateriale gjør politiets innsats utfordrende fordi det er vanskelig å skille mellom ekte og syntetisk materiale, og omfanget av materiale er stort. Mange barn bruker ukritisk digitale enheter og foreldre følger ikke med på hva som foregår og setter ikke grenser. Den digitale arenaen blir et lovløst rom. Mange nye tilbydere oppstår, men de tipser ikke politiet og har heller ikke etablerte samarbeidskanaler med politiet, da personvern og sikkerhetshensyn står sterkt.

5.3. Vurderinger

Det er *sannsynlig* at mengden tips vil øke de tre neste årene. Det er *sannsynlig* at økningen vil treffe Kripos i større grad enn politidistriktene, da det er *sannsynlig* at økningen vil være større totalt enn for relevante tips som importeres til videre behandling.

Ved økt bruk av KI og maskinlæring i deteksjon av tidligere ukjent overgrepsmateriale er det *sannsynlig* at politiet vil få en økning i tips som prioriteres høyt, da det må avklares om overgrepsmaterialet som er delt indikerer at gjerningspersonen har begått egne overgrep.

6. Vedlegg

6.1. Sannsynlighetsord

Vurderinger vil alltid inneholde en grad av usikkerhet. For å håndtere dette på en standardisert og strukturert måte, er det benyttet sannsynlighetsord (se tabell):

Nasjonal standard	Beskrivelse	NATO standard
Meget sannsynlig	Det er meget god grunn til å forvente…	Highly likely (>90%)
Sannsynlig	Det er grunn til å forvente…	Likely (60-90%)
Mulig	Det er like sannsynlig som usannsynlig…	Even chance (40-60%)
Lite sannsynlig	Det er liten grunn til å forvente…	Unlikely (10-40%)
Svært lite sannsynlig	Det er svært liten grunn til å forvente…	Highly unlikely <10%