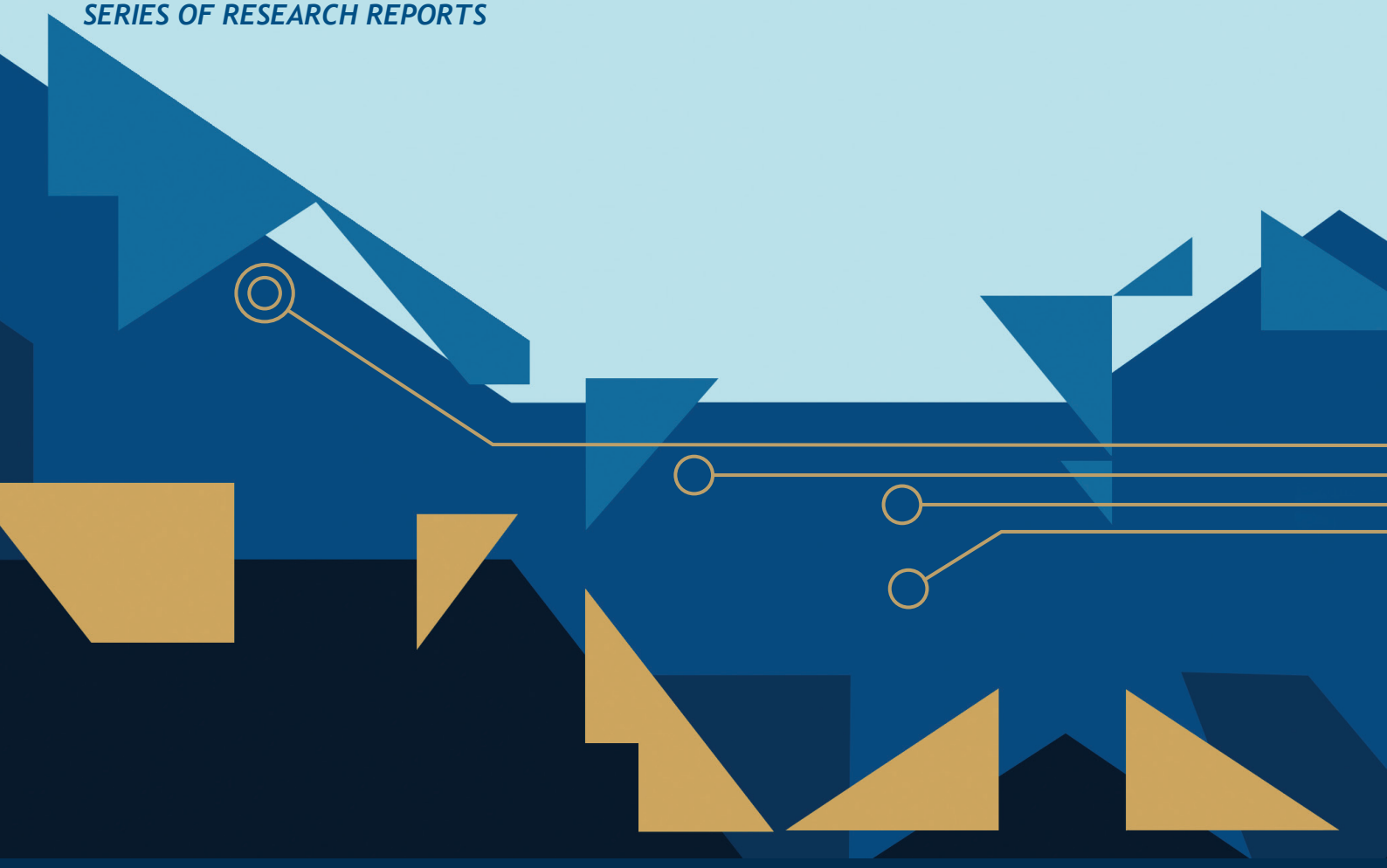
Seksuell utnyttelse av barn over internett

Rapport om analyse av teknologiske faktorer som påvirker produksjon og deling av materiale som seksuelt utnytter barn over internett.

Matilda Dorotic og Jan William Johnsen

No. 1 - 2023
SERIES OF RESEARCH REPORTS



BI Norwegian Business School

NTNU

Matilda Dorotic og Jan William Johnsen
Seksuell utnyttelse av barn over internett. Rapport om analyse av teknologiske faktorer som påvirker produksjon og deling av materiale som seksuelt utnytter barn over internett.

Research Report
1 edition
1 reprint
ISSN: 0803-2610

BI Norwegian Business School
N-0442 Oslo
Phone +47 4641 0000
www.bi.no

Seksuell utnyttelse av barn over internett

Rapport om analyse av teknologiske faktorer som påvirker produksjon og deling av materiale som seksuelt utnytter barn over internett

Prosjektleder
Basel Katt

Rapportforfattere
Matilda Dorotic og Jan William Johnsen

Datainnsamling
Patrick Bours og Marius Wang

Formatering
Oliver Dagsland Tverrå

NTNU

BI Norwegian Business School

Innhold

Takksigelser

Forskningen og denne rapporten fikk støtte fra Justis- og beredskapsdepartementet gjennom *SOBI Del III: Kartlegging og analyse av arenaer som bruker til tilgang og deling av overgrepsmateriale*.

Vi ønsker å takke vår partner Trøndelag politidistrikt og deres avsnittsleder ved digitalt politiarbeid Marius Wang for å gi oss tilgang på data for å gjøre nødvendige undersøkelser, samt for å tilrettelegge for intervjuer med deres spesialetterforskere.

Vi ønsker å takke for støtten vi har fått fra våre partnere i Kripos, Celina Røstgård Flatner og Bente Skattør i Oslo politidistrikt, for deres innsikt og støtte i datainnsamling og for å tilrettelegge for intervjuer med politibetjenter og etterforskere.

Svært viktige bidrag ble gitt av bedrifter, sivile organisasjoner og enkeltpersoner gjennom intervjuer, samt informasjon og kontekst for utviklingen av et flerinteressentperspektiv. For å bevare anonymiteten til våre intervjusubjekter har vi unnlatt å nevne navnene på bedriftene og institusjonene som deltok i denne forskningen, men herved ønsker vi å takke dem alle sammen.

Vi er takknemlige for sivile organisasjoner som har gitt viktig innsikt i utfordringene. Takk til Redd Barna, en del av den internasjonale organisasjonen Save the Children med Kaja Hegg og til Amnesty International Norway med Ingrid Westgaard Stolpestad. Vi retter en spesiell takk til United Nations Interregional Crime and Justice Research Institute (UNICRI) og Datatilsynet for innsiktsfulle kommentarer de har gitt til denne rapporten.

Avslutningsvis ønsker vi å takke professor Katrin Franke ved Norges teknisk-naturvitenskapelige universitet (NTNU) for hennes innsats med å forske og skrive forslaget som var utgangspunktet for denne forskningen.

Forord

Teknologiske utviklinger, spesielt de som er relatert til elektroniske tjenester på internett, gir viktige fordeler i å fremme kommunikasjon, tilgang til og deling av informasjon. Men denne utviklingen byr også på betydelige utfordringer for å gjøre internettbaserte miljøer trygge for barn og samtidig beskytte personvernet og ytringsfriheten. Denne rapporten tar sikte på å belyse den komplekse rollen teknologien og internettet har for å produsere og dele materiale knyttet til seksuell utnyttelse av barn, men også deres kritiske rolle i å skape en motreaksjon med det formål å oppdage og forhindre misbruk.

Nittitallets Amerikanske posttjenester hadde en enorm innsats for å bekjempe distribusjonen av materiale knyttet til seksuell utnyttelse av barn (CSAM). Overvåkingen av posttjenestene var vellykket mht. reduksjonen i delingen av CSAM [1], [2]. Delingen av CSAM har imidlertid eksplodert over hele verden med utviklingen og utbredt bruk av internett og elektroniske tjenester [3], [4]. I perioden mellom 2005 og 2020 har det vært en kontinuerlig økning i antall rapportert overgrepsmateriale til det globale rapporteringssenteret National Center for Missing and Exploited Children (NCMEC). NCMEC rapporterte om en økning på 35% av nytt overgrepsmateriell i omløp mellom 2020 og 2021 [5].

Den store tilgjengeligheten av elektroniske tjenester og plattformer (både på internett og mobil) gjør det mulig for lovbrytere å enkelt kontakte flere hundre mindreårige samtidig, samt gjennomføre kjøp, salg og utveksling av overgrepsmateriale med både mindreårige ofre og likesinnede. I tillegg gjør den økende utvikling av anonymiseringsteknikker (som ende-til-ende kryptering eller mørke nett-tjenester) og kunstig intelligens skapte bilder det vanskeligere å oppdage og fjerne overgrep og CSAM. Det store volumet av eksisterende overgrepsmateriale på nettet samt hastigheten nytt innhold skapes gjør arbeidet med å identifisere eksisterende og nytt materiell krevende. Manuell gjennomgang blir umulig. Teknologiske løsninger og tett privat-offentlig samarbeid mellom elektroniske tjenesteleverandører og andre interessenter (som foreldre, sivilsamfunn, myndigheter og politi) er nødvendig og alle har en rolle for både å hjelpe og bekjempe problemet.

Oppsporing og forebygging av seksuell utnyttelse av barn over internett er et nyansert og komplekst fenomen. På grunn av den komplekse strukturen som gjør produksjon og distribusjon av overgrepsmateriale enklere og anonymt, så kan politimyndigheter ikke nærme seg disse problemene alene eller isolert fra andre. Selv om alle er enige om at dette representerer et viktig sosialt problem, påvirker ofte oppnåelsen av målene til en interessent (f.eks. tillate økt overvåking av internett fra politiets side) direkte rettighetene og evnene til andre interessenter (f.eks. inntrenging i personvernet til enkeltpersoner eller brudd på kundeforhold til elektroniske tjenesteleverandører).

Det er en meningskonflikt om hvordan man skal nærme seg løsningene mellom de som støtter sterkere statlig overvåkning og de som motsetter seg det. Denne rapporten tar sikte på å fremheve de mest fremtredende nåværende og fremtidige teknologitrender, mottiltak og strukturelle og juridiske problemstillinger knyttet til fenomenet teknologiassistert overgrep mot barn. Vi håper dette arbeidet vil bidra til en bedre forståelse av kompleksiteten rundt problemet og bidra til å skape et enkelt rammeverk for et tryggere og bedre internett for barn!

Kapittel 1 Introduksjon

1.1 Formål og målsettinger for rapporten

Seksuell utnyttelse av barn (CSA) over internett har økt raskt i løpet av de siste tre årene etter utbruddet av koronaviruspandemien (SARS-CoV-2). Meldinger som *USA Cyber Tipline* har mottatt økte kraftig fra 1 million rapporter i 2010, til 16,9 millioner rapporter i 2019. I 2021 økte rapporteringen til 29,3 millioner [5]. Økningen attribueres til at barn har større tilgang til og deltakelse på internett, samt raske teknologiske fremskritt. Denne trusselen som mindreårige møter i nettbaserte miljøer er blitt et av de store sosiale problemene rundt om i verden. Samtidig rettes viktige nasjonale og internasjonale strategiske prioriteringer for lovgivere både i USA, Norge og EU mot dette økende problemet (jf. Norges nasjonale og internasjonale satsingsområder; Europeisk strategi for et bedre internett for barn (BIK+), og drøftinger vedr. "Communication Decency Act" i USA).

Barn blir stadig flinkere til å følge med på de teknologiske fremskrittene og koble seg opp til elektroniske tjenester. I tillegg øker bruken av mobile enheter og tiden barn tilbringer på elektroniske tjenester. Denne adferden flytter i stor grad barns sosiale interaksjoner over til internett. Men god internett-tilgang eksponerer også barn for økende nettrelaterte trusler og misbruk. Et eksempel på en slik trussel er grooming, som er betegnelsen på prosessen hvor en voksen oppretter kontakt med et barn i den hensikt å møte barnet og begå et seksuelt overgrep (enten gjennom et fysisk møte eller en elektronisk tjeneste). Et annet eksempel er at barn skyver grenser på hva som er akseptabel og uakseptabel oppførsel. Slike grenseskyvninger endrer holdninger om hvilke bilder og videoer som kan deles blant jevnaldrende, slik at vi ser en økning i egenprodusert overgrepsmateriale. En gjennomgang av overgrepsmateriale av Internet Watch Foundation (IWF) i 2021 viser at gjennomsnittsalderen på overgrepsofre blir lavere, hvor i nesten 7 av 10 tilfeller så ble 11-13 åringer identifisert [6]. Presset for egenprodusert materiale er nok økende i Norge også, hvor mer enn halvparten av norske tenåringer mellom 13 og 18 år angir at de har blitt bedt om å dele nakenbilder av seg selv [7].

Å bli utnyttet gjennom internett er spesielt skadelig for mindreårige fordi overgrepsmateriale forblir på internett [8]. Det er ofte umulig å bli kvitt materialet helt, og jevnlig deling av materiale betyr at ofrene opplever overgrepet om og om igjen. 70% av overgrepsofre har angitt at de hele tiden bekymrer seg for at de kan bli gjenkjent av noen som har sett materialet [9].

Tilsynsmyndigheter, påtalemyndigheter, sivilsamfunnsorganisasjoner og foreldre har reist sterke bekymringer om barns sikkerhet på nettet, og de krever umiddelbare handlinger. Men ønsket om handlinger lider imidlertid på grunn av flere viktige spenninger som gjør forebyggende tiltak spesielt tungvint:

- Utilstrekkelige teknologiske ferdigheter hos foreldre, lærere og politimyndigheter.
- Juridiske tvetydigheter fordi teknologien utvikler seg raskere enn lovgivningen.
- Krenkelse av personvern og menneskerettigheter.
- Kommersiell konfidensialitet av brukerinformasjon hos tjenesteleverandører.
- Krenkelse av immaterielle rettigheter til teknologileverandører.
- Ikke-transparente og partiske algoritmer i kunstig intelligens.

Det største problemet som hindrer forsøk på å forebygge spredning av overgrepsmateriale er særlig internettets globale natur. Det krever at juridiske rammer og lovverk harmoniseres på tvers av land før man skal kunne iverksette globale, forebyggende tiltak. Harmoniserende lovverk er imidlertid ikke tilfellet, og noe av forskjellen ligger i at noen land pålegger rapportering av CSAM, mens andre land gjør rapporteringen frivillig. Mer enn halvparten av landene over hele verden har fortsatt ikke lover relatert til CSAM [10], [11].

Over 60% av materialet knyttet til seksuell utnyttelse av barn verden over er lagret på europeiske servere [12] på grunn av manglende regulatoriske forutsetninger (i motsetning til USA) som pålegger at elektroniske tjenesteleverandører rapporterer CSAM. Nye regulatoriske forslag i EU og Storbritannia (f.eks. BIK+ og Online Safety Bills) har som mål å endre lovgivningen og redusere de gunstige vilkårene for lagring og formidling av CSAM over internett i Europa [13]. Disse prosessene påvirker direkte fremtiden for norsk rettshåndhevelsespraksis og evne til å forebygge skader på barn og ungdom i Norge. Ifølge BIK Policy Map-profilen fra mars 2021 har Norge ikke ett enkeltstående koordinert rammeverk for barns sikkerhet på internett, tiltak for å iverksette standarder for kvalitetsinnhold på internett for barn, tiltak for samarbeid mellom politi og alarmtelefontjenester eller tiltak for å overvåke rapporteringsmekanismer eller etiske retningslinjer på nasjonalt nivå [13].

Denne rapporten tar sikte på å bidra til de nasjonale strategimålene for å tilrettelegge for at barn og unge skal være trygge på nettet. Rapporten vil gå gjennom en evaluering av teknologiske arenaer, kanaler og trender som påvirker seksuelle overgrep og utnyttelse av barn på nettet [14]. Denne rapporten tar for seg tre hovedproblemstillinger:

- Hvordan utviklingen av digital teknologi og tjenester påvirker: A) muligheter for tilgang og deling av materiale knyttet til seksuell utnyttelse av barn og B) muligheter for gjerningspersoner til å etablere kontakt.
- Hva er de mest fremtredende nåværende og fremtidige teknologiske trender.
- Hvilke tekniske og andre muligheter (som strukturelle og juridiske) finnes for å bekjempe disse problemene.

Vi håper at denne rapporten skal bidra med informasjon og legge til rette for å bygge opp nasjonale strategiske tiltak.

1.2 Rapportens struktur

Å skape effektive strategier og retningslinjer for å oppdage og forebygge utnyttelse av barn på internett krever kunnskap om arenaene som muliggjør og tilrettelegger for slik utnyttelse. I tillegg krever det kunnskap om innsatsen og fallgruvene for ulike interessenter som må samarbeide mot disse målene. Siden evnen til å innføre metoder for å redusere seksuell utnyttelse av barn på internett uunngåelig er avhengig av samarbeidet og koordinasjonen mellom flere interessenter, så har vår evaluering som mål å være helhetlig. Det betyr at vi inkluderer perspektivene til flere interessenter for å fremheve deres gjensidige avhengighet.

Hovedfokuset i denne rapporten er likevel på hvordan teknologi påvirker produksjonen og delingen av overgrepsmateriale, samt forebyggingen av deling av materiale og seksuell utnyttelse av barn på internett. Gitt kompleksiteten og mangfoldet av ulike teknologiske løsninger, måtte vi uunngåelig sette

søkelys på de mest fremtredende aspektene og la andre relaterte aspekter forbli mindre utredet, slik som juridiske forhold, aspekter knyttet til næringslivet, den sosiale siden av CSA, osv.

I første kapittel skisseres den metodiske tilnærmingen som er tatt, samt dens begrensninger og gjøre leseren kjent med viktige terminologier som er brukt i denne rapporten. Andre kapittel forklarer de viktigste kildene til seksuell utnyttelse av barn på nettet, med hovedfokus på produksjonen av CSAM.

Det andre kapittelet beskriver viktige kilder til seksuell utnyttelse av barn på internett med fokus på produksjon og distribusjon av overgrepsmateriale. Målet er å samle et omfattende bilde av hovedformene og kildene til bilde og videomateriale, fordi vi selv har møtt et stort mangfold og variabilitet i kildene som brukes i litteraturen.

I rapportens tredje kapittelet beskrives eksisterende mottiltak hos politiet, samt trender og fallgruver som politiet møter på dette området.

Det fjerde kapittelet dekker strukturelle og juridiske utfordringer i forebygging av produksjon og distribusjon av overgrepsmateriale. Vi fremhever relevante aspekter og ulemper basert på innsikt fra allmenheten, bedrifter og lovgivere som beskrev sine utfordringer og avveininger.

Gjennom hele rapporten har vi som mål å gi en balansert, uavhengig vurdering og anbefalinger om de mulige aspektene som bør hensyntas i utformingen av fremtidige retningslinjer for å gjøre barn trygge i nettbaserte miljøer.

1.3 Metode

Med utgangspunkt i den tidligere beskrevne kompleksiteten av fenomener og relaterte problemstillinger blant flere interessenter, brukte vi i vår analyse en multimetode-tilnærming der vi kombinerte en litteraturgjennomgang av *Desk-Research bevis* (både fra offentlige registreringer og akademiske kilder), med en analyse av tilgjengelige empiriske bevis fra nasjonale og regionale kriminalitetsforebyggende enheter og primær datainnsamling gjennom intervjuer med de viktigste interessentene.

Litteraturgjennomgangen fokuserte primært på teknologiske trender og løsninger for mottiltak**.** Den første analysen av Web of Science-databasen av fagfellevurderte artikler innen områdene informatikk, kriminologi, rettsmedisin og psykiatri ved hjelp av søk etter emnesøkeordene "seksuell utnyttelse av barn", "CSA", "overgrepsmateriale" og "barnepornografi" resulterte i 18 528 treff, der de fleste artiklene falt innunder kategoriene psykologi, psykiatri, familiestudier og sosialt arbeid. En analyse av disse artiklene viste at de fleste av disse studiene ikke så på teknologiaspektene. Ofte analyserte disse studiene rettsdokumenter for å forstå profilen og egenskapene til lovbrytere eller sosiale arbeidsdatasett og undersøkelser av ofre for å forstå deres oppfatninger.

Mangelen på teknologi-orienterte studier førte til at vi så nærmere på offentlig tilgjengelige rapporter fra organisasjoner som jobber med beskyttelse av barn. Organisasjoner som International Centre for Missing & Exploited Children (ICMEC), NCMEC, InHope, WePROTECT Global Alliance, UNICEF, INTERPOL, EUROPOL, osv. I tillegg brukte vi andre offentlige rapporter som beskrev eller diskuterte anvendte strategier for å dele overgrepsmateriale som et grunnlag for videre henvisninger. Med referansene fra disse studiene gjennomførte vi en videre gjennomgang av akademisk litteratur som avdekket behovet vårt for tilgang til juridiske studier og artikler om informatikk og samfunnsvitenskap. Dette førte til flere

fagfellevurderte kilder som ledet videre til rapporter og treff i åpen kildekode via *Google Scholar*-analyser, der vi undersøkte rundt 130 kilder som refereres til i denne studien.

Kvalifiseringskriterier for inkludering av artiklene omfattet faglig nøyaktighet og kvalitet (basert på vitenskapelige tidsskrift og konferanserangering av fagartikler) og den enkelte frivillige organisasjonens troverdighet til å beskytte barn. Når vi inkluderte rapporter, fokuserte vi på de ledende frivillige organisasjonene og det lovgivende grunnlaget. I tillegg har vi supplert analysene med evalueringer av åpenhetsrapporter fra de største elektroniske tjenesteleverandørene som rapporterte til NCMEC. Denne analysen inkluderte åpenhetsrapporter fra Meta, Google, TikTok, Microsoft, Dropbox, Snapchat, Twitter, Imgur og Reddit.

For å komplettere litteraturundersøkelsen med empiriske data, utvidet vi analysen vår med politirapporter og dybdeintervjuer med interessenter fra politi, lovgivere, sivile organisasjoner som representerer barn, ideelle organisasjoner som bistår foreldre og barn og selskaper. Vi gjennomførte en serie av 16 intervjuer og arbeidsmøter for å få inngående innsikt i spørsmål sett fra perspektivet til flere forskjellige interessenter. Bedriftsrepresentanter fra ulike elektroniske tjenesteleverandører ble inkludert (nettspill, finansinstitusjoner, kommunikasjon og programvaretjenester). Interessenters navn er anonymisert for å beskytte personvernet til enkeltpersoner og organisasjoner.

Totalt intervjuet vi 16 respondenter: Åtte dybdeintervjuer med funksjonærer på ulike nivåer i det norske politisystemet (etterforskere på nasjonalt og distriktsnivå, politibetjenter og første respondenter); tre intervjuer med tilsynsmyndigheter og representanter for sivile samfunn/eksperter på barnerettigheter samt fem intervjuer med representanter for næringslivet.

Tilnærmingen som ble brukt til datainnsamlingen er en analyse av aggregerte empiriske bevis hentet fra norsk politi og Kripos med det formål å lage denne rapporten. Vi bruker også aggregering av materiale til å representere et problem når det enn er mulig. Ingen personopplysninger ble benyttet i forbindelse med denne studien.

1.4 Begrensninger

På grunn av kompleksiteten i aspektene knyttet til utnyttelse av barn over nettet, måtte vi være restriktive og til tider begrense omfanget og inkludering av aspekter. Den endelige versjonen av rapporten er derfor ikke nødvendigvis uttømmende når det gjelder hvilke aspekter den tar opp, men den har som et mål å fremheve noen hovedaspekter og koblinger som vi anser for å være mest relevante for å forstå virkningen teknologi har på dette problemområdet.

Analysens geografiske fokus er begrenset til de aspekter og praksis som er relevante for Norge spesielt, og noen relaterte aspekter knyttet til USA og EU. Vi registrerer en generell utfordring for at vi kunne gi en systematisk litteraturgjennomgang om virkningen av teknologi på seksuelle overgrep mot barn over internett. Utfordringen skyldes at forskjellige fagområder har ulikt søkelys på mindre aspekter og et ganske begrenset fokus på teknologiske artikler om bestemte teknologier, samt generell mangel på empiriske studier i større skala.

Denne begrensningen i datakilder vanskeliggjør analysen på tvers av studien og begrenser enhver mulighet til å levere store empiriske generaliseringer. Vi registrerer spesielt at vi hovedsakelig måtte

stole på årsrapporter fra noen få viktige frivillige organisasjoner (NCMEC, IWF og InHope), samt åpenhetsrapporter fra noen få store elektroniske tjenestetilbydere med hensyn til analyse av volumer, omfang og trender. Begrensningene når det gjelder å gi hele bildet er utdypet i avsnitt 2.2.

På grunn av svakheten at den eksisterende straffeloven ikke skiller mellom overgrep begått på visse steder eller med bruk av teknologi, så kan ikke dataene som er hentet fra politikilder fullt ut skille mellom seksuelle overgrep som er utført fysisk eller gjennom bruk av teknologi og andre kommunikasjonsmedium. Mye av klassifiseringen i politiets registrering av kriminalitet gjøres manuelt av mange politiansatte, og det finnes ikke en konsekvent tilnærming til registrering eller skriving av kommentarer. Derfor kan noen tolkninger av analysefunn være utydelige.

Selv om vi har forsøkt å gi en objektiv vurdering av akademisk litteratur og hentet materiale fra feltarbeidet, er tolkningene og alle mulige feil eller unøyaktigheter forfatternes egne. Partnere i prosjektet, institusjoner, politimyndigheter og intervjuede enkeltpersoner er ikke ansvarlige for tolkningen av innholdet.

1.5 Terminologi

Det er ingen internasjonalt oppnådd enighet om definisjon eller terminologi knyttet til utnyttelse og misbruk av barn over internett. UNICEF advarer om at begrepet ofte omfatter ulike former for seksuell utnyttelse og misbruk av barn som er tilrettelagt av teknologi [10].

Utnyttelse og misbruk av barn (CAE, eng.: "Child Abuse and Exploitation") kommer i mange former, som barneprostitusjon, egenproduksjon, seksuelle overgrep, grooming eller deling av overgrepsmateriale. Disse forbrytelsene kan bli begått i både den fysiske og digitale verden. Denne rapporten har et spesielt fokus på *seksuell utnyttelse og misbruk av barn over internett*, som UNICEF refererer til som "seksuell utnyttelse og misbruk av barn [som delvis eller helt er] tilrettelagt gjennom teknologi", via teknologi, internett eller andre kommunikasjonskanaler [10].

I denne rapporten bruker vi definisjonen av seksuell utnyttelse og misbruk som er vedtatt av Europarådets konvensjon om beskyttelse av barn mot seksuell utnytting og seksuelt misbruk (Lanzarote-konvensjonen), artikkel 18 [15].

Seksuell utnytting av barn (CSA, eng.: "Child Sexual Abuse") gjelder aktiviteter i flere domener, bl.a.:

- engasjere seg i seksuelle aktiviteter med en mindreårig person;
- produksjon, besittelse og distribusjon av materiale knyttet til seksuell utnyttelse av barn;
- grooming hvor en mindreårig kontaktes over nettet (og i den fysiske verden) i den hensikt å utsette det for seksuelt overgrep, eller
- direktestrømming av barn som utsettes for seksuell utnyttelse og misbruk.

Skillet mellom utnyttelse (exploitation) og misbruk (abuse) relateres først og fremst til arten av utveksling [10]. Hvis en part drar økonomisk nytte av aktivitetene, blir seksuelt misbruk av barn til seksuell utnyttelse. Noen ganger brukes *barnepornografi* som et synonym, men ifølge UNICEF sine konvensjoner avstår vi fra å bruke dette begrepet fordi det å drive med seksuelle aktiviteter med barn bør alltid anses å være seksuell misbruk av barn og det bør ikke knyttes til terminologien forbundet med

voksenpornografi [10], [16]. I denne rapporten bruker vi forkortelsen CSA i vid forstand til å omfatte alle typer misbruk eller utnyttelse.

Materiale knyttet til seksuell utnyttelse av barn (CSAM, eng.: "Child Sexual Abuse Material") omfatter innhold produsert i ulike formater (oftest bilder, videoer og opptak av direktestrømming) som deles via digitale kanaler.

Elektronisk tjenesteleverandør (ESP, eng.: "Electronic Service Provider") eller Internettleverandør (ISP, eng.: Internet Service Provider) refererer til bedrifter som tilbyr digitale kommunikasjonstjenester som tillater mottak og overføring av informasjon ved bruk av elektroniske kanaler. I denne rapporten bruker vi begrepet ESP for bredt å referere til ulike IT-selskaper, inkludert leverandører av telekommunikasjonstjenester og nettbaserte digitale tjenesteleverandører (f.eks. digitale plattformer som brukes til underholdning, sosiale medier, o.l.)

Grooming refererer til aktiviteten der voksne individer søker å bygge relasjoner med barn på nettet. Aktivieten kan bestå i å overbevise barnet til å sende nakenbilder, usensurerte videoer, strømming av seksuell karakter, eller som engasjerer seg i annen seksuell aktivitet som en del av interaksjonen med barnet. Vanligvis vil gjerningspersonen opprette en eller flere false profiler for å utgi seg for å være en annen, som også kan være på samme alder som barnet. Gjerningspersonen kan også ha flere profiler for å gi barnet inntrykk av at flere går god for hovedprofilen [17]. Gjerningspersonen viser betydelig innsikt i hvordan barn og unge snakker og kommuniserer med hverandre, og dette gjør at de kan kommunisere med barn på en troverdig måte. Ved å gjøre det kan de lure eller tvinge (f.eks. med utpressing) barnet til å produsere og dele overgrepsmateriale.

IP adresse er en forkortelse for Internett-protokolladresse som er en numerisk etikett (f.eks. 192.168.2.1) som identifiserer en datamaskin i et nettverk som bruker Internet Protocol (IP) for kommunikasjon [18]. Både avsenderens og mottakerens IP-adresser er nødvendige for å sende datapakker til hverandre over internett. IP-adressen tildeles kundens datautstyr av internettleverandøren [17].

Det åpne nettet består av informasjon på internett (eng.: "World Wide Web") som kan nås og indekseres av vanlige søkemotorer som Google, Bing, Yahoo og lignende. Resultatet vises som et søk på søkemotorene.

Det mørke nettet (eng.: "The Dark Web") består av krypterte nettverk som koder informasjon på en slik måte at det ikke kan indekseres av vanlige søkemotorer [19]. Darknet-krypteringsteknologien ruter også brukernes data gjennom et stort antall mellomservere slik at det skjuler brukerens identitet. Gjennom det mørke nettet kan private datanettverk kommunisere og drive virksomheten anonymt uten å avsløre identifiserbar informasjon, for eksempel brukerens plassering (IP adresse). Tilgang til det mørke nettet krever også spesielle nettlesere eller programvare som The Onion Router (TOR).

Kryptovaluta er *digitaliserte/virtuelle eiendeler* spredt gjennom flere datamaskiner i et delt nettverk [20]. Den mest kjente kryptovalutaen er Bitcoin, brukes som et alternativ til digital betalingsvaluta. Siden kryptovaluta deles gjennom desentraliserte nettverk, kan det ikke styres direkte av statlige reguleringsorganer (som banker).

Kapittel 2 Kilder og kanaler for seksuell utnyttelse av barn over internett

2.1 Historisk oversikt over den teknologiske utvikling innen spredning av materiale knyttet til seksuell utnytelse av barn over internett - fra nittitallet til 2021

Det var en nedgang i spredning av overgrepsmateriale gjennom offisielle posttjenester før internett dukket opp på 1990-tallet [1], [21]. I starten av internett ble overgrepsmateriale for det meste delt gjennom kommunikasjonssystemer som e-post eller applikasjoner for direkte meldinger og på nettsteder. Mellom 1996 og 2004 besøkte de fleste lovbryterne nettsteder for å få tilgang til overgrepsmateriale som bilder og video [2]. De delte også URL-koblinger (lenker) til materiale som ble lagret på fillagringstjenester [22]. Den utstrakte spredningen av overgrepsmateriale dukket ikke opp før utviklingen av nye fildelingsteknologier mellom 2004 – 2008, som peer-to-peer serversystemer (P2P) og BitTorrent-programvare. P2P kobler lovbrytere sammen i desentraliserte nettverk som tillater dem parallelt å laste ned flere filer fra forskjellige nettverksbrukere [2], [23]. Mengden tilgjengelig materiale fortsatte å vokse i denne perioden.

I årene 2008 – 2014 så man en drastisk økning i anonymitet med bruk av kryptovalutaer, Virtuelle Private Nettverk (VPN), og TOR nettverk. Perioden fra 2014 frem til i dag preges av den utbredte bruken av mobilteknologi og elektroniske tjenestetilbydere, både for produksjon og deling av materialer [2]. Mobilteknologi har spesielt gjort produksjon, distribusjon, deling og konsum av overgrepsmateriale enklere på grunn av faktorer som billige datapakker, høy kvalitet på mobilskjermer og -kameraer, og en bred tilgjengelighet av strømmings- og opptaksprogrammer. Enheter som nettbrett og smarttelefoner blir i økende grad brukt til å spre overgrepsmateriale, og de utgjorde 32% av alle søk knyttet til CSAM på Microsofts søkemotor Bing i 2015 [24].

Mobile enheter har fortsatt en viktig påvirkning. En rapport [25] fra 2021 viser at 62% av de unge respondentene som mottok seksuelt eksplisitt materiale, hadde mottatt det på mobilenheten sin. Mobil teknologi har vært en driver for økningen i video- og direktestrømming av overgrep mot barn på nett. Utviklingen i mobil bruk øker også risikoen for at yngre barn kan misbrukes. En bestemt faktor for denne trenden er at det er mer selvprodusert amatørinnhold tilgjengelig [26] (se også avsnitt 0).

Den utbredte bruken av internett og sosiale medier, kombinert med at datamaskiner, nettbrett og andre mobile enheter er lett tilgjengelig for barn og unge, skaper store muligheter for lovbrytere som søker å etablere seksuell kontakt med dem [1], [2]. Utvikling av internett og relaterte digitale tjenester skaper tre hovedstøtter for nettmisbruk:

i) Bred og enkel tilgang til materiale over internett som tilrettelegger for og normaliserer deling av materiale,
ii) Økt mulighet for gjerningspersoner til å målrettet nå flere mindreårige samtidig og styre overgrep i sanntid via direktestrømming, og
iii) Økt mulighet til å skjule identiteten til gjerningspersonen på grunn av høyt anonymiseringspotensial og mulighet til enkelt å opprette flere kontoer.

Teknologiske fremskritt fortsetter å utfordre politi- og påtalemyndighetenes evne til å forebygge, undersøke og rettsforfølge seksuell utnyttelse og misbruk av barn over internett. Lovbrytere bruker teknologi for å skaffe og vise materiale på nye måter, og som et mottiltak for å beskytte seg selv eller skjule sine aktiviteter på nett [27]. Blant de siste trendene legger vi merke til at lovbrytere i økende grad bruker ende-til-ende-kryptering og det mørke nettet for å beskytte privatlivet ved kryptert kommunikasjon, både gjennom elektroniske meldingstjenester og mobile enheter generelt, som igjen har et potensial til å ytterligere øke lovbryteres anonymitet og redusere sjansene for at de blir identifisert og sanksjonert. Videre øker nye former for produksjon, distribusjon og forbruk av overgrepsmateriale. For eksempel kunstig skapt materiale (for eksempel via utvidet virkelighet, eng.: "Extended Reality", og DeepFake). vil utfordre evnen til å identifisere identiteten til ofre og lovbrytere, samtidig som at det tillater nye former for produksjon av CSAM som tidligere var ukjent. For å få en bedre forståelse av denne kompleksiteten, gir vi i de neste avsnittene en oversikt over de forskjellige formatene, kildene og teknologi som legger til rette for distribusjon av CSA over internett.

2.2 Problemets omfang

Begrensninger i å forstå hele volumet av overgrepsmateriale

Det virkelige omfanget av spredningen og det faktiske volumet av overgrepsmateriale er vanskelig å spore og evaluere fordi det er umulig å vite det store volumet av uoppdaget materiale. Flere hindringer gjør det vanskelig å estimere hele volumet. For det første er en del materiale utilgjengelig for allmennheten og ESP, fordi det er produsert og delt gjennom krypterte nettverk eller proprietære digitale tjenester der bare avsender og mottaker kan se meldingene. For det andre gjør det store volumet av digitalt materiale på internett det vanskelig å undersøke, identifisere og spore spredningen av overgrepsmateriale. For eksempel, hver dag blir det produsert mer enn én million timer video hvert minutt over hele verden, 16 millioner delte meldinger, 5,9 millioner søk på Google, 2,4 millioner delinger på Snapchat og 1,7 millioner innlegg delt via Facebook [28]. Derfor blir identifisering og sporing av overgrepsmateriale en stor utfordring for både politimyndigheter og ESPer.

De store volumet samt mangfoldet av teknologier som brukes gjør det vanskelig for politi og frivillige organisasjoner å spore spredning av CSAM. I tillegg til det faktum at informasjon om tidligere identifisert og kjent overgrepsmateriale er fragmentert på tvers av ulike lovgivningsmyndigheter, frivillige organisasjoner og ESPer. Den største globale kilden til rapporterte overgrepsmateriale kommer fra NCMEC, som amerikanske ESPer (Meta, Google, Microsoft, osv.) plikter i henhold til amerikansk lov å rapportere til når de oppdager CSAM på sine tjenester. I motsetning til dette der det for øyeblikket i Europa ikke noen juridisk pålagt rapporteringskrav. Derfor er de avhengig av tips fra NCMEC og lokale/nasjonale hjelpetelefoner som mottar rapporter fra publikum eller ESPer som frivillig detekterer og rapporterer nettadresser, bilder eller videoer på nettet som inneholder overgrepsmateriale. De viktigste europeiske hjelpetjenestenettverkene er InHope i EU og IWF i Storbritannia.

Vi forsøkte å sammenligne de nåværende systemene som bruker hele CSAM-volumet, ved å analysere åpenhetsrapporter fra ESPer og rapporter fra rapporteringssentre og hjelpetelefoner for å utforske effektiviteten til offentlig rapportering versus ESP-identifisering av CSAM gjennom deres interne systemer [29]. NCMEC rapporterte at i 2021 kom 99% av rapportene fra ESPer sammenlignet med de fra allmennheten [5]. Med andre ord så ESP meldte over 29,1 millioner av 29,3 millioner totalt rapporter. En

gjennomgang av gjennomsiktighetsrapporten fra Meta (Facebook sin Community Standards Enforcement Report) viser at så mye som 99% av alt rapportert materiale med barn i fare oppdages proaktivt gjennom bruk av deres interne programvareløsninger, mens de resterende 1% av rapportene blir sendt inn av tjenestens brukere [30]. Tilsvarende prosentandeler rapporteres av Microsoft, Google, Snap, Twitter og andre tjenesteleverandører [29].

Dette funnet illustrerer at det er ineffektivt å stole på offentlig rapportering om tilgjengelig CSAM. Analysen viser at innsatsen og juridiske krav overfor ESPer for å spore opp og fjerne overgrepsmateriale spiller en avgjørende og uunngåelig rolle i å begrense det sosiale problemet med CSA over internett. Likevel kritiserer og advarer overvåkningsorganisasjoner og frivillig foreldre som kartlegger og rapporterer om utnyttelse over populære sosiale plattformer om feil algoritmer og hvor enkelt gjerningspersonene kan unngå å bli avdekket av interne programvareløsninger til ESPer [31].

Manglende globale juridiske krav for aktivt å søke etter CSA og CSAM i ESP tjenester, samt frivillig rapportering og inkonsekvente og sporadiske tilnærminger til avdekking av CSAM gjør at mange ESPer (spesielt blant mindre og mellomstore bedrifter) kan bli brukt som delingsplattformer for overgrepsmateriale. Konkret rapporterer NCMEC at så mye som 93% av alle rapporter kommer fra én leverandør, Meta (som eier Facebook, WhatsApp og Instagram) [5]. NCMEC ble kontaktet av ytterlige 1400 leverandører. På en annen side så melder Storbritannias viktigste hjelpetelefon, IWF, at de er i kontakt med om 175 selskaper [6]. Men en oversikt fra 2017 viser at Storbritannia har flere enn 351 000 registrerte IKT-virksomheter. Likevel rapporterer IWF at så mye som 66% av alle rapporter som ble vurdert og 94% av alle det ble aksjonert mot, ble hentet av deres egne analytikere som søkte gjennom internett, i stedet for at rapporteringene kom fra allmennheten, politirapporter, hjelpetelefoner og ESPer [6].

Vår analyse fører oss til å tro at mengden av uoppdaget CSAM som sirkulerer på internett er vesentlig større enn tallene vi har kunne avdekke. Forskjellene i regulatoriske rammer, manglende evne til å spore produksjon og distribusjon av CSAM gjennom nettbaserte tjenester og enorme mengder med innhold som lastes opp kontinuerlig gjør det vanskelig å avdekke mørketallene.

Med dette som bakteppe diskuterer vi videre tall og trender som er hentet inn gjennom vår analyse av litteratur og primære dybdeintervjuer fra norsk politi.

Omfang og globale trender av overgrepsmateriale basert på rapporter fra rapporteringssentre og hjelpetelefoner

CSA-trender blir hovedsakelig estimert via antall tips (rapporter) som hjelpetelefoner og rapporteringssentre mottar. Fra begynnelsen i 1998 har NCMEC rapportert å ha mottatt totalt over 82 millioner meldinger om ulike former for seksuell utnyttelse av barn på nettet. I tillegg har de samarbeidet med politimyndighetene for å gjennomgå over 322 millioner bilder og videoer, som resulterte i over 19 100 identifiserte ofre [32]. Bare i 2021 mottok NCMECs Cyber-tipstelefon 29,3 millioner rapporter, hvorav 99% tilhørte kategorien overgrepsmateriale, mens 1% omfattet andre former for CSA, slik som lokking av barn, grooming, sexhandel osv. [32].

Den globale trenden er at antallet rapporter øker over tid. I 2021 økte antall rapporter til NCMEC med 35% sammenlignet med 2020 [32]. Det europeiske nettverket av hjelpetelefoner, InHope, rapporterer

om å ha mottatt 928 278 nettadresser med mulig ulovlig og skadelig materiale som viser utnyttelse av og seksuelle overgrep mot barn i 2021. Hver nettadresse kan inneholde flere bilder eller videoer. I 2021 vurderte IWF over 361 000 rapporter om nettadresser, hvorav 7 av 10 rapporter fant bilder der barn ble seksuelt misbrukt [6]. IWF registrerte en økning på 20% i antall rapporter i 2021 sammenlignet med 2020 [6].

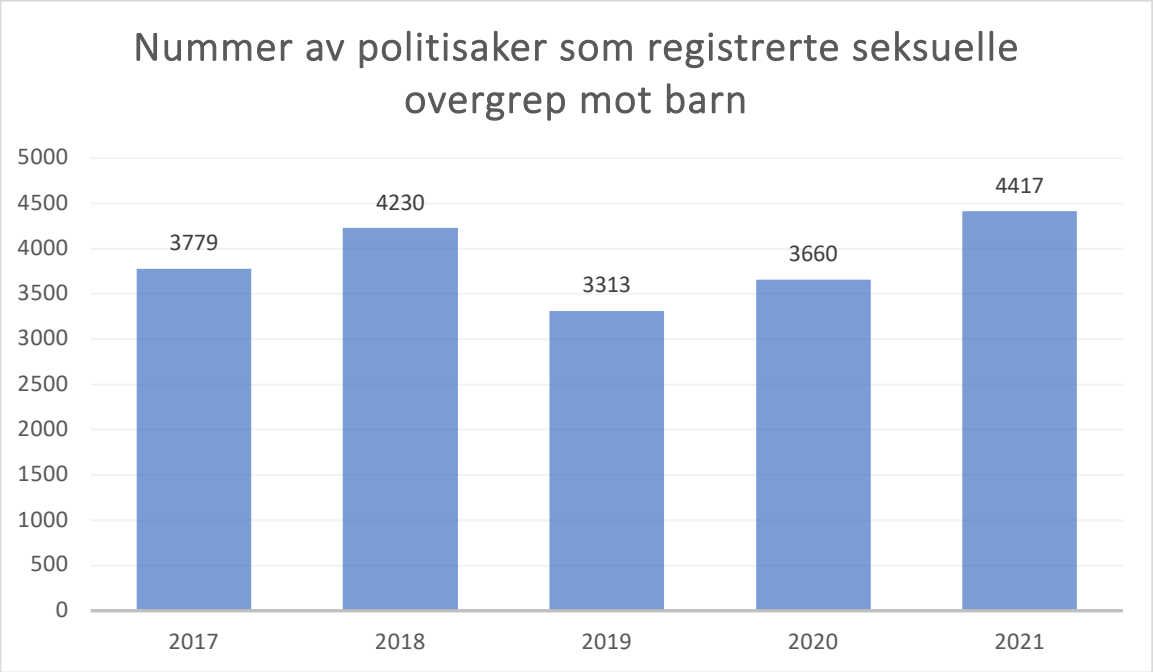
Denne oversikten illustrerer den betydelige forskjellen i rapporteringstall mellom NCMEC og andre hjelpetelefoner. Siden rapportering kan gjøres per nettsted (med mer materiell) eller for enkelt filer, og fordi det samme materialet kan rapporteres av mer enn én person, så er det ikke nyttig å ha en direkte sammenligning på tvers av hjelpetelefoner. Vi analyserte derfor antall unike (ikke-repeterende) materiale rapportert til rapporteringssentre og antall rapporter som bekrefter å inneholde overgrepsmateriale. Ifølge NCMEC-rapporter fra 2021 var rundt 42% (16,9 av 39,9 millioner) av alle rapporterte bilder var unike, mens 11% (5,1 av 44,8 millioner) av rapporterte videoer var unike [32]. Rundt 70% av IWF-rapportene er bekreftet å være overgrepsmateriale, der rundt 13% av den samlede rapporteringen fra allmenheten har vært rettsstridig (bekreftet å inneholde CSAM) [6]. Mens InHope melder om at 82% av rapporterte nettsteder som ble analysert i 2021 var tidligere ukjent for dem [33]. Det er uklart hvor mye av dette materiale er unikt og hvor mye materiale som overlapper med rapporter identifisert av NCMEC eller andre hjelpetelefoner.

Til sammen viser disse tallene at antallet overgrepsmateriale som blir rapportert er flere titalls millioner per år. Antall rapporter har de siste årene jevnlig økt mellom 20 - 30%. Den mest betydningsfulle kilden til å finne overgrepsmateriale er de proaktive søkene ESPer og frivillige organisasjoner foretar seg. De kan ikke stole på retroaktiv merking eller tips fra brukere eller allmenheten. Å stole på rapporter fra allmenheten ser ut til å være mindre pålitelig når det gjelder nøyaktighet, kan være mer sporadisk og ubetydelig i det totale omfanget av rapporterte materiale.

Oversikt over seksuell utnyttelse av barn og overgrepsmateriale trender i Norge

Etter å ha sett på de globale tallene og trendene, går vi inn på andelen av saker som er rapportert i Norge. I dette avsnittet ser vi på trender som er rapportert av norske politimyndigheter så vel som mengden av saker som er hentet fra rapporteringssenteret (NCMEC), som er den viktigste eksterne kilden til rapporter.

Figur 1 illustrerer trender i antall politisaker relatert til seksuell utnyttelse av barn i Norge for perioden fra 2017 til 2021. Riktignok har antallet politisaker vært noe varierende gjennom årene, men vi ser likevel en samlet økning i antall saker over tid. Rekorden ligger på 4417 saker i 2021. Det er viktig å bemerke at det norske strafferegisteret ikke skiller mellom seksuell misbruk av barn begått i den fysiske og virtuelle/digitale verden. Derfor mangler politiet en tydelig sentral veiledning for hvordan de registrerer rapporterte lovbrudd i systemet (STRASAK), noe som gjør at ulike saksbehandlere registrerer saker inkonsekvent. Derfor kan disse statistikkene ikke gi et klart bilde av overgrepsmateriale på nett og digitale seksuelle trender for utnyttelse av barn.



Figur 1: Totalt antall politisaker knyttet til alle aspekter av seksuell utnyttelse av barn, på tvers av alle politidistriktene i Norge. Kilde: Data hentet fra det norske straffesaksregisteret (STRASAK).

For å forstå de nettbaserte seksuelle utnyttelsene av barn så utforsket vi den viktige eksterne rapporteringskilden NCMEC som gir innblikk i den internettbasert bruk og delingen av overgrepsmateriale for norske statsborgere og IP adresser. NCMEC sender sine rapporter til Kripos, som deretter distribuerer sakene videre til regionale politidistrikter. Tabell 1 viser rapportene om overgrepsmateriale som norsk rettshåndhevelse mottok fra NCMEC. Norge mottok rundt 7850 rapporter i 2021 fra den globale mengden NCMEC-rapporter. NCMECs fordeling på tvers av land viser at det største antallet rapporter kom fra India, Filippinene og Pakistan [5], som har mye større befolkning og mindre utviklet juridiske systemer i forhold til Norge, så en relativt liten andel (mindre enn 1%) av globale rapporter knyttet til Norge er forståelig.

	2018	2019	2020	2021
Antall NCMEC-rapporter globalt*		16 987 361	21 751 085	29 397 681
Antall NCMEC-rapporter til Norge	10 463	6 868	7 039	7 850
Rapporter som er inntatt for videre analyse	1 468	1 928	2 549	3 644
Prosentandel av importerte saker	14,0 %	28,1 %	36,2 %	46,4 %

*Tabell 1: Oversikt over mottatte rapporter fra NCMEC-organisasjonen til norsk politi. Kilde: Kripos, NC3-enhet (2022). Statistikk fra seksjon for nettrelaterte overgrep - behandling av NCMEC. * Statistikk fra NCMECs nettside: NCMEC-data (missingkids.org).*

En inngående drøfting med politimyndighetene om tolking av trender i NCMEC-rapportering viser at nedgangen i antall rapporter mellom 2018 og 2019 ikke er en indikator på lavere grad av utnyttelse av barn som forekommer i Norge. I stedet gjenspeiler det at gjerningspersonene i større grad tok i bruk

ende-til-ende-kryptering (f.eks. i WhatsApp, Skype og Snapchat) og nedleggelsen av Yahoo Messenger som gav en nedgang i antall NCMEC-rapporter mellom 2018 og 2019 [29].

Prosentandelen av NCMEC-saker som er tatt med til videre etterforskning av straffbare forhold har økt fra 14% i 2018 til 36,2% i 2020 og 46,4% i 2021. *Antall rapporter som er inntatt for videre analyse* i Tabell 1 gjelder rapporter som er manuelt lagt inn i straffesaksdatabasen. For å sette en sak i databasen må det finnes en klar indikasjon på brudd på norsk straffelov. Videre må det foreligge et potensiale for å knytte den rapporterte informasjonen til en person, adresse eller annen lignende identifisering. Våre dybdeintervjuer med politifolk som samhandlet med straffesaksdatabasen viste at i de tilfellene hvor rapporten ikke ble lagt inn, så var det ufullstendige opplysninger som gjorde det uegnet for videre undersøkelser, slik som:

- tvil om alderen til personene som er avbildet,
- ingen vedlagte filer,
- det er ofte umulig å fastslå identiteten til gjerningspersonen om de brukte VPN-tjenester eller lignende anonymiseringsteknikker.

De fleste av disse problemstillingene er relatert til juridiske problemstillinger eller teknologiske utfordringer ytterligere utdypet i Kapittel 4.

2.3 Formater og kilder for seksuell utnyttelse av barn over internett

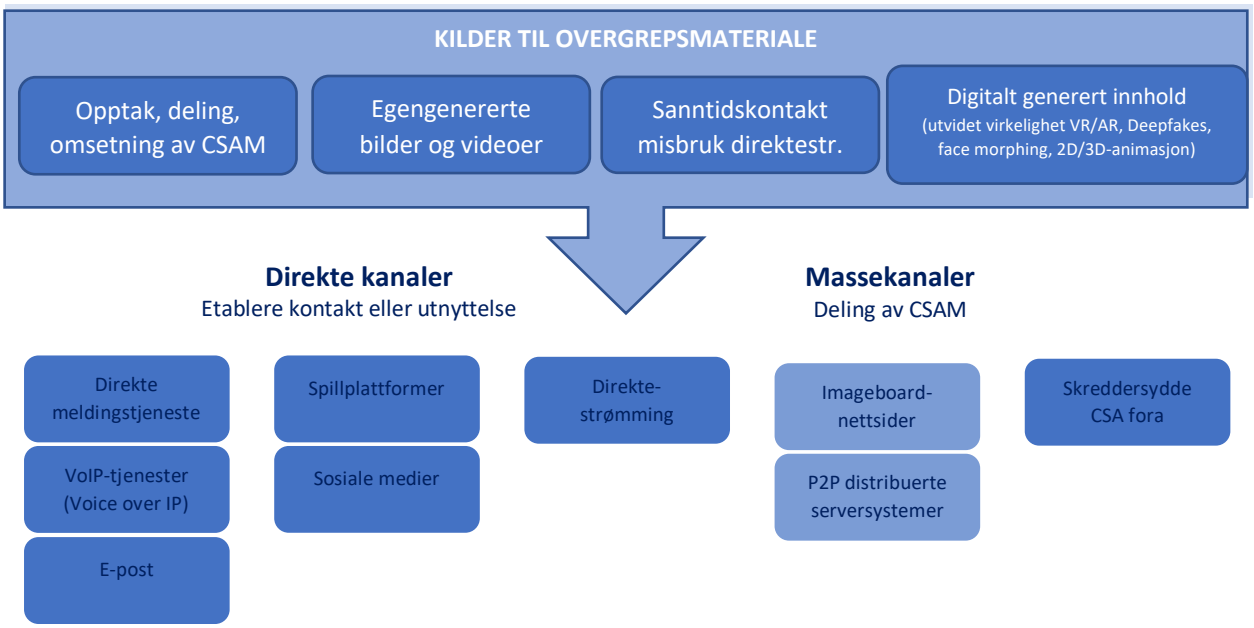
For å redusere kompleksiteten rundt virkningen av teknologi på seksuell utnyttelse av barn over internett, så skiller denne rapporten mellom to former for misbruk: I) deling av upassende materiale som seksualiserer barn og II) etablere direkte kontakt med barn gjennom grooming. Det er fordi disse handlingene representerer ulike kriminelle aktiviteter, selv om de kan bruke samme eller lignende teknologiske kanaler. Derfor skiller Figur 2 mellom kildene til internettrelatert overgrepsmaterialer og teknologiske arenaer/kanaler hvor gjerningspersonene kan etablere kontakt med mindreårige og/eller dele overgrepsmateriale. Grupperingen av kildene til nettbasert overgrepsmateriell i Figur 2 er som følger:

- Deling eller handel med overgrepsmateriale som allerede eksisterer slik som tidligere opptak.
- Produksjon og opprettelse av nytt overgrepsmateriale, ofte tilrettelagt av mobilteknologi (direktestrømming) og egenprodusert innhold gjennom tvang, utpressing eller grooming.
- Ny trend med kunstig og digitalt produsert materiale.

Resten av dette avsnittet beskriver disse kildene. Underavsnitt 0 beskriver direkte opprettelse og deling av overgrepsmateriale. Underavsnitt 0 og 0 viser detaljer i hvordan seksualiserende materiale erverves fra ofre gjennom henholdsvis egenprodusert innhold og direktestrømming. Til slutt beskriver Underavsnitt 0 opprettelse av kunstig og digitalt materiale, som sannsynligvis kommer til å representere en viktig trend i fremtiden.

Nedre del av Figur 2 klassifiserer ulike kanaler og plattformer der materialet blir produsert og delt. Dette rammeverket er ikke ment til å være uttømmende, men det skal gi en viss klarhet og syntese av den komplekse og fragmenterte bildet av måten teknologien påvirker produksjonen og delingen av overgrepsmateriale. Vi registrerer at ulike lovgivningsmyndigheter og land regulerer ulike former for

overgrepsmateriale på nettet ulikt, samt at den kriminelle handlingens alvorlighetsgrad varierer mellom kildene. Det vil si at deling av egenprodusert materiale imellom mindreårige og produksjon av kunstig/digital overgrepsmateriale ikke kan likestilles med faktisk barnemisbruk eller grooming. I våre forsøk på å gi et generelt bilde av kildene, klarte vi åpenbart ikke å illustrere nyansene og forskjellene som finnes hos ulike lovgivningsmyndigheter samt i de ulike typene, se også Kapittel 4.



Figur 2: Formater og kilder for overgrepsmateriale og seksuell utnyttelse av barn over internett.

2.3.1 Opptak, deling og omsetning av overgrepsmateriale

Det er som oftest tidligere eksisterende overgrepsbilder og -videoer som blir delt og omsatt i de fleste områdene på nettet gjennom forskjellige distribusjonskanaler og -teknikker (se Avsnitt 2.4). Lovbrytere tilgjengeliggjør og deler overgrepsmateriale seg imellom gjennom en-til-en kommunikasjonsmetoder eller bred/massedistribusjon gjennom en-til-mange nettverksdelingsteknologi.

Det delte materiale inkluderer flere ulike typer formater, som for eksempel bilder, videoer, direktestrømming eller opptak av direktestrømmet overgrep [34]. En analyse av rapporterte tilfeller til NCMECs varslingstjeneste Cyber Tipline viser at rundt halvparten knyttes til videoer (45 millioner av 85 millioner) og resten knyttes til annet materiale som bilder (rundt 40 millioner) [32]. Flest rapporter kommer fra bildedelingstjenester, nettskylagring og chattjenester. Av disse blir omtrent 42% av bildene og 11% av videoene identifisert som unike. Derfor forblir store mengder tidligere produsert og distribuert overgrepsmateriale i omløp. Men nytt innhold og nylig produsert materiale er ennå ikke identifisert (se Underavsnitt 2.2).

De direkte kildene til overgrepsmateriale på nettet kommer fra at man tar bilder og videoer og legger disse ut på nettet. Men det kan også legges til rette for direktestrømming av det aktuelle misbruket.

Sistnevnte har blitt mer utbredt de siste årene gjennom en utbredt bruk av direktestrømming og Voice over IP-teknologier (VoIP) [11] samt digitale betalingssystemer. Opptak av misbruket kan gjøres skjult slik at lovbrytere tar opptak av skjermen, men det kan også være at lovbrytere får tilgang til eller hacker usikrede nettverkskameraer (webkameraer) eller laste ned upassende innlegg publisert i sosiale medier. Lovbrytere kan også direkte be eller tvinge mindreårige til å produsere egenprodusert overgrepsmateriale, og de kan groome mindreårige ved å oppmuntre eller presse dem til å sende videoer eller bilder. I de fleste tilfellene hvor lovbryterne produserer overgrepsmateriale så kjenner de sine ofre, hvor 37% er ofrenes familiemedlemmer og 36% er andre bekjente [16].

Store arkiver hvor eksplisitt overgrepsmateriale kan bli funnet, er lagret på bildetavlenettsteder (eng.: "imageboards") dedikert til opplasting av bilder. Som verter for disse bildetavlenettstedene kan de blant annet:

- Skreddersy ulovlige nettsteder dedikert til arkiver med overgrepsmateriale.
- Legitime nettsteder med lovlig voksent innhold (f.eks. pornografisk) kan lenke til andre nettsteder med overgrepsmateriale.
- Andre legitime nettsteder som brukes til distribusjon av overgrepsmateriale uten tillatelse eller kjennskap fra eieren [22].

I 2021 rapporterte InHope at 31% av alt materiale de identifiserte var plassert på nettsteder, mens rundt 26% var plassert på fildelingstjenester og 25% på bildedelingstjenester. De poengterte at det hadde vært en 17% nedgang i overgrepsmateriale funnet på nettsteder (fra 48% i 2020 til 31% i 2021) og en dobling av mengden av CSAM funnet på fillagringsservere (26% i 2021, sammenlignet med 13% i 2020) [33].

Lovbrytere synes å bruke skylagringsleverandører til å lagre og distribuere overgrepsmateriale via lenker eller nettadresser som annonseres på bildetavlenettsteder, illegale fora og samtalerom (chatrom) [22]. Nettadressene (URL) til CSAM kan videre tilgjengeliggjøres gjennom skreddersydde fora for deling av overgrepsmateriale eller andre (også legitime) nettsteder som fungerer som fora (grupper, rom osv.) som tillater brukere å dele lenker.

81% av ofrene ble avbildet som prepubertale (i alderen 3-13) [22]. Spesielt problematisk er det faktum at deling av CSAM gjør at barn gjentatte ganger til offer. I en undersøkelse [9] med de som har vært utsatt for seksuelle overgrep, der bilder ble distribuert, anga 67% av dem at distribusjonen av deres bilder påvirker dem sterkt. I tillegg til det faktiske misbruket de ble utsatt for, fortsetter de å lide på grunn av at bildene tilgjengeliggjøres og at distribusjonen aldri slutter.

Mens deling og omsetning av overgrepsmateriale representerer tradisjonelle kilder, så ønsker vi å rette spesiell oppmerksomheten mot de nyere kildene som sannsynligvis vil representere fremtidige trender for kilder til CSAM: *Egenprodusert innhold, direktestrømming og kunstig frembrakt innhold.*

2.3.2 Egenprodusert innhold

Egenprodusert materiale er seksuelt eksplisitte bilder eller videoer som er laget, overført eller utvekslet av mindreårige under 18 år. De lager vanligvis slikt materiale selv med web-kameraer eller smarttelefoner for så å dele det direkte med en mottaker eller via et økende antall plattformer [35]. IWF rapporterer at nesten tre fjerdedeler (72%) av gjennomgått materiale i 2021 kan klassifiseres som

egenprodusert innhold [36]. I løpet av bare de tre første månedene i 2021 doblet egenprodusert innhold seg i forhold til samme periode i 2020. Mindreårige jenter representerer en spesielt sårbar gruppe, hvor 99% av egenprodusert innhold viser jenter. Opptil 81% av alle bilder og videoer omfatter jenter i alderen 11 til 13 år, på deres eget soverom eller et annet rom hjemme [36].

Egenprodusert innhold fra mindreårige økte under koronaviruspandemien [35], og alle intervjusubjekter i vår primære forskning fant dette spesielt bekymringsfullt. Denne trenden kan være knyttet til popularisering av "sexting" (å sende seksuelt eksplisitte meldinger) blant mindreårige og endring av sosiale normer for hva som kan deles på nett og med hverandre. For eksempel fant en undersøkelse [35] ut at rundt 40% av amerikanske barn mener "det er normalt for folk på deres egen alder å dele nakenbilder".

Det å sende og motta egenprodusert materiale har også økt blant europeiske ungdommer de senere årene [37]. Det kan også ha resultert i at et økende antall unge har blitt dømt de siste årene for å ha produsert og/eller distribuert seksualiserte bilder eller videoer av andre på sin egen alder [38]. Ungdommer fra nordeuropeiske land (som Norge og Storbritannia) rapporterte høyere antall sendt og mottatt seksualisert materiale i forhold til ungdommer fra Sør-Europa (som Bulgaria, Italia og Kypros) [38]. For eksempel, halvparten av alle tenåringer mellom 13 og 18 år i Norge er angivelig blitt bedt om å dele nakenbilder av seg selv, og 4 av 10 tenåringer har innrømmet å ha fått nakenbilder av andre [7]. Manglende bevissthet om juridiske bestemmelser er en fellesnevner blant de domfelte.

Problemet med denne kilden til materiale er at ikke all sexting anses som ulovlig. Deling av eksplisitt innhold er juridisk problematisk når man ikke kan bevise et juridisk gyldig samtykke mellom barn; når materialet videresendes uten samtykke; når det brukes av voksne over myndighetsalder på 18 år eller når det brukes til nettmobbing. I tillegg er det å "gi sitt samtykke" omdiskutert når det dreier seg om CSA på nettet. Kriminalisering av alle krenkelser knyttet til CSA forsvares på bakgrunn av at barn under 18 år ikke kan anses å ha samtykkeevne til å la seg misbruke og utnytte seksuelt [16].

2.3.3 Grooming og egenprodusert innhold

Volumet av overgrepsmateriale vokser også gjennom *barneforførelse*, som omfatter mange typer forbrytelser og vanligvis innebærer å lokke barn (dvs. grooming) til å engasjere seg i seksuell krenkende adferd og andre lignende aktiviteter. Lovbrytere kommuniserer med barn via internett med den hensikt å begå seksuelt overgrep eller forlede barn til å ta seksuelt eksplisitte bilder og videoer. Omfanget av grooming som foregår på internett har økt med 97,5% fra 2019 til 2020 og utgjør så mye som 38 millioner rapporter [39]. FNs spesialtalsmann anslo at det til enhver tid finnes omtrent 750 000 lovbrytere koblet til internett som har grooming som formål [16].

Groomere har en tendens til å bruke flere teknikker for å be om eller lure barn til selv å produsere CSAM. I noen tilfeller kan en groomer be barn sende bilder eller videoer av seg selv, og mange barn vil gjøre dette i den tro om at de er i et slags romantisk forhold [12], [17]. I andre tilfeller sender gjerningspersonen bilder av personen de utgir seg som, og overbeviser deretter barna til å sende lignende bilder av seg selv. En tredje metode er å be om seksualiserte bilder mot betaling i form av penger, sigaretter, alkohol eller andre ting barnet ønsker seg.

Gjerningspersonene betaler via ulike digitale betalingsløsninger ved hjelp av tjenester for deling av penger (jf. Vipps-appen i Norge), digitale gavekort eller betalinger i kryptovaluta. Noen ganger mottar offeret midler på kontoen til en venn eller noen over 18 år for å unngå at foreldrene får vite om mistenkelige transaksjoner fra fremmede [38]. I 2019 rapporterte Europol [7] derimot om økende tendens blant lovbrytere til å bruke egenprodusert materiale for å presse eller tvinge ofre til å produsere mer materiale og/eller involvere andre barn i produksjonen (eng.: "sextortion", en sammensetting av de engelske ordene for "sex" og "utpressing").

Intervjuepersoner fra nettunderholdningstjenester og sosiale medier anga at groomere og andre lovbryteres typiske modus operandi består i målrettet å velge barn på spill- og sosiale plattformer og søke å vinne deres tillit, før de forfører dem og oppfordrer dem til å bruke kanaler med strømmingsmuligheter og tvinger dem deretter til å utføre seksuelle handlinger som filmes. En nylig tematisk analyseevaluering av rettsavgjørelser i Sverige knyttet til 50 lovbrytere som var involvert i CSA over nettet (med en medianalder på 29 år), viste at lovbrytere vanligvis brukte to hovedtyper manipuleringsstrategier [28]:

- Den mest brukte strategien var å bruke utpressing (trusler, bestikkelser eller masing).
- Den økende strategien var å gi komplimenter, smigre, opptre som en venn, eller uttrykke kjærlighet. Denne strategien synes å være oftere brukt av yngre lovbrytere.

NOVAs rapport [40] om utnyttelse av barn over internett i Norge viste at 30-50% av lovbrytere i 2018 var yngre enn 18 år. NOVA advarer om at denne typen grooming – der ofrene føler at de var en del av det romantiske forholdet og derfor utvekslet bilder eller ble seksuelt misbrukt – blir mer vanlig, og at barn unngår å rapportere disse overgrepene [41], [42].

Intervjusubjekter fra allmennheten mener at denne trenden sannsynligvis kommer til å vokse i fremtiden ettersom samspill mellom ungdommer og barn i økende grad flytter seg til digitale arenaer. Motivene for frivillig egenproduksjon av seksualiserende bilder og videoer er spesielt lite kjent og forstått. De kan variere, men de inkluderer ofte romantiske forhold, nettmobbing eller ønske om å motta ressurser eller oppnå anerkjennelse på nettet.

En norsk rapport tyder på at de romantiske forholdene mellom ungdom i stor grad har flyttet på nettet og at det råder en felles antakelse blant ungdom: "Hvis du liker meg, må du dele et [naken] bilde med meg" [41]. Nye sosiale normer *"normaliserer ulovlig atferd og flytter grensene for hva som er akseptabelt og hva som ikke er det, da barn avviser myndighetenes og foreldrenes tolkning av hva som er normalt"* – oppfatningen til ett intervjusubjekt fra en barnevernsorganisasjon.

Nettmobbing med deling av materiale representerer også en av de større utfordringene for barnevernsorganisasjoner [43]. Uautorisert deling av nakenbilder er den vanligste metoden for nettmobbing og en av de mest sårende for ofrene. Kripos har lagt merke til en bekymringsfull trend [44] der mindreårige barn administrerer såkalt sosiale kontoer for "eksponert materiale" der informasjon om deres jevnaldrende (ofte skolekamerater) deles med andre barn. Disse kontoene administreres av barn, hvorav noen er knapt 11 år gamle [44].

En urovekkende trend er at mindreårige selv selger eksplisitte bilder, videoer eller strømmer seksuelle handlinger. Nyere undersøkelser i Storbritannia [45], [46] og Norge [38] viser tilfeller der mindreårige produserer og selger seksuelt eksplisitt innhold av seg selv på sosiale medieplattformer som OnlyFans

eller gjennom applikasjoner for deling av penger. En tilsvarende kommersialisering av egenprodusert innhold inkluderer å lagre bilder eller ta opptak av videoer fra det opprinnelige opplastningsstedet og distribuere materialet videre i forskjellige nettfora, med hensikt å ta betaling for nedlastninger [47].

Egenprodusert materiale er ofte med på å skade ofrene på flere måter fordi materialet ofte deles med den indre gruppen som kjenner offeret. Hvis materialet lastes opp på internett er det vanskelig å spore og fjerne. Vi vet at ofrene tar sjelden kontakt med politiet selv, og at politiet vanligvis får kunnskap om saken først når foreldrene rapporterer hendelsen. I noen tilfeller har offeret sagt ifra til venner eller skolehelsesøster, barnevernsansatte eller andre personer utenfor familien [48]. Egenproduksjon av innhold blir sannsynligvis en av de største utfordringene for forebygging av seksuell utnyttelse av barn på nett, og det vil kreve koordinert innsats mellom skoler, foreldre, sivilsamfunn, myndigheter og bedrifter.

2.3.4 Direktestrømming som en kommende kilde til overgrepsmateriale

Å seksuelt utnytte barn på nettet er blitt enklere og lovbruddene som blir begått er mer ekstreme når gjerningspersonene er i stand til å nå flere barn samtidig eller styre direktestrømmet overgrep i sanntid [42]. Direktestrømmet overgrep og misbruk er når lovbryteren kan samhandle med overgriperen og å be om handlinger som ønskes begått mot barnet i sanntid [49]. Direktestrømming vil sannsynligvis fortsette å øke [50], tilrettelagt av økt tilgjengelighet av VoIP-plattformer, samt utbredelse av 4G og 5G og mer bruk av populære sosiale medieapplikasjoner med innebygde strømmingsfunksjoner (f.eks. WhatsApp). Tilgang til slik teknologi har gjort det nesten uproblematisk for lovbrytere å danne nettverk for å utnytte barn.

Direktestrømmet misbruk sprer seg på grunn av lovbryternes motivasjon for å unngå å etterlate digitale spor og inkriminerende materiale. Dette fører til at man heller bestiller strømmet misbruk i sanntid i stedet for å laste ned filer [17]. Misbruk er ofte organisert og/eller begått av tilretteleggere som har et allerede eksisterende forhold til barna, for eksempel et familiemedlem eller en groomer [51]. Enkelte utviklingsland fungerer som episenter for omsetting av direktestrømmede seksuelle overgrep, for eksempel Filippinene [52], [53], der det i 2020 ble rapportert at ett av fem barn mellom 12 og 17 ble utsatt for seksuelt overgrep over nettet [54].

Kontakten mellom lovbryter og tilrettelegger er ofte etablert på nettsteder som tilbyr kamera-til-kamera seksuelle tjenester for voksne og som også har "tjenester" for seksuell utnyttelse av barn. I noen tilfeller er tilretteleggeren den som tilbyr såkalte "live show" (direktesendt visning) med barn, i andre tilfeller ber eller etterspør gjerningspersonen om slik tjeneste. Lovbrytere betaler tilretteleggerne gjennom digitale betalingssystemer over internett. Noen ganger via kryptovaluta, som er vanskeligere å spore (se Underavsnitt 4.2.2). Tilretteleggerne som tilbyr og tilrettelegger for direktestrømmet misbruk vil tjene mellom 40 og 70 prosent av betalingen fra lovbryteren [17]. Betalinger sendes alltid før materialet strømmes, noe som gjenspeiler det økonomiske insentivet til tilretteleggere.

Straks betalingen er mottatt eller på et avtalt tidspunkt, blir seksuelle overgrep deretter strømmet via kommunikasjonstjenester som tilbyr meldinger og video. Normalt lagres ingen bilder eller videoer av seksuelle overgrep automatisk. Skulle gjerningspersonen eller tilretteleggeren lagre noe og deretter dele det, så blir materialet en del av det totale volumet av overgrepsmateriale tilgjengelig på internett. I 2018

viser IWFs undersøkelse av direktesendte opptak [55] at 98% av ofrene var barn i alderen 13 eller yngre og 28% var i alderen 10 år eller yngre. 18% av misbruket ble kategorisert som voldtekt og seksuell tortur, og så mye som 40% av materiale representerte alvorlig seksuelt misbruk av barn. Det vanligste scenarioet var jenter i eget hjem, ofte på soverommet eller badet, uten noen voksne. Lovbrytere instruerer ofrene til å misbruke seg selv og å strømme aktiviteten [55].

Ofre kan også bli groomet til å engasjere seg i nettstrømming av seksuelle aktiviteter på digitale plattformer, hvoretter materialet finner sin vei til andre seksuelle lovbrytere på nettet gjennom "capping". Begrepet "capping" refererer til permanente opptak av direktestrømmet barnemishandling ved hjelp av programvare som lagrer videoen fra web-kameraet. Disse opptakene (ofte kalt "captures") av direktestrømming blir deretter delt i mørke nettfora eller andre spesialutviklede kommunikasjonskanaler (se Figur 2 og Avsnitt 2.3.1). Det produseres og distribueres også stillbilder fra disse opptakene [47]. Denne typen krenkelse gjør offeret utsatt for sextortion, og annen type press for å sende ytterligere bilder eller ulovlig innhold. Australian Center to Counter Child Exploitation rapporterer at "capping" for tiden er den mest problematiske og krenkende trenden som genererer mellom 60-70% av rapporter til dens enhet for identifisering av ofre (Victim Identification Unit) [51].

Materiale fra 18 forskjellige direkteavspillingstjenester, inkludert sosiale nettverk, chatnettsteder og mobilapper [47], viser at barnet selv oppfordret til seksuelle aktiviteter for å få "liker" (eng.: likes, en type positiv reaksjon) eller respons fra seere. Ett jentebarn som oppga å være 12 år gammelt, anga å ha 50 seere i sitt kringkastings rom. Etter gjentatte ganger å ha stilt seg foran webkamera, uttalte hun at hun ville at det var ikke noe poeng i at hun fortsatte og at hun skulle stoppe sendingen hvis folk ikke begynte å kommentere eller "like" strømmen [47].

2.3.5 Digital og kunstig skapt overgrepsmateriale

Lovbrytere bruker teknikker innen kunstig intelligens (AI) for å skape nytt materiale eller å tilsløre eksisterende materiale gjennom animasjonsmedier, datagenererte 3D-modeller, eller ved å bruke utvidet virkelighetsteknologi (både virtuell og utvidet virkelighet). Disse teknikkene bruker visuelle filtre og bildemanipulering for å kunstig fremstille ofrene som yngre og/eller for å tilsløre identiteten til offeret og overgriperen.

Kunstig genererte CSA-bilder av barn i virtuelle miljøer inkluderer alt fra tegneserier (2D) til hyperrealistiske (3D) bilder og videoer. Digitale og kunstige framstillinger av barn har allerede eksistert i minst ett tiår. Et tidlig eksempel er seksuell 'alderslek' og simulert misbruk av barneavatarer i virtuelle verdener som Second Life fra 2003. Nye teknologiske fremskritt gir imidlertid lovbrytere nye muligheter for å skape kunstig genererte CSA og å tilsløre eksisterende materiale.

Forlenget virkelighet (XR) er et paraplybegrep for alle de ulike typene fengende teknologier som inkluderer utvidet virkelighet (AR), blandet virkelighet (MR) og virtuell virkelighet (VR). Formen disse utvidede realitetene tar, varierer mye, men kjerneteknologien går ut på å simulere en tredimensjonal verden og presentere den til en deltakers sanser på en slik måte at de behandler sensoriske innganger på samme måte som de opplever den virkelige verden. XR begynner å bli populær i voksen sexindustri, hvor det har blitt brukt til å skape fengende seksuelle spill og filmer, til å integrere haptiske enheter (teledildonics) og utvide tradisjonell illegal filming i virtuelle chat-rom [56].

Trenden vil trolig bli tatt i bruk av lovbrytere som seksualiserer barn ettersom teknologien modnes. XR forenkler etableringen av sexsimulatorspill og/eller modifisering av karakterer i eksisterende spill til å fremstille dem som barn, hvilket tillater lovbrytere å samhandle med dem som i den virtuelle verden. MR-teknologien tillater også en endring av eksisterende pornografiske bilder og videoer av voksne til å gi et falskt usømmelig bilde av et barn ved hjelp av filtre som 'babylinse' med det formål å fremstille den opprinnelige deltakeren som mer ungdommelig.

Ekte barn kan indirekte skades gjennom legitimering og normalisering av krenkelser relatert til seksuell interesse [56]. Simulert sex med barneavatarer kan innbefatte virkelige barn så vel som voksne; selv hvis dette ikke var tilfellet, kan dette ha konsekvenser for ekte barn ved at det forsterker lovbryteres seksuelle interesse for barn og kognitive forvrengninger som relaterer seg til lovbrudd.

Å endre bilder gjennom bilderedigeringsprogrammer (som Adobe Photoshop) krever ferdigheter og erfaring for å skape realistiske skildringer som er vanskelige å skille fra bilder av virkelige barn. Fremskritt i AI tillater imidlertid enkeltpersoner å automatisk redigere eller manipulere bilder uten behov for å tilegne seg de ferdighetene som er nødvendige for å skape realistiske bilder. Et eksempel på AI-drevet manipulasjon er 'deepfake'.

Deepfake erstatter bildet av en person i en video med en annen, på en slik måte at det er nesten umulig å oppdage. Deepfake-programvare blir for tiden brukt til å lage pornografi som ser ut til å inneholde kjendiser, ved at et kjendisansikt er slått sammen med kroppen av en pornostjerne. Denne teknologien kan ikke bare gjøre ofrene fremstå som yngre, men det kan også brukes til å tilsløre identiteten til offeret og gjerningspersonen ved at man erstatter et barneansikt i et usømmelig bilde med et annet barn som aldri har blitt filmet i en seksualisert sammenheng. Dette vil forhindre identifisering av ofre eller misbrukere og dermed forlenge offerets lidelse. På samme måte gjør nye AI-teknikker det mulig for lovbrytere å endre stemmen til å virke mer ungdommelig eller barnlig [57], noe som kan være av stor betydning i å gi støtte ved grooming.

I 2020 ble det anslått at en AI-robot som opererer på Telegram har generert 100 000 pornografiske 'deepfakes' av kvinner og jenter [51]. Utviklingen av AI har skapt en ny kategori av CSAM kjent som "morfet" (eng.: morphing) CSAM, der barneansikt redigeres inn på kroppen til en voksen som utfører seksuelt eksplisitte handlinger [58]. Slikt materiale er umulig å skille fra ekte bilder og videoer. Utviklingen av AI bør vekke bekymring fordi det kan føre til en generasjon av ny personalisert overgrepsmateriale [59].

Kunstig generert CSAM materiale er et voksende problem, spesielt på grunn av juridisk sanksjonstvetydelighet for denne type generert CSAM materiale [18]. I de fleste land i verden er denne typen kriminalitet for tiden ikke tydelig regulert og hva mer er, slik datagenerert materiale er sett på som lovlig [58]. Bare i tilfeller der et virkelig barns bilde brukes, er det grunnlag for rettslige skritt. Rapporten fra FNs spesialtalspersoner forsvarer kriminalisering av virtuelt barneovergrepsmateriale fordi realismen i bildene skaper illusjon om at barn egentlig er involvert. Realismen har en skadelig påvirkning fordi personer ser at slikt materiale likner på annet overgrepsmateriale [16]. Av denne grunn anbefaler rådene fra FN og legislativutvikling (som Lanzarote-konvensjonen og Europarådets konvensjon om beskyttelse av barn mot seksuell utnytting og seksuelt misbruk, CETS 201) at alle former for materiale som inneholder barn i seksuelt eksplisitt atferd eller som viser barns kjønnsorganer skulle kriminaliseres dersom generering av innholdet er realistisk eller simulert [16]. Likevel sliter politimyndigheter med denne typen teknologiutvikling på grunn av deres utilstrekkelige tekniske

ferdigheter i å håndtere slike tilfeller og mangel på tilgjengelige verktøy. Kunstig opprettet innhold har alvorlige implikasjoner for politi, for eksempel idet det stilles spørsmål ved ektheten av bevis, og det vanskeligjør og hindrer etterforskningen [59]. Intervjuede etterforskere i Norge er spesielt bekymret for feltet som omfatter kunstig frembrakt overgrepsmateriale:

> *«Vi begynner å se deepfake hvor barneansikter plasseres på en liten voksen (pornostjernekropp). Denne trenden vil sannsynligvis øke i fremtiden. Virtuell virkelighet vil videre sannsynligvis utvikle seg til en arena for misbruk. Pornoindustrien beveger seg i retning salg av sexleketøy som simulerer handlingene i videofilmer. Denne [teknologien] vil bli det neste store problemområdet. Det vi tror vil skje, er mer direktestrømming av misbruk i andre land.»*

2.4 Oversikt over store distribusjonskanaler for overgrepsmateriale

For å effektivt avdekke distribusjonskilder for overgrepsmateriale, er det viktig å forstå hvor mye innhold som deles på tvers av ulike distribusjonskanaler. E-post var en gang den viktigste metoden for å distribuere CSAM-filer. Imidlertid har distribusjonskanalene fulgt utviklingen av nye former for internett-teknologi [49]. CSAM distribusjonskanaler finnes på nettsteder, søkemotorer, chat-tjenester, fora, sosiale medieplattformer, fildelingsprogrammer og de fleste andre steder som er koblet til internett [21], [60], [61].

Gjerningspersoner bruker alle tilgjengelige kanaler som gjør dem i stand til å kommunisere og dele overgrepsmateriale på det åpne og mørke nettet [17]. Uavhengig om kanalene er sikre eller usikre. Som oftest benyttes distribusjonskanaler som er gratis og offentlige eller benytter offentlig tilgjengelig teknologi [2]. Selv om alle typer kanaler blir brukt uavhengig av personlig risiko, så vil mange gjerningspersoner vanligvis velge kanaler basert på deres oppfattelse av nytte og risiko.

Peer-to-peer-deling og nettlesere er de vanligste teknologiene som ble en inngangsport til overgrepsmateriale blant domfelte lovbrytere i USA. Disse distribusjonskanalene viser betydelig vedvarende bruk [27]. De senere årene rapporterer politiet om nye personvernbeskyttende programmer er i betydelig vekst, slik som ende-til-ende lagring og kommunikasjon, kryptering, TOR og andre anonymiseringsteknikker [62].

Dette avsnittet vil gi en oversikt over de viktigste kanalene som brukes av lovbrytere som får tilgang på og skaper overgrepsmateriale. I Figur 2 har vi forsøkt å skille mellom de kanalene som brukes til å etablere en-til-en eller en-til-flere kontakter (dvs. direkte kommunikasjon som e-post- og meldingstjenester), og de som er mer egnet for massedeling av CSAM (bildetavle- og nettsteder eller distribuerte serversystemer). Naturligvis er det ikke mulig å lage et klart skille, gitt at disse kanalene ofte brukes til ulike formål. Vi starter med å gi oversikt over de vanligste og tradisjonelle kanalene før vi fortsetter å beskrive relativt nye kanaler som bruker ny teknologi og som sannsynligvis vil vise seg å være viktige trender i fremtiden.

2.4.1 Nettsøkemotorer og bildetavlenettsider

Nettsteder på internett fungerer ofte som en inngangsport for de som leter etter overgrepsmateriale. Disse nettstedene inneholder allerede eksisterende og tilgjengelig materiale som er blitt delt og omsatt over lenger tid. Lovbrytere bruker nettsøkemotorer og nøkkelord for å få finne tilgang til nettsteder som inneholder overgrepsmateriale. Materialet kan være innebygd i legitime pornografiske nettsteder, eller nettsteder som spesifikt leverer overgrepsmateriale av barn. Nettstedene kan også virke legitime vet første øyekast, men de fungerer bare som et mellomledd og leder besøkende til andre nettsteder hvor de kan få tilgang til overgrepsmateriale [63]. I 2021 identifiserte IWF 252 194 individuelle nettadresser som enten inneholdt CSA-bilder eller lenket til bildemateriale [64]. 39% av barna som ble identifisert i bildene var under 11 år [42].

Nettsteder spesialiserer seg på enten å lagre eller vise overgrepsmateriale av barn, hvorav kun 20% av nettsteder gjør begge deler [60]. Undersøkelser av nettsteder har vist at de fleste nettstedene gjør svært lite for å skjule materialet [65] og er mer fokusert på å organisere det i f.eks. en mappestruktur med år/måned for enklere tilgang og markedsføring av materialet [60]. Over 27% av nettstedene viste overgrepsinnhold på forsiden [60]. Denne handlingen viser at det primære målet med nettsteder som viser overgrepsmateriale er å samle seere og distribuere materialet. Nettstedene lenker også til andre (kanskje konkurrerende) nettsteder for å ha en større sjanse til å vedvare [60]. Mange nettsteder er åpent tilgjengelige og krever ingen registrering for å vise innhold. Det er vanlig for flere nettsteder å hente overgrepsmateriale fra de samme lagringslokasjonene eller -tjenestene [60].

De fleste bildene lagres hos en bildelagringstjeneste (også referert til som bildetavlenettsteder). Bildetavlenettsteder tillater brukere å laste opp bilder som får tilordnet en unik nettadresse og kan bli lenket til og vises på tredjeparts nettsteder, f.eks. fora eller sosiale nettverkssteder. Denne metoden brukes vanligvis til å distribuere overgrepsbilder (og video) av barn [47]. Ved å bruke bildetavlenettsteder kan distributørene av overgrepsmateriale utnytte juridiske smutthull som finnes i alle land for å sikre at nettstedet forblir tilgjengelig på internett.

Det gjelder å ha innsikt i dynamikken til disse nettsamfunnene for å oppspore ulovlig innhold som blir distribuert. Nettsteder som spesialiserer seg som vertskap (dvs. lagring) for overgrepsmateriale er utsatt for større risiko enn nettsteder som viser materialet. Derfor er det ingen overraskelse at slike vertskapsnettsteder går langt for å maskere eller på en annen måte skjule innholdet. For eksempel, de unngår å bruke eksplisitte mappe- og filnavn, men bruker å kamuflere filnavnene for å skjule materialet. Til sammenlikning forsøker visningsnettsteder sjeldnere å merke overgrepsmaterialet feilaktig og de bruker oftere eksplisitte søkeord.

Søkemotorleverandører, som Alphabets Google og Microsofts Bing, spiller en viktig rolle i å identifisere og fjerne nettstedadresser og søkeresultater relaterte til overgrepsmateriale fra søkemotorene sine. For eksempel, i 2021 annonserte Google at de har rapportert og fjernet 1,18 millioner nettadresser som inneholder overgrepsmateriale fra søkeindeksen gjennom deres egenutviklede automatiserte programvare og ved manuell gjennomgang [66]. Flere slike tiltak finnes i Underavsnitt 3.5.

2.4.2 Applikasjoner for sosiale medier og direktemeldingstjenester

Den stigende populariteten av applikasjoner for sosiale medier og deres utbredte bruk blant barn og ungdom gjør dette mediet attraktivt for både å nærme seg og groome barn samt for å dele overgrepsmateriale [42] (se Underavsnitt 2.3.2). Sosiale medier og spillplattformer brukes flittig av gjerningspersoner for å kommunisere med barn og få tilgang til informasjon om barnet, for bruk i grooming aktiviteter [67]. Det er også tilfeller der falske kontoer på sosiale medier er opprettet for å spre private bilder og videoer av mindreårige ofre og deres personlige opplysninger [42].

En undersøkelse blant norske barn i 2021 viser at de får tilgang til porno og annet upassende materiale i stor grad gjennom bilde- og videodelingsplattformer som Instagram og YouTube, eller gjennom sosiale medieplattformer som Facebook og Twitter [68]. Videre er TikTok, som er mye brukt blant norske barn i alderen 9-10 år, et populært sted for salg av hjemmelaget pornografi [68]. Det antas at mindreårige kan legge ut eksplisitte videoer privat gjennom «Only me»-feed på TikTok [31], hvor det deretter kan nås av alle med et delt passord.

Overgrepsmateriale blir regelmessig funnet og fjernet av store sosiale medieplattformer som har installert overvåkning og moderering av sine brukere. Facebook [30] rapporterte i andre kvartal i 2022 at det ble aksjonert mot 20,4 millioner innhold som var ansett for å være skadelig for barn (som seksuell utnyttelse), hvilket er en betydelig økning fra 16,5 millioner aksjoner mot innhold i første kvartal i 2022. TikTok i har i den tilsvarende perioden i 2022 fjernet 102 millioner problematiske videoer. Fjerningen skjer fordi innholdet omfatter brudd på sikkerheten for mindreårige (41,7% av fjernet materiale) og voksen nakenhet og seksuell aktivitet (11,3% av fjernet materiale). TikTok rapporterte om en betydelig økning i kategorien voksen nakenhet og seksuell aktivitet med 21,3% i tredje kvartal i 2022. TikTok hevder at de fjernede videoene utgjør ca. 1% av alle videoer lastet opp til deres tjeneste [69].

De største leverandørene av direktemeldingstjenester, som Facebooks Messenger, Googles meldingstjeneste, WhatsApp, Skype, Twitter osv.) oppdager for tiden den største andelen av overgrepsmateriale sendt til rapporteringssentret NCMEC. F.eks. Meta bidrar med 93,4% av alle rapporter som NCMEC mottar, Google rundt med 2,5% og andre store leverandører som Snapchat, Microsoft, Twitter, TikTok og Imgur bidrar i fellesskap med ca. 1,5% av rapporter [29].

Sosiale medieselskapers direktemeldingssystemer som bruker VoIP og ende-til-ende kryptering er spesielt egnet for seksuelle overgrep mot barn og deling av overgrepsmateriale på en slik måte at aktiviteten går ubemerket hend. VoIP og ende-til-ende kryptering gjør det vanskelig for ESPer å overvåke, oppspore og avdekke seksuelle overgrep mot barn over internett. Dette reduserer evnen til at politimyndigheter også kan avdekke og oppklare slike lovbrudd. WhatsApp (applikasjonen for direkte meldinger) har angivelig blitt brukt til å lage chatterom spesielt for distribusjon av overgrepsmateriale [70]. Applikasjoner som bruker ende-til-ende kryptering kan ikke oppdage materiale i private meldinger, med mindre andre brukerne rapporterer det om materialet. Likevel angir WhatsApp å utestenge 300 000 kontoer hver måned grunnet deling av overgrepsmateriale, som de får kjennskap til gjennom brukerrapporteringer og avdekket gjennom ukryptert informasjon i brukerprofiler og gruppebilder [71].

En uavhengig undersøkelse av pornografiske grupper på direktemeldingsapplikasjonene WhatsApp og Telegram i løpet av en periode på én måned (juni/juli 2020) identifiserte 1 299 og 350 pornografiske grupper på WhatsApp og Telegram [72], respektivt. Ingen av gruppene ble fjernet etter å ha rapportert dem til WhatsApp; bare fire av 29 brukere ble utestengt. 171 kanaler ble fjernet etter å bli rapportert til

Telegram [72], [73]. Videre drøfting av utfordringer i samarbeid med private personer og allmennheten som gjelder forebygging av seksuelt misbruk av barn over internett og deling av overgrepsmateriale finnes i Avsnitt 4.2.

2.4.3 Peer-to-Peer nettverk og virtuelle private nettverk

Peer-to-Peer (P2P) nettverk er en vanlig form for fildeling for å skaffe musikk, filmer og annet digitalt materiale. I sin enkleste form opprettes et P2P-nettverk når to eller flere datamaskiner (peers) er koblet sammen og deler ressurser uten å gå gjennom en server. Den vanlige måten å få tilgang til et globalt P2P-nettverk på, er ved bruk av spesielle nettverksprotokoller og -applikasjoner for å konfigurere en direkte tilkobling mellom brukere på internett. Applikasjonene som brukes til å bli med i et P2P-nettverk, er tilgjengelige, brukervennlige og gratis å bruke.

Vanligvis søker brukerne etter filer ved hjelp av søkeord, og de mottar informasjon om filene, for eksempel navn, størrelse og nettverksplassering. Brukere kan deretter velge og laste ned den ønskede filen, ved å opprette en ny kopi på den lokale harddisken som også deles med andre likesinnede i nettverket. Lukkede P2P-fildelingsnettverk fungerer hovedsakelig på samme måte, men brukeren trenger en invitasjon til å bli med i nettverket [17].

P2P-nettverk er en av de hyppigste teknologiene som brukes av lovbrytere til å dele overgrepsmateriale med hverandre [27], [74]. De inneholder i tillegg sannsynligvis den største andelen av nettbasert overgrepsmateriale [49]. På grunn av at P2P-programvaren er utbredt, er den ofte en teknologi som tjener som en annen inngangsport for å få tilgang til og dele overgrepsmateriale for første gang [27].

Bruk av P2P-nettverk som distribusjonskanaler er spesielt interessante fordi de ikke krever servere. Dermed kan de overføre overgrepsmateriale uten tilsyn fra tjenesteleverandører [34]. Dette gjør det mulig for en liten gruppe lovbrytere å levere store mengder overgrepsmateriale [74]. En undersøkende studie [75] om P2P-nettverket eDonkey2000 stadfestet at 0,25% av alle forespørsler som ble gjort er relatert til pedofili. Siden identifikasjonsmetoden for denne studien var basert på en forhåndsdefinert liste over søkeord, som ikke kan oppdage nye eller tidligere ukjente begrep, vil den faktiske andelen av forespørsler relatert til seksuell utnyttelse av barn sannsynligvis være enda høyere. Kripos sitt etterforskningsteam identifiserte følgende P2P-fildelingsnettverk som fremtredende ved deling av overgrepsmateriale i Norge: BitTorrent, Gnutella og eDonkey2000 [76]. Intervjuobjektene fra norsk politi og Kripos bekrefter utbredelsen av denne trenden i Norge:

> *«P2P er de største kanalene for deling av overgrepsmateriale som vi møter i våre saker. Vi er også borti sosiale mediekanaler og andre direkte meldingsprogrammer (Skype, WhatsApp). I saker der vi møter barn og mindreårige som ikke forstår hva de deler eller gjør, møter vi også voksne som deler [overgrepsmateriale] med hverandre.»*

For å unngå å bli oppdaget, må P2P-samfunn i økende grad velge ut likesinnede og strengt kontrollere tilgangen, for eksempel med medlemsregler, adferdskodekser, oppdeling av oppgaver og strenge hierarkier, for å kunne håndheve regler og støtte brukerne innen nettverket. For å maskere bostedslandet bruker gjerningsmennene åpne proxy-servere eller VPN-løsninger (virtuelle private nettverk) som tilbyr tilkobling i Norge.

VPN-teknologien brukes til å opprette en sikker og kryptert tilkobling mellom den enkeltes datamaskinenhet og en VPN-tjeneste. Når denne teknologien brukes, kan politiet bare se at personen bruker en VPN-tjeneste, mens IP-adressen til den enkelte forblir skjult. VPN-tjenesten endrer IP-adressen til en person slik at det ser ut som om vedkommende kommer fra landet der VPN-serveren befinner seg, enda personen oppholder seg i et annet land. Gjerningspersonene utnytter denne teknologiske egenskapen for å skjule sin opprinnelse. Politiet er avhengig av VPN-tjenesteleverandørene for å få tilgang til loggført brukerinformasjon. Men mangelen på forskrifter som regulerer VPN-tilbydere, hindrer denne prosessen [17].

2.4.4 Det mørke nettet og distribuerte serversystemer

"Det mørke nettet" er et begrep som refererer kollektivt til alle kommunikasjonsnett som er skjult. Disse nettverkene indekseres ikke av søkemotorer og er kun tilgjengelige via autorisasjon eller gjennom spesiell programvare [77]. For lovbrytere gir det mørke nettet en sikrere og anonym plattform for distribusjon av overgrepsmateriale. Egenskapene til det mørke nettet gjør det vanskelig å estimere hele omfanget av ulovlig trafikk gjennom det [78].

Man når det mørke nettet oftest ved hjelp av TOR-nettverket. Til tross for at det finnes annen programvare for det mørke nettet, er TOR fortsatt et av de mest brukte og kjente og blir foretrukket av brukere som ønsker å skjule sine aktiviteter [79]. Brukere får tilgang til TOR-nettverket ved hjelp av den spesialiserte "TOR nettleseren". Det fungerer ved å rute trafikk gjennom andre brukere som har erklært seg som noder i nettverket. Når en TOR-bruker, referert til som en kilde, blir med i nettverket gjennom TOR-nettleseren, opprettes en virtuell krets ved hjelp av et tilfeldig utvalg av (vanligvis tre) mellomliggende TOR-noder plassert rundt om i verden. Denne virtuelle kretsen brukes i omtrent ti minutter, hvoretter en ny virtuell krets opprettes. Denne kretsen inneholder tre typer noder: (1) inngangsnoder – den første noden i kretsen som godtar innkommende trafikk; (2) mellomnoder – som sender data fra en node til den neste; og (3) utgangsnoder – den siste noden i kretsen som leverer trafikk til internettet.

Når en TOR-bruker ber om tilgang til et nettsted, krypteres forespørselen gjennom flere lag og sendes til inngangsnoden. Fra inngangsnoden sendes forespørselen til en mellomnode i den virtuelle kretsen. Etter hvert hopp i kretsen, blir et enkelt lag med kryptering fjernet fra forespørselen før den sendes til neste node. Når forespørselen når utgangsnoden, blir alle krypterte lag fjernet og den ukrypterte forespørselen sendes til nettadressen på Internett. I løpet av denne prosessen går all informasjon om kilden tapt, og TOR-brukeren forblir anonym. Trafikken kan bare spores tilbake til den forrige koblingen i den virtuelle kretsen. En analyse [80] av type og popularitet av innholdet på TOR-nettverket over en periode på seks måneder i 2015, konkluderte med at flertallet av nettsteder hadde en kriminell orientering. Selv om bare 2% av nettstedene på det mørke nettet var vert for overgrepsmateriale, tiltrakk de seg så mye som 80% av alle forespørsler.

Begrepet "skjulte tjenester" gjelder elektroniske tjenester som er satt opp gjennom skjulte nettverk (slik som over det mørke nettet). Det er kjent at gjerningspersonene misbruker TOR sine skjulte tjenester for å være vert for fora dedikert til overgrepsmateriale [81]. En undersøkelse tyder på at i løpet av et år, fra 2019 til 2020, har bruken av skjulte tjenester for å distribuere overgrepsmateriale økt med 155% [82]. I 2019 ble det registrert 3,45 millioner kontoer globalt på de ti største mørke nettstedene relatert til seksuell utnyttelse av barn, en økning på nesten 20 prosent i forhold til året før [83]. Europols

undersøkelse i Tyskland i mai 2021 avdekket et mørkt nettsted med fokus på deling av overgrepsmateriale med mer enn 400 000 registrerte brukere [78].

TOR sin metode for å rute nettverkstrafikk er et innebygd mottiltak som gir anonymitet til distributører og brukere av overgrepsmateriale [2], samtidig som risikoen for å bli oppdaget reduseres. Både VPN-nettverk og det mørke nettet kan brukes til dette formålet. VPN skjuler IP-adressen til kilden ved å rute trafikken gjennom et VPN-mellomledd, mens TOR sender trafikken gjennom en krets som forhindrer identifisering av IP-adressen til kilden.

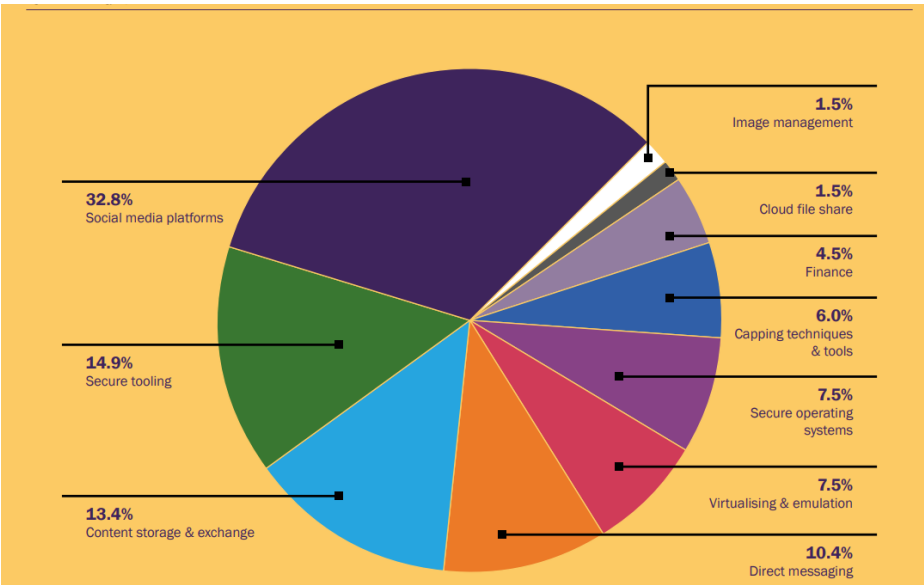
På grunn av den begrensede lagrings- og båndbreddekapasiteten til det mørke nettet, så ligger det meste av det tilgjengelige seksuelle overgrepsmaterialet på plattformer (slik som fillagringstjenester og i fildelingsnettverk) på internett [17]. Det betyr at mye av delingen av overgrepsmateriale på det mørke nettet skjer gjennom å dele lenker til filer lagret på det åpne nettet. Selv om mer ekstreme og nyere overgrepsmaterialer finnes på det mørke nettet [84], så er det ofte at materialet er lagret på internett. Lovbrytere oppfordres ofte gjennom åpne nettfora, noen ganger aktivt, til å flytte seg til stadig mer nettsteder på det mørke nettet som deler mer alvorlig overgrepsmateriale.

2.4.5 Fora

Gjerningspersoner kan kommunisere med likesinnede gjennom chatter og fora, funnet på både det mørke og det åpne nettet. Chatter som seksualiser barn dekkes av straffeloven § 311 [17]. Tjenestene er vanligvis ende-til-ende kryptert. I tillegg har gjerningspersonene en tendens til å bruke skjulte eller pseudoidentiteter, noe som gjør dem i stand til fritt å dele seksuelle tanker og fantasier, men også erfaringer med faktiske fysiske seksuelle overgrep mot barn. Noen av foraene gjør det mulig å utveksle filer, slik at overgrepsmateriale kan deles mens en chatt pågår.

Det foreligger en kollektiv tilnærming for å forbedre sikkerheten og derav anonymiteten for brukere av fora [42]. Analyser fra Storbritannia viste at forumbrukere regelmessig publiserer informasjon og sikkerhetsmanualer som har som mål å unngå å bli oppdaget av politimyndighetene [42]. For å unngå aksjoner fra politiet og påtalemyndighetene, så velger forumsamfunn ut hvem som kan delta og kontrollerer møtestedet strengt, for eksempel med medlemsregler, adferdskodekser, oppdeling av oppgaver og strenge hierarkier. Med å strengt håndheve regler og kontrollere hvem som er deltagende, så prøver de å unngå at politiet får tilgang på forumet.

En analyse av temaene som ble diskutert i dedikerte mørke nettfora hvor overgrepsmateriale ble delt ble utført av Crisp, en leverandør av sikkerhetsteknologi på internett. Crisp [51] viste at to tredjedeler av diskusjonstemaene var rettet mot etterretningsmetoder og verktøy som kan forenkle tilgangen til barn og informasjonsinnhenting for å begå seksuelle overgrep mot dem. Så mye som en tredjedel av diskusjonene var relatert til råd på plattformer der lovbrytere prøver å engasjere barn eller sårbare brukere, som vist i Figur 3. Emner om etterretningsmetoder handler ofte om utveksling av informasjon om sikkerhetstiltak for å skjule sine kriminelle aktiviteter, for eksempel kryptering og anonymisering av tjenester og programvare for sletting av digitalt materiale.



Figur 3: Mest diskuterte emner i lovbryternes mørke nettfora. Kilde: We Protect Global Alliance (2021). Global Threat Assessment 2021 [51]. Side 28.

I tillegg spiller foraene ofte også en sentral rolle ved utveksling av informasjon med andre kanaler. Deriblant viste undersøkelsene til IWF at i tilfeller med direktestrømmet seksuelle overgrep mot barn, ble så mye som 73% av innhold delt i 16 fora dedikert til distribusjon av bilder fra direktestrømmet overgrep av barn [55]. Bildeforhåndsvisninger av overgrepsvideoene brukes til å annonsere for innholdet som brukere kan betalte for å laste ned gjennom tredjeparts cyberlocker-nettsteder. Cyberlockere (fillagringstjenester) betaler opplasterne hver registrering og påfølgende nedlasting av filene deres. Bruken av betalte cyberlocker-kontoer hindrer derfor ikke bare fjerning av overgrepsmateriale, men det gjør det mulig for lovbrytere å ha en direkte økonomisk fortjeneste av distribusjonen.

Kapittel 3 Politiets tiltak og teknikker for oppsporing, etterforskning og forebygging av seksuelle overgrep mot barn over internett

I løpet av en relativt kort periode har politimyndigheter vist fremgang når det gjelder håndteringen av nettbasert seksuell utnyttelse og overgrep mot barn [10]. Politimyndigheter kontinuerlig overvåker P2P-nettverkskommunikasjon for å identifisere store CSAM-distributører, for å lokalisere og straffeforfølge personer i besittelse av CSAM, for å identifisere barn som er ofre og for å fjerne materialet [85].

For noen få år siden, i perioden mellom 2000 og 2011, brukte de fleste av de pågrepne lovbryterne ikke sterke teknologiske mottiltak for å skjule sin identitet [86]. For eksempel, 54% av australiere arrestert for besittelse av overgrepsmateriale brukte ikke noe form for tiltak for å skjule materialet [87]. Årsakene til denne praksisen kan ligge i lav teknisk kunnskap/kompetanse for å sette opp et sikkert miljø. Mens lovbrytere fortsetter å tilpasse seg endringer i internett-relatert teknologi, skjer ikke denne justeringen alltid veldig raskt. De fleste som oppsøker overgrepsmateriale benytter seg ikke av det mørke nettet som vert, men oppsøker det gjennom lett tilgjengelige nettsteder på internett [2].

Gjerningspersoner som seksuelt misbruker barn eller oppsøker overgrepsmateriale forbedrer imidlertid stadig sine teknologiske ferdigheter ved å bruke teknologi for å bli bedre organisert, og de bruker fora og andre former for kommunikasjon for å dele informasjon om hvordan de kan forbedre sikkerheten og anonymiteten [4]. For å beskytte sin anonymitet bruker lovbrytere også beskyttede nettverkstilkoblinger (VPN), kryptering og proxy-servere, sammen med tilgangen til og kommunikasjonen via det mørke nettet [86].

Dette tvinger politiet i økende grad til å tilegne seg kunnskap, verktøy og mer sofistikerte metoder for oppsporing og forebygging. Dette kapitlet har som mål å gi en oversikt over de viktigste teknologiske metodene og fremskrittene for mottiltak i kampen mot seksuelle overgrep mot barn over internett.

3.1 Hash-databaser og -lister

Hash-databaser eller -lister er globalt sett hovedkilden for identifikasjon av kjent overgrepsmateriale. Verdiene i databasen blir laget av hash-funksjoner, som er algoritmer som utgir en kort numerisk verdi med en fast lengde (en såkalt hash-verdi) fra en potensielt ubegrenset lenge inndata. Hash-algoritmene er konstruert på en slik måte at de samme inndata alltid danner samme utdata. Hash-verdien kan derfor fungere som et digitalt fingeravtrykk for å gjøre en unik identifikasjon av det underliggende materialet. De to mest kjente hash-funksjonene er Message-Digest Algorithm 5 (MD5) og Secure Hash Algorithm (SHA) [34], [88].

Hashing er en av de primære teknologiene som brukes av politi, sosiale medieplattformer og andre ESPer for å oppdage kjent overgrepsmateriale [34], [89]. I en hash-basert gjenkjenningsmekanisme lagres hash-verdier av bekreftet og verifisert overgrepsmateriale (vanligvis bilder) i en database eller en hash-liste. Politiet og ESPer kan bruke denne databasen til å sammenligne en hash tilhørende opplastet materiale for å finne samsvarende hasher i databasen. Automatiske systemer kan på denne måten finne allerede kjent overgrepsmateriale raskere, uten at analytikere trenger å se de samme bildene gjentatte ganger [1]. Ved å skanne et materiale som brukere laster opp på nettet for å matche det med hash-

listene, forhindrer man at kjent overgrepsmateriale lastes opp, og/eller man flagger ulovlig innhold for å identifisere distributører av overgrepsmateriale og forhindre gjentatt misbruk.

Ved å analysere det digitale, visuelle og lydinnholdet i bilder og videoer som er identifisert gjennom hash-databaser, kan eksperter på identifikasjon av ofre innhente ledetråder, identifisere overlapping i forskjellige saker og samkjøre innsatsen for å finne ofrene for seksuelle overgrep [90]. Slik har for eksempel startet over 13 000 etterforskninger i USA ved at man har først identifiserte bilder som viser én jente [16]. IWF og NCMEC har de to største hash-databasene. I 2021 la NCMEC til 1,4 millioner hash-verdier i deres voksende database med over 5 millioner hash-verdier [5]. Interpols ICSE (International Child Sexual Exploitation) har også en internasjonal bilde- og videodatabase over barn og gjerningspersoner. Denne databasen har 2,7 millioner hash-verdier av bilder med seksuelle barnemisbruk som har bidratt til identifisering av 13 794 lovbrytere [90].

De viktigste løsningene for å finne hash-verdier som samsvarer som industrien og politiet bruker er Microsofts PhotoDNA og Googles Content Safety API og CSAI Match (for videoer). PhotoDNA er en bildeidentifikasjonsprogramvare som skaper en hash (en unik digital signatur) av et bilde som deretter sammenlignes mot hash-verdier av andre bilder for å finne kopier av samme bilde. Disse løsningene leveres fritt til frivillige organisasjoner og berettigede bedrifter. Google rapporterer å ha bidratt (kumulativt over flere år) med 1 997 505 hasher til NCMECs database gjennom deres proprietære verktøy for å identifisere bekreftet overgresmateriale på sine plattformer og tjenester [66].

Eksempler på store ESPer som bruker hash-baserte løsninger fra PhotoDNA eller Google (eller begge) er Meta (Facebook), Snap Inc, Twitter, Dropbox, osv. Mindre ESPer og de uten tilgang til databaser med hash-verdier (ikke-medlemmer av IWF eller NCMEC) har imidlertid begrenset evne til å oppdage overgrepsmateriale i sine tjenester [60]. Antallet bedrifter som bruker den mest utbredte PhotoDNA-løsningen, utgjør bare 70 selskaper [91]. Dette viser problemet med begrensninger som skanning av opplastet materiale har.

Tradisjonelt sett har hash-baserte deteksjonsmekanismer noen godt kjente begrensninger [89]:

- De finner ikke nytt og uidentifisert materiale.
- De kan ikke finne materiale hvis det er litt endret, f.eks. ved hjelp av transkoding, skalering, re-dimensjonering eller fargejusteringer.
- Andre formater, for eksempel video, må tilpasses i søket etter overgrepsmateriale.

På grunn av disse begrensningene må hash-databaser oppdateres jevnlig med hash-verdier av nye og modifiserte overgrepsmateriale. På denne måten økes muligheten for å finne gjenopplastet materiale. Det finnes mange hash- og URL-lister, men de fleste av dem er ikke knyttet sammen, noe som tyder på at mye av arbeidet som gjøres på tvers av organisasjoner holdes innenfor den egne organisasjonen slik at ting gjøres dobbelt opp [4]. Nedlasting og bruk av hash-lister krever en betydelig mengde investering når det gjelder teknisk kompetanse og frigitt tid. Men mangel på veiledning eller mandat fra offentlige etater om hvordan de skal iverksette hash-listen hindrer innsatsen, fordi det er nødvendig å koble databaser sammen for å sikre at bilder deles på riktig måte mellom byråer og på tvers av sektorer, nasjonalt og internasjonalt.

Det er viktig å ikke gjøre seg for avhengig av hash-lister, siden lovbrytere kan lære seg å omgå dem for å unngå å bli oppdaget (f.eks. ved å endre piksler). Noen nye utviklinger bidrar til å overvinne de

tradisjonelle begrensningene som hash-metodene medfører, slik at man kan finne fram til materiale med små endringer og utvikle hasher for videoer. Mens en kryptografisk hash (f.eks. MD5, SHA-1) kan brukes for å sjekke om to filer er helt like, kan nyere utviklinger innen perseptuell hash-teknologi (f.eks. PhotoDNA) brukes til å gjenkjenne om to filer ligner på hverandre.

Hash-algoritmer, for eksempel PhotoDNA, har gjort forbedringer for å motstå noen endringer i bildet, som gjør dem i stand til å oppdage endrede kopier av det samme bildet. Disse forbedringene inkluderer re-dimensjonering og mindre fargeendringer [49]. Imidlertid er den store begrensningen deres manglende evne til å oppdage nytt overgrepsmateriale. Dette er spesielt bekymringsfullt gitt det faktum at egenprodusert innhold vokser. Så mye som 82% av innholdet i det totale antallet nettadresser som IWF har behandlet i 2021 var ennå ukjent. Det er riktignok ikke mulig fullt ut å skille ut om dette antallet er virkelig nyprodusert innhold som er satt i omløp og eksisterende endret materiale som ennå ikke er identifisert av politiet eller om det bare er innhold som IWF ikke har i sin database.

3.2 Nettsøkeroboter/-programmer

Nettsteder som er vert for eller viser overgrepsmateriale er ofte koblet sammen [63]. Søkeroboter (eng.: "webcrawler") hjelper politiet med å oppdage nettstedene og kartlegge relasjoner mellom dem. Søkeroboter er automatiserte skripter eller programmer som brukes til å flytte seg over mange nettsteder for å bla gjennom og samle inn data om hvert besøkte nettsted basert på forhåndsdefinerte kriterier. Kriteriene er spesifikke egenskaper relatert til nettsteder som deler overgrepsmateriale. Spesifikke egenskaper inkluderer søkeord som ofte brukes av lovbrytere og hash-verdier for kjent CSAM. Søkeroboter bruker en liste over nettsteder som allerede er verifisert til å inneholde overgrepsmateriale som et utgangspunkt for et nettsøk. Søkeroboten utnytter forbindelsene mellom nettsteder for å finne nye nettsider ved å følge hyperkoblingene (dvs. lenkene) på hver nettside som er besøkt.

Søkerobotteknologien fungerer mye raskere enn manuelle metoder for å spore overgrepsmateriale og relaterte nettsteder [49]. Denne metoden kan også brukes for å identifisere volumet av kjent overgrepsmateriale på internett [89]. Lovbrytere er klar over at politiet bruker søkeroboter mot populære overgrepsnettsteder, noe som igjen gjør det vanskeligere for lovbrytere å få tilgang til visse nettsteder når politiet tar ned nettstedene.

Canadian Centre for Child Protection (C3P) har laget søkeroboten *Project Arachnid* [92] som bruker Microsofts PhotoDNA-teknologi og hash-databaser fra flere organisasjoner: NCMEC, Royal Canadian Mounted Police og Interpol. Når søkeroboten identifiserer overgrepsmateriale, så vil materialet bli lagt inn i et klassifiseringssystem og tre forskjellige analytikere vil verifisere det underliggende innholdet. Når materialet er bekreftet, sender de en melding om å fjerne innholdet til leverandøren hvor materialet er lagret. Systemet følger deretter opp at tjenesteleverandøren sletter innholdet.

I løpet av en seks ukers periode behandlet Project Arachnid over 230 millioner nettsider. Over 5,1 millioner av dem var vert for kjent overgrepsmateriale, med over 40 000 unike bilder [49]. Dette viser nytten av søkeroboter når man skal avdekke CSAM. Søkeroboter blir også brukt til å søke i det mørke nettet. Men fordi leverandørene av lagringstjenestene er ukjent, kan de bare identifisere lenker fra mørke nettsteder som fører tilbake til internett for å fjerne materialet.

IWF bruker en søkerobot med PhotoDNA som besøker flere millioner nettsider per dag i søk etter overgrepsmateriale. Målet med søkeroboten er å beskytte ofre mot gjentatt misbruk ved at materiale distribueres over nettet [88], [93]. IWF prøver også å automatisere gjennomgangsprosessen ved å innlemme AI-klassifiseringer for å svare på sannsynligheten for at materialet som er gjennomsøkt av en søkerobot er seksuell misbruk av barn. Det meste av materialet som finnes i dag er vanligvis gammelt og har allerede en stor spredning (se Avsnitt 2.3.1).

Hovedbegrensningen til søkeroboter er at for at en søkerobot skal kunne klare å identifisere nettsteder som deler overgrepsmateriale, så må passende kriteriene (for eksempel søkeord og hash-verdier) være valgt. Politiet trenger ikke bare de nødvendige ferdighetene for å bruke søkeroboter, men de må også kunne velge kriterier og finne store nettsteder til et utgangspunkt for nettsøk. Valg av passende søkeord og hash-verdier krever at man gjør undersøkelser først, og dette må fortløpende vedlikeholdes på grunn av utviklingen på dette feltet. I tillegg må søkeord være effektive for å unngå store antall falske positiver fra nettsteder som inneholder lovlig voksenpornografi [94]. Derfor er det viktig å få en forståelse av hvordan lovbrytere merker filer eller ord som brukes av personer som søker overgrepsmateriale. Politiet må også sjekke regelmessig søkerobotens resultater [49].

3.3 Nettsteders fingeravtrykk

Lovbrytere kan enkelt få tilgang til nettsteder med overgrepsmateriale gjennom nettleseren, noe som gjør denne tilnærmingen til den enkleste måten å få tilgang til slikt materiale og den primære porten for folk som leter etter overgrepsmateriale for første gang. Lovbryteren får tilgang til nettsteder ved å besøke et domenenavn ("eksempel.com", hvor det andre nivånavnet "eksempel" tilhører topplevel-domenet (TLD) "com"). Domenet har minst én tilknyttet IP-adresse. IP-adressen er stedet der serveren er på internett og der materialet lagres, og folk sendes dit når de besøker domenet.

Websøkemotorer og ISPer har en liste over domener og søkeord som hindrer lovbrytere i å få tilgang til nettsteder med overgrepsmaterialet. Både fra målrettet etterspørsel og tilfeldig besøkende. Ved bruk av mottiltak er det enklere å skanne for visningsnettsteder da det er mer sannsynlig at materiale vises fremtredende og at det brukes beskrivende og nøyaktige navn på filene. Politiet har en strategisk målfokusering mot å stoppe verter for overgrepsmateriale for å ha størst påvirkning på å forstyrre distribusjonsnettverket [95], [96]. Grunnen er at leverandører av lagringstjenester for overgrepsmateriale kan formidles av mange visningsnettsteder. Ved å fjerne en leverandør, så fjernes også overgrepsmateriale fra alle visningsnettsteder.

Administratorer av nettsteder anser serverplasseringen og domenenavnet som del av deres "burner website". En "burner" er et billig nettsted som er designet for midlertidig bruk, hvoretter det kan kastes. Dette innebærer å bli stengt ned på grunn av tiltak fra politimyndigheter, ISPer og registre over domenenavn. Derfor fokuserer lovbrytere sine anstrengelser på strategier for raskt å flytte sitt operative miljø til nye webhoteller. De benytter forskjellige strategier for å holde seg på nettet [87]:

- *TLD-hopping* er når et nettsted beholder det andre nivået i domenenavnet, men endrer sitt TLD. For eksempel registrerer eiere av "badsite.no" også domener som "badsite.se", "badsite.dk", "badsite.com" og lignende. Ved å endre TLD-en kan et nettsted forbli på nettet etter at det opprinnelige domenet er tatt ned, samtidig som nettstedet er gjenkjennelig og lett å finne [97].

- *Domain tasting* er en praksis der man utnytter "add-grace"-perioden (betalingsutsettelse) for å få tilgang til et domene uten kostnad [87], [98]. En slik betalingsutsettelsesperiode refererer til antall dager der en registrering av et domenenavn kan kanselleres uten kostnad. Dette ble opprinnelig innført for at registrert domenenavn kan korrigeres for skrivefeil eller andre feil [99]. *Domain kiting* er en utvidelse av domain tasting. Dette betegner framgangsmåten med gjentatte registreringer og slettinger av et domenenavn hos en domeneregistrator, fordi sistnevnte ikke sjekker for re-registreringer av samme domene.

Nettsteder som deler overgrepsmateriale gjør vanligvis lite for å skjule sin intensjon [65], og det er ikke nødvendig å prøve å endre nettsidene ved bruk av en ny vert. Det er sannsynlig at nettsteder som er flyttet til en ny vert vil se ut som de gamle, og dette skaper en mulighet til å automatisk oppdage nettsteder som dukker opp på nytt igjen, basert på sammenligningsteknikker for visuell likhet. Når nettstedene gjentatte ganger endrer leverandøren av lagringstjenesten [92], er det en mulighet til å automatisk oppdage at de har dukket opp igjen.

Det er mange egenskaper som kan trekkes ut og sammenlignes mellom nettsteder, alt fra tekst og pikselbaserte inspeksjoner til underliggende nettstedstrukturer, stilark og nettverkstrafikkmønstre. Tilnærminger som bruker flere tekstbaserte og strukturelle egenskaper i kombinasjon med visuelle likheter, har en tendens til å være mer vellykket. Visuelle likhetsmetoder ser på det grafiske innholdet på et nettsted, for eksempel gjennom å sammenligne hash-verdier for bilder og spesielt tilbakevendende bildekomponenter som logoer.

En multiheuristisk tilnærming er å foretrekke, dvs. en metode som vurderer blokknivålikhet, tekstlikhet, bildelikhet, osv. Ved å legge til bildeklassifisering og CSAM-sporing får man en ytterligere verifiserings- og prioriteringsmåling. Ordlyden av eksterne nettstedfunksjoner (som ansvarsfraskrivelser, merknader om opphavsrett eller juridiske og pseudojuridiske påstander) kan ofte gjenbrukes uendret. De grammatiske og ortografiske feilene kan fungere som signaturer for sekundært innhold som overføres fra ett sted til et annet. Innholdsfunksjoner som kan brukes til å identifisere mistenkelige nettsteder, for eksempel spesifikk HTML-kommentartekst og identifikatorer som er inkludert i trafikkovervåking og annonseplasseringsskript [100], [101].

Likevel kan teknikker for innhold og visuell likhet produsere falske positive match, siden HTML-strukturer ofte gjentas på tvers av nettsteder som bruker samme malsystem eller verktøy for nettsideproduksjon.

3.4 Filnavn og metadata

En utfordring når man skiller mellom vanlige pornografiske filer og filer med overgrepsmateriale av barn, er at de bruker et svært likt, sexrelatert vokabular. Forskere har undersøkt dette problemet ved å bygge statistiske maskinlæringsmodeller for å analysere innhold av filer samt deres metadata for å gjenkjenne og lage en forskjell mellom disse filtypene. En maskinlæringsmodell kan gjenkjenne forespørsler fra gjerningspersoner eller filnavn i dataen til P2P-nettverk som inneholder overgrepsmateriale med et treff på 78% [102]. Modellene inkluderer klassifiseringsverktøy for å skille filnavn fra overskrifter på pornografiske nettsider i forhold til Wikipedia-artikler [103].

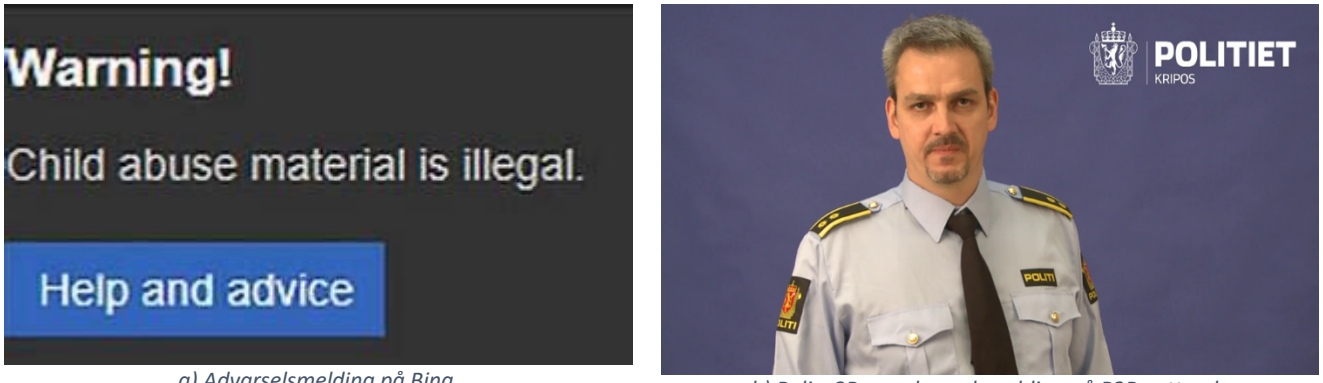
3.5 Popup-advarsler og omadressering på internett

Popup-advarsler og omadressering brukes til å hindre lovbrytere, spesielt førstegangslovbrytere, fra å få tilgang til overgrepsmateriale. Søkemotorer som Google og Bing kommer med advarselsmeldinger når enkeltpersoner legger inn CSA/CSAM-relaterte søkeord i søkemotoren. Popup-varselmeldinger bidrar til å redusere følelsen av anonymitet, noe som styrker den enkeltes oppfatting av risikoen for å bli tatt [104]. En undersøkelse [104] viste effekten med advarselsmeldinger (spesielt de som inneholder informasjon om at aktiviteten er ulovlig). 60% av personer som ikke fikk varsel forsøkte å besøke et nettsted med lovlig pornografi, mens bare 38% av personene gjorde det etter å ha sett advarselsmeldingen.

Internett-omadressering er en teknisk løsning som flytter internettrafikk fra domener som politiet tidligere har verifisert å inneholde overgrepsmateriale. Internettrafikken blir omdirigert til et "stopp-nettsted" hos tjenesteleverandøren eller politiet. Denne teknikken har blitt brukt i Norge siden 2004. Stopp-nettstedet opplyser at brukeren har forsøkt å få tilgang til et nettsted som brukes til distribusjon av materiale knyttet til seksuelle overgrep mot barn og viser til gjeldende straffebestemmelser. Stopp-nettstedet angir også at den har et forebyggende formål og at ingen brukerinformasjon lagres.

Lignende forsøk på å blokkere søk via Google og Bing registrerte en reduksjon på 67% i nettsøk etter overgrepsmateriale på disse søkemotorene i en ett års periode (2013 og 2014) [24]. En sammenligning med Yandex søkemotoren i Russland (som ikke implementerer de samme anstrengelsene for blokkering og som ikke har sett et tilsvarende fall i denne perioden) indikerer at det foreligger potensielle positive kausale effekter når man bruker nettstedblokkering [24]. Fordi Google og Bing brukte samtidig både blokkerings- og advarselsmeldingstiltak, er det imidlertid ikke mulig å skille effekten av blokkeringer fra varselmeldinger som enkeltstående mottiltak. Vi klarte ikke å finne noen nyere studier som har gjort en slik sammenligning.

Advarselsmeldinger og omadresseringsteknikker gir ikke støtte eller hjelp til lovbrytere med den destruktive adferden deres, men i mange tilfeller (for eksempel i Google- eller Bing-varselmeldingene) er det gitt en lenke til en hjelpetjeneste, som man ser i Figur 4a. I tillegg til disse avskrekkingstiltakene på nettet, blir lignende forebyggende teknikker gjennomført i P2P fildelingsnettverk, som forklart i neste avsnitt.



a) Advarselsmelding på Bing.

b) Police2Peer advarselsmelding på P2P nettverk.

Figur 4: Eksempler på advarselsmeldinger hos søkemotorer og P2P nettverk.

3.6 Overvåke P2P nettverk

Overvåking av P2P-nettverkskommunikasjon hjelper politimyndigheter med å identifisere store distributører av overgrepsmateriale. Overvåkingen kan være med å lokalisere for deretter å straffeforfølge personer i besittelse av overgrepsmateriale, identifisere ofre og fjerne overgrep-relaterte nettsteder [85]. P2P nettverksovervåking innebærer at politiet bruker verktøy for å samle inn data om brukere som prøver å laste ned overgrepsmateriale. Inkludert i dataene som samles inn er IP adressen, hash-verdier og filnavn for de datamaskinene som er en del av kommunikasjonen.

Et eksempel av P2P nettverksovervåking er *Police2Peer* [105], et teknisk forebyggende prosjekt i regi av Europol og European Multidisiplinary Platform Against Criminal Threats (EMPACT), rettet mot brukere av åpne P2P-fildelingsnettverk. Prosjektet oppretter filer med navn som indikerer at de inneholder overgrepsmateriale, men disse filene har ikke noe innhold eller inneholder bilder eller videoer av politifolk som forklarer risikoen ved å distribuere slikt materiale. Om lovbrytere laster ned materiale fra politiet i den tro at det er overgrepsmateriale, så øker det dermed følelsen av deteksjonsrisiko og motiverer dem til å slutte å distribuere overgrepsmateriale (se Figur 4b).

En studie som evaluerte effektiviteten av å stoppe 1%-delen med datamaskiner med høyest bidrag på et P2P-nettverk (Gnutella), tyder på at politimyndighetene kan redusere tilgjengeligheten av overgrepsmateriale med 30% [106]. P2P nettverksovervåking har også den ekstra effekten av å varsle lovbrytere om aktiv tilstedeværelse av politimyndigheten i nettverket, noe som kan påvirke noen brukeres beslutninger om å fortsette å se dette materialet.

Denne strategien har imidlertid flere begrensninger. Den krever intensivt arbeid og investering av politiets ressurser [106] som forsterkes av politiets behov for å finne nytt overgrepsmateriale og behov for å øke deres teknologiske ferdigheter. Siden metoden bygger på hash-listematching, så kan ikke politimyndigheter oppdage nye bilder som ikke har en kjent hash-verdi (se Avsnitt 3.1). IP adressen kan også endres av lovbryteren etter behag. Politiet er nødt til å bruke relevant programvare for analyser, proaktiv etterforskning og innstevning av ISPer for å identifisere brukeren tilknyttet IP adressen.

I Norge er det Kripos og et dedikert team ved Trøndelag politidistrikt, Seksuelle overgrep mot barn over Internett (SOBI), som overvåker utvalgte P2P-fildelingsnettverk for å identifisere datamaskiner som laster ned, gir tilgang til og distribuerer filer verifisert som overgrepsmateriale. Dette verktøyet knyttet ca. 15 000 unike norske IP adresser til distribusjon av overgrepsmateriale mellom 2017 og 2018. Videre undersøkelser er nødvendig for å kontrollere om IP adressebrukerne besitter overgrepsmateriale av barn. Siden flere brukere kan operere fra én enkelt IP adresse, og én bruker kan ha flere IP adresser i løpet av et år, kan antall IP adresser ikke fullt ut avsløre antall personer som laster ned CSAM-filer.

3.7 Automatiserte sporingsteknikker som bruker maskinlæring og kunstig intelligens

Overfloden av overgrepsmateriale på internett har nødvendiggjort bruk av automatiserte analyseteknikker for raskere oppsporing av krenkende materialer. Sporingsteknikker har tradisjonelt vært avhengig av søkeordanalyse og hash-verdisammenligning. Begrensningene til disse to metodene

har ført til utviklingen av verktøy som innlemmer maskinlæringsteknikker for automatisk å oppdage kjente ulovlige bilder, identifisere nakenhet i bilder og nytt (men uverifisert) overgrepsmateriale.

Utviklingen av maskinlæringsalgoritmer og kunstige nevrale nettverk har vesentlig forbedret evnen til å skille overgrepsmateriale fra annet pornografisk voksenmateriale. En annen fordel er at de er ikke påvirket av forsøk på å omgå f.eks. hash-verdideteksjon. Dyptgående maskinlæringsmetoder som analyserer ansiktssignaler er - sammenlignet med bruken av hasher og filnavn - mer robuste og stabile mot modifikasjoner [107]. Ansiktets unike egenskaper (f.eks. avstand mellom øyne, nesebredde osv.) brukes til å danne en tydelig identifikator av en person, som kan evalueres mot en ansiktsgjenkjenningsdatabase for å finne eventuelle forekomster av den mistenkte (eller offeret).

En oppsamling av et sett med ansiktstrekk og hudtoneområder brukes for å designe et klassifiseringssystem som kan skille mellom innhold med og uten (f.eks. vanlig pornografisk innhold) overgrepsmateriale, samt utføre en aldersklassifisering med en nøyaktighet på 74,19% [108]. Den største utfordringen for klassifiseringen av overgrepsmateriale er tilstedeværelsen av lovlig pornografisk materiale [49], og ikke-ulovlig materiale av barn (f.eks. vanlige barnebilder). Et spesielt vanskelig problem representerer aldersklassifisering av barn i puberteten (dvs. alderen 15-16 år) der klassifiseringsverktøy viser lave nøyaktighetstall [109]. I disse sakene har AI-løsninger som anvender en kombinasjon av nakendetektorer med aldersklassifiseringer vist lovende framskritt [110]. Ved klassifiseringen av videoer der man legger til lydinformasjon forbedrer nøyaktigheten for å spore overgrepsmateriell seg betydelig.

Multimodal klassifiseringstilnærming for å identifisere overgrepsvideoer og -bilder gir større mulighet for å skille ut materialet, noe som forbedrer nøyaktigheten av å oppdage og identifisere overgrepsmateriale. En enkelt form for å oppdagelse (f.eks. hudtoneanalyse) er ikke pålitelig nok for å skille overgrepsmateriale av barn fra voksenpornografi. Derfor brukes flere metoder (f.eks. form, tekst og farge) for å en mer robust og nøyaktig måte å klassifisere materiale [34], [107], [111].

En av de viktigste utfordringene for videre utvikling av deteksjonsmetoder er mangelen på større datasett med overgrepsmateriale som utviklere kan få tilgang til og bruke for å teste sine algoritmer. Det er nødvendig at forskere har et større samarbeid med politimyndigheter for å få tilgang til databaser med eksisterende overgrepsmateriale for å kunne levere bedre algoritmer for sporing. Til dags dato finnes det svært lite forskning på å avdekke seksuelle overgrep mot barn i formater slik som direktestrømming. Dette skyldes vanskeligheter med å fange opp krypterte datastrømmer som disse systemene ofte bruker. Det er spesielt vanskelig å finne direktestrømming av overgrep, da de etterlater svært lite eller ingen digitale spor etter at sendingen er over, med mindre strømmingen er tatt opp og lagret for ettertid. Framtidig forskning innen dette teamet kan bidra til å finne måter for å harmonisere metoder på tvers av ulike lovgivninger og utvikle en enhetlig internasjonal standard for merking av overgrepsmateriale.

Vi nevner spesielt FNs initiativ til å utforme et globalt senter for maskinlæringsløsninger for politiet. FNs Interregional Crime and Justice Research Institute (UNICRI), med sitt senter for kunstig intelligens og robotteknologi (Centre for Artificial Intelligence and Robotics), har lansert initiativet 'kunstig intelligens for tryggere barn'. I tillegg til å bygge nettverk, øke bevisstheten og være en støttespiller, har dette initiativet utviklet Global Hub, en nettbasert plattform som er tenkt som støtte til politimyndigheter i effektiv bruk av maskinlæring for å hindre, spore opp og straffeforfølge nettbasert seksuelt misbruk og utnyttelse av barn. Det er kun politimyndigheter som har adgang til plattformen. Plattformen tilbyr både

informasjon om maskinlæringsverktøy som politimyndigheter kan ta i bruk samt tilgang på etterforskningsteknikker, utvikle ny kunnskap og nettverksbygging for å dele erfaringer og framgangsmåter for beste praksis [110].

Som angitt i Underavsnitt 2.3.4, utgjør kunstig generert overgrepsmateriale en stor trussel mot politimyndigheters mottiltak på grunn av tvetydige juridiske bestemmelser og manglende evne til å straffeforfølge kunstig (f.eks. deepfake) og manipulert overgrepsmateriale. Fremveksten av ny teknologi som deepfakes er bekymringsfull fordi slike metoder gjør det i enkelte tilfeller umulig å skille mellom ekte og uekte overgrepsbilder og -videoer.

Politiet har imidlertid brukt mottiltak med automatiserte analysemetoder. Et eksempel på automatiserte verktøy som støtter politiet i å forhindre seksuelle overgrep mot barn i chatterom gir anslag om alder og kjønn bak nettaliaser som er engasjert i seksualiserte samtaler med barn [112]. Dette verktøyet kan også hjelpe politiet med å identifisere tidligere lovbrytere som har gjenopptatt den kriminelle aktiviteten på internett. "Sweetie" et datagenerert, virtuelt barn som brukes til å avsløre gjerningspersoner som tar kontakt med barn på nettet. Sweetie er programmert til ikke bare å se ut som en ti år gammel jente, men å bruke tone, ansiktsuttrykk og bevegelser som gjengir de er et ekte barn, for slik å få identifiserbar informasjon fra seksuelle overgripere [113].

Utviklingen av maskinlæringsteknikker byr både på noen utfordringer, men også viktige muligheter for å forbedre oppsporing og forebygging av overgrepsmateriale og seksuell utnyttelse av barn på nettet. Det må imidlertid studeres nærmere for å fastslå nøyaktig hvilken påvirkning og hvilke utfordringer implementeringen av slike løsninger medfører.

Kapittel 4 Strukturelle og juridiske utfordringer i bekjempelsen av seksuelle overgrep mot barn på nett

Tidligere kapitler fremhevet at forebygging av nettbasert seksuelle overgrep mot barn er et komplekst, mangesidig fenomen som ikke kan utføres eller reguleres fra én side. Hver av de flere interessentene (sivilsamfunn, foreldre, lærere, politi, bedrifter og regulatorer) kan bare delvis påvirke problemet og derfor er de avhengig av samarbeid. Innsatsen til lærere og foreldre har vært vellykket i å øke bevisstheten om farer på nettet, men sosiale pådrivere av deling av seksualiserte bilder, normaliseringen av tilgangen på pornografi og økt sofistikert fremgangsmåte hos groomere medfører alvorlige utfordringer for forebyggende tiltak som er avhengige av sivilsamfunnet [114], [115] (se diskusjon i Avsnitt 2.2). På den annen side er politiets evne til effektivt å håndtere saker på nettet avhengig av de rettslige aspektene og bestemmelsene som spesifiserer hva de ulike interessenters ansvar er for å spore og forebygge misbruk av barn på nett. I tillegg kommer samarbeidet med ESPer som kan fungere både som tilretteleggere og portvakter ved å forebygge og påvise forbrytelser relatert til seksuelle overgrep mot barn på nettbaserte plattformer.

Vår analyse av akademisk litteratur og intervjuer med ulike interessenter peker på to store utfordringer for fremtiden: juridiske utfordringer og utfordringer rundt samarbeidet på tvers av ulike interessenter.

4.1 Juridiske hindre og mangel på standardisering

4.1.1 Juridiske tvetydigheter og mangel på global håndheving av forskrifter

Forskrifter, regler og samsvarsretningslinjer rundt ansvaret til de ulike interessentene som jobber med å hindre overgrep på nettet varierer betydelig fra land til land. En nylig gjennomført UNICEF-undersøkelse [10] på tvers av 29 land avslørte at så mye som 86% av landene bare har en delvis regulering på plass for avdekke, rapportere og fjerne overgrepsmateriale fra nettet. Disse landene rapporterte en mangel på dedikerte etterforskningsenheter, ressurser og kapasitet til å håndtere disse forbrytelsene. Bare 7% av landene (to av 29 land) rapporterte at de har satt opp dedikerte enheter som er ansvarlige for etterforskning av overgrep mot barn, inkludert teknologitilrettelagt overgrep [10]. Dette er problematisk når man ser på internettets globale natur og hvor enkelt det er å bruke VPN-tjenester for å endre plasseringen på verdenskartet. Som en illustrasjon, 93% av alle rapporter til NCMECs CyberTipline i 2021 førte til steder utenfor USA, hovedsakelig steder der overgrepsmateriale ble lastet opp.

Mangel på globale standarder for å kategorisere og straffe besittelse av overgrepsmateriale, og forskjeller i regulering av overgreps-relaterte lovbrudd hindrer muligheten til globalt samarbeid mellom land og nasjonale politimyndigheter [116], [117]. Selv om det er sterkt anbefalt, eksisterer det fortsatt ikke et universelt system av standarder for å identifisere, analysere og klassifisere overgrepsmateriale, og internasjonalt samarbeid mellom jurisdiksjoner er tungvint. Saken illustreres av en intervjuet person som jobber med etterforskning av straffbare forhold:

> *«De fleste av tjenesteleverandørene har hovedkvarter i utlandet, for det meste i USA. Politiet kan be om grunnleggende abonnentinformasjon (BSI), med utgangspunkt i informasjonen som gis når en elektronisk profil opprettes. Det kan politiet få uten en*

ransakelsesordre. Men situasjonen blir mye vanskeligere når politiet prøver å få informasjon om innholdet i en bestemt profil. Da må politiet få en ransakelsesordre fra en regional påtalemyndighet, som deretter sendes til øverste påtalemyndighet, som deretter går til Justisdepartementet, deretter til Utenriksdepartementet, som sender saken til det amerikanske utenriksdepartementet, deretter videre til statlige myndighetsorganer, så lokale myndigheter som deretter bruker amerikanske forskrifter om samsvarskontroll (for eksempel i California). I Norge kan vi ha andre regelverk enn i USA, men saken må være straffbar i begge land for å være kvalifisert. I tråd med USAs lover må norsk politi dokumentere at innholdet i disse profilene er knyttet til en straffbar handling. Det er ikke deres [Californias tilsynsmyndigheters] problem hvis norsk politi ikke kan dokumentere tilknytning til saken og profilen fordi de ikke kan gå inn i profilens innhold. Norsk politi er fullt ut avhengig av samarbeid med tjenesteleverandører og deres raske svar.»

Lignende saker av *forskriftsmessig tvetydighet* oppstår også på nasjonalt nivå. De spurte tjenestepersonene fra norsk politi påpeker den manglende evnen til å følge trender for seksuelle overgrep mot barn over tid, spesielt de som oppstår på tvers av ulike teknologiløsninger. Dels påpekes grunnen å være svakhetene i straffeloven som ikke kan skille lovbrudd begått på nettet fra mer "fysiske" lovbrudd og ev. teknologiske kilder som er brukt. Resultatet er at politietterforskere blir usikre på hvordan et bestemt lovbrudd skal kategoriseres, og dette fører til subjektivitet i kategoriseringen.

I tillegg påvirker utilstrekkelig deling av undersøkelsesmetoder mellom regioner i Norge oppklaringsprosenten, mens de eksisterende etterforskningsenhetene med spesialfelt for seksuelle overgrep mot barn har stor utskifting av personale som skaper kunnskapshull. Tilgjengelig statistikk kan derfor ikke representere den faktiske statusen i praksis på grunn av den subjektive komponenten i det hvordan saker registreres. Likevel illustrerer Figur 5 straffekoder i politidatabasen over straffesaker (STRASAK) relatert til seksuell misbruk av barn i perioden 2017 til 2021. Framstillingen eller bildevisningen av overgrepsmateriale representerer den største gruppen av lovbrudd (kode 1470).

4.1.2 Mangelen på tvangsfullbyrdelse mot elektroniske tjenesteleverandører

Den andre viktige juridiske utfordringen for å forebygge delingen av overgrepsmateriale er feilvurderingen som blir gjort i diskusjonen om frivillig eller obligatorisk regulering av ESPer. Regulering relatert til rapportering av overgrepsmateriale på egne plattformer og tjenester. Mens den amerikanske føderale loven (18 USC 2258A) krever at amerikanske ESPer rapporterer overgrepsmateriale når det oppdages på deres plattformer til informasjonssentralen NCMEC, så har forpliktelsene til ikke-amerikanske ESPer overfor lokale myndigheter utenfor USA vært blandet. I Europa er rapportering av nettbasert seksuelle overgrep mot barn og overgrepsmateriale frivillig, og det er ingen nasjonale eller europeiske ekvivalenter til en informasjonssentral med obligatorisk rapporteringsplikt eller ileggelse av straff. I Finland finnes et unntak som er verdt å merke seg. Politimyndighetene i Finland utleverer en sensureringsliste over nettsider med overgrepsmateriale som skal blokkeres til ESPer, noe som er støttet gjennom finsk lovgivning, og finske ESPer bør iverksette denne blokkeringen frivillig [16].

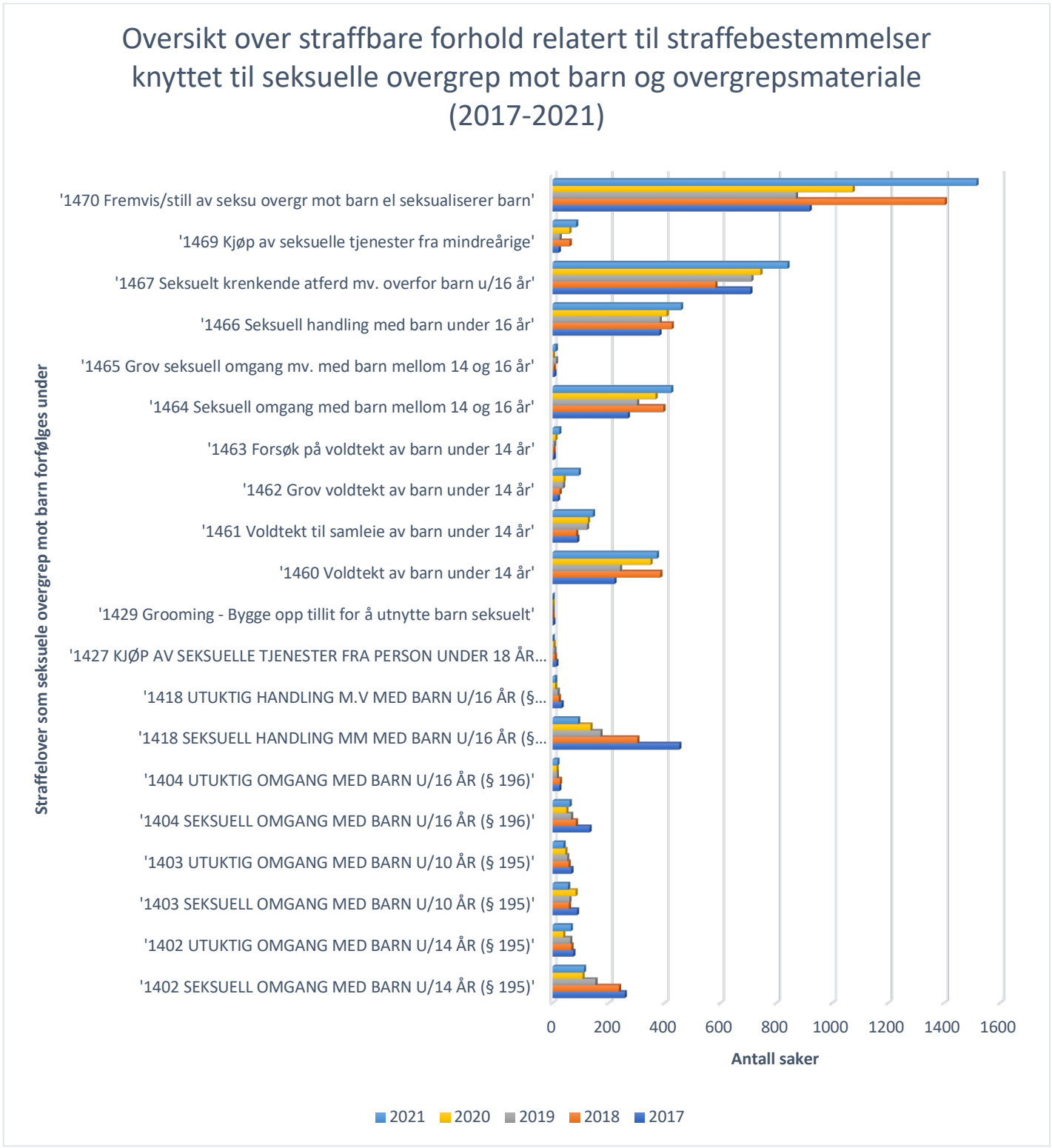
Generelt sett fører mangelen på en tydelig regulatorisk veiledning og et regulatorisk tilsynsorgan til at ESP-er praktiserer å stole på blokkering eller sletting av CSAM med utgangspunkt i brudd på deres interne samfunnsregler og algoritmer som ikke er transparente for lovgivere og politimyndigheter.

En annen utfordring er at amerikanske selskap er juridisk beskyttet mot ansvar for innhold som legges ut på deres plattformer eller via deres tjenester (§ 230 i 1996 Communication Decency Act), og det er ingen rettslig mekanisme som kan pålegge eller tvinge selskapene til aktivt å søke etter innhold på sine tjenester. Snarere tvert imot er det amerikanske (så vel som det globale) systemet avhengig av en "gode samaritaner" som gjør en frivillig innsats hos (noen) ESPer.

Det juridiske grunnlaget for at en tjeneste avvises eller innhold fjernes fra plattformen, avhenger av egne interne etiske retningslinjer i selskapet. I tillegg finnes det ingen klar veiledning om hva som utgjør beste praksis eller om selskapet må bruke et anerkjent sporingsverktøy [1]. Dette bidrar til en varierende villighet til å rapportere tilfeller med seksuelle overgrep mot barn eller overgrepsmateriale, og mangel på klare standarder for datakvaliteten. Dette problemet forverres av det faktum at det er lett å opprette flere og falske kontoer for å få tilgang til elektroniske tjenester, og at i henhold til gjeldende juridiske forpliktelser ESPer ikke trenger å lagre dataene (f.eks. IP adressene) i en lengre periode.

I Norge ble den tidligere forskriften om å lagre data i 21 dager forlenget til ett år i 2021 [118]. Denne informasjonen er kritisk for å etterforske seksuelle lovbrudd begått mot barn via nettet. I 2021 ble rundt 30% av saker relatert til seksuelle overgrep mot barn klassifisert som uløste i STRASAK-databasen på grunn av ulike årsaker. Ofte er begrunnelsen knyttet til mangel på informasjon og manglende spor (fordi selskaper ikke lagret data over tid). Dette problemet blir illustrert av et intervjuobjekt fra den nasjonale straffesakenheten:

> *«Utfordringen er at den elektroniske tjenesteleverandøren jobber på en slik måte at han sletter eller blokkerer en krenkende konto på grunnlag av at den bryter med tjenestevilkårene eller samfunnsstandardene. Når profilen slettes, er alle inkriminerende bevis borte. Politiet kan bare straffe lovbrudd som det kan framlegges bevis for, og for det må politiet be om informasjon, men politiet kan ikke gjøre det hvis informasjonen er slettet eller ikke er tilgjengelig.*»



Figur 5: Oversikt over straffbare forhold knyttet til CSA og deres trender fra 2017-2021. Kilde: STRASAK database, Seksjon strategi, plan og utvikling i virksomhetsstyringsstaben,Trøndelag politidistrikt, 2022.

Hittil har Norge ikke hatt et obligatorisk rapporteringsorgan som overvåker ESPer/ISPer og plattformer eller selskap der bruker-til-bruker-meldinger anvendes. Forsøk på å endre systemet i USA og Europa er fortsatt pågående, hovedsakelig i form av forslag til å endre lovgivningen gjennom forslag som EUs "Bedre internett for barn" (BIK+) og EARN IT-loven i USA, som tar sikte på å innføre større krav til tjenesteleverandører. Europakommisjonen har i 2022 foreslått BIK+ strategien [13] vedrørende digitale opplevelser hos barn på nettet der både alderstilpasset utforming av tjenester og obligatorisk rapportering av innhold er hovedtrekkene. Dette flytter regulatoriske forhold mot obligatorisk rapportering med et sentralt europeisk ansvarssenter, som amerikanske NCMEC. Det er usikkert om Norge umiddelbart vil følge dette og bli med i den nye EU-forordningen og/eller pålegger selskapene som driver i Norge til å rapportere til det europeiske ansvarsorganet. Den viktige faren ved å ikke bli med i disse regulatoriske endringene er faren for at disse overgrepsmaterialene fra EU-serverne flyttes til ikke-medlemsstatene der reguleringen fortsatt er frivillig.

Vi ser at begge forslag til endring av reguleringen i USA og EU fortsatt diskuteres og er sterkt omstridt hos ESPer og parter som frykter at denne utviklingen kan skade brukernes personvern, ytringsfrihet og ende-til-ende-krypteringstendenser.

Den andre beslektede problemstillingen er spørsmålet om hvem som skal ha ansvaret for driften av en hjelpetelefon eller et ansvarssenter for rapportering av seksuelle overgrep mot barn og overgrepsmateriale i Norge. Den nåværende operative strukturen i Norge setter rapporteringen (tipstelefonen) under politiets jurisdiksjon (Kripos og politidistriktene), i stedet for en uavhengig sivil organisasjon som frivillige organisasjoner (som er praksis i Danmark, Finland, USA og Storbritannia). Bekymringen er at det vil ha en avskrekkende virkning og at selskaper vil rapportere mindre om rapporteringen skjer til politiet i stedet for en uavhengig institusjon. Den avskrekkende virkningen som oppstår når man vet at et bestemt område (f.eks. chatterom) overvåkes av politimyndigheter, medfører at personer trolig vil undertrykke samtalen av redsel for mulig straff mot enkeltpersoner eller grupper som de nevner i samtalen, som igjen kan påvirke den (følte) ytringsfriheten. Videre er det uklart hvilke fordeler og ulemper det kan medføre for norske statsborgere og bedrifter hvis hovedrapporteringen er plassert utenfor Norge (f.eks. i EU).

4.1.3 Juridiske utfordringer knyttet til bruk av maskinlæringsløsninger

Den rettslige og regulatoriske utfordringen som vi diskuterer i denne delen av rapporten gjelder bekymringer for politimyndighetens bruk av automatiserte maskinlæringssystemer. Spørsmålet er knyttet til mangelen på normaliserte standarder ved bruk av høy-risiko maskinlæringssystemer for å overvåke borgernes aktiviteter på nettet [119] og dagens debatt i den foreslåtte lovgivningen som gjelder politimyndighetenes bruk av maskinlæring.

Kjernen i diskusjonen som pågår hos både myndighetene og allmennheten er om søk etter overgrepsmateriale på personlige enheter krenker grunnleggende menneskerettigheter og personvernlovgivningen [120], [121]. Problemet oppstår i spenningen mellom behovet å identifisere overgrepsmateriale på plattformer og personlige enheter og behovet for å verne om privatsfæren og integriteten til den enkelte. Vedkommendes data kan gi maskinlæringssystemer mulighet til å komme fram til ikke bare den enkeltes identitet, men også vedkommendes preferanser, seksuell orientering,

alder, kjønn, religiøse og politiske ståsteder. Dette gir grunn til bekymring om man ved å tillate en slik inngripen også tillater ulovlig bruk av informasjon mot eller diskriminering av enkeltpersoner [12], [122].

Lover i EU og andre demokratiske land tillater ikke at styresmakter (eller politiet) utfører ulovlig søk av personlige samtaler og enheter, siden det ville vært en overvåking og inntrenging i retten til folks privatliv og ytringsfrihet. Med bakgrunn i dette er det vanskelig å få godkjenning fra offentligheten om at deres private enheter og samtaler gjennomsøkes, og samtidig er det vanskelig å få et politisk samtykke til at det gis tillatelse til massesøk til tross for at hensikten er å hindre seksuelle overgrep mot barn. Denne generelle frykten for overvåking framprovoserer lekfolks aversjon mot automatisert beslutningstaking av maskinlæringssystemer i flere domener [123], slik som i politiarbeid.

Problemet gjelder hovedsakelig frykt for at maskinlæringssystemer (i forhold til mennesker) fortsatt ikke er gode nok til å gjenkjenne menneskelig unikhet, identifisere sammenhenger og være følsom overfor omstendigheter, noe som kan føre til økt frykt for falske positiver (der vanlig pornografisk innhold blir feilaktig identifisert som overgrepsmateriale). Watchdog mødre (foreldregrupper som frivillig overvåker og rapporterer misbruk i populære sosiale medier på nettet) advarer om slike feil i algoritmer hos ESPer som tagger pedagogiske videoer om seksuelle overgrep [31].

Frykt mot automatiserte deteksjonsløsninger av overgrepsmateriale lever av den økte debatten i offentlige og sosiale medier om obskur bruk av algoritmer og mangelen på konsensus om man skal bruke mennesker eller maskinlæring for overvåking av innhold relatert til seksuelle overgrep mot barn. Det siste mislykkede forsøket fra Apple på å introdusere NeuralHash viser at dette ikke er et trivielt problem. Etter å ha kunngjort intensjonen om å lansere NeuralHash i september 2021, har Apple utsatt lanseringen "i løpet av de kommende månedene for å samle inn innspill og gjøre forbedringer" etter den harde kritikken fra offentligheten om frykt for overvåkning, inntrenging i personvernet og falske positiver. Dette til tross for at bare tre falske positive kollisjoner ble rapportert i en test av 100 millioner bilder [124].

Våre intervjuobjekter fra både sivilsamfunnet og privat sektor fremhevet en sterk frykt for en stor mengde med falske positive feil i dagens maskinlæringssystemer, samt potensielle rasemessige, etiske og kjønnsskjevheter og diskriminering i algoritmene (kjent som algoritmiske skjevheter [125]). Forskjellige interessenter fra vår primære undersøkelse (fra frivillige organisasjoner til styresmakter og politifolk) advarer alle mot deres bekymringer om at automatiserte algoritmer som er opplært på historiske rettslige data sannsynligvis vil gjenta og øke fordommer mot visse (minoritets-) grupper i samfunnet, som for eksempel diskrimineringen av afroamerikanske og latinamerikanske lovbrytere slik det ble oppdaget ved bruk av maskinlæringsalgoritmer i amerikanske domstoler for å anslå sannsynligheten for gjentagelsesfaren (nye lovbrudd) [122]. På grunn av begrensningene i omfang har vi ikke kunnet fordype oss fullt ut i disse problemene, men vi nevner dem her siden de sannsynligvis kommer til å være del av de kritiske rettslige og regulatoriske debattene i framtiden, når behovet hos politimyndighetene for å iverksette maskinlæringsmetoder blir uunngåelig, som omtalt i Avsnitt 3.7. Vi mener at hovedproblemene i debatten vil kretse rundt oppfatningen av hva maskinlæringssystemer overvåker/oppsporer (filer, innhold (verbalt og visuelt) eller selve personene) og om obligatorisk overvåking av innhold vil bli pålagt ESPer og personlige enheter.

4.2 Samarbeidet mellom bedrifter og politimyndigheter er en kritisk faktor for å identifisere og straffeforfølgelse besittelse av overgrepsmateriale

Som nevnt i denne rapporten er ISPer, ESPer, samt finansinstitusjoner som følger pengestrømmer kritiske samarbeidspartnere for politimyndighetene innen to domener: deres enestående evne til å tilby toppmoderne tekniske løsninger for identifisering og bekjempelse av seksuelle overgrep mot barn på nett, og deres hjelp til å identifisere lovbrytere/ofre og forhindre deling av overgrepsmateriale. Som omtalt i Underavsnitt 4.1.2 er det samtidig mangel på engasjement innad i hele bransjen, og næringen har generelt sett ingen standardisert plikt til å gjennomsøke sine tjenester [11].

For bedrifter kan målene med å engasjere seg i sosiale saker (f.eks. for å hindre overgrep mot barn) komme i konflikt med juridiske og strategiske mål for å beskytte kundenes personvern og forbedre kundeopplevelsen og tilfredsheten. På den annen side er bedrifter egenmotivert til å beskytte sin merkevare og pleie kundenes tillit. Dette var også den viktigste motivasjonen bedriftene oppgav og som gjør at de engasjerer seg proaktivt i å søke etter støtende materiale på sine tjenester. Noen av de intervjuede lederne føler at økt sikkerhet er en viktig konkurransestrategi for fremtiden.

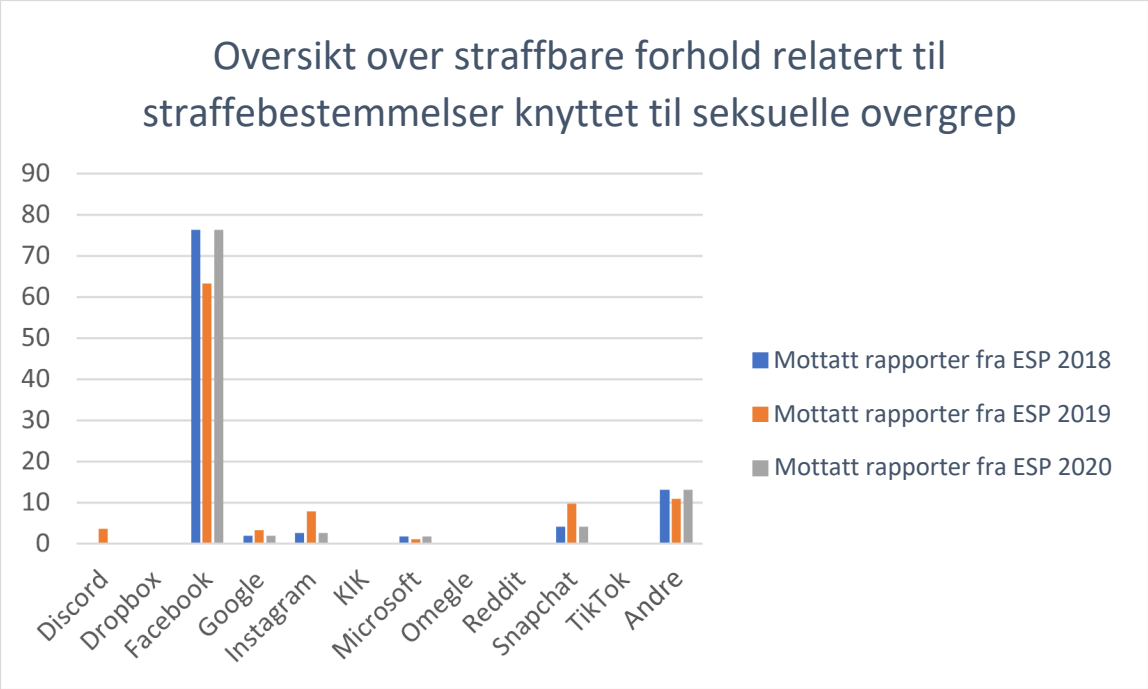
> *"Samtidig ønsker vi at våre kunder skal vite at våre tjenester er trygge, og at vi ikke er et knutepunkt for slikt materiale, så vi er villige til å gjøre det lille ekstra for å sikre det.*" – Intervjusubjekt, programvareselskap

> *"Dette selskapet ser barnas sikkerhet som en hovedstrategi, selv på bekostning av personvern eller lønnsomhet!"* – Intervjusubjekt, nettbasert underholdningstjeneste

Vår analyse viser at det i Norge er svært få ESPer som direkte samarbeider med politiet rundt å forebygge spredningen av overgrepsmateriale. Hovedårsakene er at leverandører rapporterer til landet der deres hovedkontor ligger (vanligvis USA), ikke lokalt, og at mange mellomstore og mindre leverandører ikke har etablert noen systemer og heller ikke har ferdighetene eller de økonomiske ressursene for å søke gjennom sine tjenester. Dette fører til en situasjon der avsløringen av de fleste sakene hvor barn blir seksuelt misbrukt avhenger av NCMEC-rapporter (se følgende avsnitt).

4.2.1 Samarbeidet mellom elektroniske tjenesteleverandører og norsk politi

Selv om intervjusubjektene fra politiet mener at samarbeidet mellom politiet og (internasjonale) ESPer kan forbedres, erkjenner de også at disse eksterne rapportene representerer hovedkilden for ledetrådene til nettbasert seksuelle overgrep mot barn. Figur 6 gir en oversikt over bidragene fra ulike ESPer til de samlede ledetrådene som politiet jobbet videre med. I tråd med det store antallet kunder de har, kommer det største antallet rapporter til norske myndigheter fra Facebook, etterfulgt av Snapchat og Instagram.



Figur 6: Fordelingen av rapporter fra elektroniske tjenesteleverandører til Kripos fra 2018-2020. Kilde: Kripos, NC3 rapport, 2022.

For å få dyptgående innsikt, gir Tabell 2 en oversikt over det årlige antallet rapporter som NC3-enheten hos Kripos har mottatt fra ulike ESPer. Den importerte prosentandelen beskriver andelen av totalt antall mottatte saker som er importert for videre etterforskning hos politiet i Norge.

Tabell 2: Fordelingen av mottatte rapporter fra ESP-er per år. Kilde: Kripos, NC3 internt materiale. 2022.

Mottatt fra NCMEC	2018	Importert	2019	Importert	2020	Importert	2021	Importert
Discord	0	0,0 %	247	91,9 %	65	90,8 %	122	81,1 %
Dropbox	7	100,0 %	13	100,0 %	36	88,9 %	139	73,4 %
Facebook	7982	6,6 %	4341	11,1 %	3819	20,2 %	2013	14,0 %
Google	197	70,6 %	220	77,3 %	312	71,5 %	427	80,1 %
Instagram	263	13,3 %	535	21,3 %	793	22,7 %	341	19,1 %
KIK	0	0,0 %	0	0,0 %	62	98,4 %	114	86,8 %
Microsoft	175	86,9 %	78	89,7 %	154	81,2 %	207	76,8 %
Omegle	23	47,8 %	17	35,3 %	170	28,8 %	405	10,1 %
Reddit	4	75,0 %	1	0,0 %	8	25,0 %	79	53,2 %
Snapchat	436	84,9 %	669	79,5 %	1082	67,0 %	3105	64,3 %
TikTok	0	0,0 %	3	100,0 %	64	82,8 %	327	53,8 %
Øvrige	1376	16,2 %	744	41,7 %	474	56,8 %	571	42,6 %
Totalt	10463		6868		7039		7850	

Samlet sett viser Tabell 2 store forskjeller mellom ESPer når det gjelder antall importerte saker, men også på kvaliteten på informasjonen mottatt i disse rapportene. Kolonner som indikerer importerte prosentandeler viser at selv om noen tjenesteleverandører har lavere totalt antall rapporter, er kvaliteten på oppgitt informasjon, som etterforskerne er avhengige av for å igangsette en sak, betydelig høyere. Mens Facebook for eksempel sender mer enn 75% av alle rapporter, inneholder bare mellom 10-20% av rapportene tilstrekkelig dokumentasjon for å starte etterforskning. I motsetning til det inneholder tipsene som er levert inn av KIK, Microsoft eller Dropbox en andel på 75-100%.

4.2.2 Samarbeid med finansinstitusjoner basert på hvitvaskingsbestemmelser

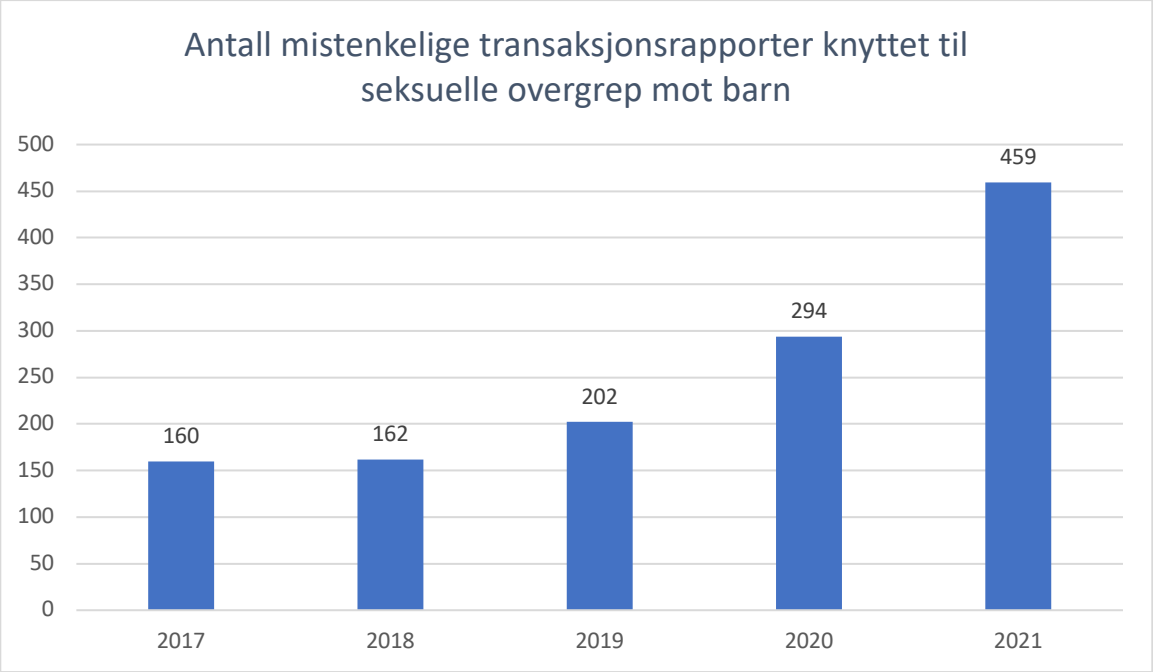
Seksuelle overgrep og utnyttelse av barn på nettet støttes ofte av økonomiske transaksjoner fra lovbrytere som kjøper overgrepsmateriale eller bestiller direktestrømmet overgrep [50]. Selv nye former for overgrepsmateriale er vanligvis finansiert med betaling gjennom ulike finansielle instrumenter [49]. Ofte vil lovbrytere foreta betalinger ved hjelp av ulike anonyme tjenesteleverandører, finansinstitusjoner og kryptovalutaer for å unngå å tiltrekke seg mistanke [49]. Ved å benytte seg av dataene som det globale nettverket av finansielle etterforskningsenheter innehar, får man muligheten til å forbedre strategisk og taktisk etterretningsinnsats for å bekjempe seksuelle overgrep mot barn på nett. Betaling skjer gjennom både anonymiserte betalingsløsninger og mer tradisjonelle løsninger, for eksempel nettbaserte betalingstjenester. Ifølge Europol bruker gjerningspersoner i økende grad kryptovalutaer som betaling for overgrepsmateriale seg imellom, mens mer tradisjonelle betalingstjenester oftere er i bruk i forbindelse med direktestrømmede overgrep [17], [126].

I Norge ble et privat-offentlig samarbeid [127] (OPS AT prosjektet) lansert i august 2021, med sikte på å styrke det nasjonale samarbeidet mellom rapporteringsenheter og relevante myndigheter innen forebygging og avdekking av hvitvasking av penger og finansiering av terrorisme. Det overordnede målet er å etablere bedre koordinering og informasjonsdeling mellom finansnæringen og offentlige myndigheter. Fra politiets side omfatter det Økokrim (Nasjonal myndighet for etterforskning og utredning av økonomisk og miljømessig kriminalitet) som er hovedkilden når det gjelder spesialistkompetanse for politiet og påtale for økonomisk kriminalitet.

Finansielle indikatorer og søkeord knyttet til direktestrømming av CSA kan brukes av Enheten for finansiell etterretning (EFE) i finansinstitusjoner for proaktivt å identifisere transaksjoner som sannsynligvis vil være knyttet til direktestrømming av overgrep med deres datasett. Våre analyser og intervjuer viser at Økokrim og EFE [128] har gjort fremskritt i samarbeidet med finanssektoren for å identifisere aktiviteter relatert til seksuelle misbruk av barn gjort av norske borgere til de transnasjonale betalingene som kan rettes mot krenkende kontoer i utlandet, spesielt kjente kontoer på Filippinene (kilden til denne informasjonen er interne rapporter og intervjuer både med politietterforskere og ledere i økonomisektoren).

I perioden 2017-2021, har Økokrim registrert 1 277 mistenkelige transaksjonsrapporter (STR) knyttet til mistanke om nettbasert seksuelle overgrep mot barn. Antall rapporter som er registrert har økt siden 2017 og nådde en topp i 2021 med 459 rapporter; som vist i Figur 7 [129]. Denne økningen i antall identifiserte saker kan skyldes økt bevissthet rundt finansielle transaksjoner i disse tilfellene, en indikatorliste over straffbare forhold utarbeidet av EFE og økt mediedekning som økte bevisstheten blant bedrifter.

Samarbeidet som det norske EFE har med andre nasjonale enheter for finansiell etterretning gjennom Egmont-gruppen, rapporterer å ha resultert i økt informasjonsutveksling [128]. Egmont gruppe-prosjekt for økt deling av finansiell etterretning ble etablert med tanke på utviklingen av kriminelle forretningsmodeller som er spesielt fokusert på strømming på internett [128]. Våre intervjuer med eksperter innen finanssektoren og politibetjenter viser imidlertid at forebygge og spore seksuelle overgrep mot barn over internett ikke er hovedoppgaven til finansielle svindelenheter (som hovedsakelig fokuserer på hvitvasking av penger og finansiering av terrorisme), og derfor har de muligens ikke hatt full oppmerksomhet på dette. I tillegg vil dette kreve flere dyktige medarbeidere.



Figur 7: Antall mistenkelige transaksjonsrapporter som er registrert av finansinstitusjoner i Norge per år. Kilde: Økokrim. Årsrapport 2021. Enheten for finansiell etterretning [129]. Side 23.

Etterforskere og ledere som jobber med overvåking av betalingsoverføringer fra norske statsborgere til tilretteleggere for direktesendte seksuelle overgrep viser til at mye av denne aktiviteten ikke blir oppdaget. Vår undersøkelse indikerer at det er vanskelig å avgrense økonomiske transaksjoner knyttet til betaling for internettstrømming fra betaling for voksent seksuelt innhold, svindelaktiviteter eller saker relatert til overgrepsmateriale, fordi de har lignende økonomiske profiler. På en annen side vil betalinger gjennom kryptovaluta vanskeliggjøre arbeidet med å identifisere de økonomiske transaksjonene knyttet til seksuelle overgrep mot barn.

4.2.3 Bedrifter svarer at samarbeid med politi bør gå begge veier

Som vi indikerte i målene i denne rapporten, ønsker vi også å presentere de begrensningene og flaskehalsene som bedrifter med sterkere engasjement for møter ved forebygging og deteksjon av

overgrepsmateriale. For bedrifter som frivillig samarbeider med politimyndigheter er et av de viktigste punktene de er misfornøyde med, deres erfaring med at kommunikasjon bare går i en retning - fra bedrifter til politimyndigheter. Bedriftene påpeker at, dersom de hadde fått tilbakemeldinger fra politiet samt en forklaring på hvordan lovbryternes modus operandi (arbeidsmåte) er, ville det gjort det lettere for bedriftene å justere sine algoritmer og metoder.

Alle våre intervjusubjekter fra industrien og noen politimyndigheter indikerte imidlertid at på grunn av taushetsplikten, juridiske forpliktelser til å beskytte informasjonen under etterforskningen og kompliserte prosedyrer knyttet til etterretningsdata, gir politiet minimale tilbakemeldingene til bedriftene om hvordan man kan forbedre oppsporingsinnsatsen. Barrierene for å fremme samarbeid ses først og fremst i sammenheng med nåværende strukturer og måter å jobbe på, i tillegg til at man er veldig påpasselig med å beskytte informasjon og har en frykt for å dele politietterretning. Et intervjusubjekt fra industrien forklarte problemet på følgende måte:

> *"Jeg må si at jeg har fått frie tøyler av selskapet samt ressurser til å sette opp et system for sporing av CSA, men jeg møtte en ganske stor motstand spesielt fra noen politimyndigheter. Det som skjer, er at de sier at det ikke er mulig å dele informasjon med oss. Det er imidlertid viktig å ha eksempler på saker og profiler samt mønstre som de kan dele med oss, slik at vi kan skape systemene, men ingen våger å dele informasjonen, og jeg har snakket med dem alle. De svarer oss ikke med konkret informasjon eller eksempler som kan bidra til å sette opp flagg i systemet, sannsynligvis på grunn av disse reglene om deling av sensitiv personinformasjon og for å beskytte personvernet til personen under etterforskning."*

Vår analyse av de utfordringene som intervjuobjektene fra offentlig sektor har skissert, viste at:

- Toppledelsen i selskaper som kan være berørt av CSAM-deling, fremmer ingen systematiske strategier offentlig av frykt for å øke bevisstheten hos brukerne.
- For tiden er det få bedrifter som har igangsatt bekjempelse av seksuelle overgrep mot barn. Om de har igangsatt noe så er disse vanligvis de største aktørene i bransjer som teknologitjenester, finansinstitusjoner og telekommunikasjon. Et stort antall andre tjenester har imidlertid per nå utilstrekkelig kunnskap og ressurser for å nå dette målet.
- Mens ledelsen i bedrifter som håndterer CSA eller CSAM oppfordrer til oppsporing og fjerning, er initiativene, metodene og tilnærmingene drevet fra bunnen - av driftsenheter som ofte bruker tidligere politibetjenter/etterforskere og dataanalytikere. De blir som regel overbelastet med v andre arbeidsoppgaver og mangel på retningslinjer.
- Dagens utvikling er avhengig av automatiserte teknikker og systemer som, til tross for en rask utvikling, fortsatt lider av betydelige falske positive avvik og andre algoritmiske avvik. På grunn av økt frykt for systematiske avvik og behovet for omfattende investeringer i metodeutvikling samt høyt nivå av ferdigheter, vil de fleste bedriftene fortsatt stole på hash-sammenligningsteknikker til tross for de svakheter dette medfører.

Konklusjon

Europarådets Lanzarote-konvensjon [15] om beskyttelse av barn mot seksuell utnyttelse og seksuelt misbruk (ratifisert av land som blant annet Norge), samt norsk nasjonal strategi [14] for koordinert innsats for forebygging og bekjempelse av internettrelaterte overgrep mot barn, krever kriminalisering av alle typer seksuelle lovbrudd mot barn, både lovbrudd som har oppstått i den virkelige eller digitale verden. Beskyttelse av barn og andre sårbare grupper på nettet kan imidlertid kreve at man må ofre noe på andre områder og hos andre interessenter, slik som f.eks. brudd på personvern ved statlig eller bedriftsovervåking, krenkelse av forretningsalgoritmer og -hemmeligheter, eller skade som kan oppstå i bruker-merkevareforholdet hos bedrifter mot deres kunder, osv.

Reduksjon av overgrep mot barn på internett er en felles bestrebelse fra flere interessenter, inkludert politi, industri, sivilsamfunn, foreldre og selve barna [49]. Dette betyr at det å redusere tilfeller av seksuelle overgrep begått på internett verken er ansvaret til en organisasjon alene eller en oppgave som politimyndigheten kan påta seg alene. Denne rapporten tar sikte på å gi en oversikt over hvordan teknologi generelt og ulike teknologiske løsninger påvirker særlig mulighetene for å få tilgang til og dele overgrepsmateriale på internett og mulighetene for gjerningspersoner til å etablere kontakt med ofre.

Vår gjennomgang av tilgjengelig litteratur, analyser av eksisterende empiriske bevis fra politiregistre og intervjuer med ulike interessenter viser at digitale løsninger i betydelig grad:

1. Forverrer problemet med seksuelle overgrep mot barn over internett og deling og distribusjon av overgrepsmateriale ved å utvide mulighetene for gjerningspersoner til å komme i kontakt med barn gjennom spill- og sosiale medieplattformer og dele store mengder materialer.
2. Det gir anonymitet til gjerningspersoner eller gjør identifisering av digitale materiale tungvint og hindrer derfor politimyndighetenes evne til å identifisere gjerningspersonene, fordi flere teknologiske løsninger tillater gjerningspersonene å maskere sin identitet og de digitale sporene til sine aktiviteter (f.eks. gjennom VPN-tilkoblinger, det mørke nettet, ende-til-ende-kryptering, og betalinger med kryptovaluta,)
3. Samtidig representerer teknologiske løsninger som identifiserer hasher (digitale fingeravtrykk av overgrepsmateriale) og maskinlæringsløsninger som gjør det mulig å identifisere nye overgrepsmaterialer de viktigste mottiltakene mot seksuelle misbruk av barn på internett. Bruk av teknologi som muliggjør raskt søk av et stort volum med data, er den eneste veien fremover i å motvirke det store volumet og teknologiske fremskritt i distribusjonen av overgrepsmateriale.

De viktigste teknologitrendene som vi har identifisert i analysen av utfordringene norske politimyndigheter står overfor, samsvarer med utfordringene som ble identifisert i studier om politimyndighetene i andre land globalt [29], [83], [117]. Totalt sett viser aktørene fra både politi og rettssystemet at de føler at de ofte er flere skritt bak gjerningspersonene når det gjelder teknologisk utvikling [117]. Dette problemet ble spesielt forverret under og i etterkant av koronaviruspandemien da man så en høy topp i saker relatert til overgrepsmateriell [83].

Vår analyse viser at det å være vert for overgrepsmateriale på nettsteder og distribuerte serversystemer betyr at man er den med det større volumet av kjent materiale som er i omløp. Verktøyene som de (største) ESPer og frivillige organisasjoner bruker for å avdekke overgrep, er rettet mot identifisering av kjente overgrepsmateriale, spesielt på nettsteder og filservere. Den viktigste teknologien for identifisere overgrepsmateriale bruker digitale hash-verdier for å samsvare verdiene med allerede kjent materiale

(bilder og video) relatert til seksuelle overgrep. Denne teknologien fungerer godt på å identifisere kjente overgrepsbilder og er noe mindre effektiv på å identifisere videomaterialer. Problemet er at denne teknologien ikke kan identifisere nytt og tidligere ukjent overgrepsmateriale. Bare sofistikert maskinlæringløsninger har en evne til å gå gjennom dataene og identifisere nye tilfeller av CSAM.

Våre intervjuer med ansatte hos politiet, sivile samfunnsorganisasjoner og bedrifter om de teknologiske trendene knyttet til spredning av overgrepsmateriale i Norge og Europa gir den viktigste innsikten og understøtter det vi har funnet i denne rapporten om det politifolk opplever globalt. En undersøkelse av polititjenestepersoner fra 39 land som arbeider med CSA og CSAM-saker [83] fant at 80% av polititjenestepersonene rapporterte en (betydelig eller moderat) økning i gjerningspersoner som forsøkte å kontakte barn på internett, mens 60% av polititjenestepersonene rapporterte en økning av egenprodusert CSAM. Våre funn tyder på en økning i CSA-relaterte saker fra 2017 til 2021; en økning i antall eksterne rapporter om overgrepsmateriale som angår norske borgere og IP adresser og en økning i antallet mistenkelige finansielle transaksjoner som er relatert til seksuell misbruk av barn. Dette tyder på en samlet økning i trusselen mot barn, men også mulig en økning i evnen ESPer og politiet har til å avdekke og rapportere seksuelle overgrep mot barn.

I likhet med våre funn i intervjuer med tjenestepersoner, føler så mange som halvparten av alle tjenestepersoner i en global undersøkelse seg ikke i stand til å estimere trender knyttet til det mørke nettet og direktestrømming i sitt arbeid [83]. Nye teknologiske utviklinger som imøtekommer anonymisering og økt personvern (som i punkt 2 ovenfor) gjør det vanskelig for tredjeparter (om det nå er ESPene, politimyndigheter eller andre) å overvåke transaksjoner og deling. I hvilken grad disse utviklingene påvirker politimyndighetenes evne til å spore overgrep mot barn, kan oppsummeres med estimatet gitt av et intervjusubjekt fra politiet:

> *"Hvis gjerningspersonene bruker VPN, blir de i stor grad anonymisert og kan utføre kriminelle aktiviteter utenfor rekkevidden til politimyndigheter. Dette er en stor utfordring for politiet. Politiet klarte å identifisere 80% av gjerningspersonene som delte CSAM i 2017-2018, nå er andelen redusert til 40% fordi lovbrytere bruker tjenester og teknologiske løsninger som skjuler deres identitet. Mulighetene for å identifisere gjerningspersonene blir vanskeligere for politietterforskere."*

Dette estimatet tilsvarer NCMEC sine estimater som at Meta sin implementering av ende-til-ende-kryptering vil redusere antallet CSAM-rapporter med mer enn 50% [29]. Vi mener at virkningen kan være enda større, gitt at Meta leverer mer enn 93% av alle rapporter (hovedsakelig fra Facebook Messager som Meta forsøker å gjøre ende-til-ende-kryptert).

Siden utviklingen av teknologi er ustoppelig, øker behovet for mottiltak, men sammen med det kommer utfordringen med å balansere sikkerhetsbehov mot behovet for vern mot inntrenging i private sfærer av livet. Utbredelsen av smarttelefoner og sosiale medier har skapt en delingskultur der deling av bilder og videoer med andre, både venner og fremmede, er en integrert del av hverdagen [17]. Disse sosiale aktivitetene er beskyttet av personvernlover og ytringsfrihet. Men samtidig må disse sivile og politiske rettighetene ikke komme på bekostning av sosiale og kulturelle rettigheter som retten til sosial beskyttelse, til en tilstrekkelig levestandard og til de høyeste oppnåelige standarder for fysisk og mental velvære [130].

Gitt betydningen av gjensidig samarbeid mellom privat sektor, sivilsamfunn og politi i forebygging og straffeforfølgelse av seksuelle overgrep mot barn på internett, kan to konklusjoner trekkes ut av denne rapporten:

- Tempoet i utviklingen av skreddersydde teknologiske verktøy i industrien overgår i stor grad politiets ferdigheter, økonomiske og menneskelige ressurser. Imidlertid er skreddersydde verktøy ofte brukt som proprietære verktøy eller for kommersielle formål og er ikke allment gjort tilgjengelig for politimyndigheter (eller små og mellomstore bedrifter). Foreløpig er det ingen obligatoriske krav til ikke-amerikanske ESPer om å rapportere oppdaget overgrepsmateriale; selv for amerikanske ESPer er det ingen obligatoriske krav til å søke alt innhold i en tjeneste for overgrepsmateriale. I tillegg gjør interne bransjesystemet at bedriftene ender opp med å slette kontoer som gjør informasjon utilgjengelig hvor det kunne finnes bevis om misbruk. Ved å lage forskrifter bør lovgivere kreve at ESPer proaktivt søker i sine digitale tjenester og er forpliktet til å rapportere forekomster av seksuelle misbruk av barn.
- Samarbeid mellom anerkjente industripartnere (ESPer) og politimyndigheter må fremmes og aktiveres gjennom utvikling av samarbeidsrammer og standarder som gagner begge sider i utviklingen av effektive strategier. For tiden lider politimyndighetene av mangel på tekniske ferdigheter, teknologiske fremskritt og verktøy som ville økt effektiviteten. På den annen side lider utviklingen av sofistikert verktøy som ville forsterket slik effektivitet på grunn av mangel på samarbeid for å dele informasjon/etterretningsdata. En rettslig avklaring av standarder for samarbeid må muliggjøre dette samarbeidet.

Vi konkluderer med at den svært nødvendige videreutviklingen i forebygging og etterforskning av seksuelle overgrep mot barn på internett vil være kritisk avhengig av toveissamarbeid mellom bedrifter (som utvikler verktøy og bruker forebyggende teknikker i sine tjenester) og politiet (som må gi tilbakemelding for opplæring av modeller og skreddersydde verktøy). Disse samarbeidene må bygge på økt regulering slik at det tillater at bedriftene kan unngå å jobbe reaktivt med problemet. Gitt manglende tilgang til proprietære tjenester fra ESPer, må politimyndigheter stole på rapporteringen fra ESPene (som i mange tilfeller blir den viktigste kilden til å avdekke overgrepsmateriale og utgjør over 90% av rapporterte saker) og hjelpetelefoner som InHope-nettverket i Europa. Til slutt, siden bedrifter står overfor avveiningen mellom å beskytte sikkerheten og brudd på personvern og forbrukernes tilfredshet, og siden mange små og mellomstore bedrifter for tiden ikke har evner og ressurser til å skanne etter overgrepsmateriale, må iverksettelsen av strategier for å forbedre sikkerheten for barn komme fra lovgiver som må definere beste praksis samt verktøy som ESPer og politi bør bruke og gjøre dem allment tilgjengelige. Det er strengt nødvendig at lovgiver involverer ESPer og politimyndigheter i arbeidet med å definere beste praksis, nødvendig verktøy og retningslinjer for samarbeid.

Vi håper at denne rapporten kan bidra til å bekjempe seksuelle overgrep mot barn på internett og skape et tryggere miljø for våre barn.

Kilder

[1] Thorn, “The Intersection of Technology and Child Sexual Abuse,” *Thorn*, 2020. https://www.thorn.org/child-sexual-exploitation-and-technology/ (accessed Mar. 17, 2022).

[2] A. L. Newton, “An Evaluation of the Rise of Online Sexual Exploitation of Children and Technology: How the Past Three Decades Speak to Future,” PhD Thesis, 2021.

[3] D. M. Hughes, “The use of new communications and information technologies for sexual exploitation of women and children,” *Hastings Women’s LJ*, vol. 13, p. 127, 2002.

[4] E. Martellozzo and J. DeMarco, “Exploring the removal of online child sexual abuse material in the UK: Processes and practice,” *Crime Prev Community Saf*, vol. 22, no. 4, pp. 331–350, Dec. 2020, doi: 10.1057/s41300-020-00099-2.

[5] National Center for Missing and Exploited Children, “CyberTipline Data,” *National Center for Missing & Exploited Children*, 2022. http://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata.html (accessed May 19, 2022).

[6] Internet Watch Foundation, “The Annual Report 2021,” 2021.

[7] Medietilsynet, “Nakenbilder og porno,” *Medietilsynet*, May 18, 2021. https://www.medietilsynet.no/digitale-medier/barn-og-medier/foreldreguide/ (accessed Nov. 30, 2022).

[8] Thorn, “We Build Tools to Defend Children From Sexual Abuse | Thorn,” *We Build Tools to Defend Children From Sexual Abuse | Thorn*, Nov. 30, 2022. https://www.thorn.org/ (accessed Nov. 30, 2022).

[9] Canadian Centre for Child Protection, “Survivors’ survey - Executive summary 2017,” Canadian Centre for Child Protection, 2017. Accessed: Nov. 30, 2022. [Online]. Available: https://protectchildren.ca/pdfs/C3P_SurvivorsSurveyExecutiveSummary2017_en.pdf

[10] United Nations Children’s Fund, “Ending Online Sexual Exploitation and Abuse: Lessons learned and promising practices in low- and middle-income countries.” Dec. 2021. Accessed: Feb. 05, 2022. [Online]. Available: https://www.unicef.org/media/113731/file/Ending%20Online%20Sexual%20Exploitation%20and%20Abuse.pdf

[11] Child Dignity Alliance, “Technical Working Group Report - Child safety.” 2018. Accessed: Nov. 30, 2022. [Online]. Available: https://static1.squarespace.com/static/5a4d5d4e7131a5845cdd690c/t/5f15c93f7370541bfad45b15/1595263315850/Child+safety+Report+vD+for+web+%284%29.pdf

[12] European Commission, “EU strategy for a more effective fight against child sexual abuse.” European Commission, Jul. 24, 2020. Accessed: Dec. 04, 2022. [Online]. Available: https://home-affairs.ec.europa.eu/system/files/2020-07/20200724_com-2020-607-commission-communication_en.pdf

[13] European Commission, “A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+),” European Commission, COM(2022) 212 final, Nov. 2022. Accessed: Nov. 30, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0212&from=EN

[14] Justis- og beredskapsdepartementet, “Forebygging og bekjempelse av internettrelaterte overgrep mot barn.” Justis- og beredskapsdepartementet, Aug. 15, 2021. Accessed: Nov. 30, 2022. [Online]. Available: https://www.regjeringen.no/contentassets/2915ff68eb2849edb3218055be32d8cb/strategi-mot-internettrelaterte-overgrep-mot-barn_uu.pdf

[15] Council of Europe, “Lanzarote Convention,” *Children’s Rights*, 2022. https://www.coe.int/en/web/children/lanzarote-convention (accessed Nov. 30, 2022).
[16] N. M. Maalla, “Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development.” Koninklijke Brill NV, 2009. doi: 10.1163/2210-7975_HRD-9970-2016149.
[17] Kripos, “Online Sexual Exploitation of Children and Young People.” Aug. 11, 2019. Accessed: Feb. 06, 2022. [Online]. Available: https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/seksuelle-overgrep-mot-barn/online-sexual-exploitation-of-children-and-young-people.pdf
[18] Wikipedia contributors, “IP address — Wikipedia, the free encyclopedia.” 2022. Accessed: Nov. 30, 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=IP_address&oldid=1119302818
[19] Wikipedia contributors, “Dark web — Wikipedia, the free encyclopedia.” 2022. Accessed: Nov. 30, 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Dark_web&oldid=1106032026
[20] Byju’s, “Cryptocurrency: Definition, Advantages & Disadvantages,” *BYJUS*, 2021. https://byjus.com/current-affairs/cryptocurrency/ (accessed Nov. 30, 2022).
[21] B. G. Westlake, “The Past, Present, and Future of Online Child Sexual Exploitation: Summarizing the Evolution of Production, Distribution, and Detection,” in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, T. J. Holt and A. M. Bossler, Eds. Cham: Springer International Publishing, 2020, pp. 1225–1253. doi: 10.1007/978-3-319-78440-3_52.
[22] GCHQ Government Communications Headquarters, “A thematic overview of how the internet facilitates the distribution of Child Sexual Abuse Material.” GCHQ Government Communications Headquarters, 2022.
[23] M. Liberatore, R. Erdely, T. Kerle, B. N. Levine, and C. Shields, “Forensic investigation of peer-to-peer file sharing networks,” *Digital Investigation*, vol. 7, pp. S95–S103, Aug. 2010, doi: 10.1016/j.diin.2010.05.012.
[24] C. M. S. Steel, “Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms,” *Child Abuse & Neglect*, vol. 44, pp. 150–158, Jun. 2015, doi: 10.1016/j.chiabu.2014.12.009.
[25] WeProtect Global Alliance, “Estimates of childhood exposure to online sexual harms and their risk factors,” Oct. 19, 2021. https://www.weprotect.org/economist-impact-global-survey/ (accessed Nov. 30, 2022).
[26] ECPAT International, “Trends in Online Child Sexual Abuse Material.” Apr. 2018. Accessed: Sep. 05, 2022. [Online]. Available: https://ecpat.org/wp-content/uploads/2021/05/ECPAT-International-Report-Trends-in-Online-Child-Sexual-Abuse-Material-2018.pdf
[27] C. Steel, E. Newman, S. O’Rourke, and E. Quayle, “Technical Behaviours of Child Sexual Exploitation Material Offenders,” *JDFSL*, 2022, doi: 10.15394/jdfsl.2022.1794.
[28] Statista, “User-generated internet content per minute 2022,” *Statista*, 2022. https://www.statista.com/statistics/195140/new-user-generated-content-uploaded-by-users-per-minute/ (accessed Feb. 15, 2023).
[29] C. Teunissen and S. Napier, *Child sexual abuse material and end-to-end encryption on social media platforms: an overview*. Australian Institute of Criminology, 2022. doi: 10.52922/ti78634.
[30] Meta, “Child Endangerment: Nudity and Physical Abuse and Sexual Exploitation,” *Community Standards Enforcement | Transparency Center*, 2022. https://transparency.fb.com/data/community-standards-enforcement/child-nudity-and-sexual-exploitation/facebook/ (accessed Nov. 30, 2022).

[31] S. M. Kelly, "'Watchdog moms' on TikTok are trying to keep minors safe | CNN Business," *CNN*, Jun. 27, 2022. https://www.cnn.com/2022/06/27/tech/tiktok-watchdog-moms-wellness-parenting/index.html (accessed Nov. 30, 2022).
[32] National Center for Missing and Exploited Children, "CyberTipline," *National Center for Missing & Exploited Children*, 2021. http://www.missingkids.org/gethelpnow/cybertipline.html (accessed Nov. 30, 2022).
[33] InHope Association, "Annual report 2021," InHope Association, 2021. Accessed: Nov. 30, 2022. [Online]. Available: https://inhope.org/media/pages/articles/annual-reports/8fd77f3014-1652348841/inhope-annual-report-2021.pdf
[34] H.-E. Lee, T. Ermakova, V. Ververis, and B. Fabian, "Detecting child sexual abuse material: A comprehensive survey," *Forensic Science International: Digital Investigation*, vol. 34, p. 301022, Sep. 2020, doi: 10.1016/j.fsidi.2020.301022.
[35] WeProtect Global Alliance, "'Self-generated' sexual material - WeProtect Global Alliance," Aug. 26, 2022. https://www.weprotect.org/issue/self-generated-sexual-material/ (accessed Nov. 30, 2022).
[36] Internet Watch Foundation, "Self-generated Child Sexual Abuse Online - IWF Annual Report 2021," 2021. https://annualreport2021.iwf.org.uk/trends/selfgenerated (accessed Nov. 30, 2022).
[37] M. Wood, C. Barter, N. Stanley, N. Aghtaie, and C. Larkins, "Images across Europe: The sending and receiving of sexual images and associations with interpersonal violence in young people's relationships," *Children and Youth Services Review*, vol. 59, pp. 149–160, Dec. 2015, doi: 10.1016/j.childyouth.2015.11.005.
[38] Kripos, "Barn som selger egenprodusert overgrepsmateriale: En beskrivelse av fenomenet og omfanget." Oct. 03, 2021. Accessed: Jun. 16, 2022. [Online]. Available: https://www.politiet.no/globalassets/dokumenter/kripos/seksuelle-overgrep/barn-som-selger-egenprodusert-overgrepsmateriale.pdf
[39] B. O'Donnell, "Rise in Online Enticement and Other Trends: NCMEC Releases 2020 Exploitation Stats," *National Center for Missing & Exploited Children*, Feb. 24, 2021. http://www.missingkids.org/blog/2021/rise-in-online-enticement-and-other-trends--ncmec-releases-2020-.html (accessed Nov. 30, 2022).
[40] L. M. T. Aanerød and S. Mossige, "Nettovergrep mot barn i Norge 2015–2017," *NOVA Rapport*, p. 108, 2018.
[41] S. Berggrav, "Hvis du liker meg, må du dele et bilde," Redd Barna, 2020. Accessed: Nov. 30, 2022. [Online]. Available: https://www.reddbarna.no/content/uploads/2020/12/Hvis-du-liker-meg-m%C3%A5-du-dele-et-bilde.pdf
[42] Government Communications Headquarters, "The interim code of practice on online child sexual exploitation and abuse." Dec. 2020. Accessed: Jun. 10, 2022. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944034/1704__HO__INTERIM_CODE_OF_PRACTICE_CSEA_v.2.1_14-12-2020.pdf
[43] K. Hegg and P. Lang-Holmen, "Kommuners kriminalitetsforebyggende arbeid med barn og ungdoms nettrisikoer." Redd Barna, 2020. Accessed: Nov. 30, 2022. [Online]. Available: https://resource-centre-uploads.s3.amazonaws.com/uploads/redd_barna_vi_ser_bare_toppen_av_isfjellet_kommuners_kriminalitetsforebyggende_arbeid_med_barn_og_ungdoms_nettrisikoer.pdf
[44] Kripos, "Ungdrom henges ut på nett: Deling av ulovlig og bekymringsverdig materiale av barn og ungdom." Jan. 2022. Accessed: Jun. 16, 2022. [Online]. Available: https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/voldtekt-og-seksuallovbrudd/fenomenrapport-exposed-kontoer.pdf
[45] N. Titheradge and R. Croxford, "The children selling explicit videos on OnlyFans," *BBC News*, May 26, 2021. Accessed: Nov. 30, 2022. [Online]. Available: https://www.bbc.com/news/uk-57255983

[46] R. Swier, “A Look Into OnlyFans: Child Sexual Abuse Material and Trafficking,” *Dr. Rich Swier*, Jun. 12, 2021. https://drrichswier.com/2021/06/12/a-look-into-onlyfans-child-sexual-abuse-material-and-trafficking/ (accessed Nov. 30, 2022).
[47] Internet Watch Foundation, “Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-Streamed Child Sexual Abuse.” 2018. Accessed: Feb. 06, 2022. [Online]. Available: https://www.iwf.org.uk/media/23jj3nc2/distribution-of-captures-of-live-streamed-child-sexual-abuse-final.pdf
[48] Medietilsynet, “Barn og medier 2020: Seksuelle kommentarer og nakenbilder - Delrapport 4.” May 2020. Accessed: Jun. 22, 2022. [Online]. Available: https://www.medietilsynet.no/globalassets/publikasjoner/barn-og-medier-undersokelser/2020/200519-delrapport-4-seksuelle-kommentarer-og-deling-av-nakenbilder---barn-og-medier-2020.pdf
[49] G. Edwards and L. Christensen, *Cyber strategies used to combat child sexual abuse material*. Australian Institute of Criminology, 2021. doi: 10.52922/ti78313.
[50] Egmont Group, “Combatting Online Child Sexual Abuse and Exploitation Through Financial Intelligence - Public Bulletin.” 2020. Accessed: Jan. 06, 2022. [Online]. Available: https://egmontgroup.org/wp-content/uploads/2021/09/2020_Public_Bulletin_Combatting_Online_Child_Sexual_Abuse_and_Exploitation_Through_Financial_Intelligence.pdf
[51] WeProtect Global Alliance, “Global Threat Assessment 2021.” 2021. Accessed: Nov. 30, 2022. [Online]. Available: https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2021.pdf
[52] A. Brown, “Safe from harm: Tackling webcam child sexual abuse in the Philippines,” Mar. 06, 2016. https://www.unicef.org/stories/safe-from-harm-tackling-webcam-child-sexual-abuse-philippines (accessed Nov. 30, 2022).
[53] Interpol, “COVID19 - Child Sexual Exploitation and Abuse threats and trends.pdf.” Sep. 2020. Accessed: Mar. 28, 2022. [Online]. Available: https://www.interpol.int/content/download/15611/file/COVID19%20-%20Child%20Sexual%20Exploitation%20and%20Abuse%20threats%20and%20trends.pdf
[54] ECPAT International, Interpol, and United Nations Children’s Fund, “Disrupting harm in the Philippines - Evidence on online child sexual exploitation and abuse.” 2022. Accessed: Nov. 30, 2022. [Online]. Available: https://www.end-violence.org/sites/default/files/2022-04/DH_Philippines_ONLINE_FINAL.pdf
[55] Internet Watch Foundation, “IWF research on child sex abuse live-streaming reveals 98% of victims are 13 or under,” May 14, 2018. https://www.iwf.org.uk/news-media/news/iwf-research-on-child-sex-abuse-live-streaming-reveals-98-of-victims-are-13-or-under/ (accessed Nov. 30, 2022).
[56] S. Pettifer, E. Barrett, J. Marsh, K. Hill, P. Turner, and S. Flynn, “The Future of eXtended Reality Technologies, and Implications for Online Child Sexual Exploitation and Abuse,” Jun. 2022. Accessed: Jun. 12, 2022. [Online]. Available: https://www.weprotect.org/wp-content/uploads/2022-June-XR-OCSEA-FINAL-PUBLISHED.pdf
[57] H. Heide, “Nå kan hvem som helst lage en troverdig, kunstig stemme,” *Digi.no*, Jan. 29, 2022. https://www.digi.no/artikler/na-kan-hvem-som-helst-lage-en-troverdig-kunstig-stemme/516813 (accessed Nov. 30, 2022).
[58] A. Crochetiere, “Deep-Fake, Real Pain: The Implications of Computer Morphing on Child Pornography | MTTLR,” *Michigan Technology Law Review*, Mar. 2021. http://mttlr.org/2021/03/deep-fake-real-pain-the-implications-of-computer-morphing-on-child-pornography/ (accessed Nov. 30, 2022).

[59] Europol, “The Internet Organised Crime Threat Assessment (IOCTA) 2019,” 2019. [Online]. Available: https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf
[60] E. Guerra and B. G. Westlake, “Detecting child sexual abuse images: Traits of child sexual exploitation hosting and displaying websites,” *Child Abuse & Neglect*, vol. 122, p. 105336, Dec. 2021, doi: 10.1016/j.chiabu.2021.105336.
[61] C. M. S. Steel, E. Newman, S. O’Rourke, and E. Quayle, “An integrative review of historical technology and countermeasure usage trends in online child sexual exploitation material offenders,” *Forensic Science International: Digital Investigation*, vol. 33, p. 300971, Jun. 2020, doi: 10.1016/j.fsidi.2020.300971.
[62] E. Bursztein *et al.*, “Rethinking the Detection of Child Sexual Abuse Imagery on the Internet,” in *The World Wide Web Conference on - WWW ’19*, San Francisco, CA, USA, 2019, pp. 2601–2607. doi: 10.1145/3308558.3313482.
[63] B. G. Westlake and M. Bouchard, “Liking and hyperlinking: Community detection in online child sexual exploitation networks,” *Social Science Research*, vol. 59, pp. 23–36, Sep. 2016, doi: 10.1016/j.ssresearch.2016.04.010.
[64] Internet Watch Foundation, “Total number of CSAM reports - IWF Annual Report 2021,” *Internet Watch Foundation*, 2021. https://annualreport2021.iwf.org.uk/trends/total (accessed Nov. 30, 2022).
[65] B. G. Westlake, M. Bouchard, and A. Girodat, “How Obvious Is It? The Content of Child Sexual Exploitation Websites,” *Deviant Behavior*, vol. 38, no. 3, pp. 282–293, Mar. 2017, doi: 10.1080/01639625.2016.1197001.
[66] Google, “Rapportering – Google Innsynsrapport,” 2021. https://transparencyreport.google.com/child-sexual-abuse-material/reporting?lu=urls_deindexed&urls_deindexed=period:2021H2 (accessed Feb. 15, 2023).
[67] K. J. Mitchell, D. Finkelhor, L. M. Jones, and J. Wolak, “Use of Social Networking Sites in Online Sex Crimes Against Minors: An Examination of National Incidence and Means of Utilization,” *Journal of Adolescent Health*, vol. 47, no. 2, pp. 183–190, Aug. 2010, doi: 10.1016/j.jadohealth.2010.01.007.
[68] S. Berggrav, “‘Et skada bilde av hvordan sex er’ - Ungdoms perspektiver på porno.” Redd Barna, May 2020. Accessed: Nov. 30, 2022. [Online]. Available: https://resource-centre-uploads.s3.amazonaws.com/uploads/rapport_et_skada_bilde_av_hvordan_sex_er_ungdoms_perspektiver_pay_porno.pdf
[69] TikTok, “Community Guidelines Enforcement Report Jan - Mar 2022,” *TikTok*, Jun. 30, 2022. https://www.tiktok.com/transparency/en/community-guidelines-enforcement-2022-1/ (accessed Nov. 30, 2022).
[70] J. Constine, “WhatsApp has an encrypted child abuse problem | TechCrunch,” *TechCrunch*, Dec. 20, 2018. https://techcrunch.com/2018/12/20/whatsapp-pornography/?fbclid=IwAR1bhm3Zp5OffLeOy-fwdCK2dAjj9O4D8_LpuEEm6lg0r1r3mIHTnnilV-4&guccounter=1 (accessed May 09, 2022).
[71] WhatsApp Help Center, “How WhatsApp Helps Fight Child Exploitation,” *WhatsApp*, Feb. 2021. https://faq.whatsapp.com/154956905959033/?locale=en_US (accessed Nov. 30, 2022).
[72] A. Singh, N. Chandan, R. Pagariya, S. Sahni, S. Sahu, and S. Iyer, “End (-to-end-encrypted) Child Sexual Abuse Material.” 2020. Accessed: Nov. 30, 2022. [Online]. Available: https://www.cyberpeace.org/wp-content/uploads/2022/01/End-to-end-Encrypted-CSAM-2.pdf
[73] G. Mantri, “How can WhatsApp act against child abuse material in encrypted chats? Report suggests,” *The News Minute*, Sep. 29, 2020. https://www.thenewsminute.com/article/how-can-whatsapp-act-against-child-abuse-material-encrypted-chats-report-suggests-134136 (accessed Nov. 30, 2022).

[74] U.S. Department of Justice, “National Strategy for Child Exploitation Prevention and Interdiction,” Apr. 15, 2016. https://www.justice.gov/psc/national-strategy-child-exploitation-prevention-and-interdiction (accessed May 05, 2022).
[75] M. Latapy, C. Magnien, and R. Fournier, “Quantifying paedophile activity in a large P2P system,” *Information Processing & Management*, vol. 49, no. 1, pp. 248–263, Jan. 2013, doi: 10.1016/j.ipm.2012.02.008.
[76] Kripos, “Internal analysis of peer-to-peer file sharing offences.” Kripos, 2022.
[77] P. Biddle, P. England, M. Peinado, and B. Willman, “The Darknet and the Future of Content Distribution,” p. 16.
[78] Europol, “4 arrested in takedown of dark web child abuse platform with some half a million users,” *Europol*, Mar. 05, 2021. https://www.europol.europa.eu/media-press/newsroom/news/4-arrested-in-takedown-of-dark-web-child-abuse-platform-some-half-million-users (accessed Nov. 30, 2022).
[79] S. Lu, “What is the dark web and who uses it?,” *The Globe and Mail*, Aug. 19, 2015. Accessed: Jul. 06, 2022. [Online]. Available: https://www.theglobeandmail.com/technology/tech-news/what-is-the-dark-web-and-who-uses-it/article26026082/
[80] G. H. Owen and N. J. Savage, “The Tor Dark Net.” Centre for International Governance Innovation and the Royal Institute of International Affairs, Sep. 2015. Accessed: Jun. 07, 2022. [Online]. Available: https://pure.port.ac.uk/ws/portalfiles/portal/19636608/The_tor_dark_net.pdf
[81] R. S. Portnoff, *The dark net: De-anonymization, classification and analysis*. 2017.
[82] Internet Watch Foundation, “Hidden ‘dark web’ services - IWF Annual Report 2020,” *Internet Watch Foundation*, 2020. https://annualreport2020.iwf.org.uk/trends/international/other/hidden (accessed Nov. 30, 2022).
[83] NetClean, “COVID-10 impact 2020 - A report about child sexual abuse crime.” NetClean, 2020. Accessed: Nov. 30, 2022. [Online]. Available: https://www.datocms-assets.com/74356/1662373830-netcleanreport-2020.pdf
[84] Europol, “The Internet Organised Crime Threat Assessment (IOCTA) 2014,” 2014. Accessed: Jan. 19, 2017. [Online]. Available: https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web.pdf
[85] B. H. Schell, M. V. Martin, P. C. K. Hung, and L. Rueda, “Cyber child pornography: A review paper of the social and legal issues and remedies—and a proposed technological solution,” *Aggression and Violent Behavior*, vol. 12, no. 1, pp. 45–63, Jan. 2007, doi: 10.1016/j.avb.2006.03.003.
[86] M. Balfe, B. Gallagher, H. Masson, S. Balfe, R. Brugha, and S. Hackett, “Internet Child Sex Offenders’ Concerns about Online Security and their Use of Identity Protection Technologies: A Review: Security Internet Technology,” *Child Abuse Rev.*, vol. 24, no. 6, pp. 427–439, Nov. 2015, doi: 10.1002/car.2308.
[87] T. Krone and R. G. Smith, “Criminal misuse of the Domain Name System,” p. 85, 2018.
[88] NetClean, “Hash Values– Fingerprinting Child Sexual Abuse Material,” *NetClean.com*, n.d. https://www.netclean.com/technical-model-national-response/hash-values-fingerprinting-csam/ (accessed May 12, 2022).
[89] B. Westlake, M. Bouchard, and R. Frank, “Comparing Methods for Detecting Child Exploitation Content Online,” in *2012 European Intelligence and Security Informatics Conference*, Odense, Denmark, Aug. 2012, pp. 156–163. doi: 10.1109/EISIC.2012.25.
[90] Interpol, “International Child Sexual Exploitation database,” 2022. https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database (accessed Jun. 22, 2022).

[91] T. Ith, “Microsoft’s PhotoDNA: Protecting children and businesses in the cloud,” *Microsoft News Stories*, Jul. 15, 2015. https://news.microsoft.com/features/microsofts-photodna-protecting-children-and-businesses-in-the-cloud/ (accessed Nov. 30, 2022).
[92] Canadian Centre for Child Protection, “Project Arachnid: Online Availability of Child Sexual Abuse Material.” Aug. 06, 2021. Accessed: Jun. 15, 2022. [Online]. Available: https://www.protectchildren.ca/pdfs/C3P_ProjectArachnidReport_en.pdf
[93] NetClean, “Using crawling and hashing technologies to find child sexual abuse material - The Internet Watch Foundation,” *NetClean.com*, Feb. 11, 2019. https://www.netclean.com/2019/02/11/using-crawling-and-hashing-technologies-to-find-child-sexual-abuse-material-the-internet-watch-foundation/ (accessed May 27, 2022).
[94] C. M. S. Steel, “Child pornography in peer-to-peer networks,” *Child Abuse & Neglect*, vol. 33, no. 8, pp. 560–568, Aug. 2009, doi: 10.1016/j.chiabu.2008.12.011.
[95] B. G. Westlake and R. Frank, “Seeing the Forest Through the Trees: Identifying Key Players in the Online Distribution of Child Sexual Exploitation Material,” p. 37, 2016.
[96] B. R. da Cunha, P. MacCarron, J. F. Passold, L. W. dos Santos, K. A. Oliveira, and J. P. Gleeson, “Assessing police topological efficiency in a major sting operation on the dark web,” *Sci Rep*, vol. 10, no. 1, p. 73, Dec. 2020, doi: 10.1038/s41598-019-56704-4.
[97] Internet Watch Foundation, “Top-level domain hopping - IWF Annual Report 2020,” 2020. https://annualreport2020.iwf.org.uk/trends/international/other/toplevel (accessed Jun. 13, 2022).
[98] Wikipedia contributors, “Domain tasting — Wikipedia, The Free Encyclopedia.” 2022. Accessed: Jun. 13, 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Domain_tasting&oldid=1071746199
[99] J. Kharub, “Domain Tasting - A Profiteering Venture,” 2022. https://www.legalserviceindia.com/article/l73-Domain-Tasting---A-Profiteering-Venture.html (accessed Jun. 14, 2022).
[100] Chun-Ying Huang, Shang-Pin Ma, Wei-Lin Yeh, Chia-Yi Lin, and Chien-Tsung Liu, “Mitigate web phishing using site signatures,” in *TENCON 2010 - 2010 IEEE Region 10 Conference*, Fukuoka, Nov. 2010, pp. 803–808. doi: 10.1109/TENCON.2010.5686582.
[101] A. K. Jain and B. B. Gupta, “Phishing Detection: Analysis of Visual Similarity Based Approaches,” *Security and Communication Networks*, vol. 2017, pp. 1–20, 2017, doi: 10.1155/2017/5421046.
[102] M. W. Al-Nabki, E. Fidalgo, E. Alegre, and R. Aláiz-Rodríguez, “File Name Classification Approach to Identify Child Sexual Abuse:,” in *Proceedings of the 9th International Conference on Pattern Recognition Applications and Methods*, Valletta, Malta, 2020, pp. 228–234. doi: 10.5220/0009154802280234.
[103] A. Panchenko, R. Beaufort, and C. Fairon, “Detection of child sexual abuse media on p2p networks: Normalization and classification of associated filenames,” in *Proceedings of the LREC Workshop on Language Resources for Public Security Applications*, 2012, pp. 27–31.
[104] J. Prichard, J. Scanlan, T. Krone, C. Spiranovic, P. Watters, and R. Wortley, “Warning messages to prevent illegal sharing of sexual images: Results of a randomised controlled experiment,” *Trends and Issues in Crime and Criminal Justice*, 2022.
[105] Europol, “Police2Peer,” *Europol*, Sep. 12, 2021. https://www.europol.europa.eu/partners-collaboration/police2peer (accessed Nov. 30, 2022).
[106] J. Wolak, M. Liberatore, and B. N. Levine, “Measuring a year of child pornography trafficking by U.S. computers on a peer-to-peer network,” *Child Abuse & Neglect*, vol. 38, no. 2, pp. 347–356, Feb. 2014, doi: 10.1016/j.chiabu.2013.10.018.
[107] C. Schulze, D. Henter, D. Borth, and A. Dengel, “Automatic Detection of CSA Media by Multi-modal Feature Fusion for Law Enforcement Support,” in *Proceedings of International Conference on*

Multimedia Retrieval, Glasgow United Kingdom, Apr. 2014, pp. 353–360. doi: 10.1145/2578726.2578772.
[108] N. Sae-Bae, X. Sun, H. T. Sencar, and N. D. Memon, "Towards automatic detection of child pornography," in *2014 IEEE International Conference on Image Processing (ICIP)*, Paris, France, Oct. 2014, pp. 5332–5336. doi: 10.1109/ICIP.2014.7026079.
[109] J. A. Kloess, J. Woodhams, H. Whittle, T. Grant, and C. E. Hamilton-Giachritsis, "The Challenges of Identifying and Classifying Child Sexual Abuse Material," *Sex Abuse*, vol. 31, no. 2, pp. 173–196, Mar. 2019, doi: 10.1177/1079063217724768.
[110] United Nations Interregional Crime and Justice Research Institute, "250 Law enforcement representatives and experts from more than 60 countries joined the stakeholder meeting of the 'AI for safer children initiative,'" *United Nations Interregional Crime and Justice Research Institute*, Jun. 22, 2021. https://unicri.it/News-First-Stakeholder-Meeting-AI-Safer-Children-Initiative (accessed Nov. 30, 2022).
[111] A. Gangwar, E. Fidalgo, E. Alegre, and V. González-Castro, "Pornography and child sexual abuse detection in image and video: A comparative evaluation," 2017.
[112] N. Sunde and I. M. Sunde, "Conceptualizing an AI-based Police Robot for Preventing Online Child Sexual Exploitation and Abuse:: Part I – The Theoretical and Technical Foundations for PrevBOT," *NJSP*, vol. 8, no. 2, pp. 1–21, Jan. 2022, doi: 10.18261/issn.2703-7045-2021-02-01.
[113] Wikipedia contributors, "Sweetie (internet avatar) — Wikipedia, the free encyclopedia." 2022. Accessed: Nov. 30, 2022. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Sweetie_(internet_avatar)&oldid=1108753708
[114] Medietilsynet, "En kartlegging av 9-18-åringers digitale medievaner." Medietilsynet, Oct. 2020. Accessed: Nov. 30, 2022. [Online]. Available: https://www.medietilsynet.no/globalassets/publikasjoner/barn-og-medier-undersokelser/2020/201015-barn-og-medier-2020-hovedrapport-med-engelsk-summary.pdf
[115] L. R. Frøyland, G. M. Solstad, P. L. Andersen, and S. B. Tveito, "Seksuelle overgrep mot barn og unge via digitale medier," *NOVA Rapport*, p. 211, 2021.
[116] F. Mayer *et al.*, "Age estimation based on pictures and videos presumably showing child or youth pornography," *Int J Legal Med*, vol. 128, no. 4, pp. 649–652, Jul. 2014, doi: 10.1007/s00414-014-1012-2.
[117] O. Cullen, K. Z. Ernst, N. Dawes, W. Binford, and G. Dimitropoulos, "'Our Laws Have Not Caught up with the Technology': Understanding Challenges and Facilitators in Investigating and Prosecuting Child Sexual Abuse Materials in the United States," *Laws*, vol. 9, no. 4, p. 28, Nov. 2020, doi: 10.3390/laws9040028.
[118] T. W. Trøen, "Lovvedtak 165," p. 2, Aug. 2021.
[119] C. Ongre, "Feedback from: Ministry of Local Government and Modernisation." Apr. 08, 2021. Accessed: Nov. 30, 2022. [Online]. Available: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements/F2665314_en
[120] M. R. Calo, "The Boundaries of Privacy Harm," *Indiana Law Journal*, vol. 86, no. 3, p. 31, Jul. 2010.
[121] D. K. Citron and D. J. Solove, "Privacy Harms." Boston University Law Review, Sep. 02, 2021. Accessed: Nov. 30, 2022. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222
[122] J. Larson, S. Mattu, L. Kirchner, and J. Angwin, "How We Analyzed the COMPAS Recidivism Algorithm," *ProPublica*, May 23, 2016. https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm (accessed Feb. 16, 2023).
[123] Y. E. Bigman and K. Gray, "People are averse to machines making moral decisions," *Cognition*, vol. 181, pp. 21–34, Dec. 2018, doi: 10.1016/j.cognition.2018.08.003.

[124] Apple Fandom, “NeuralHash,” *Apple Wiki*, 2021. https://apple.fandom.com/wiki/NeuralHash (accessed Feb. 15, 2023).
[125] P. N. K. Schuetz, “Fly in the Face of Bias: Algorithmic Bias in Law Enforcement’s Facial Recognition Technology and the Need for an Adaptive Legal Framework,” *lawineq*, vol. 39, no. 1, pp. 221–254, 2021, doi: 10.24926/25730037.626.
[126] Europol, “The Internet Organised Crime Threat Assessment (IOCTA) 2017,” 2017.
[127] V. A. Jensen, “Offentlig og privat satsning mot hvitvasking og terrorfinansiering (OPS AT),” *Bits AS*, Nov. 05, 2021. https://www.bits.no/offentlig-og-privat-satsning-mot-hvitvasking-og-terrorfinansiering-ops-at/ (accessed Nov. 30, 2022).
[128] Økokrim, “Enheten for finansiell etterretning (EFE) - Økokrim,” *Økokrim*, 2022. https://www.okokrim.no/finansiell-etterretning-fiu.549302.no.html (accessed Nov. 30, 2022).
[129] Økokrim, “Årsrapport 2021 - Enheten for finansiell etterretning.” 2021. Accessed: Jan. 06, 2022. [Online]. Available: https://www.okokrim.no/getfile.php/5020921.2528.ptpjjbqmjkpnbj/%C3%85rsrapport+2021.pdf
[130] United Nations, “Human Rights,” *United Nations*, 2022. https://www.un.org/en/global-issues/human-rights (accessed Nov. 30, 2022).

Akronymer

AI	Kunstig intelligens (Artificial Intelligence)
AR	Utvidet virkelighet (Augmented Reality)
BIK+	Europeisk strategi for et bedre internett for barn
BSI	Grunnleggende abonnentinformasjon (Basic Subscriber Information)
C3P	Canadian Centre for Child Protection
CAE	Misbruk og utnyttelse av barn (Child Abuse and Exploitation)
CSA	Seksuell misbruk av barn (Child Sexual Abuse)
CSAM	Materiale knyttet til seksuell misbruk av barn (Child Sexual Abuse Material)
EFE	Enheten for Finansiell Etterretning
EMPACT	European Multidisiplinary Platform Against Criminal Threats
ESP	Elektronisk tjenesteleverandør (Electronic Service Provider)
ICMEC	International Centre for Missing and Exploited Children
ICSE	International Child Sexual Exploitation
ISP	Internettleverandør (Internet Service Provider)
IWF	Internet Watch Foundation
MD5	Message-Digest Algorithm 5
MR	Blandet virkelighet (Mixed Reality)
NCMEC	National Center for Missing and Exploited Children
NTNU	Norges teknisk-naturvitenskapelige universitet
P2P	Peer-to-Peer
SARS-CoV-2	Koronaviruspandemien (Covid-19)
SHA	Secure Hash Algorithm
SOBI	Seksuelle overgrep mot barn over Internett
STR	Mistenkelige transaksjonsrapporter (Suspicious Transaction Report)
STRASAK	Det norske straffesaksregisteret
TLD	Topplevel-domene (Top-Level Domain)
TOR	The Onion Router
UNICRI	Interregional Crime and Justice Research Institute
URL	Nettadresse (Uniform Resource Locator)
VoIP	Voice-over-IP
VPN	Virtuelle private nettverk (Virtual Private Network)
VR	Virtuell virkelighet (Virtual Reality)
XR	Forlenget virkelighet (Extended Reality)

BI Norwegian Business School is a leading Nordic research and teaching institution with campuses in the four largest Norwegian cities. Our activity is organized under nine departments covering the range of business research disciplines, and eight BI Research Centres concentrated around themes where we are especially strong.

Departments

- Accounting and Operations Management
- Communication and Culture
- Data Science and Analytics
- Economics
- Finance
- Law and Governance
- Leadership and Organizational Behaviour
- Marketing
- Strategy and Entrepreneurship

BI Research Centres

- Centre for Asset Pricing Research
- Centre for Construction Industry
- Centre for Corporate Governance
- Centre for Creative Industries
- Centre for Experimental Studies and Research
- Centre for Health Care Management
- Centre for Applied Macroeconomics and Commodity Prices
- Nordic Centre for Internet and Society

For an archive of all our PhD-dissertations/reports, please visit https://www.bi.edu/research/publications/

SERIES OF RESEARCH REPORTS 01/2023
ISSN 0803-2610

BI Norwegian Business School

BI Norwegian Business School
N-0442 Oslo
Phone: +47 46 41 00 00
www.bi.no