

Underlagsrapport 2026:1

TEKNIKENS ROLL I VÅLDSUTÖVANDE OCH STÖDINSATSER

En litteraturöversikt gällande digitala och teknologifaciliterade dimensioner av våld

Jämställdhetsmyndigheten publicerar flera olika typer av rapporter.
Underlagsrapporter från externa forskare eller aktörer som fungerar som ett kunskapsunderlag är en typ av rapport.

Jämställdhetsmyndigheten

Göteborg, februari 2026

Underlagsrapport 2026:01

Dnr: 25/00247

Har du frågor om denna publikation, kontakta:

Mikael Thörn, tf avdelningschef

Telefon 070-784 74 72

INNEHÅLL

Förord	4
Sammanfattning	5
Bakgrund och genomförande	6
Inledning	6
Bakgrund till litteraturöversikten	6
Syfte och frågeställningar	7
Genomförande	7
Begreppsanvändning	8
Om underlaget	8
Forskningsfältet och dess centrala utmaningar	8
Fokus på teknologifaciliterat våld i bredare bemärkelse	12
Återkommande utmaningar	12
Studiernas ansatser och resultat i korthet	13
Fokus på dokumenterade sexuella övergrepp och exploatering av barn online	19
Återkommande utmaningar	19
Studiernas ansatser och resultat i korthet	20
Fokus på artificiell intelligens, sakernas internet och metaversum	25
Återkommande utmaningar	25
Studiernas ansatser och resultat i korthet	28
Fokus på förebyggande strategier och verktyg	36
Återkommande utmaningar	36
Studiernas ansatser och resultat i korthet	37
Sammanfattande slutord	48
Källförteckning	50
Bilaga 1. Förkortningar och engelska begrepp	53
Tabell 1. Förkortningar (A–Ö)	53
Tabell 2. Engelska uttryck (A–Z)	55
Bilaga 2: Dokumentation av sökstrategi	57
Bilaga 3: Inklusions- och exklusionskriterier	67
Bilaga 4: Flowchart	68

FÖRORD

Regeringen gav 2024 Jämställdhetsmyndigheten i uppdrag att kartlägga och sammanfatta kunskapsläget om de digitala dimensionerna av mäns våld mot kvinnor (A2024/00815). Kartläggningen skulle utgå ifrån forskning och andra studier som är relevanta för svenska förhållanden. Denna forskningsöversikt är en av flera underlagsstudier som tagits fram inom ramen för uppdraget, vars syfte är att skapa en samlad bild av kunskapen och behov av åtgärder, samt bidra till en gemensam förståelse av vad teknologifaciliterat våld (TFV) innebär.

Jämställdhetsmyndighetens uppdrag omfattar digitala dimensioner av mäns våld mot kvinnor, våld i nära relationer, hedersrelaterat våld och förtryck samt prostitution och människohandel. Uppdraget omfattar dessutom brottslighet i pornografiska syften samt kontaktförsök med barn under 18 år i sexuellt syfte. Uppdraget tar avstamp i rekommendationer från GREVIO, som är det oberoende expertorgan som har ansvar för att övervaka staters genomförande av Europarådets konvention om förebyggande och bekämpning av våld mot kvinnor och våld i hemmet (Istanbulkonventionen).

För att bättre stämma överens med den internationella begreppsanvändningen så använder underlagsstudierna i första hand paraplybegreppet teknologifaciliterat våld. Det innebär våld som begås med hjälp av informations- och kommunikationsteknik (IKT). Nationellt centrum för kvinnofrid (NCK) vid Uppsala universitet har tagit fram en separat forsknings- och kunskapsöversikt gällande teknologifaciliterat våld i vuxnas nära relationer.

Den här forskningsöversikten sammanställer och analyserar litteratur gällande de digitala och teknologifaciliterade dimensionerna av de andra våldsformer som täcks av uppdraget, med särskilt fokus på teknikens roll i våldsutövande och stödinsatser.

Forskningsöversikten har tagits fram av förste forskare Anders Strindberg på Totalförsvarets forskningsinstitut (FOI), på uppdrag av Jämställdhetsmyndigheten. Texten har därefter bearbetats språkligt av Jämställdhetsmyndigheten, men slutsatserna och analysen som presenteras i denna rapport är forskarens.

SAMMANFATTNING

Denna rapport sammanställer kunskapsläget om digitala och teknologifaciliterade dimensioner av våld. Rapporten är en litteraturöversikt baserad på 27 internationella forskningsöversikter, publicerade mellan 2019 och 2025, med fokus på teknikens roll i våldsutövande och stödinsatser. Litteraturöversikten har sammanställts av forskare på Totalförsvarets forskningsinstitut (FOI) på uppdrag av Jämställdhetsmyndigheten.

Digitalisering och ny teknik har förändrat hur våld, hot och övergrepp kan utövas. Våld sker i dag inte bara fysiskt utan även genom digitala miljöer och verktyg, såsom sociala medier, appar, spelplattformar och uppkopplade tekniska system. Detta benämns i forskningen som teknologifaciliterat våld (TFV) - det vill säga våld som helt eller delvis möjliggörs genom informations- och kommunikationsteknik (IKT). I rapporten identifieras forskningsstudier inom fyra huvudsakliga områden:

1. **Teknologifaciliterat våld i bred bemärkelse**, exempelvis kopplat till dejtingappar, pornografi utan samtycke, virtual reality (VR) och trakasserier.
2. **Sexuella övergrepp och sexuell exploatering av barn online**, såsom grooming, livestreamade övergrepp och spridning av övergreppsmaterial.
3. **Ny och framväxande teknik** som påverkar brottsligheten, såsom artificiell intelligens (AI), deepfakes, sakernas internet (IoT) och metaversum.
4. **Förebyggande strategier och tekniska verktyg**, till exempel automatiserad upptäckt, utbildningsinsatser, appar för stöd och säkerhet samt varningssystem.

Flera av de inkluderade forskningsstudierna identifierar likande utmaningar på området:

- **Begreppsmässig otydlighet.** Avsaknad av gemensamma definitioner för centrala begrepp försvårar forskning, lagstiftning och internationellt samarbete.
- **Begränsade empiriska underlag.** Det är svårt att samla in tillförlitliga och etiskt försvarbara data och vissa grupper är underrepresenterade i forskningen.
- **Snabb teknikutveckling.** Våldsutövare anpassar sig snabbt till ny teknik, medan lagstiftning, myndigheter och skyddssystem ofta släpar efter.
- **Avvägningar mellan säkerhet och integritet.** Området medför en mängd dilemman, och insatser riskerar leda till integritetskränkningar och överblockering.

Rapporten visar att teknologifaciliterat våld är ett brett och växande samhällsproblem med allvarliga konsekvenser. Kvinnor, barn och unga och sexuella minoriteter är särskilt utsatta. Samtidigt rymmer tekniken också möjligheter till förebyggande arbete och stöd, exempelvis genom AI-baserad upptäckt av övergreppsmaterial, digitala stödverktyg och utbildningsinsatser. En övergripande slutsats är att forskningsfältet i dag är brett men fragmenterat. För att utveckla effektiva åtgärder krävs större begreppslig och metodologisk tydlighet, mer tvärvetenskaplig forskning, samt ökad samverkan mellan forskning, myndigheter, civilsamhälle och teknikföretag.

BAKGRUND OCH GENOMFÖRANDE

Denna forskningsöversikt bygger på en sammanställning av 27 tidigare forskningsöversikter som rör olika aspekter av teknologifaciliterat våld. I detta kapitel beskrivs bakgrunden till forskningsöversikten och hur den tagits fram. Här presenteras även de inkluderade studierna övergripande, samt de begrepp som används i texten.

Inledning

Under de senaste två decennierna har digitaliseringen kommit att forma hur vi förstår, upplever och hanterar våld, hot och tvång. Övergrepp sker i dag inte enbart i fysiska miljöer, utan också i digitala sammanhang. Digitala plattformar och dataflöden formar hur människor möts, syns och kan påverka varandra. De skapar nya möjligheter för övervakning, kontroll, trakasserier och spridning av kränkande material. I dessa miljöer uppstår det som brukar kallas teknologifaciliterat våld (*technology facilitated violence, TFV*). Det kan handla om övergrepp som sprids genom delning i digitala kanaler, tvång som utövas genom digital övervakning eller hat som organiseras och förstärks i digitala nätverk. I denna nya verklighet kan våld inte bara förstås som en enskild handling utan måste ofta ses som del av en process som äger rum i digitala infrastrukturer såväl som det fysiska rummet. Blythe och Johnson (2019) beskriver detta som ett skifte från "episodiskt våld" till "kontinuerligt våld" där informations- och kommunikationsteknik (IKT) inte bara används för att orsaka skada utan dessutom håller skadan levande långt efter att den fysiska händelsen avslutats.

Samtidigt har IKT skapat nya förutsättningar för att upptäcka, förebygga, spåra och lagföra övergrepp och våld på sätt som tidigare inte varit möjligt. Utvecklingen på området går framåt - både för de som begår brott, och de som arbetar för att upptäcka, förebygga och bekämpa brottsligheten. Forskningen som granskats i denna översikt visar dock tydligt att utvecklingen av verktyg och modeller som är till för att skydda individer och samhället ständigt släpar efter utvecklingen av verktyg som används för att skada dem.

Bakgrund till litteraturöversikten

Jämställdhetsmyndigheten har i uppdrag att kartlägga kunskapsläget om, och åtgärder mot, digitala dimensioner av mäns våld mot kvinnor, våld i nära relationer, hedersrelaterat våld och förtryck samt prostitution och människohandel. Myndigheten ska även föreslå åtgärder för ökad kompetens, samt vid behov föreslå åtgärder för att minska utsattheten för de digitala dimensionerna av våld. För att bidra till detta arbete är Totalförsvarets forskningsinstitut (FOI) inskrivet i Jämställdhetsmyndighetens uppdrag med särskilda medel. FOI ansvarar, enligt överenskommelse med Jämställdhetsmyndigheten, för att sammanställa och analysera litteraturen gällande digitala och teknikbaserade dimensioner av våld. Arbetet med att söka fram litteraturen har genomförts av Malmö universitet inom ramarna för en separat överenskommelse mellan universitetet och Jämställdhetsmyndigheten.

Syfte och frågeställningar

Denna översikt syftar till att sammanställa och analysera forskningslitteratur gällande digitala och teknologifaciliterade dimensioner av våld med fokus på teknikens roll i våldsutövande och stödinsatser, inklusive generativ artificiell intelligens (AI) och sakernas internet (Internet of things, IoT). Eftersom urval och utvärdering av källorna inte ingått i FOI:s uppdrag är översikten inte att betrakta som en systematisk litteraturgranskning. Snarare handlar det om en översiktsstudie av andra relevanta översiktsstudier. Syftet är inte att värdera enskilda studiers kvalitet, utan att ge en helhetsbild och identifiera forskningsluckor. Mer specifikt syftar översikten till att:

1. ge en övergripande bild av forskningsläget gällande digitala och teknologifaciliterade dimensioner av våld
2. identifiera områden där forskning gällande digitala och teknologifaciliterade dimensioner av våld saknas eller är begränsad
3. identifiera luckor i fråga om kunskap, åtgärder och verktyg för att hantera digitala och teknologifaciliterade dimensioner av våld.

Genomförande

Denna forskningsöversikt kompletterar kunskap- och forskningsöversikten *Digitala dimensioner av våld i vuxnas nära relationer* som genomförts av Nationellt centrum för kvinnofrid (NCK) vid Uppsala universitet inom ramen för detta uppdrag (NCK 2025:4). Denna forskningsöversikt utgår från samma söksträngar som NCK:s, men har justerats för att i stället avgränsas till digitala och teknologifaciliterade dimensioner av de övriga våldsområden som omfattas av Jämställdhetsmyndighetens uppdrag. Det vill säga mäns våld mot kvinnor utanför nära relationer, hedersrelaterat våld och förtryck, prostitution och människohandel, våld i ungas nära relationer, sexuella kontaktförsök med barn samt brottslighet i pornografiska syften.

Jämställdhetsmyndigheten gav informationsexperter vid Malmö Universitetsbibliotek i uppdrag att ta fram söksträngar och genomföra databassökningar (se bilaga 2). Sökningen avgränsades till litteraturöversikter publicerade på engelska eller nordiska språk från och med 2019 till juni 2025. Sökningarna avgränsades även till studier med huvudsakligt fokus på Europa, Nordamerika, Australien och Nya Zeeland, då dessa geografiska områden utgör sammanhang med liknande social och teknologisk utveckling (för inklusions- och exklusionskriterier, se bilaga 3). Litteratursökningen utfördes i följande databaser under juni 2025: ASSIA, Cinahl, PsycInfo, Scopus, Sociological Abstracts och Web of Science.

Totalt identifierades 1143 studier, varav 406 dubbletter rensades bort. De återstående 737 studierna granskades på titel- och abstraktnivå av en utredare på Jämställdhetsmyndigheten, varav 689 exkluderades. De kvarvarande 48 studierna granskades därefter på titel- och abstraktnivå av tre utredare på Jämställdhetsmyndigheten. Vid en samlad bedömning exkluderades ytterligare 18 studier som inte bedömdes uppfylla inklusionskriterierna. Totalt tillhandahölls 30 studier till Totalförsvarets forskningsinstitut (FOI). Av dessa exkluderades därefter ytterligare tre studier i samband med fulltextläsning, på grund av fel geografiskt fokus. Det slutliga underlaget som inkluderats i denna forskningsöversikt består därmed av 27 forskningsartiklar, huvudsakligen översiktsstudier (scoping reviews).

Begreppsanvändning

Som vanligt i en litteraturöversikt utvecklar denna rapport inga egna teoretiska ramverk eller definitioner utan redogör för de som förekommer i forskningen. När rapporten hänvisar till "forskningen" eller "litteraturen" avses, om inget annat anges, de 27 artiklar som utgör rapportens underlag. Begreppet "teknologifaciliterat våld" används därför i bred mening för att beteckna tvång, hot, exploatering eller integritetskränkningar som helt eller delvis utövas genom IKT. En central utmaning i sammanställningen av denna rapport och i arbetet mot teknologifaciliterat våld generellt, är den begreppsmässiga oreda som råder i litteraturen. Detta identifieras i forskningen som en svår utmaning för forskningen själv, för lagstiftning och för adekvat teknikutveckling. Denna rapport återger forskningens egna språkbruk med centrala begrepp. Begrepp återges ibland på engelska då etablerade svenska översättningar saknas. Relevanta förkortningar och engelska begrepp har kursiverats i texten. Dessa listas och förklaras närmare i bilaga 1.

Om underlaget

Det har inte varit möjligt eller bedömts som meningsfullt att dela in grundmaterialet enligt artiklarnas eller tidskrifternas ämnesområden. Samtliga studier fokuserar på IKT-baserade dimensioner av våld men kommer från ett flertal forskningsdiscipliner och tvärvetenskapliga forskningssammanhang. Flera av översiktsstudierna lyfter i sin tur fram och analyserar källmaterial från olika discipliner och traditioner. Avsaknaden av tydliga ämnesgränser gör det svårt att dela in underlaget i separata ämnesområden. Nästan ingen studie behandlar endast en aspekt av teknologifaciliterat våld.

En viktig gräns i materialet är den mellan studier som diskuterar teknikens roll i utförandet av brott (16 studier) och de som diskuterar teknikens roll i arbetet att upptäcka, förhindra och förebygga brott (11 studier). Inom dessa två övergripande perspektiv finns dock flera mer specifika teman som ligger till grund för studiens kapitelindelning:

- Teknologifaciliterat våld (*technology facilitated violence*, TFV) i bredare bemärkelse
- Sexuell exploatering och sexuellt övergreppsmaterial på barn via IKT (*child sexual abuse material*, CSAM, och *online child sexual abuse and exploitation*, OCSAE)
- Teknik som kopplar samman fysiska och virtuella dimensioner vid våldsutövande (artificiell intelligens, sakernas internet och metaversum),
- Förebyggande strategier och verktyg.

Forskningsfältet och dess centrala utmaningar

Teknologifaciliterat våld (*Technology facilitated violence*, TFV) är gemensam nämnare för samtliga studier i underlaget. Det är ett paraplybegrepp för ett spektrum av handlingar som kan innefatta mobbning och cyberstalking, livestreamade sexuella övergrepp och AI-genererat sexuellt övergreppsmaterial på barn. Var tonvikten läggs varierar från en disciplin till en annan. I den kriminologiska forskningen behandlas TFV främst som en form av cyberkriminalitet (Edwards m.fl., 2021; Decoster, 2021), inom genus- och

rättsvetenskap ligger fokus på könsbaserad maktutövning (Falduti och Tessaris, 2023; Filice m.fl., 2024) och inom datavetenskapen behandlas TFV som en utmaning för informationssäkerhet (Sangwan och Bhatia, 2023; Singh och Nambiar, 2024). Dessa skilda ansatser har kanske bidragit till att synliggöra våldets många dimensioner (tekniska, sociala, rättsliga och så vidare) men de olika förståelserna av gemensamma begrepp verkar ha försvårat samlad kunskapsuppbyggnad och tvärvetenskapligt samarbete.

Studier kring TFV är ofta sektorsspecifika och nationellt avgränsade eftersom olika rättslägen i olika länder begränsar deras relevans och tillämpbarhet. Forskningen saknar sammanhållande eller övergripande teoretiska och metodologiska ramar. Sammantaget framträder ett forskningslandskap som är brett men grunt. Det innehåller en bredd av empiriska observationer och resonemang men saknar den analytiska sammanhållning som ofta kännetecknar ett mer etablerat studiefält eller ämnesområde. I den litteraturgenomgång som presenteras i följande kapitel återkommer tre utmaningar. Dessa kan ses som grundläggande anledningar för att förstå varför både forskningen och det bredare praktiska arbetet mot teknologifaciliterat våld är angelägna.¹

Utmaning 1: Definitioner och rättsliga ramar

I litteraturen skapar avsaknaden av gemensamma definitioner och avgränsningar för viktiga företeelser – såsom *lifestreamed child sexual abuse* (LSCSA) och *technology assisted child sexual abuse* (TA-CSA) – en fragmenterad grund för både forskning och brottsbekämpning. Skillnader i rättsliga definitioner inom olika rättssystem leder till inkonsekventa tolkningar av vad som faktiskt är att betrakta som *child sexual abuse material* (CSAM). Detta hindrar utvecklingen av enhetliga forskningskategorier (Bleakley m.fl., 2024; Falduti och Tessaris, 2023) och hämmar tvärvetenskapliga samarbeten och komparativ forskning (Chauvire Geib och Fevert, 2024). Eftersom sexuella övergrepp mot barn online är transnationella till sin natur är nationella lagar och regler otillräckliga, men samtidigt nödvändiga för brottsbekämpande och rättsvårdande myndigheter (Falduti och Tessaris, 2023; Gómez-Quintero m.fl., 2024). Flera studier belyser hur klyftor mellan olika rättssystem och tolkningar hindrar utredningar och försvårar informationsutbyte (Falduti och Tessaris, 2023; Bleakley m.fl., 2024; Chauvire Geib och Fevert, 2024; Parti och Szabó, 2024; Decoster, 2024; Gómez-Quintero m.fl., 2024).

Utmaning 2: Begränsade empiriska underlag

En annan återkommande utmaning handlar om bristen på tillförlitliga, representativa och samtidigt etiskt inhämtade data. Det är svårt att samla in empiriskt material. Forskare står inför allvarliga juridiska och etiska begränsningar i insamlandet av primärdata, i synnerhet när forskningen berör minderåriga. Detta har lett till forskning som arbetar med små populationer och därför lider av begränsad generaliserbarhet (Chauvire Geib och Fevert, 2024). Bristen på empiri försvåras av den ovannämnda begreppsmässiga rörligheten och av det faktum att forskningen kring TFV är relativt ny (Porta m.fl., 2024).

¹ De källor som anges löpande i texten är källor till, eller illustrationer av ett påstående.

Även metodologiska utmaningar såsom opålitliga minnesbilder i återblickande studier och en konsekvent underrepresentation av minoriteter och marginaliserade grupper är problematiska (Chauvire Geib och Fevert, 2024; Quilty och Flynn, 2025). Tillgången till data från den privata sektorn, exempelvis internetleverantörer och olika plattformar, begränsas samtidigt av affärssekretess och olika riktlinjer för datalagring (Parti och Szabó, 2024). Etiska krav på att inte återtraumatisera eller på andra sätt åsamka lidande hos brottsoffer, samt svårigheter med anonymitet begränsar forskningsprojekt på ett tidigt stadium. Anonymitet utgör en begränsning både i fråga om att få kontakt med brottsoffer och i fråga om att bevara deras anonymitet inom projekt (Falduti och Tessaris, 2023; Sangwan och Bhatia, 2022). Sammantaget begränsar dessa faktorer både den empiriska tillförlitligheten och den etiska hållbarheten i forskningen.

Utmaning 3: Den snabba teknikutvecklingen

Den snabba utvecklingen av IKT ger våldsutövarna nya verktyg och fler möjligheter. Kriminella är ofta tidiga anhängare ("early adopters") av nya teknologiska verktyg, motiverade av behovet att undgå upptäckt. Nya tekniska utvecklingar som exempelvis deepfakes, kryptering och metaversum har medfört nya sätt att både begå och dölja övergrepp som rättsvårdande och brottsbekämpande myndigheter har svårt att hantera (Parti och Szabó, 2024; Sandoval m.fl., 2024; Gómez-Quintero m.fl., 2024). Utvecklingen av motåtgärder är förhållandevis långsam och styrs ofta av rättsliga, byråkratiska och etiska krav som kriminella inte behöver ta hänsyn till. Algoritmer avsedda att upptäcka övergrepp är ofta begränsade och potentiellt missvisande på grund av partiskhet i träningsdata såsom över- eller underrepresentation av olika hudtoner eller etniska särdrag. De blir dessutom snabbt föråldrade när brottslingar hittar nya verktyg (Falduti och Tessaris, 2023). Quilty och Flynn (2025) pekar på att bristande mångfald i befintliga empiriska data påverkar forskningens generaliserbarhet och tillämplighet inom olika demografiska grupper. Dessutom släpar rättsvårdande och brottsbekämpande myndigheters förmåga ofta efter den tekniska utvecklingen på grund av bristande utbildning och träning, finansiering och tekniska resurser (Decoster, 2024). Forskningen belyser en ständig "kapprustning" mellan våldsutövare och brottsbekämpande myndigheter och en utmaning i att balansera innovation och reglering.

Fältets mest centrala behov: begreppsmässig stringens

Den litteratur som har granskats i denna rapport omfattar i stort sett hela bredden av TFV. Studierna behandlar allt från föräldrainerventioner och våld på dejtingappar till livestreamade sexuella övergrepp och användning av deepfakes i syfte för att utöva utpressning. Nästan samtliga områden som identifierats beskrivs vara i behov av ytterligare forskning. TFV är ett relativt ungt forskningsområde vars mognad kräver omfattande forskning inom ett mycket brett spektrum av frågor. I fråga om rekommendationer för framtida forskning framträder i första hand ett kritiskt behov av ökad metodologisk stringens och begreppsmässig tydlighet i förhållande till alla teman och frågor, snarare än ett visst avgränsat ämnesområde eller tema. Nära nog samtliga studier pekar på detta behov. Framtida forskningsinsatser måste vara medvetna om detta för att kunna förbättra generaliserbarheten i forskningens resultat, något som flertalet studier menar att dagens forskningsresultat saknar. Det finns ett behov av bredare, mer integrerade forskningsstrategier (Patterson m.fl., 2022). Framtida inriktningar för

forskning och tillämpning bör anta ett flernivå- eller ”helhetssystem”-perspektiv för att öka träffsäkerhet och effektiviteten i åtgärder. Forskningslandskapet i sig spänner naturligt över flera discipliner, vilket kanske är särskilt tydligt i studier om deepfakes (Birrer och Just, 2024), men disciplinerna är varken begreppsmässigt eller metodologiskt samstämmiga. Studier som fokuserar på teoretiska eller principiella aspekter bidrar till metodologiskt djup (Sangwan och Bhatia, 2022) och ett tvärvetenskapligt tillvägagångssätt kan ses som nödvändigt för fältets fortsatta utveckling.

FOKUS PÅ TEKNOLOGIFACILITERAT VÅLD I BREDARE BEMÄRKELSE

Sex artiklar fokuserar på teknologifaciliterat våld (TFV) i bredare bemärkelse.² I dessa artiklar kan vissa genomgripande och centrala utmaningar identifieras. Dessa rör begränsningar i lagstiftning, begrepp, kunskap och teknik, samt etiska utmaningar.

Återkommande utmaningar

Begränsningar i lagstiftning och regleringar

I sin studie om pornografi utan samtycke (*non-consensual pornography*, NCP) konstaterar Falduti och Tessaris (2023) att hoten i onlinemiljö är globala. De menar att statistik från brottsbekämpande myndigheter pekar på en dramatisk ökning av anmälda fall och utredningar gällande övergrepp globalt. Estellés och Doyle (2025) konstaterar att riskerna online sträcker sig från det personliga och intima till det politiska och samhällseliga. Trots det saknas fortfarande bredare strategier för att förebygga kränkande beteende och övergrepp online, samt för att skilja mellan legitimt respektive kränkande sexuellt innehåll. Befintliga strategier baseras ofta på nationella juridiska definitioner av vad som är olagligt. Detta leder till nationella strategier som saknar förutsättningar för samverkan och bredare tillämplighet (Falduti och Tessaris, 2023), och som inte heller kan ligga till grund för robust och generaliserbar forskning.

Begreppsmässiga, kunskapsmässiga och tekniska begränsningar

Porta m.fl. (2024) pekar på att den fortsatt begränsade kunskapen om förekomsten och effekterna av sexuellt våld, tillsammans med inkonsekventa definitioner av centrala begrepp, utgör en betydande utmaning för forskningen. Olika definitioner av sexuellt våld, inklusive olika definitioner av begrepp som "våldsutövare" och "brottsoffer," påverkar forskningen negativt (Porta m.fl., 2024). Filice m.fl. (2022) och Gewirtz-Meydan m.fl. (2024) efterlyser därför fler studier i bredare, och mer tvärkulturella sammanhang, särskilt när det gäller forskning om dejtingappar. I båda studierna identifieras även ett tydligt behov av ytterligare longitudinell och experimentell forskning för att fastställa kausala samband mellan nätdejting och sexuellt våld. Falduti och Tessaris (2023) konstaterar att avsaknaden av enhetlig terminologi inom deras fokusområde, "hämndporr" och icke-samtyckesbaserat pornografiskt material (NCP), hindrar arbetet med att förstå och motverka företeelsen. Quilty och Flynn (2025) pekar samtidigt på att bristande kunskap om TFV bland poliser och utredare kan leda till att brotten missförstås och att brottsoffren inte tas på allvar. Digitala metoder för att

² Estellés, M., & Doyle, A. (2025), Falduti, M., & Tessaris, S. (2023), Filice, E., Abeywickrama, K. D., Parry, D. C., & Johnson, C. W. (2022), Gewirtz-Meydan, A., Volman-Pampanel, D., Opuda, E., & Tarshish, N. (2024), Porta, C. M., Frerich, E. A., Hoffman, S., Bauer, S., Jain, V. M., & Bradley, C. (2024), Quilty, E., & Flynn, A. (2025)

upptäcka kränkande bildmaterial har dessutom tydliga begränsningar. Nakenhet i sig är inte kränkande och det saknas konsensus om igenkännbara mönster för NCP, vilket försvårar automatiserad upptäckt (Falduti och Tessaris, 2023). Metoder för att upptäcka deepfakes riskerar också att snabbt bli inaktuella i takt med den snabba tekniska utvecklingen. Samtidigt är manuell granskning av sexuellt kränkande innehåll både tidskrävande och medför psykiska hälsorisker för dem som utför arbetet. (Falduti och Tessaris, 2023).

Etiska utmaningar

Falduti och Tessaris (2023) påpekar att det finns olösta etiska problem i spänningsfältet mellan censur, innehållsmoderering och yttrandefrihet. Teknik som installeras i mobiltelefoner för att upptäcka pornografiskt innehåll väcker exempelvis frågor om datakontroll och rätten till privatliv, i synnerhet när det handlar om barns mobiltelefoner (Falduti och Tessaris, 2023). I forskningen är risken att utsätta barn och unga som har varit utsatta för övergrepp för ytterligare trauman en verklig risk som måste beaktas. Kvalitativa studier, intervjuer och annan forskning som involverar människor kan öka risken för sekundär viktigmisering av offer. Dessa etiska utmaningar tycks vara utbredda men saknar i stor utsträckning etablerade lösningar.

Studiernas ansatser och resultat i korthet

Estellés och Doyle (2025) genomför en systematisk granskning av 75 artiklar om hur *online security education* (OSE) utformas och tillämpas för att skydda barn och vuxna mot ett spektrum av hot och risker; från cybermobbing och sexuella övergrepp till vidmakthållandet av orättvisa maktordningar. De identifierar fyra olika ansatser för OSE.

- *Safeguarding* ("skyddande") är en strategi som fokuserar på att skydda unga från risker online genom kontroll, begränsningar och övervakning. Inom denna ansats betraktas teknik som farlig.
- *Equipping* ("utrustande") betonar vikten av att bygga upp digitala färdigheter, kunskaper och motståndskraft för att kunna navigera i digitala miljöer på ett säkert och produktivt sätt. Här betraktas teknik som ett neutralt verktyg.
- *Empowering* ("att ge makt") kopplar samman säkerhet i digitala miljöer med social rättvisa och syftar till att ta itu med ojämlikheter som reproduceras i digitala utrymmen. Denna ansats främjar kritiskt engagemang och uppmuntrar till att använda IKT för aktivism.
- *Resisting* ("att göra motstånd") ifrågasätter antagandet att digital teknik i sig främjar demokrati eller jämlikhet. Strategin uppmuntrar till kritiskt tänkande kring övervakning och maktordningar och uppmuntrar etiskt avståndstagande från exploaterande digitala system.

Författarna finner att strategier med fokus på *safeguarding* och *equipping* kanske har mest direkt bäring på TFV och övergrepp mot individer dominerar. De finner samtidigt att myndigheters och IT-företags ansvar för en säker onlinemiljö inte diskuteras i litteraturen, vilket bidrar till en individualisering av sociala risker och en okritisk syn på IKT. Författarna menar att den granskade litteraturen främst lägger ansvaret för OSE på lärare och pedagoger, samtidigt som stater, IT-företag och större organisationer i stort sett undantas från ansvar. De förklarar detta med en nästan total avsaknad av

samhällsvetenskapliga studier som kan sätta OSE i ett historiskt, politiskt, ekonomiskt och socialt sammanhang. Författarna förespråkar därför mer kritiska och politiskt informerade sätt för forskare, beslutsfattare och pedagoger att närma sig OSE. De framhåller också ett behov av kritiska granskningar av IKT och menar att framtida forskning kring OSE bör ifrågasätta de idag rådande ofta okritiska sätten att se på IKT.

Falduti och Tessaris (2023) presenterar en "systematic mapping study" (SMS) om forskning kring *non-consensual pornography* (NCP) ur ett tekniskt och kvantitativt perspektiv. Denna ansats är viktig, menar de, eftersom tidigare litteraturöversikter om NCP oftast har fokuserat på samhällsvetenskapliga eller psykologiska perspektiv. Studien identifierar 53 artiklar som fokuserar på NCP ur ett tekniskt perspektiv. Dataanalys var det mest förekommande innehållet (47 procent av arbetena), följt av verktyg för att upptäcka kränkande innehåll (28 procent). Studier kring nya applikationer och teknikutveckling utgjorde 15 procent av artiklarna och forensiska metoder utgjorde 9 procent. Verktyg för att upptäcka kränkande innehåll fokuserar på upptäckt av deepfake och pornografiskt innehåll med hjälp av bland annat avancerad djupinlärning och biometrisk kriminalteknik. Detta genom att identifiera manipulerade medier och tekniskt skapat material genom de digitala spår som uppstår när innehåll har skapats eller förändrats med hjälp av artificiell intelligens eller annan digital teknik. Studier kring nya applikationer och teknikutveckling inbegriper bland annat "blockkedjeverifiering", "smarta kontrakt" och "video hashing" (en process genom vilken man skapar ett digitalt fingeravtryck eller en så kallad hashkod) för att autentisera innehåll och spåra dess ursprung. Forensiska metoder och digital kriminalteknik utnyttjar bland annat "bildåtervinning" för att spåra ursprunget och spridningen av kränkande material.

Författarna hävdar att det saknas robusta strategier för att förebygga kränkande beteende och för att skilja mellan legitimt och kränkande sexuellt innehåll, men att litteraturen om NCP nu är tillräckligt omfattande och mogen för att kunna ligga till grund för nya riktlinjer på både nationell och internationell nivå. De konstaterar att avsaknaden av strategier för att sälla kränkande från icke-kränkande material gör det svårt att moderera innehåll effektivt på plattformar för vuxna där nakenhet är tillåten. De noterar också ett behov av att formalisera begreppet samtycke och identifierar dessutom ett behov av forskning om stöd till brottsoffer för NCP genom kunskapsbaserade och datadrivna AI- eller hybridverktyg. Enligt Falduti och Tessaris krävs dessutom analys av bland annat minoriteter och kränkande interaktioner i metaversum för att bättre förstå hur bildbaserat sexuellt utnyttjande förändras.

Filice m.fl. (2022) genomförde en översiktsstudie i syfte att undersöka sexuellt våld och sexuella övergrepp inom nätdejting. Studiens underlag består av 55 forsknings-artiklar som används för att identifiera problemets förekomst och förutsättningar, hur tekniken kan underlätta eller motverka problemet samt för att identifiera kunskaps- och forskningsluckor. Studien pekar på att sexuella trakasserier och övergrepp inom nätdejting är utbredda och uppvisar vissa mönster. I en studie rapporterade 11,1 procent av nästan 3 000 australiska vuxna att de utsatts för ett oönskat sexuellt närmande av någon de först träffat online, varav 10,1 procent specifikt angav att det initiala mötet ägt rum via dejtingappar. En kanadensisk studie fann att 11,4 procent av männen och 25,3 procent av kvinnorna upplevt oönskade sexuella möten via dejtingsajter eller -appar.

Bland vuxna australier uppgav 22,5 procent av de som använt *geosociala nätverksappar* (GSNA) att de utsatts för olämpliga eller trakasserande meddelanden, fysiskt våld, oönskad sexuell uppmärksamhet och/eller sexuellt våld. Andelen var ännu högre bland personer som använde andra former av dejtingplattformar online. Av dessa rapporterade 33,5 procent att de utsatts för samma typ av övergrepp.

En återblickande granskning gällande sexuella övergrepp i Australien visade att 14,5 procent av fallen involverade en initial kontakt via en dejtingsajt eller -app. 44 procent av australiska användare av dejtingappar och 35 procent av amerikanska användare uppgav att de hade utsatts för trakasserier. 9 procent av de amerikanska användarna hade även hotats med fysiskt våld. I USA uttryckte 71,4 procent av kvinnliga studenter och 83,3 procent av män som har sex med män (men who have sex with men, MSM) oro över säkerheten när de träffade partners online. Detta pekar på en medvetenhet om risker, men även en utbredd rädsla i digitala dejtingmiljöer för dessa grupper. I översiktsstudien framträdde bildbaserat sexuellt utnyttjande som ett betydande problem. I en undersökning rapporterade 53,3 procent av kvinnor samt homo- och bisexuella män att de hade fått bilder av manliga könsorgan skickade till sig, varav 90 procent av dessa bilder var oönskade. Bland MSM-användare av geosociala nätverksappar rapporterade 14,5 procent att deras egna sexuellt explicita bilder hade spridits eller offentliggjorts utan deras samtycke. Denna siffra är dubbelt så hög som bland HBTQ-användare i allmänhet.

Författarna påpekar att det till stor del är okänt hur sexuellt våld och sexuella övergrepp i samband med nätdejting påverkar offren och hur dessa hanterar konsekvenserna. Nuvarande antaganden om att effekterna liknar andra former av sexuellt TFFV behöver enligt författarna bekräftas genom empiriska studier. Vidare finns en påtaglig brist på forskning om erfarenheter av sexuella övergrepp bland sexuella minoriteter, trots att dessa grupper är en högriskkategori i detta sammanhang. Detta gäller inte minst transpersoner. I en kvalitativ studie uppgav 8 av 14 transpersoner att de kände sig otrygga eller hade utsatts för våld eller trakasserier när de använde dejtingappar. Författarna lyfter dessutom att våldsutövarnas motiv och drivkrafter är kraftigt understuderade och pekar bland annat på behovet av forskning om den roll som "avindividualisering" kan spela i förhållandet mellan anonymitet, "teknokulturella miljöer" och sexuellt våld online. Det innebär att den anonymitet som digitala plattformar erbjuder, i kombination med de normer och förväntningar som främjas inom nätdejtingkulturer kan leda till ett minskat fokus på individen, både i fråga om det egna ansvaret och den andres känslor och värde. Detta uppges i sin tur kunna minska hämningar och öka sannolikheten för att individer begår sexuellt våld online. Detta gör det, enligt författarna, till ett viktigt område för framtida tvärvetenskaplig forskning.

I fråga om praktiska åtgärder uppmanar Filice med kollegor dejtingplattformar att implementera tekniska lösningar för att motverka sexuellt våld. Exempelvis förbättrade autentiseringsprotokoll³, funktioner för blockering och rapportering, samt "paniklarm" som kan användas då fara uppstår. De föreslår även att enskilda användare bör utveckla aktiva strategier för att minska riskerna för att utsättas.

³ De regler och steg som används för att verifiera en användares identitet innan åtkomst beviljas.

Gewirtz-Meydan m.fl. (2024) genomförde en översiktsstudie i syfte att undersöka befintlig kunskap om sexuella trakasserier via dejtingappar för smartphones. Studien inkluderade analyser av övergreppens karaktär, frekvens, riskfaktorer och sociala/kulturella aspekter. Översikten omfattade tolv kvantitativa och kvalitativa studier med varierande studiepopulationer. Studien visade att sexuella trakasserier på dejtingappar är utbredda, komplexa och uppvisar ett starkt samband med negativa effekter på brottsoffrens psykiska hälsa. Studiens underlag visar att mellan 57 och 89 procent av användare har utsatts för sexuella trakasserier minst en gång, inklusive bildbaserade övergrepp, oönskade sexuella meddelanden, eller muntliga trakasserier, eller förolämpningar baserade på kön eller sexualitet. Cirka en av tre användare uppger att de har fått oönskade sexuella bilder, ofta innan de har tagit kontakt med våldsutövaren. Trakasserierna kan fortsätta offline. Enligt en australisk studie som granskade 76 anmälningar om fysiska sexuella övergrepp (som även refererades av Filice med kollegor) ägde 14,5 procent av dessa rum efter ett möte som arrangerats via en dejtingapp. Underlaget visar även på möjliga geografiska och kulturella variationer, då amerikanska användare av dejtingappar, särskilt studenter, rapporterar högre förekomst av trakasserier än kinesiska användare.

Granskningen visar att två grupper är särskilt utsatta: kvinnor under 30 år och sexuella minoriteter. Båda utsätts i oproportionerligt hög grad för trakasserier och sexuella övergrepp som har koppling till dejtingappar. En omfattande studie med 5 798 deltagare visade att en av tio australiska kvinnor och nästan 12 procent av kvinnor i Storbritannien någon gång hade utsatts för en oönskad sexuell kontakt av någon de först träffat online. Alla anmälningar om sexuella övergrepp i samband med möten till följd av kontakt via dejtingappar gjordes av kvinnor, varav de flesta var under 30 år. Personer som tillhör sexuella minoriteter utsätts också i oproportionerligt hög grad. I synnerhet är homo- och bisexuella oftare utsatta för "hämndpornografi" än både heterosexuella användare och andra medlemmar av HBTQ-gemenskapen. Inom dejtingappkulturen för män som har sex med män (MSM) råder en utbredd feluppfattning att alla MSM välkomnar oönskade sexuella bilder eller "*dick pics*". Att uttrycka obehag i dessa sammanhang är ofta socialt stigmatiserat, vilket avskräcker de utsatta från att anmäla eller konfrontera trakasserierna.

Studien visar att konsekvenserna för de utsattas psykiska hälsa inkluderar depression, ångest, post-traumatisk stress, ensamhet, låg självkänsla och minskad självkontroll. Individer som utsatts för fysiskt våld som barn var mer benägna att uppleva sexuella trakasserier eller utsatthet, vilket tyder på att redan existerande sårbarheter ökar risken för utsatthet. Enligt författarna bör framtida forskning sträva efter att mer noggrant mäta förekomsten, typerna av, och riskfaktorerna för trakasserier, inklusive dess omgivande sociala och kulturella strukturer. Särskild uppmärksamhet bör ägnas åt kvinnor under 30 år och sexuella minoriteter, åt de psykiska hälsoeffekterna av appanvändning, samt åt de processer som omgärdar samtycke på dejtingappar, då dessa enligt författarna är oklara och underutforskade. Utöver det är tvärkulturella studier nödvändiga, eftersom de nuvarande resultaten främst grundas på västerländska underlag.

Porta m.fl. (2024) har genomfört en översiktsstudie som inkluderar 47 studier i syfte att förstå forskningsläget rörande sexuell våld och trakasserier i samband med spel i *virtual reality* (VR), samt de potentiella användningsområdena för VR inom vård och vid

intervention. Av de 47 artiklarna var fem översiktsartiklar, 31 forskningsstudier som beskrev sexuellt våld och elva artiklar som testade VR vid genomförandet av interventionsstrategier. Enligt författarna rapporterar de flesta VR-användare positiva upplevelser, men under 2020 uppgav 81 procent att de hade utsatts för någon form av trakasserier. Nästan hälften av kvinnorna i sociala VR-miljöer rapporterade minst en incident av sexuella trakasserier. Detta inkluderade stalking och doxxing men även virtuella sexuella övergrepp eller tortyr utförda genom avatarer. Övergrepp genom avatarer kan utlösa fysiska reaktioner och trauman som kvarstår även efter att spelet avslutats. Såväl utsatta som vittnen till trakasserier i VR upplever en rad psykologiska konsekvenser, inklusive ångest, depression, posttraumatisk stress och självmordstankar, samt minskad självkänsla. Trakasserier i VR-miljöer kan alltså utgöra ett allvarligt hot mot individers psykiska och fysiska hälsa. Författarna menar att maskulinitetsnormer, social dominansorientering och långvarigt engagemang i fientliga spelmiljöer kan identifieras som viktiga riskfaktorer för sexuella övergrepp online. Sexistiska åsikter offline och exponering för sexualiserade kvinnliga karaktärer i spel ökar ytterligare sannolikheten för trakasserande beteenden.

Porta med kollegor understryker att kunskapen om förekomsten och effekterna av sexuellt våld i VR-miljöer är begränsad. I de fyra studier som specifikt undersökte förekomsten av sexuella övergrepp varierade de rapporterade nivåerna av sexuella trakasserier mellan 34,2 procent och 84,3 procent. Icke desto mindre framträdde en tydlig skillnad mellan könen. Även om män och kvinnor rapporterar liknande totala nivåer av trakasserier online utsätts kvinnor för betydligt allvarligare och mer sexualiserade övergrepp. Exempelvis utsätts kvinnor i oproportionerligt hög grad för sexuella trakasserier (16 procent mot 5 procent) och stalking (13 procent mot 9 procent) jämfört med män. Unga kvinnor är särskilt utsatta – en av tre kvinnor under 35 år har utsatts för sexuella trakasserier online, jämfört med ungefär en av tio män i samma ålder. Nästan hälften av kvinnorna i sociala VR-miljöer har utsatts för sexuella trakasserier och en studie fann att kvinnor utsätts för elva gånger fler sexuellt trakasserande kommentarer än män. Män utsätts i högre grad för rasism, homofobi eller våldsamma hot. Studien påvisar påtagliga mönster av övergrepp i VR-miljöer med kön som viktig faktor.

En nämnvärd studie bland de elva som undersökte VR-baserade interventioner för att förebygga och bemöta sexuellt våld använde en VR-simulering där åskådare kunde agera för att förhindra utsatthet.⁴ Detta tycktes förhöja deltagarnas känsla av ansvar och avsikt att ingripa. En annan simulering hjälpte kvinnor att öva på hur de kan reagera på och hantera trakasserier. Sex studier undersökte hur kroppslighet (*embodiment*) – det vill säga att uppleva en virtuell kropp som skiljer sig från den egna – i VR kan påverka empati och minska fördomar. När manliga deltagare förkroppsligades genom kvinnliga avatarer som utsattes för trakasserier rapporterade de större empati och medvetenhet om könsrelaterat våld. Tre studier undersökte VR-interventioner för traumabehandling, med fokus på personer som utsatts för sexuellt våld och posttraumatisk stress. Terapin tillämpades på både kvinnor och män och visade förbättringar av symtom på depression och posttraumatisk stress. Icke desto mindre påpekar Porta med kollegor att forskningen

⁴ Ernest N. Jouriles m.fl., "Measuring bystander behavior to prevent sexual violence: Moving beyond self reports", *Psychology of Violence* 6, nr 1 (2016): 73–81, <https://doi.org/10.1037/a0038230>.

kring VR inom interventionsstrategier och vård är begränsad och uppvisar blandade resultat. I vissa fall föreföll användandet av VR öka rädslan och minska kvinnliga deltagares förmåga att reagera och försvara sig. I andra fall fanns ett observerbart positivt samband mellan åskådares beteenden och förbättrade symptom på posttraumatisk stress. Sammantaget pekar dessa studier på att VR kan vara effektivt som utbildningsverktyg och som stöd vid psykologisk behandling.

Quilty och Flynn (2025) genomförde en översiktsstudie som identifierade 57 relevanta studier om *technology facilitated violence* (TFV) i Indo-Stillahavsområdet, inklusive Australien och Nya Zeeland. Dessa studier användes för att undersöka regionala trender i TFV, dess konsekvenser, våldsutövarers taktik, samt motåtgärder. Studien konstaterar att de skadliga effekterna av TFV i stort sett kan delas in i tre breda kategorier: emotionella/psykologiska, sociala och ekonomiska. Övergreppens beständighet genom att material finns kvar online förstärker de skadliga effekterna. Författarna hävdar att TFV är ett betydande globalt problem kopplat till juridik, folkhälsa, sociala relationer och mänskliga rättigheter. I Indo-Stillahavsregionen är de mest diskuterade beteendena av TFV: trakasserier, bildbaserade sexuella övergrepp, identitetsstöld, doxxing, förtal och övervakning/kontroll genom IKT. Quilty och Flynn menar att TFV förekommer och utövas i högre grad bland unga än bland äldre, samt att kvinnor utsätts för könsbaserade och sexuella trakasserier online i oproportionerligt högre utsträckning än män. Författarna menar att den brist på mångfald i empiriska data som observerats i andra studier (Falduti och Tessaris, 2023; Decoster, 2024) också var märkbar i studier som fokuserade på Indo-Stillahavsområdet inklusive Australien och Nya Zeeland. Särskilt i fråga om representation av ursprungsbefolkningar, HBTQ+ personer, personer med funktionsnedsättning, samt individer och förhållanden i geografiska områden andra än just Australien och Nya Zeeland. Quilty och Flynn konstaterar att detta hindrar en heltäckande förståelse av beteenden, erfarenheter och trender inom dessa områden. De noterar också en brist på intersektionalitet i befintliga data, vilket förhindrar forskning kring mönster i TFV och skillnader relaterade till kön, sexualitet, status som ursprungsbefolkning, etnisk/rasmässig bakgrund och funktionsnedsättning. Dessutom kan begränsade studier publicerade på engelska utesluta relevant forskning på andra språk, vilket leder till en västdominerad förståelse gällande upplevelser av TFV.

Liksom flera andra studier ser Quilty och Flynn ett behov av mer standardiserad terminologi och definitioner av TFV för att förbättra mätvärden och driva policyutveckling. För att åtgärda dessa brister efterlyser de evidensbaserad och granskad (peer-reviewed) empirisk forskning som fångar upp perspektiven från olika demografiska grupper. De uppmanar också forskare att undersöka nya och framväxande former av TFV såsom övergrepp genom sexualiserade deepfakes för att kunna ta fram strategier för att förebygga, stödja och respondera. De ser också ett behov av tydliga definitioner och standardiserad terminologi för TFV i syfte att bättre kunna mäta prevalens och konsekvens.

FOKUS PÅ DOKUMENTERADE SEXUELLA ÖVERGREPP OCH EXPLOATERING AV BARN ONLINE

Fem studier har primärt fokus på *online child sexual abuse and exploitation* (OCSAE) och *child sexual abuse material* (CSAM).⁵ Bland dessa framträder ett antal genomgripande och systemiska utmaningar. Dessa rör problemets omfattning, definitionssvårigheter, de individuella och sociala konsekvenserna samt tillgången på empiriska data.

Återkommande utmaningar

Problemets omfattning och spridning

Sexuella övergrepp mot barn online är en snabbt tilltagande företeelse, vilket gör det svårt för enskilda stater att hantera problemet (Ali m.fl., 2021). Ringenberg m.fl. (2021) konstaterar att även om grooming och sexuella övergrepp mot barn existerade redan före internet har IKT i hög grad ökat antalet strategier som våldsutövare har tillgång till. När det gäller onlinespel väcker deras ökande popularitet oro för barns säkerhet och skydd, eftersom de ger sig in i en miljö där de kan utsättas för cybermobbing och olika integritetskränkningar (Faraz m.fl., 2022). Traditionella polismetoder och områdesavgränsade rättsliga befogenheter kompliceras av den globala, diffusa och immateriella cyberrymden (Bleakley m.fl., 2024).

Definitioner och regler

Avsaknaden av enhetliga rättsliga definitioner utgör en utmaning i fråga om upptäckt, utredningar och åtal. Definitionerna av *child sexual abuse material* (CSAM) varierar beroende på rättsliga befogenheter och aktörer, vilket leder till olika tolkningar (Bleakley m.fl., 2024). På samma sätt innebär avsaknaden av en allmänt accepterad definition av *technology assisted child sexual abuse* (TA-CSA) och dess olika typer ett hinder för forskning (Chauvire Geib och Fevert, 2024). Avsaknaden av samstämmig lagstiftning mellan länder kan skapa juridiska kryphål och försvåra både gränsöverskridande samarbete som internationell forskning. Enligt Bleakley med kollegor innebär den antiregleringsanda som ofta är inbyggd i sociala medieplattformars affärsmodeller en betydande utmaning i fråga om att effektivt hantera sexuella övergrepp mot barn online och säkerställa deras säkerhet i digitala miljöer (Bleakley m.fl., 2024).

⁵ Ali, S., Haykal, H. A., & Youssef, E. Y. M. (2023), Bleakley, P., Martellozzo Elena, Spence, R., & DeMarco, J. (2024), Chauviré-Geib, K., & Fegert, J. M. (2024), Faraz, A., Mounsef, J., Raza, A., & Willis, S. (2022), Ringenberg, T. R., Seigfried-Spellar, K. C., Rayz, J. M., & Rogers, M. K. (2022)

Traumats allvar och systemiska påverkan

Den skada som *online child sexual abuse and exploitation* (OCSAE) orsakar kräver forskningens uppmärksamhet. Spridningen av sexuella övergrepp mot barn, även efter att våldsutövarna har gripits, orsakar allvarliga och bestående trauman hos offren (Chauvire Geib och Fevert, 2024; Ali m.fl., 2021). Brottsoffrens osäkerhet, rädsla för hämnd, skuld känslor, skam, och socialt tryck kan leda till att sexuella övergrepp inte anmäls och att det finns ett betydande mörkertal (Ali m.fl., 2021).

Utmaningar med datainsamling

Forskning om OCSAE som involverar minderåriga personer i studier kan vara utmanande på grund av deras utvecklingsstadium, deras förmåga att minnas och förstå frågor vilket påverkar datans tillförlitlighet (Chauvire Geib och Fevert, 2024). Utsatta kan ha svårt att minnas, särskilt när det gäller emotionellt påfrestande upplevelser, vilket påverkar datans validitet (Chauvire Geib och Fevert, 2024). Även när dessa utmaningar inte finns är det ofta svårt att rekrytera ett tillräckligt antal minderåriga deltagare till studier på grund av känsligheten och de rättsliga kraven (Chauvire Geib och Fevert, 2024). Följaktligen begränsar de små studiepopulationerna generaliserbarheten av forskningens resultat, oavsett om liknande resultat kan observeras i olika studier (Chauvire Geib och Fevert, 2024). Dessutom pekar Chauvire Geib och Fevert på bristen av mångfald i studierna, särskilt när det gäller etniska minoriteter och manliga offer. Författarna menar att detta begränsar förståelsen av kulturella och etniska skillnader. Enligt författarna gör begränsad forskning och skillnader i terminologi, studiedesign och kriterier för inkludering av populationer det svårt att dra allmänna slutsatser inom detta område när man undersöker *livestreamed child sexual abuse* (LSCSA).

Studiernas ansatser och resultat i korthet

Ali m.fl. (2021) genomförde en systematisk översikt som undersökte onlineplattformars roll i att underlätta sexuella övergrepp mot barn, i syfte att ge praktiska rekommendationer för att motverka sexuellt utnyttjande av barn på nätet, särskilt i låg- och medelinkomstländer. Översiktens urval bestod av 42 artiklar publicerade mellan 2000 och 2020, varav majoriteten (54,7 procent) publicerades mellan 2016 och 2020. Författarna diskuterar ingående hur onlineplattformar och IKT i hög grad underlättar sexuella övergrepp mot barn genom att ge våldsutövare tillgång till utsatta barn, och att OCSAE ofta involverar sexuellt övergreppsmaterial på barn för både kommersiella och icke-kommersiella syften. Författarna konstaterar även att våldsutövare använder olika strategier, såsom lockande erbjudanden och utpressning i syfte att begå övergrepp. Detta diskuteras mer ingående av Ringenberg m.fl. (2021).

Enligt Ali med kollegor underlättar onlinekommunikation avsevärt våldsutövares tillgång till utsatta barn och bidrar till ökningen av sexuella övergrepp mot barn. Barn är frekventa användare av onlineplattformar och sociala medier och många har offentliga profiler. Detta ökar deras sårbarhet och gör det möjligt för våldsutövare att få tillgång till deras personuppgifter, såsom bilder och intressen, vilket i sin tur gör det lättare att grooma dem. Den anonymitet som plattformarna erbjuder gör det samtidigt möjligt för våldsutövarna att förbli i stort sett spårlösa.

Grooming online är ett komplext manipulativt beteende som underlättas av internet. Våldsutövarna använder exempelvis smicker och kamratskap för att locka emotionellt

mottagliga barn och utvecklar ofta relationer som initialt baseras på offrets förtroende för våldsutövaren. Vissa våldsutövare använder sig inte av långvarig grooming utan förgriper sig direkt på barn via onlineplattformar genom att dela pornografi, bedriva sexuella chattar med mera. Onlineplattformar är ett primärt medium för spridning av sexuellt övergreppsmaterial på barn eftersom de erbjuder ett bekvämt och billigt sätt för våldsutövare att få tillgång till, dela och distribuera innehåll i olika format, inklusive video, foto och livestreaming.

Författarna talar om hur ”sexuella övergreppssessioner” (*”sexual abuse sessions”*) genomförs via onlineplattformar. Sessionerna är planlagda interaktioner online som våldsutövarna arrangerar och där barn utsätts. De är ofta svåra för brottsbekämpande myndigheter att identifiera, i synnerhet när de genomförs i icke-kommersiellt syfte. Våldsutövarna använder sig av personliga, snarare än enhetliga strategier och metoder för att nå, manipulera och förgripa sig på sina offer, och dessutom för att utpressa dem över tid.

Ali med kollegor identifierar en tydlig kunskapslucka i litteraturen om sexuella övergrepp mot barn, särskilt kring företeelser som grooming och sextortion. Trots en omfattande litteratur menar författarna att de övergripande mönstren, processerna och taktikerna för sexuella hot mot barn online fortfarande inte är fullt kartlagda. De framhåller därför behovet av fler empiriska studier i låg- och medelinkomstländer, särskilt där sexuella övergrepp online och spridningen av övergreppsmaterial är vanligt förekommande på grund av svaga socioekonomiska förutsättningar. Författarna betonar att brottsbekämpande myndigheter måste utveckla en djupare förståelse för komplexiteten och de olika stadierna i grooming online, såsom kontaktskapandet, genomförandet och döljandet. Bland annat genom riktade utbildningsinsatser och policybriefingar. Slutligen understryker de vikten av att föräldrar får kunskap om barns sårbarhet och riskfaktorer, att de diskuterar potentiella sexuella övergrepp online samt att de vidtar förebyggande åtgärder tillsammans med sina barn.

Bleakley m.fl. (2024) genomförde en studie som identifierade och utvärderade centrala debatter kring innehållsmoderering, med särskilt fokus på onlineövervakning av *child sexual abuse material* (CSAM), genom en empiriskt grundad policy- och litteraturöversikt. Resultaten visar att traditionella övervakningsmetoder försvåras av att internet saknar geografiska gränser. Det gör det komplicerat att tillämpa nationella, platsbaserade rättsliga befogenheter på brottslighet som rör sexuella övergrepp mot barn online. Samtidigt framkommer att teknikföretag i hög grad föredrar självreglering framför statlig reglering. I praktiken innebär detta att sociala medieplattformar som Facebook, Twitter och TikTok utgör den första försvarslinjen mot skadligt innehåll som CSAM. Företagens innehållsmoderatorer får därmed en central roll i det tidiga arbetet mot sådant material. Deras insatser begränsas dock ofta av den enorma mängd skadligt material som måste hanteras.

I sin analys av innehållsmoderering ser Bleakley med kollegor anledning att ifrågasätta den långsiktiga hållbarheten i detta kollektiva eller delade ansvar för onlineövervakning mellan stater och privata företag. Författarna framhåller även att det är oklart om överföringen av ansvar för onlineövervakning till sociala medieplattformar är den mest effektiva regleringsmodellen, eller hur och om processerna kan behöva omformas för att öka effektiviteten. Båda dessa frågor kräver vidare forskning. Därtill konstateras att innehållsmoderatorernas förmåga att hantera de sociala, emotionella och

psykologiska påfrestningarna i sitt arbete är ett område som kräver ytterligare studier och större branschövergripande insatser. När det gäller praktiska konsekvenser belyser studien de betydande svårigheterna med att tillämpa traditionella övervakningsmetoder på CSAM i en digital miljö, särskilt till följd av frågor om områdesavgränsade rättsliga befogenheter. Författarna framhåller dessutom att nuvarande praxis för innehållsmoderering som i hög grad bygger på privata aktörers ansvar väcker farhågor om att staten successivt avsäger sig sin normativa och tillsynande auktoritet.

Chauvire Geib och Fevert (2024) presenterar en översiktsstudie som analyserar hur utsatta för olika former av *technology assisted child sexual abuse* (TA-CSA) framställs i befintlig forskning, samt de emotionella, psykologiska, medicinska, fysiska och sociala konsekvenserna för dessa brottsoffer. Studien visar att forskning med direkt deltagande av brottsoffer för TA-CSA fortfarande är ovanlig, trots den snabba ökningen av sådana brott. Studien visar att brottsoffren utsätts för en rad olika typer av övergrepp och att de emotionella, psykologiska, medicinska och fysiska konsekvenserna är omfattande och genomgående negativa, samt påverkan på de utsattas sociala relationer och sammanhang. Författarna framhåller dock att deras resultat inte kan generaliseras, främst på grund av otydliga och varierande definitioner inom forskningsfältet. Författarna noterar också att studier som direkt involverar utsatta för *technology assisted child sexual abuse* (TA-CSA) är få, vilket kraftigt begränsar kunskapen om både skydds- och riskfaktorer samt om skillnader jämfört med icke-teknologiskt sexuellt utnyttjande av barn. De framhåller behovet av ytterligare forskning för att bättre förstå TA-CSA:s påverkan på brottsoffren i syfte att kunna utforma mer effektiva stöd- och interventionsinsatser. Denna framtida forskning bör vara mer inkluderande och mångsidig, med särskilt fokus på etniska minoriteter och manliga offer, för att åtgärda nuvarande begränsningar i generaliserbarhet och tillämplighet.

Chauvire Geib och Fevert betonar att det saknas en allmänt accepterad definition av TA-CSA och av vilka övergreppshandlingar som faller inom begreppet. Denna begreppsliga oklarhet utgör ett hinder för forskning och försvårar en effektiv resursfördelning. Författarna efterlyser därför en universellt giltig definition och en tydlig åtskillnad mellan olika typer av TA-CSA för att möjliggöra mer samordnade och träffsäkra insatser. De konstaterar vidare att kunskapen om vilka övergreppshandlingar som utgör TA-CSA, liksom om deras orsaker och konsekvenser för brottsoffren, fortfarande är begränsad. Studien framhåller även behovet av ökad medvetenhet bland yrkesverksamma om de olika formerna av TA-CSA, i syfte att underlätta upptäckt och möjliggöra relevanta insatser. Författarna drar slutsatsen att kunskap och insikter som inhämtas direkt från brottsoffren är avgörande för att kunna utveckla effektiva förebyggande och terapeutiska metoder. De betonar även att beslutsfattare bör beakta de utsattas perspektiv och erfarenheter vid utformningen av ny lagstiftning samt vid revidering av befintlig lagstiftning som rör TA-CSA.

Faraz m.fl. (2022) genomförde en omfattande studie av miljön och sammanhanget kring onlinespel, med fokus på risker, skyddsmekanismer och framtida riktlinjer för barns säkerhet. Studien, vars underlag utgjordes av 29 forskningsartiklar publicerade mellan 2017 och 2021, konstaterar att onlinespel innebär både möjligheter och risker för barn. En balanserad strategi krävs för att säkerställa trygghet och skydd. Författarna

identifierar centrala risker, samt beskriver befintliga tekniska och politiska lösningar för att mildra dessa och lägger fram rekommendationer. Bland riskerna för barn i spelmiljöer online återfinns bland annat att de kan exponeras för sexuellt explicit, våldsamt eller på annat sätt olämpligt innehåll. Dessutom möjliggör dessa miljöer ofta cybermobbing, trakasserier och *grooming*. Ytterligare risker inbegriper integritetskränkningar, spelberoende och ekonomisk exploatering genom exempelvis bedrägerier.

Nuvarande säkerhetsåtgärder innefattar olika verktyg som ger vårdnadshavare möjlighet att övervaka eller kontrollera barnets aktivitet online. Även åldersverifieringssystem och rapporteringsmekanismer är inbyggda i spel i syfte att övervaka beteenden och begränsa skadligt innehåll. För att stärka barns säkerhet online, menar författarna, bör åldersverifiering effektiviseras, innehållsmoderering förbättras och föräldrakontroll utökas genom utbildning och vassare kontrollverktyg. De uppmanar även till sektorsövergripande samarbeten mellan den privata sektorn, brottsbekämpande myndigheter och barnrättsaktörer. De pekar även på vikten av att beakta etiska aspekter i teknikutvecklingen. Utöver det pekar författarna på en forskningslucka gällande de långsiktiga effekterna av spel på barns utveckling, särskilt en mer nyanserad förståelse av de olika psykologiska och sociala konsekvenserna av olika spelgenrer och funktioner. De noterar en avsaknad av tvärvetenskapligt samarbete inom området, vilket enligt dem försvårar utvecklingen av sammanhållna skyddsstrategier.

Ringenberg m.fl. (2021) genomförde en studie med syfte att kartlägga groomingstrategier, identifiera likheter och skillnader mellan olika tidsperioder samt analysera hur förändrade datamängder och tekniker påverkar groomingprocessen. Studien grundas på ett urval av 93 artiklar på engelska publicerade mellan 1970 och 2020, varav 32 publicerades före internets ankomst och 61 efter.

Författarna visar att grooming före internet var en långsam och överlagd process som ofta pågick i månader eller år och byggde på upprepade personliga kontakter. Våldsutövarna attraherade de utsatta genom att erbjuda gåvor, tillgivenhet eller olika förmåner, i syfte att vinna deras förtroende. Detta kombinerades med tvång, känslomässig manipulation eller rena hot för att säkerställa lydnad. De isolerade dessutom de utsatta från sociala nätverk och använde ibland alkohol för att minska hämningarna under övergreppen. Processen innebar en gradvis sexualisering av "relationen" och strikt hemlighållande, vilket uppnåddes genom att manipulera fram skuld känslor eller rädsla. Detta för att säkerställa den utsattes tystnad och en fortsatt sårbarhet som kunde utnyttjas.

Internet har, enligt författarna, gjort grooming till en snabbare, mer anpassningsbar och ofta ännu mer manipulativ process som kan genomföras på några timmar snarare än månader. Våldsutövarna börjar vanligtvis med att etablera en "speciell relation" genom att ge komplimanger, visa empati och stöd eller andra beteenden som utformas för att skapa ett känslomässigt beroende. På ett tidigt stadium i interaktionen genomför våldsutövaren riskbedömningar för att säkerställa att polis eller vårdnadshavare inte har insyn, samtidigt som de undersöker den utsattes personliga miljö och omständigheter. Därefter arbetar de för att skapa förtroende, exempelvis genom att lyfta fram gemensamma intressen eller ge sken av personlig öppenhet, för att få "relationen" att framstå som intim och äkta. När förtroendet väl är säkrat sexualiserar kommunikationen successivt för därefter resultera i sexuella övergrepp.

Författarna beskriver hur de utsatta kan uppmuntras att hålla tyst och isolera sig från sin omgivning, samtidigt som våldsutövaren förbereder ytterligare övergrepp online eller genom faktiska möten. Strategierna för grooming har följt med den tekniska utvecklingen och övergått från kontakter via offentliga plattformar till stängda kanaler, direktmeddelanden, samt användandet av mobiltelefoner eller webbkameror. Detta för att utöka kontrollen och undvika upptäckt. Författarna menar vidare att våldsutövare ofta fabricerar information om sig själva, såsom ålder, kön, utseende, status och auktoritet med hjälp av falska profiler eller stulna bilder.

Ringenberg med kollegor visar att många centrala strategier för grooming förblev oförändrade vid internets ankomst, men att IKT på ett dramatiskt sätt har ökat på takten, omfattningen och antalet verktyg för grooming. De identifierar även ett flertal forsknings- och kunskapsluckor. Deras studie undersökte exempelvis inte om groomingstrategier förändras i relation till den utsattes ålder. Inte heller analyserades hur olika egenskaper hos våldsutövare och den utsatte samverkar i groomingprocessen. För att möjliggöra automatiserad upptäckt av grooming krävs forskning som fastställer strategiernas tidsmässiga mönster, exempelvis hur mycket tid som passerar innan våldsutövarna genomför sina riskbedömningar, eller hur snabbt de väljer att sexualisera kommunikationen. Författarna framhåller även behovet av forskning om substansmissbrukets fortsatta roll. Droger har varit en central komponent i grooming offline och var även en faktor i vissa groomingprocesser online. Slutligen kvarstår frågan om hur juridiska och kulturella skillnader mellan länder påverkar definitioner och forskning om grooming, då urvalen varierade betydligt i geografiskt ursprung.

Författarna konstaterar att internet och ny teknik har gjort både online- och offlinegrooming mer komplex. Även de våldsutövare som agerar offline använder numera mobiltelefoner och appar. En praktisk innebörd av studien är behovet av ökad vaksamhet hos brottsbekämpande myndigheter. Eftersom grooming som inleds online snabbt kan sexualiseras och resultera i övergrepp krävs även snabbare ingripanden vid misstänkta fall. Detta skapar nya möjligheter för våldsutövare, men även nya möjligheter för brottsbekämpande myndigheter att samla in bevis från digitala kommunikationer.

FOKUS PÅ ARTIFICIELL INTELLIGENS, SAKERNAS INTERNET OCH METAVERSUM

Teknik genom vilken den fysiska och digitala verkligheten binds samman utgör fokus för nio artiklar i underlaget till denna översikt.⁶ Med detta avses artiklar som undersöker våld och övergrepp inom ramarna för artificiell intelligens (AI), sakernas internet (*the internet of things*, IoT) och metaversum.

Återkommande utmaningar

Bland de nio artiklar som fokuserar på artificiell intelligens (AI), sakernas internet och metaversum framträder ett antal områden som övergripande utmaningar: den snabba tekniska utvecklingen, avvägningar mellan integritets- och säkerhetsfrågor, transnationell reglering och samarbete, samt hotet från deepfake-material.

Den snabba tekniska utvecklingen

Den snabba tekniska utvecklingen medför att nya metoder för att begå och dölja brott ständigt uppträder, vilket kräver att brottsbekämpande myndigheter löpande uppdaterar sina kunskaper, metoder och tekniska verktyg (Parti och Szabó, 2024). Sangwan och Bhatia (2022) konstaterar att ofullständighet (att inlägg eller meddelanden saknar väsentliga detaljer), otydlighet (ett informellt språkbruk där begrepp har flytande eller mångtydiga betydelser) och osäkerhet (opålitliga källor, känslomässiga uttryck och subjektiva återrapporteringar) gör det svårt att bearbeta användargenererade data med konventionella analysverktyg. Rättsväsenden är ofta oförmögna att möta nya utmaningar, såsom deepfakes, på grund av bristande kunskap och kompetens inom systemet (Sandoval m.fl., 2024). Brottsbekämpande myndigheter brottas även med brist på resurser, utbildning och teknisk expertis för att effektivt kunna utreda *child sexual abuse material* (CSAM) (Decoster, 2024). Arbetet med upptäckt ligger efter utvecklingen av deepfake-teknik, och det saknas fortfarande tydliga standarder och rättsliga riktlinjer för hur deepfake-bevis ska hanteras i domstol, vilket skapar betydande juridiska utmaningar (Sandoval m.fl., 2024). I fråga om CSAM har tekniska framsteg lett till en exponentiell ökning av material som vida överstiger kapaciteten för manuell granskning, vilket gör utvecklingen av nya IKT-baserade verktyg akut (Decoster, 2024).

Metaversum (*metaverse*) är ett förhållandevis nytt och delvis odefinierat begrepp. Det avser ett virtuellt universum som är uppslukande, kollektivt och interaktivt, och där tjänster, plattformar och applikationer är tillgängliga via en virtuell upplevelse,

⁶ Birrer, A., & Just, N. (2024), Godulla, A., Hoffmann, C. P., & Seibert, D. M. A. (2021), Sandoval, M.-P., de Almeida Vau, M., Solaas, J., & Rodrigues, L. (2024), Parti, K., & Szabó, J. (2024), Decoster, N. (2024), Blythe, J. M., & Johnson, S. D. (2021), Döring, N., Le, T. D., Vowels, L. M., Vowels, M. J., & Marcantonio, T. L. (2025), Gómez-Quintero, J., Johnson, S. D., Borrión, H., & Lundrigan, S. (2024), Sangwan, S. R., & Bhatia, M. P. S. (2022).

exempelvis ett *VR-headset* (virtual reality-headset). Begreppet är inte liktydigt med varumärket Metaverse, en specifik plattform som tillhandahålls av företaget Meta. Enligt Gómez-Quintero med kollegor (2024) råder fortfarande osäkerhet kring vilka typer av brott som kan uppstå i metaversum. De konstaterar dock att nya digitala produkter och tjänster ofta förbises ur ett brotts- och säkerhetsperspektiv vilket i sin tur leder till så kallad "crime harvesting", det vill säga att brottslingar utnyttjar nya tekniska möjligheter innan dessa regleras eller säkras. Enligt samma studie identifierades sexualbrott och hatbrott som de brottstyper som bedöms utgöra de största framtida riskerna inom metaversum och samtidigt vara svårast att hantera.

Avvägningen mellan integritet och säkerhet

Avvägningen mellan integritet och säkerhet utgör ytterligare en central utmaning. Användares krav på integritet står ofta i konflikt med behovet av säkerhet, och denna konflikt måste hanteras för att skapa en tryggare digital miljö (Gómez-Quintero m.fl., 2024). Problematiken förstärks ytterligare av generativ artificiell intelligens (AI) som idag kan skapa hyperrealistiska bilder och filmer (Parti och Szabó, 2024). Överblockering av innehåll är en av flera negativa konsekvenser av den teknik som används för att bekämpa *child sexual abuse material* (CSAM). Det riskerar även att leda till onödigt omfattande censur och obefogad övervakning av medborgarnas kommunikation (Decoster, 2024). På liknande sätt konstaterar Sangwan och Bhatia (2022) i sin litteraturgenomgång att innehållsmoderering på sociala medieplattformar ofta präglas av inkonsekvens, bristande transparens och partiskhet, vilket kan ha en negativ inverkan på yttrandefriheten. Författarna varnar också för att IoT-baserad övervakning, även om den är utformad för att öka säkerheten, kan missbrukas för övergrepp eller cyberstalking beroende på mängden av detaljerad information som samlas in. Sakernas internet (*the internet of things*, IoT) innefattar allt från smarta bärbara enheter till säkerhetskameror och system för fordonsspårning. Olika enheter samlar in data såsom plats, beteendemönster, ljud- och videoinspelningar, och uppgifter om hälsa och ekonomi. Sensorfunktioner kan göra det möjligt för obehöriga personer att fjärrövervaka privata utrymmen och den löpande datainsamlingen skapar möjlighet att spåra individer, övervaka deras vanor och utöva kontroll. Dessutom utsätter den ständiga uppkopplingen användare för säkerhetsrisker såsom hackning och identitetsstöld.

Konflikten mellan säkerhet och integritet har försvårat tillgången till data från internetleverantörer (Parti och Szabó, 2024). Många barn använder även avatarer eller pseudonymer, vilket gör dem särskilt sårbara för övergrepp eftersom skyddsmekanismerna är begränsade (Parti och Szabó, 2024). När verkliga identiteter och åldrar döljs blir det svårt för plattformarna att upprätthålla åldersanpassade skyddsåtgärder. Avsaknaden av robusta åldersverifieringssystem innebär att minderåriga lätt kan ta sig in i riskfyllda digitala miljöer avsedda för vuxna, samtidigt som våldsutövare kan utnyttja anonymiteten för sina syften. Dessa miljöer underlättar cyberstalking och olika former av sexuella övergrepp och trakasserier. Samma problem gäller även för vuxna användare och pekar på ett systemfel inom plattformarna. De digitala identiteterna försvårar dessutom identifiering av både våldsutövare och utsatta, samt insamling av bevis. Blythe och Johnson (2019) konstaterar att konsumenters användning av IoT-enheter går långsammare än förväntat på grund av utbredda farhågor om integritet och säkerhet. Många IoT-produkter uppfattas sakna tillräckliga starka

säkerhetsåtgärder, vilket gör enheterna till lätta mål för dataintrång, identitetsstöld och profilering.

Reglering och rättsliga befogenheter

Reglering och rättsliga befogenheter (jurisdiktion) utgör ett annat område med växande utmaningar. Enligt Blythe och Johnson (2019) utgör avsaknaden av stark reglering av konsumentinriktade IoT-enheter en faktor i att denna teknik breder ut sig långsammare än förväntat. Den gränsöverskridande karaktären hos cyberbrottslighet försvårar jurisdiktionsfrågor och komplicerar rättsligt samarbete mellan länder (Parti och Szabó, 2024; Birrer och Just, 2024). När det gäller *child sexual abuse material* (CSAM) hindrar bristen på enhetliga definitioner och skillnader i lagstiftning om datalagring ett ömsesidigt rättsligt samarbete och påverkar tillgången till bevis (Parti och Szabó, 2024; Decoster, 2024). Avsaknaden av harmoniserad lagstiftning mellan länder försvårar internationellt samarbete och gör rättsliga processer långsamma och ineffektiva.

I fråga om metaversum uppstår ytterligare utmaningar kopplade till dataskydd, äganderätt, beskattning och brottslighet, då det saknas tydliga juridiska ramar för virtuella miljöer (Gómez-Quintero m.fl., 2024). Forskningen kan inte idag dra klara slutsatser om hotets omfattning och allvar, vilket försvårar arbetet med att möta behoven av lagstiftning och reglering (Birrer och Just, 2024). Godulla m.fl. (2021) lyfter även hur skillnader i nationell lagstiftning komplicerar arbetet mot skadliga deepfakes. Sandoval m.fl. (2024) menar att nuvarande lagstiftning ofta inte täcker deepfake-relaterade brott såsom pornografi utan samtycke (NCP), vilket skapar luckor för både brottsoffer och åklagare. Parti och Szabó (2024) pekar dessutom på en brist i EU:s regelverk gällande realistiskt och AI-genererat övergreppsmaterial på barn. För att möta dessa utmaningar krävs samordnade internationella insatser och utvecklingen av omfattande men flexibla regelverk som kan anpassas till den snabbt föränderliga teknologiska verkligheten. Deepfake-desinformation framhålls som en särskilt allvarlig och samtidigt utbredd samhällsutmaning (Sandoval m.fl., 2024). Deepfakes som företeelse bidrar till att skapa ett klimat av osäkerhet och tvivel, vilket riskerar att underminera tilliten till myndigheter, institutioner, medmänniskor och informationsflöden i allmänhet (Birrer och Just, 2024). Bildmaterialets kvalitet förbättras ständigt med ökad förmåga att vilseleda. Godulla et al (2021) hänvisar till en studie som visade att allmänhetens felaktiga tolkning av bildmaterial, att de trodde att deepfakes var verkliga eller vice versa, var lägre än 30 procent. I en nyare studie av Birrer och Just (2024) identifierade deltagarna i genomsnitt 63,3 procent av deepfakes korrekt. Godulla m.fl. (2021) påpekar att deepfakes slår mot flera centrala samhällssektorer. De försvårar bland annat journalistiskt arbete genom att göra det svårare att verifiera källor, vilket på sikt kan underminera allmänhetens förtroende för medier. De hotar också samhällelig kommunikation i stort genom att underlätta desinformationskampanjer, sprida falsk information och konspirationsteorier samt snedvrider den demokratiska debatten (Godulla m.fl., 2021). Deepfakes förändrar även det kriminella landskapet genom att utvidga, intensifiera och diversifiera kriminella aktiviteter (Sandoval m.fl., 2024). De möjliggör nya former av cyberbrott och identitetsstöld samtidigt som de förvärrar befintliga brott, exempelvis olika former av bedrägeri och pornografi utan samtycke (*non-consensual pornography*, NCP). Detta har skapat en ny utsatthet som till överväldigande del drabbar kvinnor. Sandoval med kollegor lyfter bland annat en rapport från 2019 som visade att 96 procent av 14 600

deepfake-videor online utgjorde pornografi utan samtycke, med över 134 miljoner visningar på de populäraste deepfake-pornografisajterna. Över 90 procent av detta NCP-material avbildade kvinnor. Att människor har svårt att upptäcka deepfakes är därtill en central utmaning (Birrer och Just, 2024). Deepfakes är en utmaning för brottsbekämpande myndigheter genom att möjliggöra manipulation av bevis (Godulla m.fl., 2021). I fråga om deepfakes koppling till kriminalitet och våld orsakar deepfake-pornografi betydande och långvarig skada för enskilda, med emotionella, psykologiska, professionella och relationella konsekvenser (Birrer och Just, 2024).

Studiernas ansatser och resultat i korthet

Birrer och Just (2024) genomförde en systematisk studie om deepfakes och de regleringar som omgärdar tekniken i syfte att samla den befintlig kunskapen. Studiens slutliga underlag utgjordes av 79 artiklar. Författarna konstaterar att empirisk forskning om deepfakes fortfarande är knapp och att detta skapar betydande luckor i förståelsen av hur materialet skapas och sprids, samt deras effekter i samhället generellt. Utan denna grundläggande kunskap är det svårt att spåra utvecklingen av deepfake-tekniker eller att förstå hur de sprids. På liknande sätt är kunskapen om spridningsmekanismerna begränsad, som hur deepfakes delas och normaliseras via sociala medier och i olika nätverk. Detta begränsar i sin tur möjligheterna att identifiera insatsområden och vidta förebyggande åtgärder. Enligt författarna är även de individuella och samhälleliga konsekvenserna av deepfakes otillräckligt undersökta. De menar att det empiriska underlaget som krävs för att kvantifiera eller kontextualisera dessa skador fortfarande är begränsat och att problemets faktiska omfattning och natur därför är oklar. Samtidigt menar de att de möjliga positiva tillämpningarna av deepfake-teknik, exempelvis inom olika kreativa yrken och utbildning, är underutforskade och att detta skapar en obalanserad syn som främst fokuserar på risker. Denna brist på empiriska data gör det svårt att utvärdera kraven rörande reglering och etik som uppstår kring deepfakes. Birrer och Just framhåller att deepfake-tekniken inte skapar helt nya regleringsproblem, utan förstärker redan existerande utmaningar såsom NCP och desinformation. Omfattande tvärvetenskaplig forskning är därför nödvändig för att få en helhetsbild av deepfakes - från deras tillkomst till dess konsekvenser - för att möjliggöra relevanta och evidensbaserade åtgärder.

Sandoval m.fl. (2024) genomförde en översiktsstudie med ett underlag på 44 artiklar och rapporter, i syfte att sammanställa befintlig litteratur om deepfakes och dessas inverkan på rättsväsendet. Enligt författarna utgör deepfakes ett allvarligt hot mot rättsväsendet genom att urholka förtroendet för dessa institutioner och underlätta förfälskning av bevis. Deepfakes blotta existens leder individen, och tvingar jurister att ifrågasätta bevismaterial, inklusive bildbevis och ljudupptagningar. Det mest kritiska är förfälskning och manipulation av bevismaterial. Nuvarande praxis inom brottsbekämpande och rättsvårdande myndigheter är otillräckliga för att upptäcka och hantera sofistikerade deepfakes. Deepfakes reducerar bevisvärdet av bilder och ljudupptagningar, vilket tvingar polis och rättsväsende att ompröva verifierings- och autentiseringsprotokoll. Enligt författarna utgör deepfakes en utmaning, inte bara i enskilda fall utan även i fråga om institutioners och myndigheters legitimitet och integritet, vilket kräver omedelbara åtgärder för att värna allmänhetens förtroende.

Sandoval med kollegor konstaterar vidare att en betydande andel av deepfake-tekniken används för att skapa NCP. Utöver detta utgör deepfakes ett betydande hot mot personer utsatta för våld i nära relationer eftersom den ger våldsutövarna ytterligare verktyg för att utöva kontroll och hot, samt åsamka psykisk skada. Våldsutövare kan använda deepfake-teknik utan samtycke för att skapa kränkande innehåll såsom ”hämnpporr” och sexuellt övergreppsmaterial på barn, utöva sextortion och andra former av digitala övergrepp. Dessa handlingar ökar våldsutövares möjligheter att utöva tvång, känslomässig manipulering och våld, och kan leda till bestående trauma för offret, såväl som skadat anseende och andra fysiska konsekvenser. Enligt författarna varnar experter för att deepfakes automatiserade natur gör det möjligt att producera och reproducera så snabbt att materialet är nära nog omöjligt att begränsa när det väl har distribuerats. Underrapportering av övergrepp är fortfarande ett stort problem eftersom de utsatta ofta är rädda för förödmjukelse, hämnd eller exponering, samtidigt som våldsutövarnas anonymitet ofta komplicerar frågan om ansvar.

I grund och botten förstärker deepfake-tekniken befintliga maktordningar i hemmamiljöer och de våldsmönster som kan vara förknippade med dessa. Missbruk av tekniken undergräver offrens säkerhet, trygghet, integritet och förtroende för rättssystemet. Nuvarande rättsliga ramar misslyckas ofta med att hantera den tekniska och mänskliga problematiken på ett adekvat sätt vilket gör det möjligt för våldsutövare att agera relativt ostraffat och utnyttja avsaknaden av lagstiftning som tar sikte på deepfake-baserade övergrepp. Utöver detta uppmärksammar Sandoval med kollegor en geografisk obalans inom forskningen. I Kina ägnar sig 51 universitet åt forskning om deepfake-detektering, jämfört med 38 universitet i resten av världen. Detta antyder att utmaningen inte tas på lika stort allvar i alla regioner, vilket i sin tur kan leda till att vissa geografiska områden blir mer sårbara än andra.

Parti och Szabó (2024) genomförde en studie som syftade till att sammanställa befintlig kunskap om det rättsliga och regleringsmässiga läget för fysiskt och virtuellt sexuellt övergreppsmaterial på barn (*child sexual abuse material*, CSAM) i Europa, med särskilt fokus på *online child sexual abuse and exploitation* (OCSAE). Granskningen omfattade en tioårsperiod (2014–2024) som fångar upp relevanta EU-regelverk och strategier. Underlagets 71 källor inkluderade sakkunniggranskade artiklar och rapporter. Författarna ger en samlad översikt, värderar åtgärdernas effektivitet i relation till AI-genererad CSAM och ger policyrekommendationer för att åtgärda de brister som identifieras. De visar att nuvarande EU-ramverk fortfarande brister i hanteringen av realistisk och AI-genererad CSAM, särskilt där undantag tillåter medlemsstater att kriminalisera enbart material som visar verkliga barn men samtidigt lämnar AI-genererat innehåll oreglerat.

Parti och Szabó menar att AI-genererad CSAM måste kriminaliseras. Även när materialet inte bygger på dokumenterade fysiska övergrepp kan AI-genererat CSAM reproducera samma skadliga mekanismer som annat CSAM, exempelvis genom att återanvända eller efterlikna övergreppssituationer och därigenom bidra till återtraumatisering av barn. Dessutom avtrubbar materialet våldsutövare och normaliserar sexuella övergrepp, vilket kan leda till alltmer extrema fantasier och ytterligare urholka våldsutövarens moraliska och psykologiska hämningar. Denna normalisering kan också bidra till att våldsutövaren eskalerar från virtuella till fysiska

övergrepp. En annan faktor är att den stora mängden AI-genererat CSAM överväldigar brottsbekämpande myndigheter, försvårar utredningar och identifiering av fysiska offer. Det avleder därigenom resurser från ärenden som involverar faktiska fysiska offer. Därutöver ser forskare ett samband mellan konsumtion av CSAM och fysiska övergrepp, i synnerhet bland individer som redan är i riskzonen för att begå sexualbrott. Genom att förstärka skadliga fantasier och minska empati för offren kan AI-genererat CSAM fungera som en psykologisk inkörsport till fysiska övergrepp.

Den snabba tekniska utvecklingen innebär, enligt författarna, att AI-genererat CSAM oundvikligen kommer att översvämma internet, vilket kräver samordnade insatser från brottsbekämpande myndigheter, internetleverantörer och andra aktörer. Samtidigt framhåller de att direktiv 2011/93/EU saknar vägledning för hantering av realistiska avbildningar av barn eller av vuxna som porträtterar barn (till exempel genom virtuella alter egon eller avatarer), så väl som för frågan om sådant material bör kriminaliseras. Detta pekar på det fortsatta behovet av rättsliga ramar som kan hantera deepfake-teknikens komplexitet och dess konsekvenser för barns säkerhet och integritet. Samma författare menar att gällande rättsliga ramar inte heller hanterar ömsesidigt utbyte av självgenererat innehåll mellan minderåriga. Vilket, om det flaggas som CSAM via automatisk upptäckt, kan kränka barns integritet och leda till omotiverad kriminalisering.

Decoster (2024) analyserade 55 studier, forskningsartiklar såväl som ”grå litteratur,” med fokus på att granska automatiserade övervaknings- och rapporteringsprocesser. Det vill säga tekniska verktyg och system som kan användas för att upptäcka, klassificera, prioritera och rapportera sexuellt övergreppsmaterial på barn. Dessa processer har blivit nödvändiga på grund av den snabba ökningen av CSAM. Syftet med studien var att belysa de utmaningar och problem som olika intressenter står inför, till exempel teknikföretag och leverantörer av onlinetjänster (*online service providers*, OSP), moderatorer, civilsamhällesorganisationer, hjälplinjer, brottsbekämpande myndigheter, tillsynsmyndigheter och forskarvärlden.

Litteraturen betonar behovet av harmoniserade regler och riktlinjer för effektiv användning av tillgängliga tekniska lösningar och för att möjliggöra informationsdelning i arbetet mot CSAM. I fråga om motåtgärder är AI och tekniker som *hashing* nödvändiga för att bearbeta stora mängder material. *Hashing* innebär att man tilldelar tidigare upptäckta bilder ett unikt digitalt fingeravtryck som lagras i databaser och möjliggör skanning av stora mängder bildmaterial för att identifiera mönster och kända aktörer som skapat sexuellt övergreppsmaterial. Både AI-baserade verktyg och *hashing* kan dock medföra risker såsom överblockering och falsklarm, samt etiska problem kopplade till övervakning och integritetsintrång.

Decoster understryker behovet av ytterligare forskning för att öka de tekniska verktygens effektivitet och åtgärda deras svagheter. Därutöver finns ett behov av att säkerställa att data som används för att träna AI-verktyg innehåller en geografisk och etnisk mångfald. Databaser över exploaterade barn innehåller fler bilder och uppgifter gällande gällande vita barn än icke-vita barn. Detta leder till att många befintliga AI-verktyg för åldersuppskattning tränas på igenkänning genom att matas med begränsade eller demografiskt obalanserade data, vilket i sin tur kan orsaka felidentifiering eller misslyckad identifiering av CSAM som involverar vissa demografiska grupper. Decoster (2024) konstaterar vidare att samspelet mellan brottsbekämpande myndigheter och

civilsamhällesorganisationer är en central länk i arbetet mot CSAM som kräver mer forskning. Han påpekar också att arbetsprocesser och rutiner hos leverantörer av elektroniska tjänster (ESP) är bristfälligt studerade, vilket gör att deras påverkan på polisarbete och potentiella följder är okända (Decoster, 2024). Därtill konstateras att dagens programvaruverktyg inte alltid är anpassade till de specifika behoven hos civilsamhällesaktörer och stöddlinjer som arbetar med skydd av barn, samt att CSAM-databaser inom olika rättsområden har bristande samstämmighet och standardisering, vilket hämmar effektiviteten (Decoster, 2024).

Blythe och Johnson (2019) granskade hur konsumentinriktade IoT-enheter kan underlätta brott. Deras genomgång omfattade 114 titlar varav 2 tidningsartiklar, 1 bokkapitel, 20 tidskriftsartiklar och 91 konferensrapporter som beskriver hur konsumentprodukter inom sakernas internet (*the internet of things, IoT*) ökar bekvämligheten men samtidigt utsätter användare för en rad hot och risker. En central risk är dataläckage – det vill säga att privata ljud- eller videofiler eller personlig information som lagras på enheterna kan stjälas och användas för utpressning eller bedrägeri. Eftersom IoT-enheter kan lagra personers och ett hushålls rutiner och rörelsemönster kan de även möjliggöra profilering och stalking, inklusive långvarig övervakning. Audiovisuella enheter som kameror och babymonitorer kan utnyttjas för övervakning eller genom att material manipuleras eller sprids utan samtycke. Utöver detta kan IoT-teknik användas av politiska aktörer, inklusive stater, för att diskriminera eller diskreditera individer och grupper.

Enligt författarna uppstår sårbarheterna i konsumentinriktade IoT-enheter i en kombination av omfattande datainsamling, undermålig design och bristande säkerhetsrutiner. Exempelvis genom standardlösenord, svag kryptering och uteblivna programuppdateringar. De förordar en strategi som involverar både teknikföretag, konsumenter och forskning. För teknikföretagen är prioriteringen att bygga in robusta skyddsmekanismer som hanterar risker samt bristande säkerhetsrutiner. Författarna betonar att reglering och ekonomiska incitament är avgörande för att motivera företag att prioritera säkerhet. I fråga om konsumenterna är deras beteende en viktig faktor, exempelvis genom att strunta i uppdateringar eller konfigurera enheterna felaktigt. Författarna förespråkar att man främjar god ”cyberhygien” genom att öka allmänhetens medvetenhet och menar att det är viktigt att skyddsåtgärderna är lättillgängliga och går att föra in i konsumenternas vardag och vanor.

I fråga om forskningen betonar författarna behovet av att bättre förstå den brottslighet som underlättas av IoT. De noterar att en betydande del av brott genom konsumentinriktade IoT-enheter aldrig anmäls – många brottsoffer är kanske inte ens medvetna om att de utsatts – vilket sannolikt gör skattningar av brottslighetens omfattning och konsekvenser missvisande. Tillförlitliga bedömningar kräver därför nya datainsamlingsmetoder. Det saknas också en nyanserad förståelse av de omständigheter under vilka IoT-faciliterade brott sker, inklusive olika enheters sårbarhet och olika våldsutövarers angreppssätt. Denna kunskap är nödvändig för effektiva förebyggande och brottsbekämpande strategier. Här ser författarna en möjlighet att tillämpa principerna för situationellt brottsförebyggande arbete. Det är en strategi som syftar till att förändra specifika miljöer för att reducera möjligheterna för brottslingar att begå brott. I detta skulle kriminologisk forskning kunna bidra till att identifiera de kontextuella faktorer

som gör IoT-miljöer sårbara och identifiera sätt att minska möjligheten för våldsutövare att missbruka dessa. Detta skulle innefatta forskning om de mest sårbara enheterna och nätverken, nätverkskonfigurationer samt hur brott begås rent praktiskt. Detta kräver detaljerad empiri, såväl som tvärvetenskapligt samarbete mellan kriminologer och cybersäkerhetsexperten.

Döring m.fl. (2024) genomförde en studie som granskade 88 engelskspråkiga vetenskapliga publikationer publicerade mellan 2020 och 2024, i syfte att ge en översikt över aktuell forskning om hur generativ AI (*generative AI*, GenAI) används i sammanhang som rör sexuell hälsa och sexuella beteenden. Författarna delade in sitt fokus i fyra huvudområden: sexualupplysning och information, sexualrådgivning och terapi, sexuella relationer samt erotik och pornografi.

Inom sexualupplysning och information, menar Döring med kollegor, kan GenAI-verktyg som ChatGPT tillhandahålla korrekt, detaljerad och tillgänglig information om ämnen som sexuellt samtycke, HIV-prevention, reproduktiv hälsa och könsbekräftande vård. Studier visar att AI-genererad information ofta matchar, eller till och med överträffar, traditionella källor i fråga om noggrannhet och tydlighet. Tillgängligheten och förmågan att anpassa svaren innebär att sådana verktyg kan vara värdefulla pedagogiska hjälpmedel. Samtidigt kan verktygen tränas upp på data som innehåller sexistiska, rasistiska eller heteronormativa antaganden, vilket kan befästa fördomar och skadliga stereotyper, motverka inkludering och sprida felaktig information. Inom sexuell rådgivning och terapi uppvisar AI-baserade chatbotar betydande potential, enligt författarna, och kan erbjuda empatisk och effektiv vägledning. Till exempel har ChatGPT 4.0 i vissa sammanhang bedömts vara mer empatisk än mänskliga terapeuter. Dessa verktyg kan förbättra tillgängligheten till vård, i synnerhet för marginaliserade grupper eller personer som bor i geografiskt avlägsna områden. Risker kvarstår dock, inte minst risken för terapeutiska missuppfattningar beroende på hur frågor ställs, samt osäkra mätvärden gällande emotionella och etiska risker inom AI-assisterad terapi.

I fråga om romantiska och sexuella relationer kan "AI-vänner" som exempelvis "Replika" erbjuda emotionell intimitet, sexuell tillfredsställelse och sällskap för användare som upplever ensamhet. Generativ AI kan också fungera som medlare i kommunikationen mellan människor. Översikten betonar dock att sådana relationer samtidigt medför psykologiska risker, inte minst emotionellt beroende och situationer där AI-karaktern får användaren att känna sig manipulerad, vilket i sin tur kan påverka förtroendet och relationsdynamik i den fysiska världen. Slutligen används AI inom erotik och pornografi. Detta inkluderar *non-consensual pornography* (NCP) vilket främst kvinnor och flickor utsätts för. AI-genererade sexuella bilder väcker komplexa juridiska och etiska frågor, särskilt i fråga om NCP. Även om motåtgärder håller på att utvecklas menar författarna att forskningen om etisk AI-genererad pornografi och dess positiva tillämpningar – såsom att främja inkludering och mångfald i sexuella sammanhang – fortfarande är begränsad. Pågående tvärvetenskaplig forskning och etisk styrning är avgörande för att säkerställa att dessa tekniker utvecklas på ett ansvarsfullt och rättvist sätt.

Gómez-Quintero m.fl. (2024) genomförde en studie som kombinerade en systematisk översikt av befintlig litteratur med expertutfrågningar. Studiens huvudsakliga syften var

att försöka förutse vilken brottslighet som kan underlättas av metaversum, att identifiera övergripande teman för brottsförebyggande åtgärder i metaversum, samt att med utgångspunkt i de risker som identifierats urskilja ytterligare potentiella brottskategorier. Författarna identifierar 30 specifika brott som de delar in i fem kategorier, vilka är värda att återge i sin helhet:

Bedrägeri, förfalskning eller ekonomiska brott

1. Blockchain-attacker
2. Bedrägerier genom falska mäklare
3. Upphovsrättsintrång
4. Förfalskning (digitala varor inklusive *non-fungible tokens*, NFT)
5. Identitetsstöld för ekonomisk vinning
6. Bedrägerier med falska identiteter (exempelvis falska yrkesutövare)
7. Investeringsbedrägerier (exempelvis lotterier, gåvor, falska metavärldar)
8. Penningtvätt (genom virtuella tillgångar såsom kryptovaluta)
9. Skatteflykt (företag som endast finns i metavärlden)

Egendomsbrott

10. Cyber-fysiska inbrott (riktade mot den verkliga världen via digitala funktioner som integrerats med fysiska byggnader eller tillgångar)
11. Cyber-fysiska infrastrukturattacker (exempelvis metaversum anslutet till sakernas internet utnyttjas för att planera och genomföra attacker)
12. Olagliga intrång i metaversum (otillåten åtkomst)

Sexualbrott

13. Grooming
14. Doxxing (exponering och utpressning via personuppgifter)
15. Non-consensual pornography NCP (personligt sexuellt virtuellt material som används utan medgivande)
16. Virtuella sexuella övergrepp (genom avatarer)
17. Sexuellt övergreppsmaterial på barn (CSAM) (streaming där våldsutövare förgriper sig på barn genom VR-teknologi)
18. Virtuell människohandel för sexuell exploatering (av avatarer)

Andra brott riktade mot individer

19. Cyberfysiska angrepp (ofredande, misshandel genom VR eller AI)
20. Trakasserier
21. Hatbrott
22. Stalking
23. Radikalisering
24. Uppmaning till självskada
25. Utnyttjande av sårbara individer (utpressning, tvång som genomförs av kriminella nätverk)
26. Barnarbete och slaveri (för att skapa innehåll och tjänster)

Andra brott

27. Falsk myndighetsroll (att utge sig för att vara polis eller annan myndighetsperson)
28. Konspiration (att planera fysiska brott)
29. Obehörig användning av utbildningsmaterial (exempelvis polisiära träningsscenarier)
30. Nekande av nödvändiga tjänster (hälso- och sjukvård, utbildning)

Författarna bedömer att kategorierna sexualbrott och andra brott mot individer utgör de största framtida riskerna, både vad gäller skadans omfattning och hur ofta brotten kan komma att inträffa. Dessa brott bedöms samtidigt vara de svåraste att hantera, i synnerhet sexualbrott. Brott mot egendom bedöms däremot utgöra en lägre risk, med undantag för cyber-fysiska inbrott och attacker mot cyber-fysisk infrastruktur, vilka bedöms kunna orsaka stor skada. Gómez-Quintero med kollegor konstaterar att osäkerhetsfaktorerna är stora, vilket understryker vikten av att arbeta med att försöka förutsäga framtida brott. Det kan innebära att i ett tidigt skede försöka identifiera och förebygga hot, så att berörda aktörer kan motverka att brottslingar utnyttjar nya tekniska möjligheterna innan dessa regleras eller säkras. Författarna efterlyser även arbete som syftar till att förstå hur brottsförebyggande åtgärder och insatser kan genomföras i metaversum.

Sangwan och Bhatia (2022) genomförde en systematisk litteratursöversikt med litteratur publicerad sedan 2010, med fokus på användandet av tekniker för ”soft computing”⁷ för att upptäcka övergrepp inom cyber-fysiska⁸ och sociala stordata-system⁹ i så kallade ”smarta städer.”¹⁰ För att systematisera och automatisera upptäckt av övergrepp i sådana system, det vill säga cyberövergrepp, menar författarna att det är viktigt med större begreppsmässig precision. För att precisera begreppet cyberövergrepp (*cyber abuse*, CA) delar studien in det i tre kategorier: näthat (*cyber-hate*, CH), nätmobbning (*cyber-bullying*, CB) samt övergrepp i realtid (*real-time abuse*, RTA) genom cyber-fysiska system.

Cyberövergrepp (CA) definieras som alla former av skadligt, fientligt eller toxiskt beteende online riktat mot individer eller grupper. Det omfattar ett brett spektrum av

⁷ Soft computing handlar om nya datalogiska metoder som speglar den mänskliga hjärnans förmåga att resonera och lära sig i osäkra och oprecisa miljöer. Till skillnad från traditionella matematiska modeller kännetecknas soft computing av modeller i vilka en människoliknande tolerans för oprecisa variabler, osäkerhet, ungefärliga resonemang och delvisa sanningar har byggts in. Detta i syfte att bättre kunna hantera komplexa data eller otydliga eller ofullständigt förstådda situationer.

⁸ Ett cyber-fysiskt system integrerar digitala funktioner med fysiska processer. Dessa system använder inbyggda datorer och algoritmer för att övervaka och styra fysiska processer, ofta med feedback i realtid, vilket skapar en återkopplingsloop mellan den digitala och den fysiska världen. Exempel på detta är smarta elnät, industrirobotar och självkörande fordon.

⁹ Sociala stordata-system samlar främst in data från sociala medieplattformar och bidrar på ett väsentligt sätt till den stora mängd ostrukturerade data som finns tillgänglig idag. Exempel på sådana system är plattformarna X och Facebook, men utöver specifika plattformar kategoriseras även användargenererat innehåll på internet som sociala stordata.

¹⁰ En ”smart stad” kännetecknas av en effektiv integrering av digital teknik, uppkopplade enheter och kommunikationsnätverk i syfte att förbättra invånarnas livskvalitet med minimalt mänskligt ingripande.

handlingar och företeelser, såsom hatpropaganda, rasism, sexism, trollning, trakasserier och hot, ofta i syfte att orsaka psykisk eller fysisk skada. Underkategorin näthat (CH) avser specifikt attacker och övergrepp som grundas på ras, etnicitet, religion, kön, sexuell läggning, funktionsvariation eller andra identitetsmarkörer. Näthat är rotat i ideologiska åskådningar och dess primära syfte är att sprida intoleranta eller diskriminerande budskap, vilket gör det till en digital förlängning av hatbrott. Nätmobbing (CB), å andra sidan, handlar om upprepade och avsiktliga angrepp via digitala medier som syftar till att förnedra, skämma ut eller orsaka lidande hos offren. Bland de vanliga beteenden som förknippas med CB återfinns trakasserier, hets, förtal, utfrysning, bedrägeri och social utestängning. Till skillnad från näthatets ideologiska grund är nätmobbing vanligtvis personligt och hämndinriktat. Övergrepp i realtid (RTA) kan sägas bredda begreppet cyberövergrepp (CA); CA äger rum i den digitala världen men RTA handlar om att åstadkomma effekter i den fysiska världen genom aktiviteter såsom stalking, överfall eller våld i hemmet, ofta genom IoT-enheter.

Av de studier som granskades fokuserade cirka 41 procent på nätmobbing, 19 procent på näthat och runt 40 procent specificerade inte tydligt vilken kategori som avsågs. Författarna noterar att samtliga tillgängliga studier om RTA beskriver användning av IoT-enheter som skapats för användarens säkerhet och personliga trygghet. Smarta bärbara enheter, sensorer och övervakningssystem kan förvisso upptäcka signaler som exempelvis höjda röster eller förhöjda stressnivåer som indikerar fysiskt våld, men samtidigt kan data och övervakningsmöjligheter i sådana enheter i sig skapa förutsättningar för olika övergrepp.

Enligt författarna krävs kunskap som medger större detaljrikedom vid klassificeringen av både näthat och nätmobbing, för att göra det möjligt för detekteringssystem att skilja mellan olika typer av kränkningar. Att upptäcka subtila och underförstådda former av kränkningar, som ofta är utformade för att undgå filter, är också en betydande utmaning. Författarna efterlyser detektionsmodeller som kan respektera yttrandefriheten men samtidigt motverka hatpropaganda på ett effektivt sätt, med tydliga etiska och politiska ramverk som vägledning. I fråga om teknisk forskning efterlyser författarna bland annat djupinlärning¹¹ och automatiserad funktionsinlärning¹² som kan övervinna de begränsningar som finns i manuell konstruktion av detektionsmodeller. De uppmanar också till flerspråkig dataanalys som kombinerar flera olika typer av data samtidigt, till exempel genom att text integreras med ljud, video och bild för att bättre kunna fånga upp online-kränkningar i olika sammanhang.

¹¹ Djupinlärning är en form av maskininlärning där datorer lär sig mönster själv genom att analysera stora mängder data.

¹² Automatiserad funktionsinlärning innebär att systemet själv identifierar vilka egenskaper i datan som är viktiga för att lösa en uppgift.

FOKUS PÅ FÖREBYGGANDE STRATEGIER OCH VERKTYG

Totalt tretton studier diskuterar strategier och verktyg för att upptäcka, förebygga och/eller förhindra våld och övergrepp. Av dessa har sex redan analyserats i tidigare kapitel. De sju återstående studierna har i huvudsak en teknisk inriktning.¹³ De två teman som återkommande identifieras i litteraturen som centrala utmaningar berör teknikens komplexitet och anonymitetens konsekvenser.

Återkommande utmaningar

Den snabba tekniska utvecklingen

Den snabba tekniska utvecklingen skapar ständigt nya möjligheter för produktion av *child sexual abuse material* (CSAM), vilket gör det svårt för brottsbekämpande myndigheter att hålla jämna steg (Edwards m.fl., 2021). IKT-baserade insatser för att bekämpa brotten har visserligen ökat, men kunskapen om digitala applikationer, inklusive mobilappar som är särskilt riktade till unga är fortfarande begränsad (Fraley m.fl., 2025). Enligt Galindo-Domínguez m.fl. (2024) saknar majoriteten av unga i de studier som granskades grundläggande information om sexuella övergrepp online. Samma författare framhåller dessutom att det även framgår att lärare ofta saknar tydliga riktlinjer, tillsyn eller rekommendationer för hur de ska hantera misstänkta övergrepp, vilket riskerar att försvaga skolornas arbete med att utbilda och förebygga övergrepp. Patterson m.fl. (2022) konstaterar att förbättrad kunskap i sig inte nödvändigtvis leder till förändrat riskbeteende online, vilket indikerar att nuvarande interventioner inte fullt ut lyckas påverka beteenden. En relaterad utmaning är att barn ofta har god teknisk kompetens, men att de saknar kunskap om hur tekniken ska användas på ett säkert och ansvarsfullt sätt (Patterson m.fl., 2022). Price m.fl. (2024) betonar att digitala interventioner är avgörande i kampen mot *online child sexual abuse and exploitation* (OCSAE). Trots att det finns programvaror för upptäckt av CSAM råder det fortfarande en påtaglig brist på digitala interventioner som specifikt fokuserar på förebyggande arbete.

Anonymiteten, tillgängligheten och den låga kostnaden

Anonymiteten, tillgängligheten och den låga kostnaden för att använda internet skapar en särskilt gynnsam miljö för brottslig verksamhet och utgör ett allvarligt hinder för förebyggande arbete mot sexuellt övergreppsmaterial på barn (Edwards m.fl., 2021).

¹³ Edwards, G., Christensen, L., Rayment-McHugh, S., & Jones, C. (2021). Fraley, H. E., Chechel Laura, & Varthala Balaji. (2025). Galindo-Domínguez, H., de Frutos, N. D., De-la-Maza, M. S., & Losada, D. (2024). Patterson, A., Ryckman, L., & Guerra, C. (2022). Price, S., McKillop, N., Scanlan, J., Rayment-McHugh, S., Christensen, L., & Prichard, J. (2024). Razi, A., Kim, S., Alsoubai, A., Stringhini, G., Solorio, T., De Choudhury, M., & Wisniewski, P. J. (2021). Singh, S., & Nambiar, V. (2024).

Fenomen som end-to-end-kryptering¹⁴ och steganografi¹⁵ eller att dölja meddelanden och bilder i till synes oskyldigt innehåll, försvårar upptäckten av CSAM. Våldsutövare kan med tiden utveckla metoder för att kringgå även avancerade detektionsverktyg (Edwards m.fl., 2021).

Galindo-Domínguez m.fl. (2024) framhåller att det kan vara svårt att genomföra effektiva interventioner bland unga eftersom många förebyggande strategier bygger på antagandet att unga lätt ändrar sitt beteende när de informeras om risker. I praktiken tenderar dock unga att undvika sådan information om de upplever att deras självständighet inte respekteras. Vidare kan unga föredra anonymitet och att skydda den personliga integriteten i mobilappar som syftar till att förebygga våld i ungas partnerrelationer. Att användare väljer att inte använda sig av befintliga skyddsåtgärder på rätt sätt utgör ytterligare en utmaning vid utformningen av dessa (Fraley m.fl., 2025). I sin forskning noterar Singh och Nambiar (2024) att användningen av AI-baserade verktyg, som kontinuerligt analyserar användarnas digitala aktiviteter, väcker oro för integritetsintrång och övervakning. Detta kan i sin tur avskräcka användare från att engagera sig i virtuella miljöer och därmed försvåra implementeringen av digitala skydds- och förebyggande åtgärder.

Studiernas ansatser och resultat i korthet

Edwards m.fl. (2021) genomförde en studie i syfte att identifiera och förklara befintliga nationella och internationella strategier för att reducera *child sexual abuse material* (CSAM). Studien inkluderar både grå litteratur och publicerad forskning. Studien identifierade fem huvudsakliga strategier för att bekämpa CSAM: övervakning av peer-to-peer-nätverk, automatiserade multimodala verktyg (verktyg som kan bearbeta och integrera bild-, video-, och textmaterial) för upptäckt av olagligt material, webbspindlar för att lokalisera CSAM-webbplatser, popup-varningar samt ansiktsgenkänning.

1. **Peer-to-peer-nätverksövervakning (P2P-övervakning)** gör det möjligt för brottsbekämpande myndigheter att identifiera större aktörer som sprider eller tar del av CSAM genom att övervaka peer-to-peer-fildelningsnätverk.¹⁶ Utredare samlar in IP-adresser och jämför hashvärden mot brottsbekämpande myndigheters databaser för att identifiera brottslingar. Metoden kan hjälpa till att avveckla stora CSAM-arkiv, störa nätverk och motverka anonymitet, men är samtidigt arbetsintensiv och begränsas av motstrategier som oregistrerade hashvärden och ändringar av IP-adresser. Metoden kräver bland annat

¹⁴ End-to-end-kryptering (E2EE) innebär att endast avsändaren och mottagaren kan läsa innehållet i en digital kommunikation. Meddelandet krypteras hos avsändaren och dekrypteras hos mottagaren. Varken tjänsteleverantörer, internetoperatörer eller myndigheter kan därmed läsa innehållet under överföringen.

¹⁵ Steganografi innebär att dölja information så att det inte syns att ett meddelande över huvud taget finns.

¹⁶ Peer-to-peer-fildelningsnätverk (P2P-nätverk) innebär ett sätt att dela filer där användarnas datorer eller enheter är direkt kopplade till varandra, utan att en central server lagrar eller distribuerar filerna.

specialiserad forensisk programvara, proaktivt utredningsarbete och samarbete med internetleverantörer för att spåra användarkonton.

2. **Automatiserade multimodala verktyg**¹⁷ använder avancerad AI och maskininlärning för automatisk upptäckt av CSAM. Detta genom att analysera ett flertal aspekter av bild- och videomaterial såsom färg, form och hudfärg, utöver enklare jämförelser av hashvärden. Microsofts PhotoDNA är ett exempel på ett verktyg som förbättrar träffsäkerheten och kan identifiera både känt och tidigare okänt övergreppsmaterial. Dessa verktyg minskar arbetsbelastningen för utredare och minimerar falska positiva resultat, men våldsutövares nya sätt att undgå upptäckt, exempelvis genom steganografi, innebär att ständiga uppdateringar av verktygen är nödvändiga. Trots detta har automatiserade multimodala verktyg blivit avgörande för större CSAM-utredningar och för att förbättra förmågan att identifiera våldsutövare på större digitala plattformar.
3. **Webbspindlar ("webcrawlers")** är automatiserade verktyg som kan skanna webbplatser för att upptäcka och kartlägga nätverk som innehåller CSAM. De identifierar länkar, mäter webbplatserns konnektivitet¹⁸ och prioriterar centrala webbplatser för borttagning, vilket effektivt minskar trafiken till mindre beroende nätverk. Automatiseringen möjliggör snabbare upptäckt och storskalig borttagning av olagligt innehåll. Ett exempel på detta är Project Arachnid, genom vilket kanadensiska Center for Child Protection (CCP) bearbetat hundratals miljoner webbsidor.¹⁹ Verktögen kräver fördefinierade nyckelord och hashvärden, vilket i sin tur kräver manuella inställningar och löpande underhåll. Verktögen är trots detta avgörande i arbetet att effektivt upptäcka och ta ned större mängder övergreppsmaterial på barn från nätet.
4. **Popup-varningar** är en förebyggande avskräckningsstrategi som riktar sig till potentiella våldsutövare eller "förstagångsförövare". När individer söker efter CSAM-relaterade termer visas varningar som eskalerar i allvarlighetsgrad ju mer explicit sökningen är. Meddelandena betonar brottsligheten, spårbarheten och de moraliska konsekvenserna av att titta på sådant material, vilket ökar den upplevda risken för upptäckt. Forskning visar att dessa avskräckande varningar kan minska olagliga sökningar och störa brottsmönster. Slutsatser gällande dessa verktygs långsiktig effektivitet och eventuella beteendeförändringar bland våldsutövare kräver dock ytterligare studier. Att integrera popup-fönster med länkar som hänvisar till stödtjänster skulle kunna öka deras effektivitet.

¹⁷ Multimodala verktyg innebär digitala verktyg eller system som kan hantera, analysera eller kombinera flera olika typer av information samtidigt.

¹⁸ Hur webbplatser är tekniskt och funktionellt sammankopplade med andra webbplatser, tjänster eller system på internet.

¹⁹ Även svenska Ecpat ingår i detta projekt.

5. **Ansiktsgenkänningsteknik** använder AI-drivna algoritmer för att identifiera brottsoffer och våldsutövare genom att jämföra ansiktsdrag med databaser, exempelvis de som underhålls av National Center for Missing and Exploited Children (NCMEC). Verktyg som Clearview AI kartlägger unika ansiktsmarkörer för att lokalisera försvunna barn, identifiera våldsutövare och koppla samman digitala bilder mellan olika plattformar, inklusive sådana som finns på dark web²⁰. Ansiktsgenkänningsteknik kan ge viktiga ledtrådar som breddar polisutredningar genom att identifiera våldsutövare som inte ursprungligen var föremål för misstanke, vilket i sin tur förbättrar möjligheten att återfinna de barn som utsatts. Användandet av dessa verktyg står dock inför utmaningar relaterade till integritet, begränsningar i datadelning och internationellt samarbete.

Dessa fem strategier baseras på teorin om situationell prevention och syftar till att öka de risker som våldsutövaren upplever, samtidigt som de reducerar både den upplevda njutningen och möjligheten till ursäkter och bortförklaringar. Författarna konstaterar att kunskapen är begränsad om hur och hur ofta dessa strategier används och hur effektiva de är i praktiken. De betonar dessutom behovet av ytterligare forskning för att fastställa effektiviteten hos ansiktsgenkänningsteknik vid identifiering av misstänkta och brottsoffer. Författarna betonar att ansvaret för arbetet mot *child sexual abuse material* (CSAM) inte bara ligger på brottsbekämpande myndigheter, utan att det även kräver ett nära samarbete med den privata sektorn. De efterlyser forskning som fokuserar på att ytterligare minska ”ursäkter” för CSAM-brott, att utveckla nya strategier för att identifiera känslomässiga triggers (*”trigger situations”*) för brott online, samt att utvärdera popup-varningars effektivitet. Slutligen framhåller de behovet av att belysa de etiska och juridiska frågorna kring användningen av ansiktsgenkänning, särskilt när bildmaterial hämtas från kommersiella appar, vilket enligt författarna även kräver en fördjupad rättslig analys.

Fraley m.fl. (2025) genomförde en översiktsstudie med ett underlag bestående av 15 forskningsartiklar. Studiens syfte var att kartlägga befintliga mobilappar utformade för att förebygga eller minska sexuellt våld och våld i nära relationer bland unga och unga vuxna. Den bild som, enligt författarna, framträder i forskningen är att mobilappar har förmågan att nå utsatta populationer och erbjuda skraddarsydda insatser för individer. Mobilappar utgör effektiva verktyg för säkerhetsplanering och kan därför vara användbara i förbyggande och skyddande syfte.

I översiktsstudien identifieras femton mobilappar som är utformade för att förebygga och minska sexuellt våld bland unga och unga vuxna. Dessa mobila verktyg syftar till att öka den personliga säkerheten, minska risker och ge både utsatta och åskådare möjlighet att effektivt reagera på, och hantera, våld i nära relationer och sexuella övergrepp. Enligt studien framstod appen *myPlan Safety Planning* som det mest lovande och använda av de femton apparna. *MyPlan* är specifikt utvecklad för att stödja utsatta i att planera med sin säkerhet och trygghet, fatta beslut och bedöma risker. Funktionerna

²⁰ En anonym del av internet som ofta kopplas till kriminell verksamhet.

inkluderar utvärdering av huruvida olika relationer är hälsosamma, identifiering av olika säkerhetsprioriteringar, bedömning av en situations allvarlighetsgrad och tillhandahållande av personliga säkerhetsstrategier.

I Danmark och Spanien genomfördes en randomiserad kontrollerad pilotstudie med kvinnor i åldern 20–54 år som utsatts för våld i nära relationer. Deltagarna i studien fick konsultationer med en stödperson med särskild kompetens om våld i nära relationer via videolänk och direkt tillgång till appen *myPlan*. Kontrollgruppen fick tillgång till appen först senare. Resultat uppmättes bland annat kopplat till en minskning av våldets grovhet, ökat självbestämmande, säkerhetsplanering samt pre- och postnatal depression (det vill säga depression i samband med graviditet och tiden efter förlossning). Studierna i Danmark och Spanien visade att det är möjligt att genomföra digital screening för våld i nära relationer bland gravida kvinnor som en del av mödravården. Kvinnor i både Danmark och Spanien svarade i hög utsträckning på de frågor som ställdes. En begränsning i studien var dock att två olika verktyg för screening, med olika inklusionskriterier för våldets allvarlighetsgrad, användes och att screeningen endast genomfördes en gång.

De flesta appar som ingår i studien riktar sig till unga vuxna över 18 år, vilket innebär en tydlig brist på verktyg för barn och unga. *MyPlan Teen* är en version som riktar sig till åldersgruppen 15–17-åringar (det finns även en version av appen som kan användas av personer i den utsattes omgivning för att främja positiva beteenden och skapa förutsättningar för stöd och att ingripande). Författarna konstaterar att det saknas forskning om interventioner via mobilappar som specifikt riktar sig till unga i syfte att förebygga sexuellt våld eller våld i ungas partnerrelationer. Trots att de identifierar vissa appar som mer lovande än andra identifieras en tydlig brist på empiriska belägg för slutsatsen att mobilappar är effektiva verktyg för att motverka och minska sexuellt våld bland unga och unga vuxna. De efterlyser därför framtida forskning som fokuserar på barn och unga, med särskild tonvikt på studier som kan utvärdera effekterna av appar inom denna population.

Galindo-Domínguez m.fl. (2024) genomförde en översiktsstudie i syfte att identifiera effektiva interventioner och strategier för lärare och föräldrar för att förebygga och minska *online child sexual abuse and exploitation* (OCSAE). Med ett underlag av 38 artiklar på engelska och spanska identifierade studien tretton strategier för lärare och sju för föräldrar. Dessa kan i sin tur delas in i två huvudkategorier, förebyggande strategier och hanterande strategier och är värda att återges i sin helhet:

Strategier för lärare

1. **Värderingsval** – Eleverna väljer personliga värderingar (t.ex. ärlighet, empati) och försvarar sina val för att främja reflektion, självmedvetenhet och moraliskt resonemang.
2. **Läsning av vetenskapligt material** – Eleverna granskar forskning om beteende och känslor för att förstå hur handlingar och känslor online kan medföra risker.
3. **Läsning av verkliga vittnesmål** – Genom att ta del av överlevares berättelser får eleverna möjlighet att känna empati med offer och lära sig känna igen verkliga grooming-taktiker.

4. **Skriva råd till kamrater** – Eleverna skriver råd eller fraser om hur man undviker grooming (förebyggande) och hur man ska reagera om man blir utsatt (hantering), vilket förstärker inläringen genom kommunikation med kamrater.
5. **Titta på relevanta filmer** – Lärarna använder videor som visar grooming eller utnyttjandescenarier för att väcka diskussion och öka medvetenheten om risker online.
6. **Utbildning** – Lektioner som förklarar vad grooming är, hur våldsutövare manipulerar och ger tydliga regler för säkerhet online.
7. **Reflekterande diskussioner** – Gruppreflekationer eller skriftliga reflektioner uppmuntrar kritiskt tänkande om grooming, dess konsekvenser och empati för offren.
8. **Rollspel och simuleringar** – Eleverna spelar upp scenarier med grooming online eller polisutredningar för att utveckla förståelse och säkra responsstrategier.
9. **Brädspel** – Spel som ger kännedom om kroppen, lär om känslor, internetregler och om att be om hjälp.
10. **Dataspel** – Interaktiva spel som förstärker säkerhetsbeteenden online genom att simulera verkliga digitala risker.
11. **Dela personliga erfarenheter** – Eleverna beskriver personliga svårigheter online och hur de hanterade dem, vilket normaliserar diskussionen och främjar copingstrategier.
12. **Främjande av förmågan att hantera känslor** – Aktiviteterna som stärker självkänslan, självförtroendet och den känslomässiga balansen.
13. **Uppmuntra socialt stöd** – Lärare främjar stöd från kamrater och vuxna för att minska isolering och uppmuntra till att avslöja övergrepp online.

Strategier för föräldrar

1. **Föräldrastöd och kommunikation** – Upprätthålla en öppen, icke-dömande dialog för att bygga förtroende och uppmuntra barn att rapportera oro eller övergrepp online.
2. **Föräldrautbildning** – Utbilda föräldrar om grooming-taktiker, digitala risker och positiva kommunikationstekniker utan att ta till rädsla eller bestraffning.
3. **Regler för internetanvändning** – Fastställa tydliga, åldersanpassade regler för användning av enheter, tidsgränser och beteende online, med balans mellan övervakning och integritet.
4. **Filter och spårningsprogram** – Använda tekniska verktyg för att blockera skadliga webbplatser och övervaka aktiviteter.
5. **Minska tillgängligheten av skadligt innehåll** – Ta bort eller begränsa tillgången till explicit eller riskabelt material online som kan öka risken för grooming.
6. **Traumafokuserad terapi** – Delta i professionell terapi för att hantera emotionella skador, stödja återhämtning och förhindra återupplevelse av traumat.
7. **Kontakta polisen** – Anmäla incidenter av grooming, exponering för explicit innehåll eller misstänkta övergrepp omedelbart för att säkerställa rättsligt skydd och ingripande.

Sammantaget betonar dessa strategier vikten av samarbete mellan lärare och föräldrar för att skapa säkrare digitala miljöer. Genom att kombinera kunskap, empati, struktur och kommunikation ges barn möjlighet att känna igen risker, reagera med

självförtroende och söka hjälp, vilket lägger grunden för ett långsiktigt skydd mot sexuella övergrepp online. Författarna konstaterar att de flesta studier rapporterade positiva effekter av dessa interventioner, att barnens kunskap och medvetenhet höjdes och att deras utsatthet för grooming minskades. Författarna ser dock svårigheter i underlaget och identifierar forskningsbehov inom tre huvudsakliga områden. För det första rekommenderar de att den systematiska översiktsmetodiken replikeras med studier på fler språk än spanska och engelska, för att bredda det jämförande underlaget och upptäcka kulturella skillnader i tillämpningen av förebyggande strategier. För det andra betonar de behovet av att analysera enskilda strategiers och interventioners effektivitet - särskilt de som används av föräldrar. För det tredje föreslår de att framtida forskning bör undersöka hur individuella faktorer som kön, ålder och socioekonomisk bakgrund påverkar interventionernas effektivitet.

Patterson m.fl. (2022) genomförde en bred systematisk översiktsstudie av utbildnings- och informationsinsatser för att förebygga *online child sexual abuse and exploitation* (OCSAE), med nio omfattande studier publicerade mellan 2007 och 2019 som underlag. Författarnas syfte var att identifiera effektiva metoder, framgångar och begränsningar. Studien lyfter fram ett antal effektiva strategier för att förmedla kunskap som kan förebygga OCSAE.

Insatser som aktivt involverade barn i själva utformningen visade på förbättrad förmåga bland barnen att bevara kunskapen, eftersom de kunde relatera till innehållet och kände sig delaktiga i processen. Att genomföra kunskapsförmedlingen i klassrum visade sig vara särskilt effektivt, eftersom obligatoriskt deltagande, lärarhandledning och kamratstöd främjade en trygg inlärningsmiljö. Integration av tekniska hjälpmedel förbättrade också engagemanget, genom att anpassa undervisningsmetoderna till hur barn naturligt interagerar med digitala medier. Detta ökade både relevansen och uppmärksamheten. Studien understryker vikten anpassning av material, innehåll och undervisningsmetoder till olika åldrar och utvecklingsnivåer, exempelvis genom att använda enkla, spelbaserade metoder för yngre barn och diskussionsbaserade format för äldre unga. Slutligen identifieras utbildning av föräldrar, lärare och yrkesverksamma som mycket viktigt eftersom välinformerade vuxna kan känna igen risker, inleda svåra samtal och ge känslomässigt och praktiskt stöd.

Studiens slutsats är att framgångsrika insatser för att förmedla kunskap som kan förebygga OCSAE kombinerar barns aktiva deltagande, strukturerade miljöer, digital integration, anpassat material och vuxnas engagemang. Författarna noterar dock att även om sådana insatser bidrog till ökad kunskap om säkerhet online ledde de inte till någon påtaglig förändring i riskbeteende online. Detta, menar de, understryker behovet av framtida insatser som i högre grad fokuserar på beteendeförändring. Vissa program fanns vara "mestadels effektiva" i fråga om att öka kunskap, men mindre effektiva i att stärka förmågan att faktiskt agera och vidta riskhämmande åtgärder. Fyra insatser bedömdes som "något effektiva" för att öka säkerhetskunskap, men ineffektiva i att påverka beteende. En studie rapporterade till och med en ökning av riskbeteenden efter fyra månader, vilket kan tyda på att ökad medvetenhet ibland leder till större nyfikenhet eller ökad rapporteringsbenägenhet.

Patterson med kollegor konstaterar att det fortfarande finns betydande kunskapsluckor kring hur utbildnings- och informationsinsatser kan förändra barns hantering av risker

online. En särskild forskningslucka gäller OCSAE mellan jämnåriga, där en av studiens källor visar att 39 procent av unga skickar sexuella meddelanden. Av de sexuella meddelanden som skickats har 44 procent skickats till en icke-avsedd mottagare. Hur man på ett effektivt sätt kan hantera OCSAE där både våldsutövare och den utsatte är minderåriga är fortfarande oklart. Därtill pekar författarna på en kulturell begränsning i den befintliga litteraturen, då de flesta studier enbart omfattar ekonomiskt utvecklade västländer. Detta innebär att vår förståelse för effektiva kunskapsbyggande och beteendeförändrande strategier i icke-västerländska kontexter är otillräcklig. En ytterligare lucka gäller deltagarnas åldersfördelning. I de granskade studierna var den yngsta deltagaren nio år. Patterson med kollegor framhåller dock att den ökade internetanvändningen bland upp till åtta år, i kombination med föräldrars vana att lägga ut bilder på sina småbarn online, gör det nödvändigt att utveckla utbildningsinsatser och preventiva program även för mycket unga åldersgrupper.

Price m.fl. (2024) genomförde en översiktsstudie med ett underlag bestående av sex studier för att förstå vilka IKT-baserade verktyg eller strategier som används för att avskräcka och omdirigera individer som riskerar att begå sexuella övergrepp mot barn online, eller som befinner sig i ett tidigt skede av övergreppet. Detta snarare än att fokusera på individer som redan identifierats som gärningsmän.

I studien delas digitala insatser för att förebygga OCSAE in i tre nivåer: primära, sekundära och tertiära strategier. Dessa inriktas på olika stadier av brottsligt beteende och på olika målgrupper. Primära insatser riktar sig till allmänheten och syftar till att förändra sociala normer, öka medvetenheten och förebygga brottsligt beteende. Det kan exempelvis handla om informationskampanjer online och digitala annonser som sprider förebyggande budskap eller som höjer kunskapen och medvetenheten om grooming, människohandel och de rättsliga och moraliska riskerna med att ta del av CSAM.

Sekundära insatser fokuserar på individer som riskerar att begå brott eller befinner sig i ett tidigt skede av ett brottsligt beteende online. Dessa metoder syftar till att avskräcka och omdirigera individen samt uppmuntra denne till att söka hjälp. Varningsmeddelanden i form av popup-fönster eller websidor som skapats för en specifik marknadsföringskampanj används exempelvis av Apple och Google för att informera om de juridiska och etiska konsekvenserna av att ta del av CSAM. Europols projekt Police2Peer är ett annat exempel på en metod som omdirigerar våldsutövare som försöker ladda ner CSAM, med hänvisningar till stödtjänster. Chatbots, såsom reThink som finns på bland annat porrsajten Pornhub, riktar sig mot användare som söker efter olagligt material och erbjuder information om rådgivning och vägledning. Tertiära insatser riktar sig mot personer som redan utövat våld och kan syfta till att förebygga återfall eller underlätta utredning och lagföring. Här återfinns bland annat chatbots som utger sig för att vara barn (med barnrättsorganisationens Terre de Hommes "Sweetie" som klassiskt exempel) och olika AI-baserade detektionssystem såsom webbspindlar, ansiktigenkänning, peer-to-peer-övervakning och innehållsblockering. Dessa används för att upptäcka, identifiera och slå mot nätverk och grupper där CSAM förekommer.

Författarna, som fokuserade på sekundära strategier, menar att riktade varningsmeddelanden är effektivt avskräckande genom att förhöja känslan av ansvar och samtidigt reducera möjligheten att bortförklara handlingarna. Mest effektiva var

varningsmeddelanden som betonade konkreta rättsliga risker. Författarna pekar på en randomiserad studie som visade att meddelandet att polisen spårar IP-adresser resulterade i att 49 procent av användarna avbröt sin verksamhet och 52 procent avbröt när de fick meddelandet att innehållet är olagligt, jämfört med 27 procent avbrutna sessioner inom den kontrollgrupp som inte fick något meddelande alls. Meddelanden som kombinerar avskräckning med erbjudanden om hjälp och hänvisning till stödtjänster visade sig ytterligare förstärka effekten. Dessa verktyg fungerar inom ramen för situationell prevention. I detta sammanhang nämns chatboten reThink som ett särskilt gott exempel.

Författarna noterar dock att utvärdering av digitala interventioner fortfarande är begränsad och att mångfalden av tillvägagångssätt gör det omöjligt att dra generella slutsatser om de övergripande effekterna. Dessutom saknar aktuella studier tillräckligt fokus på kulturella och kontextuella skillnader, vilket väcker frågor om global tillämpbarhet. För att säkerställa effektivitet och bred tillämpbarhet måste framtida forskning utvidga den empiriska utvärderingen, införliva kulturell mångfald och förfinas utformningen av interventioner för att uppnå större räckvidd och effekt.

Författarna fann även stöd för att föräldrars aktiva tillsyn i onlineforum kraftigt minskar sannolikheten för grooming. De hänvisar till en icke-randomiserad experimentell studie som använde tre ”honeypot chatbots” - botar som utgav sig för att vara 13-åriga flickor, men med olika nivåer av föräldratillsyn - för att undersöka hypotesen att föräldrars aktiva tillsyn minskar risken för grooming online. Dessa botar användes i 21 chattrum under två och en halv månad och identifierade 639 fall av grooming, men med avsevärt lägre förekomst i gruppen med aktiv föräldratillsyn och högst förekomst i kontrollgruppen där föräldratillsyn helt saknades. Resultaten pekar inte bara på vikten av föräldratillsyn online, utan även på att teknikdrivna ”föräldrainterventioner” effektivt kan härma faktisk tillsyn. Det skulle i förlängningen kunna bidra till att stärka skyddet av barn i digitala miljöer genom simulerad övervakning och liknande verktyg för avskräckning.

Samtidigt identifierar författarna en tydlig brist på empiriska utvärderingar av IKT-baserade insatser för att förebygga *online child sexual abuse and exploitation* (OCSAE). Författarna påpekar även att nuvarande forskning uppvisar begränsad kulturell, etnisk och geografisk mångfald, vilket kan leda till att befintliga lösningar inte fungerar för olika samhällsgrupper. Dessutom saknas publicerade data för ett antal befintliga verktyg, såsom Googles, Apples och Metas varningssystem och Lucy Faithfull Foundation och Internet Watch Foundations startsidor. Författarna efterlyser en systematisk forskningsagenda för att åtgärda dessa brister.

Razi m.fl. (2021) genomförde en litteraturöversikt vars underlag omfattade 73 forskningsartiklar om datalogiska metoder för att upptäcka av sexuella risker online. Det definieras i studien som alla typer av sexuella övergrepp online som kan leda till psykisk eller fysisk skada. Studien lägger stor vikt på sexuella risker för barn, men underlaget inkluderar även vuxna. Författarnas syfte var att undersöka förutsättningarna för att bygga in mer människocentrerade metoder i dessa ofta teknikfokuserade metoder. Razi med kollegor identifierade tre huvudsakliga fokusområden inom forskningen: sexuell grooming (75 procent av litteraturen), prostitution och människohandel (12 procent) och sexuella trakasserier och övergrepp (12 procent).

En övervägande majoritet av algoritmer för att upptäcka sexuella risker online (93 procent) har historiskt sett fokuserat på att identifiera risker i efterhand. De är alltså i första hand utformade för att upptäcka våldsutövare och brottsliga eller riskfyllda mönster *efter* att det sexuella riskmomentet redan är ett faktum. Endast 5 procent av algoritmerna var ämnade att identifiera risker i realtid eller *före* händelsen. De flesta studierna (80 procent) koncentrerade sig på att identifiera våldsutövare, medan endast 17 procent fokuserade på att identifiera de utsatta, medan resterande 3 procent fokuserade på olika mönster och strukturer i samtal online. Mer än hälften av studierna (55 procent) byggde på data från vuxna våldsutövare eller vuxna volontärer som låtsades vara barn, medan endast 12 procent fokuserade på minderåriga brottsoffer. I 33 procent av de granskade studierna var populationen antingen vuxna (utan en mer specifik åldersuppdelning) eller så angavs inga åldersgrupper alls. Vidare fokuserade 87 procent av studierna på algoritmernas tekniska effektivitet. Endast 4 procent inkluderade användarstudier för att utvärdera modellerna, för att på så sätt lägga fokus på människans upplevelse tekniken och teknikens påverkan på den fysiska verkligheten. Återstående 9 procent av studierna tycks omfatta en blandning av andra utvärderingsstrategier eller metoder. Denna obalans pekar på ett behov av människocentrerade utvärderingar för att säkerställa att algoritmer inte bara är effektiva, utan även socialt ansvarsfulla och att de fungerar för och mottas väl av användare.

Författarna identifierar flera forskningsluckor. En central brist är att det saknas data som speglar verkliga förhållanden och som kan användas för att träna modeller. Det vill säga, de flesta befintliga studier använder offentliga dataset²¹ som inte speglar verkliga och realistiska privata konversationer, vilket begränsar modellernas praktiska tillämpbarhet. Eftersom sexuella risker ofta uppstår i privata forum kan IKT-baserade verktyg som är tränade på offentliga data inte på ett tillförlitligt sätt identifiera risker i sådana privata samtal. Författarna noterar också att det saknas användarstudier och fältutvärderingar, något som är nödvändigt eftersom algoritmernas effektivitet inte på egen hand är tillräckliga för att bedöma ett verktyg eller strategiers effektivitet ur ett användarperspektiv. Vidare menar de att avsaknaden av multimodala data och kontextuell information som underlag för att träna befintliga modeller är ett problem. Befintliga modeller för upptäckt av sexuella risker online är i stor utsträckning beroende av textbaserade data och klarar inte av att på ett adekvat sätt integrera bild-, video- och ljudmaterial. Dessutom är sexuella risker bundna till olika kontexter, exempelvis relationen mellan offer och våldsutövare eller vilken tid på dygnet kommunikationen äger rum. Om dessa data inte inkluderas i träningsmodellerna kan modellernas effektivitet och precision begränsas och leda till både överrapportering och falska positiva resultat.

Razi med kollegor förespråkar att forskningen bör utvecklas så att den bättre speglar verkliga miljöer, beteenden och sammanhang, i samarbete med samhällsvetare, psykologer och kliniska experter. De betonar vikten av att använda data från privata

²¹ Offentliga dataset är öppna samlingar av data som vem som helst kan ta del av, utan särskilda tillstånd. Det vill säga datamängder som är fritt tillgängliga för allmänheten, och som kan laddas ner, användas och ofta återanvändas av forskare, myndigheter, företag och privatpersoner.

kanaler och att samarbeta med brottsoffer i datainsamlingen, samt vikten av att utveckla modeller som integrerar multimodala data och kontextuell information för att förbättra effektivitet och precision. Författarna rekommenderar också att forskningen utvidgas till att omfatta andra former av sexuella risker, exempelvis *sexting*.

Singh och Nambiar (2024) genomförde en systematisk översiktsstudie över hur AI används i arbetet mot *online child sexual abuse and exploitation* (OCSAE), med fokus på aktuella initiativ, deras begränsningar och framtida utvecklingsmöjligheter. Studien granskade 35 artiklar som uteslutande behandlade AI-baserade insatser mot sexuella övergrepp mot barn online. Tolv studier baserades på primärdata, nitton på systematiska granskningar av sekundära källor, och fem presenterade förslag på AI-drivna modeller för framtida utvärdering. Studien identifierade tre centrala teman i litteraturen: befintliga insatser, utvärdering av algoritmer och rekommendationer för framtida främjande av AI-verktyg och modeller.

Befintliga AI-baserade insatser omfattar både praktiska verktyg och konceptuella modeller. Som exempel på ett praktiskt verktyg nämns Chat Analysis Triage Tool (CATT) som identifierar sexuellt innehåll i konversationer, och olika chatbottar som bedömer och klassificerar text som sexuell eller icke-sexuell. Andra åtgärder inkluderar *honeypots* som skickar varningssignaler och *crowdsourcing*-modeller som gör det möjligt för användare att rapportera stötande information. Konceptuella modeller är teoretiska lösningar som hänger ihop med verktyg som har testats i praktiken. Ett exempel är verktyg som bygger på naturlig språkbehandling (natural language processing, NLP).²² Studier som granskade litteratur om befintliga verktyg och modeller för att upptäcka våldsutövare pekade på exempelvis peer-to-peer-nätverk, kryptering, Photo DNA och audiovisuell igenkänningsteknik som effektiva. Utvärderingarna av algoritmer visar både fördelar och nackdelar. AI-verktyg förbättrar effektiviteten i upptäckt, möjliggör rapportering i realtid och bearbetar stora datamängder för att identifiera språkliga och visuella mönster av utnyttjande. Chatbots och crowdsourcing förbättrar tillgängligheten, främjar en gemensam vaksamhet och kan stödja snabbare och mer exakt identifiering av våldsutövare. Samtidigt finns frågetecken kring integritet, etik och risken att algoritmer är partiska på grund av träningsdata, samt svårigheter att tolka kulturella och språkliga nyanser. I vissa fall fanns även frågetecken kring datasäkerhet. Den granskade litteraturens rekommendationer för vidareutveckling och främjande av AI-verktyg och modeller betonar vikten av att integrera multimodala data för att förbättra kontextuell förståelse, vikten av att främja tvärvetenskapligt samarbete mellan juridik, psykologi, datavetenskap och lingvistik, samt vikten av att bygga etiska, människocentrerade modeller. Studien noterar även ett behov av starkare rättsliga och etiska ramverk för att säkerställa transparens, dataskydd och internationellt samarbete.

Författarna konstaterar att det i dagsläget saknas tillräckliga empiriska belägg för AI-interventioners effektivitet för att motverka OCSAE. De framhåller behovet av ytterligare forskning för att bättre förstå den faktiska effekten av dessa verktyg och

²² NLP är ett forskningsområde inom datavetenskap och lingvistik som handlar om hur datorer kan förstå, tolka och skapa mänskligt språk, både i text och tal.

noterar att AI-teknologins potential inom arbetet att skydda barn kräver forskning som integrerar tekniska lösningar med barnrättslig lagstiftning. Befintliga AI-verktyg och modeller för att motverka OCSAE brottas dessutom med generaliserbarhetsproblem eftersom de ofta testas på små och icke-representativa urval. Singh och Nambiar föreslår därför att framtida forskning bör använda teoretiska ramverk som bättre fångar våldsutövares beteende, utveckla AI-modeller som främjar medvetenhet om sexuell exploatering och stärker barns psykologiska resiliens, samt genomföra fler empiriska och longitudinella studier av AI-baserade interventioner.

SAMMANFATTANDE SLUTORD

I underlaget för denna litteraturöversikt framträder teknologifaciliterat våld (TFV) inte bara som en ny arena för redan kända former av övergrepp, utan även som ett genomgripande skifte i hur våld tar sig uttryck och fungerar.

Blythe och Johnson (2019) beskriver hur informations- och kommunikationstekniken har förändrat våldets tidsmässiga och rumsliga dimensioner - från avgränsade handlingar till långvariga, kontinuerliga processer som upprätthålls i digitala miljöer. Digitaliseringens infrastruktur har på det sättet skapat ett sammanhang där tvång, hot och exploatering sker genom tekniska nätverk, där våldsutövare och utsatta binds samman av algoritmer, plattformar och dataflöden snarare än genom fysiska möten (Falduti & Tessaris, 2023; Filice m.fl., 2022). Våldet har blivit gränsöverskridande, skalbart och delvis automatiserat och kan förstås som en form av maktutövning som verkar på flera nivåer samtidigt. Samtidigt visar forskningen att denna våldsdynamik till stor del är en förlängning, eller uppdatering, av sedan länge etablerade maktordningar (Estellés och Doyle, 2025; Godulla m.fl., 2021; Sandoval m.fl., 2024) Porta m.fl. (2024) och Quilty & Flynn (2025) visar används digitala system som ursprungligen skapades för kommunikation, lärande och social delaktighet allt oftare som verktyg för kontroll, övervakning, manipulation och skada.

Samma teknik som används för våld och övergrepp erbjuder samtidigt nya sätt att upptäcka, förhindra och hantera våld. Decoster (2024) och Sangwan och Bhatia (2022) visar hur artificiell intelligens, stordata och VR-baserade interventioner kan användas i förebyggande syften; exempelvis genom varningssystem, bildigenkänning, trauma-behandling och verktyg för att förstärka empati och underlätta stöd. Forskningen visar dock tydligt att utvecklingen av dessa skyddssystem ligger efter våldsutövarnas tekniska förmåga att utveckla och tillämpa ny teknik. Detta kan beskrivas som en ”kapprustning” mellan våldsutövare och rättsvårdande myndigheter. Kriminella aktörer kan snabbt ta till sig ny teknik såsom deepfakes, kryptering och metaversum-miljöer, samtidigt som myndigheter och stödorganisationer begränsas av juridiska, etiska och organisatoriska faktorer.

Metodologiska och begreppsmässiga svårigheter framträder som centrala utmaningar. Bleakley med kollegor (2024) och Chauvire-Geib och Fevert (2024) visar att avsaknaden av gemensamma definitioner av helt centrala begrepp försvårar såväl tvärvetenskapliga studier och internationellt samarbete som kunskapsutveckling. Quilty och Flynn (2025) betonar att bristen på tvärvetenskaplighet och en begränsad representation av minoriteter i forskningsmaterialet gör att forskningen förblir fragmentarisk. Konsekvensen av detta är ett forskningsfält som är brett men grunt och där empirisk forskning alltför sällan kan omsättas i praktik eller bli användbar i bredare sammanhang. Mot denna bakgrund går det att konstatera ett behov av tvärvetenskapliga forskningsmiljöer som förenar juridikens normativa ramar, datavetenskapens tekniska förståelse, psykologins kunskap om trauma och socialvetenskapens insikter om makt och strukturer. Sådana miljöer bör också arbeta för att bredda de empiriska underlagen och genomföra longitudinella studier som kan följa och förstå företeelser över tid.

Teknologifaciliterat våld är i grunden ett gränsöverskridande fenomen som berör flera samhällssektorer. Det suddar ut etablerade gränser mellan det privata och det offentliga

- och mellan trygghet och frihet. För att kunna möta detta krävs en fördjupad förståelse för hur teknologifaciliterat våld fungerar. Det är inte bara en fråga för forskningen, utan en demokratisk nödvändighet. Att värna individers personliga integritet, skydda barn och utsatta grupper, samt upprätthålla tilliten till de tekniska system som präglar vardagslivet är avgörande, både för den enskildes trygghet och för samhällets samlade motståndskraft.

KÄLLFÖRTECKNING

- Ali, S., Haykal, H. A., & Youssef, E. Y. M. (2023). Child Sexual Abuse and the Internet—A Systematic Review. *Human Arenas*, 6(2), 404–421. Scopus. <https://doi.org/10.1007/s42087-021-00228-9>
- Birrer, A., & Just, N. (2024). What we know and don't know about deepfakes: An investigation into the state of the research and regulatory landscape. *New Media and Society*. <https://doi.org/10.1177/14614448241253138>
- Bleakley, P., Martellozzo Elena, Spence, R., & DeMarco, J. (2024). Moderating online child sexual abuse material (CSAM): Does self-regulation work, or is greater state regulation needed? *European Journal of Criminology*, 21(2), 231–250. <https://doi.org/10.1177/14773708231181361>
- Blythe, J. M., & Johnson, S. D. (2021). A systematic review of crime facilitated by the consumer Internet of Things. *Security Journal*, 34(1), 97–125. <https://doi.org/10.1057/s41284-019-00211-8>
- Chauviré-Geib, K., & Fegert, J. M. (2024). Victims of Technology-Assisted Child Sexual Abuse: A Scoping Review. *Trauma, Violence & Abuse*, 25(2), 1335–1348. <https://doi.org/10.1177/15248380231178754>
- Decoster, N. (2024). The Policing and Reporting of Online Child Sexual Abuse Material: A Scoping Review. *Revue Internationale de Droit Penal*, 2024, 323–366.
- Döring, N., Le, T. D., Vowels, L. M., Vowels, M. J., & Marcantonio, T. L. (2025). The Impact of Artificial Intelligence on Human Sexuality: A Five-Year Literature Review 2020–2024. *Current Sexual Health Reports*, 17(1), 1–39. <https://doi.org/10.1007/s11930-024-00397-y>
- Edwards, G., Christensen, L., Rayment-McHugh, S., & Jones, C. (2021). Cyber strategies used to combat child sexual abuse material. *Trends and Issues in Crime and Criminal Justice*, 636, 1–16. <https://doi.org/10.52922/ti78313>
- Estellés, M., & Doyle, A. (2025). From safeguarding to critical digital citizenship? A systematic review of approaches to online safety education. *Review of Education*, 13(1). <https://doi.org/10.1002/rev3.70056>
- Falduti, M., & Tessaris, S. (2023). Mapping the Interdisciplinary Research on Non-consensual Pornography: Technical and Quantitative Perspectives. *Digital Threats: Research and Practice*, 4(3). <https://doi.org/10.1145/3608483>
- Faraz, A., Mounsef, J., Raza, A., & Willis, S. (2022). Child Safety and Protection in the Online Gaming Ecosystem. *IEEE Access*, 10, 115895–115913. <https://doi.org/10.1109/ACCESS.2022.3218415>

- Filice, E., Abeywickrama, K. D., Parry, D. C., & Johnson, C. W. (2022). Sexual violence and abuse in online dating: A scoping review. *Aggression & Violent Behavior, 67*, N.PAG-N.PAG. <https://doi.org/10.1016/j.avb.2022.101781>
- Fraleay, H. E., Chechel Laura, & Varthala Balaji. (2025). Mobile Applications Designed for Sexual or Dating Violence Prevention Targeting Adolescents and Emerging Adults: A Scoping Review. *Clinical Nursing Research, 34*(2), 120–137. <https://doi.org/10.1177/10547738241305785>
- Galindo-Dominguez, H., de Frutos, N. D., De-la-Maza, M. S., & Losada, D. (2024). Systematic Review: Strategies to Reduce the Risk of Online Child Sexual Abuse. *Electronic Journal of Research in Educational Psychology, 22*(3)(64), 671–698. <https://doi.org/10.25115/EJREP.V22I64.9298>
- Gewirtz-Meydan, A., Volman-Pampanel, D., Opuda, E., & Tarshish, N. (2024). Dating Apps: A New Emerging Platform for Sexual Harassment? A Scoping Review. *Trauma, Violence & Abuse, 25*(1), 752–763. <https://doi.org/10.1177/15248380231162969>
- Godulla, A., Hoffmann, C. P., & Seibert, D. M. A. (2021). Dealing with deepfakes—An interdisciplinary examination of the state of research and implications for communication studies. *Studies in Communication and Media, 10*(1), 73–96. <https://doi.org/10.5771/2192-4007-2021-1-72>
- Gómez-Quintero, J., Johnson, S. D., Borrión, H., & Lundrigan, S. (2024). A scoping study of crime facilitated by the metaverse. *Futures, 157*. <https://doi.org/10.1016/j.futures.2024.103338>
- Nationellt centrum för kvinnofrid, NCK (2025) *Digitala dimensioner av våld i vuxnas nära relationer - En kunskaps- och forskningsöversikt om teknologifaciliterat våld och stödprocesser*. Uppsala Universitet. NCK-rapport 2025:4.
- Parti, K., & Szabó, J. (2024). The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe. *Laws, 13*(6). <https://doi.org/10.3390/laws13060067>
- Patterson, A., Ryckman, L., & Guerra, C. (2022). A Systematic Review of the Education and Awareness Interventions to Prevent Online Child Sexual Abuse. *Journal of Child & Adolescent Trauma, 15*(3), 857–867. <https://doi.org/10.1007/s40653-022-00440-x>
- Porta, C. M., Frerich, E. A., Hoffman, S., Bauer, S., Jain, V. M., & Bradley, C. (2024). Sexual Violence in Virtual Reality: A Scoping Review. *Journal of Forensic Nursing, 20*(1), 66–77. <https://doi.org/10.1097/JFN.0000000000000466>
- Price, S., McKillop, N., Scanlan, J., Rayment-McHugh, S., Christensen, L., & Prichard, J. (2024). A Review of Digital Interventions as Secondary Prevention Measures to Combat Online Child Sexual Abuse Perpetration.

- Journal of Child Sexual Abuse*, 33(7), 869–890.
<https://doi.org/10.1080/10538712.2024.2415549>
- Quilty, E., & Flynn, A. (2025). Technology-Facilitated Violence in the Indo-Pacific: A Scoping Review. *Trauma, Violence, and Abuse*.
<https://doi.org/10.1177/15248380251323217>
- Razi, A., Kim, S., Alsoubai, A., Stringhini, G., Solorio, T., De Choudhury, M., & Wisniewski, P. J. (2021). A Human-Centered Systematic Literature Review of the Computational Approaches for Online Sexual Risk Detection. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2).
<https://doi.org/10.1145/3479609>
- Ringenberg, T. R., Seigfried-Spellar, K. C., Rayz, J. M., & Rogers, M. K. (2022). A scoping review of child grooming strategies: Pre- and post-internet. *Child Abuse & Neglect*, 123, 1. <https://doi.org/10.1016/j.chiabu.2021.105392>
- Sandoval, M.-P., de Almeida Vau, M., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: A systematic review. *Crime Science*, 13(1). <https://doi.org/10.1186/s40163-024-00239-1>
- Sangwan, S. R., & Bhatia, M. P. S. (2022). Soft computing for abuse detection using cyber-physical and social big data in cognitive smart cities. *Expert Systems*, 39(5). <https://doi.org/10.1111/exsy.12766>
- Singh, S., & Nambiar, V. (2024). Role of Artificial Intelligence in the Prevention of Online Child Sexual Abuse: A Systematic Review of Literature. *Journal of Applied Security Research*, 19(4), 586–627.
<https://doi.org/10.1080/19361610.2024.2331885>

BILAGA 1. FÖRKORTNINGAR OCH ENGELSKA BEGREPP

Tabell 1. Förkortningar (A-Ö)

Förkortning	Fullständig form	Förklaring
AI	Artificial Intelligence	Artificiell intelligens; teknik som används för analys, bildigenkänning och automatisering.
CA	Cyber Abuse	Digitala övergrepp, inklusive trakasserier, hot eller tvång i digitala miljöer.
CB	Cyber-Bullying	Digital mobbning och upprepade kränkningar via nätet.
CH	Cyber-Hate	Hatpropaganda eller ideologiskt motiverade attacker online.
CSAM	Child Sexual Abuse Material	Material som visar sexuella övergrepp mot barn.
GSNA	Geo-social Networking App	Platsbaserad app som kopplar samman användare via geografisk närhet.
IKT	Informations- och kommunikationsteknik	Teknologiska system för kommunikation och informationshantering.

IoT	Internet of Things	Nätverk av uppkopplade fysiska enheter, t.ex. sensorer eller hushållsapparater.
LSCSA	Livestreamed Child Sexual Abuse	Sexuella övergrepp mot barn som direktsänds online.
MSM	Men Who Have Sex with Men	Män som har sex med män oberoende av den egna sexuella läggningen.
NCP	Non-consensual Pornography	Pornografiskt material som skapats utan samtycke.
OCSAE	Online Child Sexual Abuse and Exploitation	Sexuellt utnyttjande och övergrepp mot barn online.
RTA	Real-Time Abuse	Övergrepp som sker i realtid, ofta via streaming.
TA-CSA	Technology-Assisted Child Sexual Abuse	Sexuella övergrepp mot barn möjliggjorda genom teknik.
TFV	Technology-Facilitated Violence	Teknologifaciliterat våld; paraplybegrepp för våld, tvång och exploatering online.
VR	Virtual Reality	Virtuell miljö upplevd genom VR-teknik.

Tabell 2. Engelska uttryck (A–Z)

Engelskt uttryck	Förklaring
AI-generated	Beskriver innehåll skapat genom artificiell intelligens, t.ex. deepfakes eller simulerade bilder.
avatar	Virtuell representation av en användare i VR eller metaversum.
blockchain	Teknik för distribuerad datalagring.
child grooming	Process där våldsutövare manipulerar barn inför sexuella övergrepp.
content moderation	Övervakning och hantering av digitalt innehåll.
cyber-physical	Syftar på system som länkar digitala funktioner med fysiska miljöer.
deepfake/deepfakes	AI-genererat material som imiterar verkliga personer eller händelser.
doxxing	Att avslöja eller publicera någons privata uppgifter online.
embodiment	Upplevelsen av att förkroppsliga en virtuell kropp i VR.
end-to-end encryption	Krypteringsteknik som skyddar data mellan sändare och mottagare.
facial recognition	Teknik för automatisk igenkänning av ansikten.
geo-social networking app	App som kopplar samman användare baserat på fysisk närhet.
hash value	Hashvärde, en digital signatur som används för att identifiera olagligt material.
livestream	Direktsändning via internet.
metaverse	Virtuell 3D-värld där användare interagerar digitalt.

non-consensual pornography	Pornografiskt material som skapats utan samtycke.
peer-to-peer network	Direkt kommunikation mellan datorer utan central server.
popup warning	Varningsmeddelanden som visas i webbläsare för att avskräcka från brott.
real-time	Händelser som sker i samma stund som de observeras.
sexting	Sexuellt laddade meddelanden, bilder eller videor via elektroniska medier.
smart city	Stadsmiljö som styrs och optimeras genom digital teknik och sensorer.
stalking	Upprepad förföljelse eller övervakning.
virtual reality	Virtuell miljö upplevd genom VR-teknik.

BILAGA 2: DOKUMENTATION AV SÖKSTRATEGI



Dokumentation av sökstrategier - Malmö universitetsbibliotek

Datum: 2025-06-24

Ämne/forskningsfråga: Digitala och teknikbaserade former av våld med särskilt fokus på nätstalking och övervakning inom områdena mäns våld mot kvinnor, hedersrelaterat våld- och förtryck, prostitution och människohandel. Våld i nära relation inkluderas ej.

Beställare: Amanda Nyberg och Lisa Lindström, Jämställdhetsmyndigheten

Bibliotekarier: Helen Rasmussen och Jenny Magnusson, Malmö universitetsbibliotek

Databaser:

1. ASSIA (ProQuest)
 2. Cinahl (EBSCOhost)
 3. PsycInfo (EBSCOhost)
 4. Scopus
 5. Sociological Abstracts (ProQuest)
 6. Web of Science
-

Totalt antal träffar:

- Före dubblettrensning: 1143
 - Efter dubblettrensning: 737
-

Text som kan användas i metoddelen:

Sökstrategi

Litteratursökningen utfördes i följande databaser: ASSIA, Cinahl, PsycInfo, Scopus, Sociological Abstracts och Web of Science. Den senaste sökningen utfördes 2025-06-18.

Fullständig beskrivning av sökstrategin/sökstrategierna finns att tillgå i bilaga/appendix.

1. ASSIA (ProQuest)

Datum för sökning: 2025-06-17		Ämnesområde: Socialt arbete m.m.	
Antal träffar: 20			
Search no	Search terms	Results	Comments
1	TI/AB "abused women" OR "battered females" OR "battered women" OR "abused females" OR "gender* violence" OR "genderbased violence" OR "gender-based violence" OR "gender related violence" OR "emotional abuse" OR "emotional violence" OR honor OR honour OR oppression OR prostitut* OR "sexual abuse" OR "sex crime" OR "sex work*" OR "sexual assault" OR "sexual harassment" OR "sexual violence" OR "social control" OR "subjected to violence" OR trafficking OR "violence against women" OR "violence towards women" OR "victim of abuse" OR "victim of violence" OR "women abuse" OR "women violence" OR "sexual exploitation" OR misogyny OR grooming OR pornograph* OR incel*	28,865	
2	TI/AB android* OR "audio record*" OR camera* OR cellphone* OR computer* OR cyber OR digital* OR electronic OR email OR "e mail" OR gps OR "global positioning system*" OR internet OR iot OR keylogger* OR "location track*" OR "mobile app*" OR phone OR phones OR phonecall* OR photo OR photos OR photograph* OR screenlogger* OR "screen recorder" OR "smart home*" OR "social media" OR "social network*" OR technolog* OR telephone* OR "text messag*" OR "tracking device*" OR "video record*" OR "web traffic" OR wifi OR wireless OR "artificial intelligence" OR AI OR online OR ICT OR "data mining"	137,510	
3	TI/AB "surveillance systems" OR dominance OR punishment OR surveillance OR stalking OR harassment OR threats OR coercion OR coercive OR control* OR intimidat* OR monitor* OR punish*	221,896	
4	2 AND 3	27,810	
5	TI/AB cyberstalking OR cyberviolence OR doxing OR doxxing OR "revenge porn*" OR sextortion OR spyware OR "surveillance app*" OR "tech abuse" OR "cyberdating violence" OR "cyber harassment" OR cyber-victimization OR "technology mediated" OR "technology based" OR "technology facilitated" OR	1,157	

	"technological coercive control" OR "technology control" OR "technological abuse" OR "technological violence" OR "digital violence" OR "digital abuse" OR "digital control" OR "digital coercive control" OR "cyber abuse" OR "cyber control" OR "cyber coercive control" OR "cyber assault" OR "digital assault" OR "digital harassment" OR deepfake* OR online NEAR/3 violence OR online NEAR/3 abuse OR online NEAR/3 abuser		
6	4 OR 5	28,628	
7	1 AND 6	795	
8	"literature review*" OR "review of literature" OR "systematic review*" OR "research review*" OR "scoping review*" OR "rapid review*" OR "mapping review" OR "umbrella review*" OR "meta-analy*" OR metaanaly* OR "research synthesis" OR "comprehensive review*" OR "narrative review*" OR "meta-synthesis" OR "bibliometric analys*"	58,765	
9	7 AND 8	33	
10	Filter: Peer review	33	
11	Filter: 2019-2025	20	

2. Cinahl (EBSCOhost)

Datum för sökning: 2025-06-18		Ämnesområde: Omvårdnad m.m.	
Antal träffar: 95			
Search no	Search terms	Results	Comments
1	TI/AB "abused women" OR "battered females" OR "battered women" OR "abused females" OR "gender* violence" OR "genderbased violence" OR "gender-based violence" OR "gender related violence" OR "emotional abuse" OR "emotional violence" OR honor OR honour OR oppression OR prostitut* OR "sexual abuse" OR "sex crime" OR "sex work*" OR "sexual assault" OR "sexual harassment" OR "sexual violence" OR "social control" OR "subjected to violence" OR trafficking OR "violence against women" OR "violence towards women" OR "victim of abuse" OR "victim of violence" OR "women abuse" OR "women violence" OR "sexual exploitation" OR misogyny OR grooming OR pornograph* OR incel*	49,338	
2	TI/AB android* OR "audio record*" OR camera* OR cellphone* OR computer* OR cyber OR digital* OR electronic OR email OR "e mail" OR gps OR "global positioning system*" OR internet OR iot OR keylogger*	605,961	

	OR "location track*" OR "mobile app*" OR phone OR phones OR phonecall* OR photo OR photos OR photograph* OR screenlogger* OR "screen recorder" OR "smart home*" OR "social media" OR "social network*" OR technolog* OR telephone* OR "text messag*" OR "tracking device*" OR "video record*" OR "web traffic" OR wifi OR wireless OR "artificial intelligence" OR AI OR online OR ICT OR "data mining"		
3	TI/AB "surveillance systems" OR dominance OR punishment OR surveillance OR stalking OR harassment OR threats OR coercion OR coercive OR control* OR intimidat* OR monitor* OR punish*	1,109,768	
4	2 AND 3	128,985	
5	TI/AB cyberstalking OR cyberviolence OR doxing OR doxxing OR "revenge porn*" OR sextortion OR spyware OR "surveillance app*" OR "tech abuse" OR "cyberdating violence" OR "cyber harassment" OR cyber-victimization OR "technology mediated" OR "technology based" OR "technology facilitated" OR "technological coercive control" OR "technology control" OR "technological abuse" OR "technological violence" OR "digital violence" OR "digital abuse" OR "digital control" OR "digital coercive control" OR "cyber abuse" OR "cyber control" OR "cyber coercive control" OR "cyber assault" OR "digital assault" OR "digital harassment" OR deepfake* OR online N3 violence OR online N3 abuse OR online N3 abuser	3,182	
6	4 OR 5	131,166	
7	1 AND 6	1,421	
8	"literature review*" OR "review of literature" OR "systematic review*" OR "research review*" OR "scoping review*" OR "rapid review*" OR "mapping review" OR "umbrella review*" OR "meta-analy*" OR metaanaly* OR "research synthesis" OR "comprehensive review*" OR "narrative review*" OR "meta-synthesis" OR "bibliometric analys*"	368,611	
9	7 AND 8	122	
10	Filter: Peer review	122	
11	Filter: 2019-2025	95	

3. PsycInfo (EBSCOhost)

Datum för sökning: 2025-06-18 Antal träffar: 93	Ämnesområde: Psykologi, psykiatri, sociologi mm
--	--

Search no	Search terms	Results	Comments
1	TI/AB "abused women" OR "battered females" OR "battered women" OR "abused females" OR "gender* violence" OR "genderbased violence" OR "gender-based violence" OR "gender related violence" OR "emotional abuse" OR "emotional violence" OR honor OR honour OR oppression OR prostitut* OR "sexual abuse" OR "sex crime" OR "sex work*" OR "sexual assault" OR "sexual harassment" OR "sexual violence" OR "social control" OR "subjected to violence" OR trafficking OR "violence against women" OR "violence towards women" OR "victim of abuse" OR "victim of violence" OR "women abuse" OR "women violence" OR "sexual exploitation" OR misogyny OR grooming OR pornograph* OR incel*	95,141	
2	TI/AB android* OR "audio record*" OR camera* OR cellphone* OR computer* OR cyber OR digital* OR electronic OR email OR "e mail" OR gps OR "global positioning system*" OR internet OR iot OR keylogger* OR "location track*" OR "mobile app*" OR phone OR phones OR phonecall* OR photo OR photos OR photograph* OR screenlogger* OR "screen recorder" OR "smart home*" OR "social media" OR "social network*" OR technolog* OR telephone* OR "text messag*" OR "tracking device*" OR "video record*" OR "web traffic" OR wifi OR wireless OR "artificial intelligence" OR AI OR online OR ICT OR "data mining"	574,442	
3	TI/AB "surveillance systems" OR dominance OR punishment OR surveillance OR stalking OR harassment OR threats OR coercion OR coercive OR control* OR intimidat* OR monitor* OR punish*	1,044,893	
4	2 AND 3	117,842	
5	TI/AB cyberstalking OR cyberviolence OR doxing OR doxxing OR "revenge porn*" OR sextortion OR spyware OR "surveillance app*" OR "tech abuse" OR "cyberdating violence" OR "cyber harassment" OR cyber-victimization OR "technology mediated" OR "technology based" OR "technology facilitated" OR "technological coercive control" OR "technology control" OR "technological abuse" OR "technological violence" OR "digital violence" OR "digital abuse" OR "digital control" OR "digital coercive control" OR "cyber abuse" OR "cyber control" OR "cyber coercive control" OR "cyber assault" OR "digital assault" OR "digital harassment" OR deepfake* OR online N3 violence OR online N3 abuse OR online N3 abuser	5,612	
6	4 OR 5	122,040	
7	1 AND 6	3,078	

8	"literature review*" OR "review of literature" OR "systematic review*" OR "research review*" OR "scoping review*" OR "rapid review*" OR "mapping review" OR "umbrella review*" OR "meta-analy*" OR metaanaly* OR "research synthesis" OR "comprehensive review*" OR "narrative review*" OR "meta-synthesis" OR "bibliometric analys*"	195,654	
9	7 AND 8	140	
10	Filter: Peer review	126	
11	Filter: 2019-2025	93	

4. Scopus

Datum för sökning: 2025-06-18		Ämnesområde: Bred databas inom flertalet ämnesområden, citeringsdatabas	
Antal träffar: 270			
Search no	Search terms	Results	Comments
1	TI/AB "abused women" OR "battered females" OR "battered women" OR "abused females" OR "gender* violence" OR "genderbased violence" OR "gender-based violence" OR "gender related violence" OR "emotional abuse" OR "emotional violence" OR honor OR honour OR oppression OR prostitut* OR "sexual abuse" OR "sex crime" OR "sex work*" OR "sexual assault" OR "sexual harassment" OR "sexual violence" OR "social control" OR "subjected to violence" OR trafficking OR "violence against women" OR "violence towards women" OR "victim of abuse" OR "victim of violence" OR "women abuse" OR "women violence" OR "sexual exploitation" OR misogyny OR grooming OR pornograph* OR incel*	289,257	
2	TI/AB android* OR "audio record*" OR camera* OR cellphone* OR computer* OR cyber OR digital* OR electronic OR email OR "e mail" OR gps OR "global positioning system*" OR internet OR iot OR keylogger* OR "location track*" OR "mobile app*" OR phone OR phones OR phonecall* OR photo OR photos OR photograph* OR screenlogger* OR "screen recorder" OR "smart home*" OR "social media" OR "social network*" OR technolog* OR telephone* OR "text messag*" OR "tracking device*" OR "video record*" OR "web traffic" OR wifi OR wireless OR "artificial intelligence" OR AI OR online OR ICT OR "data mining"	11,613,890	
3	TI/AB "surveillance systems" OR dominance OR punishment OR surveillance OR stalking OR harassment OR threats OR coercion OR coercive OR control* OR intimidat* OR monitor* OR punish*	14,587,034	

4	2 AND 3	2,474,555	
5	TI/AB cyberstalking OR cyberviolence OR doxing OR doxxing OR "revenge porn*" OR sextortion OR spyware OR "surveillance app*" OR "tech abuse" OR "cyberdating violence" OR "cyber harassment" OR cyber-victimization OR "technology mediated" OR "technology based" OR "technology facilitated" OR "technological coercive control" OR "technology control" OR "technological abuse" OR "technological violence" OR "digital violence" OR "digital abuse" OR "digital control" OR "digital coercive control" OR "cyber abuse" OR "cyber control" OR "cyber coercive control" OR "cyber assault" OR "digital assault" OR "digital harassment" OR deepfake* OR (online W/3 (violence OR abuse OR abuser))	93,542	
6	4 OR 5	2,532,213	
7	1 AND 6	9,409	
8	"literature review*" OR "review of literature" OR "systematic review*" OR "research review*" OR "scoping review*" OR "rapid review*" OR "mapping review" OR "umbrella review*" OR "meta-analy*" OR metaanaly* OR "research synthesis" OR "comprehensive review*" OR "narrative review*" OR "meta-synthesis" OR "bibliometric analys*"	1,391,009	
9	7 AND 8	401	
10	Filter: Review och Article	350	
11	Filter: 2019-2025	270	

5. Sociological Abstracts (ProQuest)

Datum för sökning: 2025-06-18		Ämnesområde: Sociologi, socialt arbete m.m.	
Antal träffar: 50			
Search no	Search terms	Results	Comments
1	TI/AB "abused women" OR "battered females" OR "battered women" OR "abused females" OR "gender* violence" OR "genderbased violence" OR "gender-based violence" OR "gender related violence" OR "emotional abuse" OR "emotional violence" OR honor OR honour OR oppression OR prostitut* OR "sexual abuse" OR "sex crime" OR "sex work*" OR "sexual assault" OR "sexual harassment" OR "sexual violence" OR "social control" OR "subjected to violence" OR trafficking OR "violence against women" OR "violence towards women" OR "victim of abuse" OR "victim of violence" OR "women abuse" OR "women violence"	82,445	

	OR "sexual exploitation" OR misogyny OR grooming OR pornograph* OR incel*		
2	TI/AB android* OR "audio record*" OR camera* OR cellphone* OR computer* OR cyber OR digital* OR electronic OR email OR "e mail" OR gps OR "global positioning system*" OR internet OR iot OR keylogger* OR "location track*" OR "mobile app*" OR phone OR phones OR phonecall* OR photo OR photos OR photograph* OR screenlogger* OR "screen recorder" OR "smart home*" OR "social media" OR "social network*" OR technolog* OR telephone* OR "text messag*" OR "tracking device*" OR "video record*" OR "web traffic" OR wifi OR wireless OR "artificial intelligence" OR AI OR online OR ICT OR "data mining"	266,891	
3	TI/AB "surveillance systems" OR dominance OR punishment OR surveillance OR stalking OR harassment OR threats OR coercion OR coercive OR control* OR intimidat* OR monitor* OR punish*	260,745	
4	2 AND 3	39,824	
5	TI/AB cyberstalking OR cyberviolence OR doxing OR doxxing OR "revenge porn*" OR sextortion OR spyware OR "surveillance app*" OR "tech abuse" OR "cyberdating violence" OR "cyber harassment" OR cyber-victimization OR "technology mediated" OR "technology based" OR "technology facilitated" OR "technological coercive control" OR "technology control" OR "technological abuse" OR "technological violence" OR "digital violence" OR "digital abuse" OR "digital control" OR "digital coercive control" OR "cyber abuse" OR "cyber control" OR "cyber coercive control" OR "cyber assault" OR "digital assault" OR "digital harassment" OR deepfake* OR online NEAR/3 violence OR online NEAR/3 abuse OR online NEAR/3 abuser	1,704	
6	4 OR 5	41,036	
7	1 AND 6	3,475	
8	"literature review*" OR "review of literature" OR "systematic review*" OR "research review*" OR "scoping review*" OR "rapid review*" OR "mapping review" OR "umbrella review*" OR "meta-analy*" OR metaanaly* OR "research synthesis" OR "comprehensive review*" OR "narrative review*" OR "meta-synthesis" OR "bibliometric analys*"	47,875	
9	7 AND 8	119	
10	Filter: Peer review	76	
11	Filter: 2019-2025	50	

6. Web of Science

Datum för sökning: 2025-06-18		Ämnesområde: Bred databas inom flertalet ämnesområden, citeringsdatabas	
Antal träffar: 615			
Search no	Search terms	Results	Comments
1	TI/AB "abused women" OR "battered females" OR "battered women" OR "abused females" OR "gender* violence" OR "genderbased violence" OR "gender-based violence" OR "gender related violence" OR "emotional abuse" OR "emotional violence" OR honor OR honour OR oppression OR prostitut* OR "sexual abuse" OR "sex crime" OR "sex work*" OR "sexual assault" OR "sexual harassment" OR "sexual violence" OR "social control" OR "subjected to violence" OR trafficking OR "violence against women" OR "violence towards women" OR "victim of abuse" OR "victim of violence" OR "women abuse" OR "women violence" OR "sexual exploitation" OR misogyny OR grooming OR pornograph* OR incel*	659,689	
2	TI/AB android* OR "audio record*" OR camera* OR cellphone* OR computer* OR cyber OR digital* OR electronic OR email OR "e mail" OR gps OR "global positioning system*" OR internet OR iot OR keylogger* OR "location track*" OR "mobile app*" OR phone OR phones OR phonecall* OR photo OR photos OR photograph* OR screenlogger* OR "screen recorder" OR "smart home*" OR "social media" OR "social network*" OR technolog* OR telephone* OR "text messag*" OR "tracking device*" OR "video record*" OR "web traffic" OR wifi OR wireless OR "artificial intelligence" OR AI OR online OR ICT OR "data mining"	8,123,184	
3	TI/AB "surveillance systems" OR dominance OR punishment OR surveillance OR stalking OR harassment OR threats OR coercion OR coercive OR control* OR intimidat* OR monitor* OR punish*	11,386,724	
4	2 AND 3	1,634,036	
5	TI/AB cyberstalking OR cyberviolence OR doxing OR doxxing OR "revenge porn*" OR sextortion OR spyware OR "surveillance app*" OR "tech abuse" OR "cyberdating violence" OR "cyber harassment" OR cyber-victimization OR "technology mediated" OR "technology based" OR "technology facilitated" OR "technological coercive control" OR "technology control" OR "technological abuse" OR "technological violence" OR "digital violence" OR "digital abuse" OR "digital control" OR "digital coercive control" OR "cyber abuse" OR "cyber control" OR "cyber coercive	49,788	

	control" OR "cyber assault" OR "digital assault" OR "digital harassment" OR deepfake* OR online NEAR/3 violence OR online NEAR/3 abuse OR online NEAR/3 abuser		
6	4 OR 5	1,665,174	
7	1 AND 6	54,123	
8	"literature review*" OR "review of literature" OR "systematic review*" OR "research review*" OR "scoping review*" OR "rapid review*" OR "mapping review" OR "umbrella review*" OR "meta-analy*" OR metaanaly* OR "research synthesis" OR "comprehensive review*" OR "narrative review*" OR "meta-synthesis" OR "bibliometric analys*"	1,356,678	
9	7 AND 8	906	
10	Filter: Review article och Article	830	
11	Filter: 2019-2025	615	

BILAGA 3: INKLUSIONS- OCH EXKLUSIONSKRITERIER

Forskningsfråga/uppdrag:

Sammanställa och analysera litteratur gällande digitala och teknikbaserade dimensioner av våld med fokus på teknikens roll i våldsutövande och stödinsatser, inklusive generativ AI och Internet of things.

Inklusionskriterier:

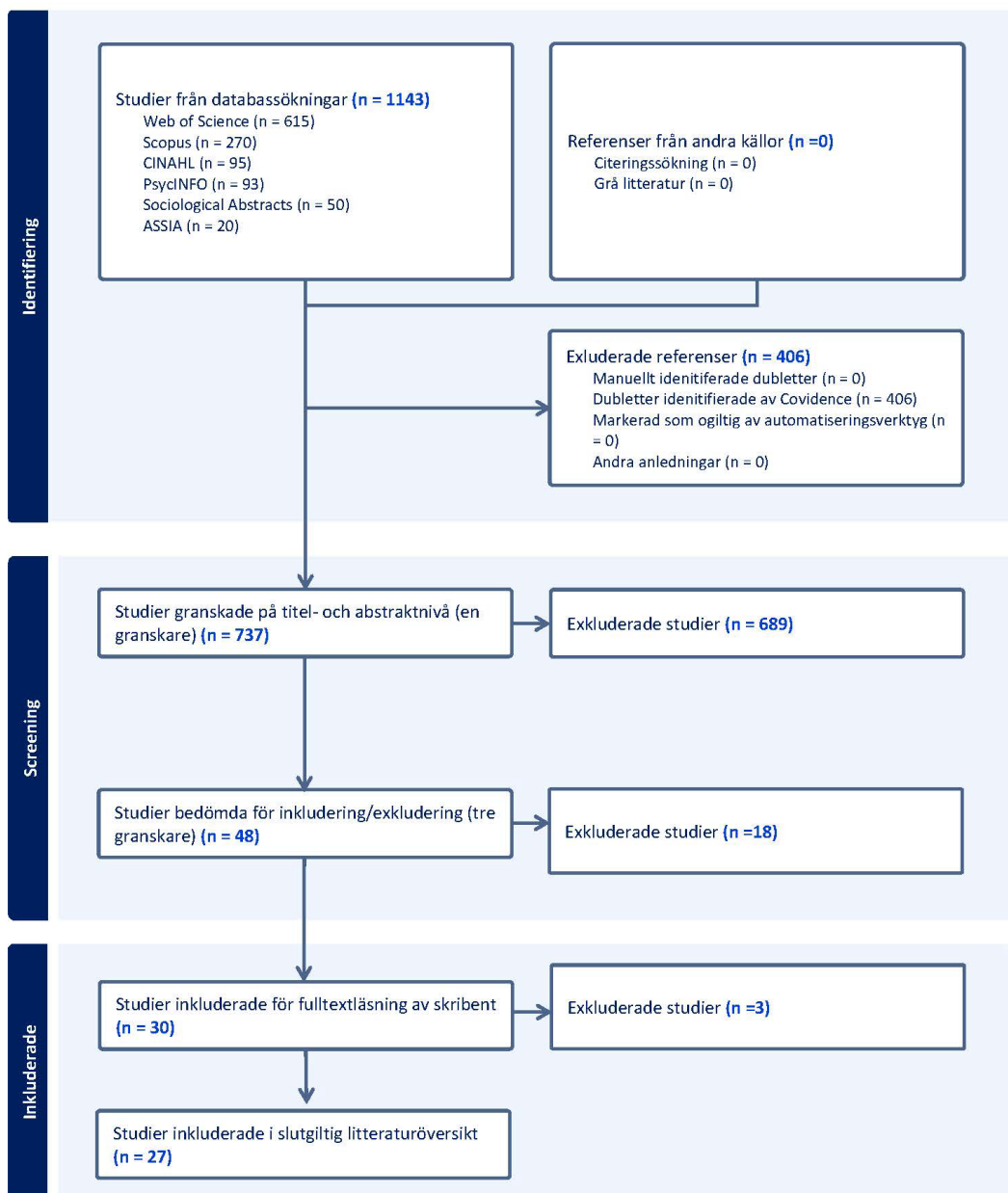
- Structured literature review (tillvägagångssätt beskrivet, sökord beskrivna)
- Publicerat från och med 2019
- Europa, Nordamerika, Australien och Nya Zeeland. Då dessa geografiska områden utgör sammanhang med liknande social och teknologisk utveckling och där barn därför har liknande tillgång till internet och därmed även till pornografi. Därför blir dessa sammanhang jämförbara men inte alltid direkt applicerbara den svenska kontexten.
- Engelska eller nordiska språk
- Teknikens roll i våldsutövande och skydd från våld
- Mäns våld mot kvinnor, könsbaserat våld, hedersrelaterat våld och förtryck, prostitution och människohandel, dating violence under 18 år
- Forskningsartiklar

Exklusionskriterier:

- #MeToo
- Covid 19
- Våld i nära relation (vuxna) (om ej även andra våldsformer)
- Cyberbullying (utan sexuell komponent)
- Treatment/interventions
- Prevalens/epidemiologi
- Inte digitalt våld (OBS innehållet i tex preventionsprogram behöver specifikt röra digitalt våld)
- Studier som i huvudsak eller uteslutande fokuserar på länder utanför Europa, Nordamerika, Australien och Nya Zeeland
- Bokkapitel

BILAGA 4: FLOWCHART

JÄMY - Teknologifaciliterat våld, reviews



19th June 2025





Jämställdhetsmyndigheten | Vikingsgatan 3, 411 04 Göteborg
031-3929000 | info@jamstalldhetsmyndigheten.se | jamstalldhetsmyndigheten.se