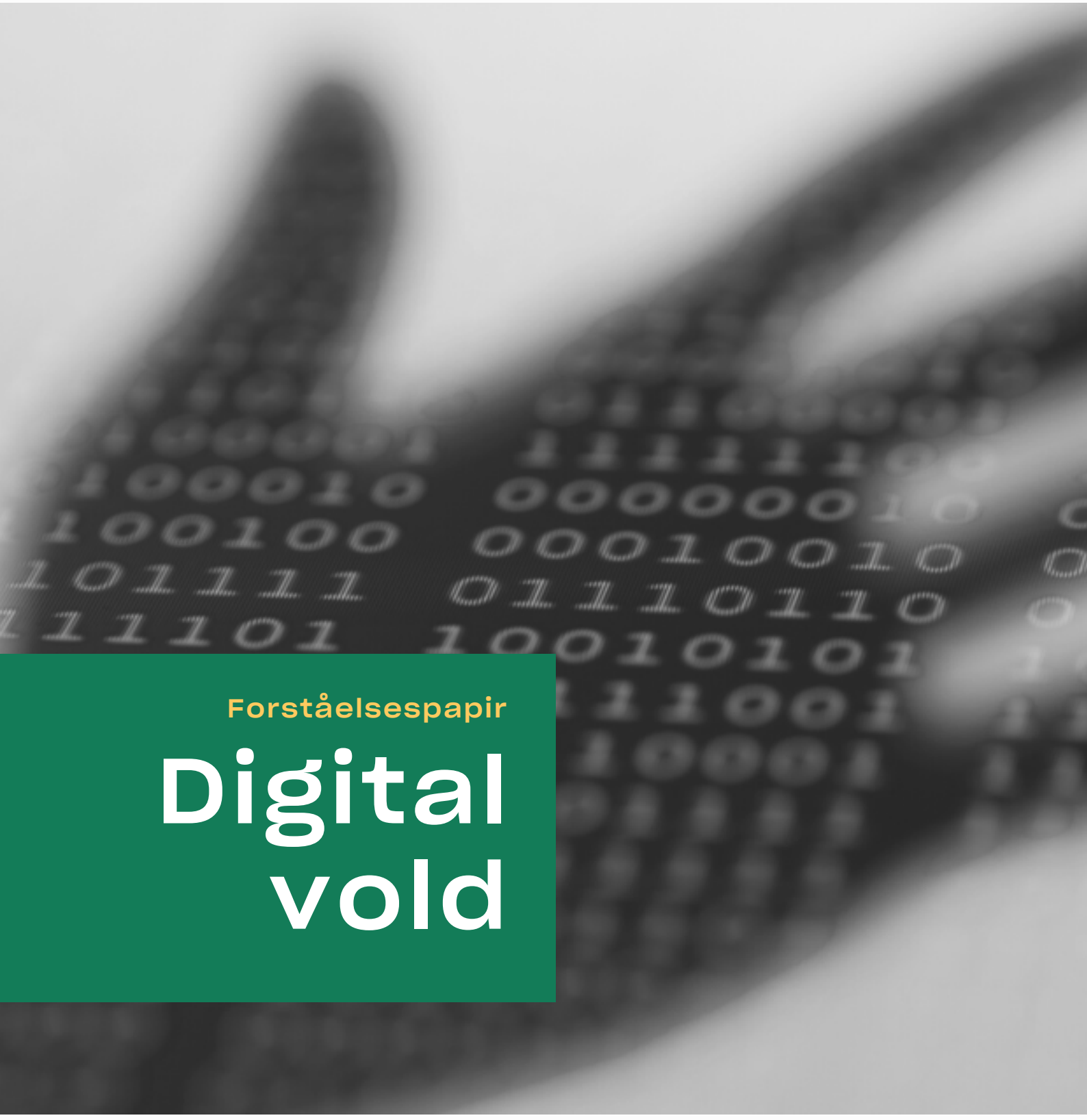
digitalt ansvar



Forståelsespapir

Digital vold

DIGITAL VOLD - FORSTÅELSESPAPIR

Udgivet af Digitalt Ansvar, februar 2022
Forståelsespapiret er udarbejdet i et samarbejde mellem Digitalt Ansvar, foreningens medlemsorganisationer og netværk, samt en redaktion bestående af følgende eksperter på det digitale og juridiske område:

Nell Rasmussen: Selvstændig juridisk konsulent og forfatter
Mie Oehlenschläger: Stifter af Tech & Childhood og ekstern lektor, New Media Studies
Signe Uldbjerg Mortensen: Ph.d. ved Aarhus Universitet
Trine Baumbach: Professor, Ph.d. hos det Juridiske Fakultet, Københavns Universitet

Ansvarlige, Digitalt Ansvar: Andrea Nielsen, Ask Hesby Krogh og Miriam Michaelsen

Projektet er muliggjort gennem støtte fra Oak Foundation Denmark. Fondens formål er at yde støtte til sociale indsatser og projekter i Danmark samt i Grønland og på Færøerne.

Digitalt Ansvar
Rigensgade 5, kl.
1316 København K
www.digitaltansvar.dk

Definition af digital vold

Digital vold er digitale handlinger, der er egnede til at skade en person psykisk eller krænke dennes privatliv gennem nedværdigende, forulempende eller krænkende adfærd.

En "digital handling" er en handling, der udføres ved brug af et digitalt medie eller teknologi som f.eks. en computer, tablet, GPS eller telefon.

Privatliv skal forstås i overensstemmelse med begrebet "familie- og privatliv" som defineret i artikel 8 i Den Europæiske Menneske-rettighedskonvention (1). Privatlivet omfatter således også en persons omdømme og arbejdsliv (2).

Introduktion

Ny teknologi, sociale medier og et internet, der aldrig sover, påvirker vores privatliv og arbejdsliv og udvider det offentlige rum med en digital dimension. Denne favre “nye” verden byder på muligheder, men skaber også udfordringer. Nye former for personrettede angreb og krænkelser er vokset frem i ly af en lovgivning, håndhævelse og forebyggelse, der halter efter. Konsekvensen er ofre og pårørende, der oplever at de rettigheder og beskyttelse, som de har i den fysiske verden, ikke er til stede i den digitale.

I dag findes der ikke én samlet definition for disse former for personrettede digitale overgreb og krænkelser. Der eksisterer enkelte definitioner, som favner nogle, men ikke alle typer handlinger. Digital kriminalitet, der alene har et økonomisk sigte – f.eks. misbrug af NemID – betegnes i dag som "økonomisk it-kriminalitet". Definitionen økonomisk it-kriminalitet skaber en fast ramme for anmeldelser, registrering og strategisk kriminalitetsbekæmpelse (3).

Herudover anvendes begrebet ”digitale sexkrænkelser” i dag om en række forskellige it-relaterede krænkelser. Men der er ikke tale om en fast definition, og det seksuelle aspekt er langt fra til stede i alle typer af digitale krænkelser. Det seksuelle er således ikke en fællesnævner for sager om grooming, chikane, hurtcore, billedmanipulation, doxing, happy slapping mv. Fællesnævneren er derimod, at handlingerne er egnede til at forvolde psykisk skade eller krænke den forurettede.

"Digital vold” anvendes i stigende grad i Danmark og udlandet som et nyt begreb, men det uden at der eksisterer en fast vedtaget definition, selvom det bl.a. er blevet efterspurgt af Nordisk Ministerråd og EU. Uden en fælles definition af digital vold er vejen til en effektiv forebyggelse, håndhævelse og tidssvarende lovgivning svær at finde. Fagfolk, myndigheder og lovgivere har brug for en fælles forståelse af hvilke digitale handlinger, der anses som skadelige, for at kunne kortlægge negative følger af disse krænkelser, skabe forebyggelse og vurdere behovet for lovændringer.

Derfor har Digitalt Ansvar sammen med vores medlemmer, organisationer og fagpersoner udarbejdet en definition af begrebet ”digital vold” samt principper og anbefalinger, der skal bidrage til en mere tidssvarende og effektiv beskyttelse mod digital vold.

Vi mener, at der er behov for at lovgivningen, politiets indsats og det forebyggende arbejde i højere grad tilpasses den digitale udvikling. Vores håb er, at en definition vil skabe et fælles sprog hos myndigheder, organisationer, forskere, ofre og pårørende, som kan bane vejen for bedre forebyggelse og retshåndhævelse. Det skal i sidste ende betyde, at færre udsættes for digital vold.

Handlinger, følger og værdigrundlag

Ved udarbejdelse af definitionen er der taget udgangspunkt i personrettede handlinger, der forvolder skade mod noget, som har et værdigt beskyttelsesbehov.

Digital vold kan – ligesom psykisk og fysisk vold – have alvorlige følger for offeret. Digital vold er egnet til at nedbryde offerets identitet, selvværd og selvtillid, og kan føre til forskellige skader hos offeret. Det er ikke en betingelse, at den digital vold konkret har krænket offeret, men at handlingen er egnet til det, på samme måde som det er tilfældet med formuleringen i f.eks. straffelovens § 266 om trusler.

Digital vold kan bl.a. have følgende konsekvenser:

- Psykiske konsekvenser – herunder stress, angst, selvmordstanker og PTSD
- Fysiske konsekvenser – herunder sygdom og andre psykosomatiske konsekvenser
- Seksuel mistrivsel – herunder seksuel ufrihed, angst og brud i parforhold
- Sociale følger – herunder mistillid til andre mennesker, frygt for omgivelserne, isolation og flytning
- Økonomiske følger – herunder udgifter til advokatbistand og psykologbehandling
- Familiemæssige følger – herunder dårlig trivsel og opbrud i familien
- Arbejds- og uddannelsesmæssige følger – herunder dårligt arbejdsmiljø, sygemeldinger og skolevægring
- Samfundsmæssige følger – herunder økonomiske, sociale og demokratiske

Digital vold påvirker desuden deltagelsen i den offentlige debat. Politikere, meningsdannere og borgere trækker sig fra den offentlige debat af frygt for repressalier. I Digitalt Ansvars undersøgelse fra 2020 oplyste hver femte voksne dansker, der er på nettet, at de afholder sig fra at deltage i den offentlige debat af frygt for trusler, chikane eller hadefulde kommentarer (Digitalt Ansvar 2020).

Bekæmpelsen af digital vold skal således både beskytte den enkeltes privatliv samt den offentlige debat. Beskyttelsen af privatlivet og af den offentlig debat er værdier, der allerede har stort fokus i det fysiske rum.

Det, der er er beskyttet i det fysiske rum, samt de værdier, der ligger til grund herfor (f.eks. beskyttelsen mod vold og retten til privatliv) bør være pejlemærket for kategorisering af nye former for skadelige, digitale handlinger. Definitionen af digital vold indeholder således ikke en fast liste over handlinger, men må forventes at blive udvidet i takt med den digitale udvikling, hvor der kontinuerligt opstår nye problemstillinger.

Værdigrundlaget bygger på EU-retten og de menneskeretlige konventioner, der forpligter staten til at beskytte borgerne mod vold og krænkelser af privatlivet (4).

Er der behov for kriminalisering?

Vores definition af digital vold omfatter en lang række digitale handlinger, hvoraf nogle allerede er kriminaliseret i straffeloven (5). Som eksempel kan nævnes deling af seksuelt overgrebsmateriale af børn (strfl. § 235) og ulovlig billeddeling (strl. § 264 d).

Definitionen omfatter imidlertid også andre former for digital vold, der ikke er kriminaliseret. Det bør overvejes at kriminalisere nogle af disse former for digitale handlinger, mens der er andre, hvor en kriminalisering ikke er hensigtsmæssig. Disse digitale handlinger kan dog alle opleves som krænkende, intimiderende eller have skadelige følgevirkninger. Digital selvskade er et eksempel på digital vold, som ikke er kriminaliseret, men som bl.a. kan have meget alvorlige følgevirkninger. Som et andet eksempel på digital vold er identitetsmisbrug (f.eks. ved at oprette falske profiler på internettet), der i dag alene er kriminaliseret, hvis det har et økonomisk sigte, men som regeringen har fremsat lovforslag om at kriminalisere.

Formålet med definitionen af digital vold er ikke nødvendigvis en kriminalisering af alle de digitale handlinger, den kan dække over. Definitionen skal dog gerne kunne bruges til at vurdere, om der er behov for yderligere kriminalisering, lovændringer og tiltag for at forebygge digital vold – både strafbar digital vold og digital vold, der ikke er strafbar, men stadig skadelig.

Principper og anbefalinger

Arbejdsgruppen ønsker at udpege en række principper og anbefalinger til alle aktører i Danmark, der kan gøre en forskel for ofre for digital vold. Principperne er overordnede og almengyldige, imens anbefalingerne er konkrete og målbare.

Princip	Anbefaling
1. HJÆLP TIL OFRE: Alle – uanset alder, køn, handicap, etnisk oprindelse, religion eller tro, seksuel orientering, politisk anskuelse, eller social oprindelse – skal have mulighed for gratis hjælp indenfor 24 timer, hvis de udsættes for digital vold.	**A)** Ofre for strafbar digital vold skal kunne anmelde online på politi.dk **B)** Rigspolitiet skal sikre, at det eksisterende "Single Point of Contact (SPOC)" fremadrettet behandler alle anmeldelser om digital vold og sikrer, at alle henvendelser bliver vurderet hurtigt, så sagsbehandlingen i kritiske sager kan igangsættes indenfor 24 timer. **C)** Rigspolitiet skal koordinere indsatsen imellem NSK, PET, Digitaliseringsstyrelsen, samt andre relevante aktører mhp. at sikre den rette og rettidige indsats ifm. tværgående sager relateret til digital vold, herunder monitorering af ny udvikling.
2. LOVGIVNING: Danmark skal have en lovgivning, der tager hånd om digitaliser-ingens konsekvenser, og som samtidig lever op til internationale konventioner og forpligtelser.	**A)** Regeringen skal fremsætte lovforslag, der pålægger sociale medier at fjerne indhold, der er ulovligt efter straffeloven, hvis de modtager en underretning herom, eller selv opdager det, indenfor følgende tidsfrister: 1. 24 timer for deling af åbentlyst ulovligt indhold. (F.eks. § 114 c-f, § 235, § 264 a og d). 2. Syv dages for andet indhold, der er strafbart efter dansk ret. Lovgivning skal endvidere sikre, at det er nemt og tilgængeligt for alle at indberette ulovligt indhold på sociale medier. **B)** Regeringen skal indføre krav om at sociale medier, foruden at blokere adgangen til ulovligt billed- og videomateriale, også skal forhindre, at det samme indhold genuploades og spredes på tværs af deres tjenester (notice and stay down).

	C) Regeringen skal gennem lovgivning tydeliggøre, hvilket ansvar aktører med mange følgere (bloggere, influencere og deres kommercielle samarbejdspartnere mv.) har på sociale medier. Derudover hvilke sanktioner, der gælder, hvis disse aktører ikke lever op til deres ansvar. **D)** Regeringen skal udarbejde lovgivning, der pålægger sociale medier og hjemmesider med mere end 30.000 brugere pligt til at aldersverificere nye brugere. **E)** Regeringen skal udarbejde lovgivning, der pålægger sociale medier med mere end 30.000 brugere årligt, at indsende en oversigt over antallet af klager over ulovligt indhold fra brugere til en kontrolinstans. Oversigten skal bl.a. indeholde: 1. Tidspunkt for klagen. 2. Oplysninger om klagens indhold. 3. Udfaldet af klagen, herunder tidspunktet for evt. fjernelse af indholdet
3. INFRASTRUKTUR: Danmark skal have en infrastruktur, der både kan håndtere ofre for digital vold og gerningspersoner hurtigt, sikkert og effektivt.	**A)** Regeringen skal oprette en tilsynsmyndighed, der skal føre tilsyn med hvorvidt sociale medier i tilstrækkelig grad beskytter deres brugere mod ulovligt indhold. **B)** Regeringen skal sikre, at ofre for digital vold har adgang til rådgivning i Danmark på tværs af alders- og målgrupper, og offertilbuddene har ressourcer til at løfte opgaven.
4. DIGITALE TJENESTER: Digitale tjenester, der faciliterer brugergenereret indhold og kommunikation, skal påtage sig ansvar ift. aktivt at forebygge digital vold.	**A)** Sociale medier og andre digitale services, f.eks. online spiludbydere, bør ikke anvende algoritmer, som forstærker spredningen af voldeligt, seksuelt krænkende og farligt indhold. Herudover bør de regelmæssigt offentligt dokumentere, hvad de gør for at undgå spredning. **B)** Alle virksomheder, der producerer ny teknologi målrettet private brugere, især børn og unge, skal offentliggøre en risikovurdering af, hvorvidt teknologien kan misbruges til digital vold. **C)** Sociale medier pålægges, at nye brugerprofiler (under 18 år) automatisk er indstillet således, at privatindstillinger er mest restriktive (f.eks privat profil, hvor kun venner kan kontakte bruegren.).

5. VIDEN OG FOREBYGGELSE: Myndigheder, organisationer og forskere skal have et fælles vidensgrundlag om digital vold i arbejdet med at forebygge, rådgive og retsforfølge.	**A)** Rigspolitiet skal inddrage og koordinere med civil-samfundsaktører mhp. at sikre viden om digital vold og nye tendenser. **B)** Rigspolitiet skal sikre, at journalkoder og emneord dækker digital vold. **C)** Anklagemyndigheden udarbejder en årlig oversigt over antallet af straffesager om digital vold, sagsbehandlingstiden, antallet af henlæggelser og væsentligste begrundelser for henlæggelser.

Noter

1. Den Europæiske menneskerettighedskonvention, Afsnit 1, Artikel 8: "Ret til respekt for privatliv og familieliv. 1. Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance. 2. Ingen offentlig myndighed kan gøre indgreb i udøvelsen af denne ret, undtagen for så vidt det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at forebygge uro eller forbrydelse, for at beskytte sundheden eller sædeligheden eller for at beskytte andres ret og frihed. **Find her.**
2. Deling af seksuelt overgrebsmateriale af børn og intime billeder uden samtykke er eksempler på privatlivskrænkelser.
3. Ofre for digital vold kan også være udsat for andre former for vold. Der vil ofte være sammenfald med andre voldsformer, som ikke beskrives i dette forståelsespapir. Eksempelvis fysisk, psykisk, materiel, økonomisk vold, seksualiseret vold og voldtægt samt stalking). Se eksempelvis Lev Uden Volds **definitioner her.**
4. Eksempelvis den Europæiske Menneskerettighedskonvention, Artikel 8, om ret til respekt for privatliv og familieliv, Børnekonventionen, Istanbulkonventionen og Den Europæiske Unions charter om grundlæggende rettigheder. Se note 1.
5. F.eks. § 232 - blufærdighedskrænkelser, § 235 - overgrebsmateriale af børn, § 263 - uberettiget adgang til IT-systemer, § 264 d - deling af billeder eller private følsomme oplysninger uden samtykke, eller § 267 - injurier.

Definitionen af digital vold støttes af:

DareGender

BØRNS VILKÅR
SAMMEN STOPPER VI SVIGT

Lev ~~uden vold~~

CfDP
Center for Digital Pædagogik

Dansk Stalking Center

LOKK
LANDSORGANISATION AF KVINDEKRISECENTRE

JOAN-SØSTRENE

MEDIESUNDHED
for børn og unge

Dansk Kvindesamfunds Krisecentre

SØSTRE
MOD VOLD OG KONTROL

OfferRådgivningen Danmark

SEX SAMFUND

SSP SAMRÅDET

Red Barnet

digitalt
ansvar