digitalt ansvar

Digital vold i Danmark

Anden del: Nye former for afpresning

Digital vold - delrapport om digital afpresning 2023

Udgivet af Digitalt Ansvar, september 2023

Ansvarshavende redaktør: Ask Hesby Krogh
Redigering: Anne Tscherning Larsen og Ask Hesby Krogh
Tekst og analyse: Anne Tscherning Larsen, Ask Hesby Krogh, Asta Iris Rohde, Mie Oehlenschläger og Nell Rasmussen.
Forsidefoto er genereret med Stable Diffusion.

ISBN 978-87-974415-1-0

Projektet er muliggjort af støtte fra Oak Foundation Denmark samt midler fra finansloven.

Digitalt Ansvar
Rigensgade 5, kl.
1316 København K

www.digitaltansvar.dk

Kapitler

Introduktion

Ny teknologi og nye medier har givet os nye muligheder for at få information og komme i kontakt med andre let, hurtigt og gratis. Men med udviklingen er der også opstået nye muligheder for at forvolde andre eller sig selv skade.

Det, der foregår digitalt, kan have alvorlige konsekvenser for offerets privatliv, psyke og omdømme. På trods af dette er lovgivning, håndhævelse og forebyggelse ikke fulgt med udviklingen af skadelige handlinger. Dette skyldes blandt andet , at den digitale udvikling er gået så stærkt, at vores viden om digital grooming, manipulation, krænkelser, had, chikane mv. er begrænset, og vi derfor ikke har udviklet en fælles forståelse og sprog for disse nye former for digitale skadelige handlinger og den digitale vold.

Der er således behov for en fælles forståelse og et kritisk blik på, om beskyttelsen af vores integritet, privatliv og omdømme er fulgt med den digitale udvikling. For lovgivning og de internationale konventioner, der skal beskytte os mod vold, bør også gælde for den vold og skade, som foregår og opstår på internettet.

For at skabe fælles forståelse og udgangspunkt har Digitalt Ansvar i samarbejde med eksperter, forskere og organisationer udarbejdet en definition af digital vold. Med dette arbejde tager Digitalt Ansvar desuden tråden op fra institutioner som UNICEF, Det Europæiske Institut for Ligestilling og Nordisk Ministerråd, som alle har efterspurgt en klar definition af digital vold.

Definitionen af digital vold lægger vægt på det skadelige ved handlingerne frem for motivet alene. Den rummer både ulovlige og ikke-ulovlige skadelige handlinger og er dermed bredere end en juridisk definition af, hvad der i dag er ulovligt. Dertil er det ikke en forudsætning, at der er tale om en gerningsperson i kød og blod. For virkeligheden er den, at teknologi som fx algoritmer og kunstig intelligens (AI) i dag er med til at forårsage og forstærke det skadelige og voldelige, vi ser på nettet, og som griber ind i det omgivende samfund.

Nærværende rapport er anden i rækken om digital vold. Hvor første rapport stillede skarpt på digital selvskade, fokuserer denne på digital afpresning.

Digital afpresning

Afpresning dækker over det, at en eller flere personer truer nogen med formålet om at opnå en gevinst. I denne rapport medtages sager om afpresning, hvor gerningspersonens gevinst kan være både økonomisk, seksuel eller af anden karakter.

Digital afpresning er, når digitale medier, -tjenester og -teknologi benyttes af en gerningsperson til at afpresse et offer. Det er en underkategori til digital vold, da truslerne har konsekvenser for offerets psykisk og kan have store konsekvenser for ofrenes privatliv og omdømme.

Rapporten bygger på tre spørgeskemaundersøgelser, som henholdsvis Epinion og Voxmeter har udført for Digitalt

Ansvar i 2020-2023, hvor voksne har oplyst, om de har været udsat for digital afpresning. Derudover bygger undersøgelsen på oplysninger fra Danmarks Statistik samt Rigspolitiet om antal og udvikling i antal anmeldelser.

I perioden 2020-2023 svarer 5% af voksne danskere, der bruger internettet minimum en gang om ugen, at de har været udsat for digital afpresning indenfor de seneste 12 måneder.

Udvider man tidshorisonten og ser på anmeldelser af afpresningssager i alt – det vil sige ikke kun digitalt – ser vi en kraftig vækst i antal anmeldelser fra cirka 2016 jævnfør tal fra Danmarks Statistik. Fra 2016 til 2022 er antallet af anmeldelser af afpresning og åger steget med hele 400%. Trods den store stigning i anmeldelser, ser det dog endnu ud til, at der er et stort mørketal, når tal for anmeldelser sammenholdes med tallet for, hvor mange der oplyser, at de har været udsat for afpresning.

Med digitale medier og tjenesters indtog i vores liv de sidste 10-15 år er der kommet nye muligheder for at udføre afpresning. Kommer en gerningsperson i besiddelse af følsomt eller privat indhold eller oplysninger, kan det udnyttes til at true et offer med deling, hvis ikke kravet om penge, modydelser eller yderligere privat indhold opfyldes.

De seneste år og især siden 2022 er digitale værktøjer, der benytter sig af kunstig intelligens (AI) – såkaldt generativ AI, blevet tilgængelige for alle forbrugere. Det har medført nye muligheder for lave kunst, markedsføring med videre, men også kriminalitet. Billedgenereringsværktøjer kan benyttes til at skabe kunstigt kompromitterende materiale og meget virkelighedstro, falske identiteter. Stemmeværktøjer kan benyttes til identitetsmisbrug, og med de avancerede chatbots som ChatGPT er det blevet nemmere at generere effektive trusselsmails på flere sprog.

Digital afpresning i tal

5%

Af voksne danskere, der er på nettet minimum én gang ugentligt, har været udsat for afpresning digitalt i løbet af det seneste år. Sådan har billedet set ud i 2020, 2022 og 2023.

Omregnet til danskere svarer det til i omegnen af **234.000** voksne danskere.

Andel af voksne danskere, der min. er på nettet én gang om ugen, som indenfor det seneste år har været udsat for afpresning:

2020	2022	2023
4,7%	5,4%	5,1%

Epinion 2020, Epinion 2022, Voxmeter 2023.

400%
er anmeldelser af afpresning og åger steget fra 2016 til 2022

200%
er antallet af ofre i sager om ulovlig tvang steget fra 2016 til 2022

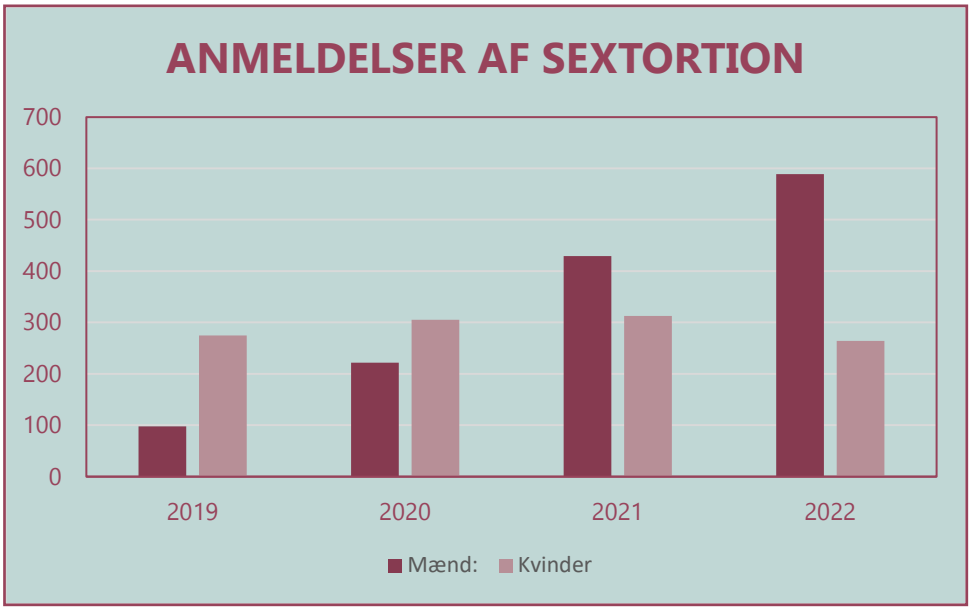
130%

Fra 2019 til 2022 er antallet af anmeldelser af sextortion steget fra 374 til 855. Det svarer til en stigning på 130%.

Generelt tegner der sig et billede af, at **der er en overvægt af mænd, som er ofre for afpresning**.

Hvor anmeldelser af sextortion mod kvinder er stagneret, er anmeldelser af sextortion med mandligt offer vokset fra 98 sager i 2019 til 589 sager i 2022.

Andelen af mænd, der indenfor det seneste år har været udsat for digital afpresning, er i både 2020, 2022 og 2023 højere end andelen af kvinder, der indenfor det seneste år har været udsat for digital afpresning.



Rigspolitiet for Politiken

Andel af voksne danskere fordelt på køn, der min. er på nettet én gang om ugen, som indenfor det seneste år har været udsat for digital afpresning:

	2020	2022	2023
Andel af mænd i alt	**7,3%**	**5,9%**	**6,2%**
Andel af kvinder i alt	**2,3%**	**4,9%**	**3,8%**

Epinion 2020, Epinion 2022, Voxmeter 2023.

Digital vold


digitalt
ansvar

1

Hvad er digital vold?

Smartphones, digitale medier, AI-chatbots, deep fake-teknologier og et internet, der aldrig sover, betyder, at det er blevet gratis, let og hurtigt at komme i kontakt med andre samt skabe og dele information. Men med udviklingen af nye teknologier og medier er der også opstået nye muligheder for at skade andre og sig selv. Nye former for personrettede angreb og krænkelser er vokset frem i ly af den situation, at lovgivning, håndhævelse og forebyggelsehalter bagefter.

Hidtil har en stor del af samtalen om skadelige digitale handlinger drejet sig om digital kriminalitet, hvor motivet er økonomisk vinding, som fx misbrug af NemID. Men mange af de skadelige digitale handlinger drejer sig ikke primært om økonomi. De rammer derimod individers integritet, privatliv og omdømme og har tydelige personlige og psykiske konsekvenser. Disse handlinger har der ikke været et samlet ord for eller definition af.

Det handler ikke kun om hævn, porno og hård tone

I Danmark blev mange først bekendt med skadelige digitale handlinger gennem begrebet "hævnporno" og debatten om "den hårde tone" og den "hadefulde debat" i midten af 2010'erne. Men "hævnporno" er som begreb ikke særligt dækkende, da hævn ikke altid er et motiv, og ordet kun dækker ulovlig billeddeling. Ligeledes er "tonen" hverken dækkende eller et særligt præcist begreb, da det som udgangspunkt kun handler om sprog i debatter og synes at dække alt fra dødstrusler til vulgært sprogbrug.

Definition skal hjælpe ofre

For at få et fælles sprog og forståelse for de skadelige fænomener via digitale medier og teknologier, har Digitalt Ansvar i samarbejde med medlemmer, organisationer og fagpersoner udarbejdet en fælles definition for digital vold. Dette arbejde er i tråd med anbefalinger fra UNICEF, Det Europæiske Institut for Ligestilling og Nordisk Ministerråd, som alle efterspørger en klar definition af digital vold.[1]

Formålet med definitionen er at bidrage til en mere tidssvarende og effektiv beskyttelse mod digital vold. Hvis ikke myndigheder, forskere, politikere og borgerne har et fælles sprog, bliver det svært at skabe en sammenhængende strategi for at hjælpe ofre og forebygge. For hvordan skal vi forebygge og bekæmpe noget, som vi ikke er enige om, hvad er?

Begrebet vold følger med tiden

Fra at vold udelukkende drejede sig om fysisk vold, er voldsbegrebet i dag udvidet til at dække handlinger, der er skadelige i fx et psykisk, seksuelt eller økonomisk perspektiv. Digital vold ligger i forlængelse af og er ofte forbundet med forskellige former for vold i den fysiske verden, især psykisk vold. Hvor fysisk vold har været kriminaliseret i århundreder, blev psykisk vold først strafbart i 2019.

Digital vold kan – ligesom andre former for vold – have alvorlige følger for offeret. Digital vold er egnet til at nedbryde offerets identitet, selvværd og selvtillid, og kan føre til forskellige psykiske mén og skader hos offeret. Det er dog ikke en betingelse, at digital vold konkret har krænket offeret, men at handlingen er egnet til det.

Ofte har digital vold også konsekvenser for offerets mulighed for at navigere i en digitaliseret verden. Det kan opstå, når ofre udelukkes af deres hackede profiler, eller gerningspersoner chikanerer ofre i en sådan grad, at de føler sig tvunget til at forlade fora, sociale medier eller lignende, som ellers var rammesættende for deres daglige liv.

Definitionen af digital vold er udarbejdet af Digitalt Ansvar i samarbejde med foreningens medlemsorganisationer og netværk samt en redaktion bestående af:

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

Definitionen af digital vold støttes indtil videre af Børns Vilkår, DareGender, Lev uden vold, Center for Digital Pædagogik, Dansk Stalking Center, Landsorganisationen for Kvindekrisecentre, Joan-Søstrene, Mediesundhed for Børn og Unge, Dansk Kvindesamfunds Krisecentre, Søstre mod Vold og Kontrol, Offerrådgivningen, Sex & Samfund, SSP-samrådet og Red Barnet.

Definition

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 Menneskerettighedskonvention[2]. Privatlivet omfatter således også en persons omdømme og arbejdsliv[3].

Fokus på det skadelige mere end motivet

Inkluderer både det ulovlige og det ikke-ulovlige

Teknologi kan også være en aktør

Digital vold rammer vores privatliv

Hver dag skabes et hav af oplysninger om os, og mange er tilgængelige online. Virksomheder, arbejdsgivere, det offentlige og andre borgere har i stigende grad adgang til mere eller mindre privat information om os. Vores privatliv, familieliv og arbejdsliv bliver i dag dokumenteret og monitoreret af os selv og andre i en grad, som få årtier tilbage ville blive anset for utænkeligt. Vores liv er blevet digitalt, og privatlivet er ikke længere forbeholdt vores hjem og vores individuelle kommunikation.

Data og viden kan bruges af os og andre til gøre livet nemmere, mere bekvemt, forme gode, sunde relationer og hjælpe os med andre selvvalgte ønsker. Gamle venner kan holde kontakt. Man kan finde en kæreste via nettet, og information er altid tilgængeligt og lige ved hånden. Der er dog også bagsider ved denne grænseløse datagenerering og -deling. De teknologiske muligheder giver hidtil usete muligheder for at misbruge og krænke vores integritet og det, vi oplever som privat.

Det er ikke længere kun en lille gruppe kendte, virksomhedsledere og politikere, der skal forholde sig til og bekymre sig om deres omdømme. Børn og unge vokser i dag op i en digital kultur, hvor blandt andet sociale medier danner rammen for, at deres person bliver vurderet konstant via likes, ratings, delinger, visninger med videre. Alle er blevet redaktører af deres eget omdømme, og hos mange er næste opslag, snap eller post hele tiden i tankerne.

Voksnes omdømme kan også rammes og blive skadet, fordi det er let, hurtigt og nemt at sprede urigtige og ærekrænkende oplysninger om andre til mange tusinde eller på anden måde hænge en person ud på nettet til offentligt skue. For 15 år siden var den offentlige gabestok forbeholdt de få, i dag kan alle ende i den digitale gabestok. Personer med minoritetsbaggrund ser ud til at være særligt udsatte[4], og det rammer både individers private og professionelle liv. En undersøgelse fra Digitalt Ansvar i 2021 viste fx, at hver tiende på det private arbejdsmarked har oplevet digital chikane fra eksterne som gæster og kunder, og 68 % af dem omhandlede løgne eller usande beskyldninger om dem.

Samtidige betyder udviklingen af kunstig intelligens (AI), at alle kan producere og sprede AI-genereret indhold om alle, kendte som almindelige mennesker, hvor man misbruger folks stemme eller ansigt. Det betyder, at vores ansigt, vores stemme – ja sågar vores tanker, har brug for en særlig beskyttelse.

I takt med disse nye digitale produkter, er der behov for en forstærket beskyttelse af vores integritet, privatliv og omdømme.

Teknologi har ændret volden

Digitale medier og tjenester giver mulighed for og opfordrer til at udbrede materiale hurtigt og gnidningsfrit, og de tilbyder let adgang til kontakt gennem mange kommunikationskanaler. Det betyder, at der i sagerne om digital vold både kan være mange gerningspersoner og mange ofre involveret. Ét offer kan blive udsat for forbrydelser fra en lang række gerningspersoner, som det skete i den såkaldte Umbrellasag, hvor 1100 personer blev retsforfulgt for at have delt krænkende materiale af en 15-årig pige[5]. Men også én gerningsperson kan have mulighed for at nå en lang række ofre, som var tilfældet i det, der er blevet omtalt "sagen om de 169 piger", hvor 169 piger blev udsat for blandt andet sextortion af én gerningsmand[6].

En særlig omstændighed ved digital vold er desuden, at det er et fænomen uafhængigt af aktør. Det vil sige, at volden ikke nødvendigvis er knyttet til gerningsperson. Volden kan også forekomme via en algoritme eller anden teknologi. Ved at løsne sammenhængen mellem vold og en gerningsperson, rummer begrebet også de skadelige

effekter, der opstår som konsekvens af teknologi og digitale tjenesters design, forretningsmodeller og effekt.

Det vil sige, at digitale tjenester og teknologi ikke bør anses som neutrale og passive, men i stedet som "performative" aktører, der kan påføre eller forværre skade. De er aktivt med til at forme fænomener og påvirke handlinger, der ikke ville kunne eksistere uden dem. Arkitekturen for de digitale tjenester kan altså i sig selv have utilsigtede og skadelige konsekvenser for brugerne[7].

Algoritmer prioriterer skadeligt indhold

Facebooks, TikToks og andre digitale medieplatformes indholdsstyring er udformet til at skabe gunstige betingelser for engagement. Det betyder, at de algoritmer, der udvælger indhold til for eksempel Facebook-brugeres feed, prioriterer indhold, som kan få os til at blive længere på mediet, klikke på mere indhold og se flere annoncer. Det er et kerneelement af virksomhedens forretningsmodel. Det kan imidlertid også virke forstærkende i forbindelse med digital vold.

Det har tidligere været afdækket, at indhold fra netmedier, der er kendt for at sprede misinformation om covid-19, er blevet vist langt oftere end opslag fra verdens førende sundhedsorganisationer[8], og at Facebooks algoritmer prioriterer hadefuldt og "kontroversielt" indhold og dermed giver skadelige opslag større eksponering og engagement[9]. På den måde kan deling af ulovligt eller skadende indhold accelereres og hjælpes på vej af de sociale mediers indholdsstyring.

Et andet eksempel på at teknologien er en aktør i sig selv, er anbefalingsalgoritmer, som fører til mere og mere ekstremt indhold. Som de fleste andre digitale tjenester er YouTube interesseret i at fastholde brugernes opmærksomhed længst muligt. Det har betydet, at YouTubes algoritme har anbefalet mere og mere ekstremt indhold til deres brugere. Den form for anbefalingsalgoritme medfører en risiko for radikalisering. Det oplevede amerikaneren Caleb Cain, som til New York Times fortalte, hvordan han oprindeligt gik på YouTube efter selvhjælpsvideoer, men oplevede at blive radikaliseret ind i et ekstremt højreorienteret univers. YouTube anbefalede ham gradvist mere og mere ekstreme, misogyne, racistiske videoer, der startede af sig selv, når den forrige video var set færdig.[10]

Push-beskeder spredte krænkende materiale

På det sociale medie Reddit foregår al deling af information i såkaldte subreddits, der er grupper dedikeret til et bestemt emne. I et subreddit kan mediets brugere diskutere eller dele opslag relateret til gruppens tema. Har et opslag fået særligt meget opmærksomhed, kan det via algoritmer blive sendt ud via push-beskeder, som Reddit bruger til at fange og fastholde brugernes opmærksomhed.

I 2021 kom det frem, at Reddits algoritmer havde været med til at udbrede kendskabet til et nøgenbillede af en 14-årig pige. Push-beskederne blev sendt ud til brugere, der ikke selv havde opsøgt den gruppe, hvori materialet blev spredt. Beskederne indeholdt blandt andet efterspørgsler på links til det ulovlige billede og gjorde brugerne opmærksomme på, at billedet eksisterede, og hvor det kunne findes. Reddits algoritmer kan altså i dette tilfælde anses som en aktør, der var med til at udøve digital vold mod flere ofre.[11]

Kunstig intelligens skaber nye, uoverskuelige udfordringer

Der har længe været forsket i og udviklet på kunstig intelligens (AI). Men området fik fornyet opmærksomhed og anvendelse i 2022, hvor Open AI gjorde deep-learning billedværktøjet Dall-E og chatbotten ChatGPT tilgængelige for den brede offentlighed.

I dag kan alle helt frit bruge AI til at generere indhold som tekst, billeder, videoer, musik mv. på et splitsekund. AI-programmer fungerer forskelligt afhængigt af, hvilken af disse slags indhold de genererer, men de har nogle ligheder. I alle tilfælde drejer det sig om, at brugerne kommer med opfordringer eller ideer, som de sender til AI-programmet, der derefter producerer indholdet ved at trække på de ofte massive datasæt, som de er blevet trænet i.

AI er således ikke forbeholdt forskningsverdenen, men allemandseje og det vurderes, at udviklingen af kunstig intelligens i øjeblikket sker eksponentielt. Den hastige udvikling, de massive investeringer fra tech-virksomhederne og det faktum, at AI er tilgængeligt for forbrugerne, betyder, at samfundet står overfor potentielt meget store forandringer.

Hvad angår kriminalitetsbilledet og den digitale vold, er udviklingen skræmmende. For hvor det for få år siden krævede it-ekspertise, stor computerkraft og tid at skabe tekst, lyd, video og billeder, som var virkelighedstro og menneskelig, kan generativ AI-produkter gøre det på sekunder for lægpersoner ved få kliks. Dermed forsvinder muligheden for at vurdere, hvad der er ægte, og hvad der er falsk. Det bliver svært at vurdere, hvorvidt folk giver sig ud for at være en anden eller en fiktiv person. Og samtidig kan dybt krænkende indhold produceres om alle, hvis billede eller stemme er til at finde på nettet. Det øger risikoen for chikane, afpresning, sextortion med videre.

Udviklingen af AI kommer til at ændre internettet, offentligheden og individers dagligdag og derfor bør der stilles krav til brugen af kunstig intelligens. Sociale mediers brug af relativt simple algoritmer, som anbefalingsalgoritmen, har allerede resulteret i store samfundsmæssige udfordringer som radikalisering, had, misinformation, udbredelse af ulovligt og skadeligt indhold og filterbobler. Med dette in mente er det afgørende, at mere avancerede teknologier som generativ AI, håndteres ud fra et forsigtighedsprincip, der tager højre for risici og bivirkninger, før de sættes på markedet.

Hvem har ansvaret for AI?

Med AI vil internettet ændre sig fra at bestå af brugergenereret indhold til at være en blanding mellem brugerindhold og AI-indhold. Spørgsmålet er, hvem der har ansvaret, hvis noget går galt, hvis nogen udsættes for AI-genereret digital vold. Hvis for eksempel selvskade resulterer i selvmord, og det kommer frem, at inspirationen til selvskaden med døden til følge kom fra AI-genererede svar og indhold. Er virksomheden bag AI-chatbotten så ansvarlig?

Spørgsmålet om, hvorvidt og i hvilken grad virksomhederne bag AI-produkter kan holdes ansvarlig for bi- og skadevirkninger er uafklaret, men særdeles relevant.

Spørgsmålet om ansvar berører flere regelsæt. Det er blandt andet regler om 'ophavsret' på den ene side og regler om 'digitale tjenester ansvar for brugerindhold på nettet' på den anden side. Dertil handler det om, hvornår straffelovens medvirkensbestemmelser kan finde anvendelse, og hvordan produktansvar skal omfatte AI.

Dette er i dag uklart. Et eksempel: Vi forestiller os, at en person efter dialog med en AI-chatbot tager sit eget liv. Familien lægger så sag an mod virksomheden bag chatbotten. Der kan tænkes to udfald:

1. Chatbotten som videreformidler. Hvis man vurderer, at chatbottens svar blot videreformidler eksisterende brugerindhold, er virksomheden ikke ansvarlig. EU-reglerne siger nemlig, at virksomheder på nettet ikke er ansvarlige for brugerindholdet på nettet. Her vil virksomheden til gengæld kunne få problemer, da det vil sige, at chatbotten de facto kvit og frit deler indhold, som andre faktisk har ophavsret til. Dermed vil AI-producenten måske have et muligt ophavsretsproblem.

2. Chatbotten som selvstændigt skabende. Hvis man derimod vurderer, at AI-chatbot-svar ikke bare er videreformidling, men skal forstås som nyt indhold, der skabes, vil virksomheden bag AI kunne gøres ansvarlige for indholdet. EU-reglerne fraskriver virksomheder ansvar for brugerindhold, ikke indhold digitale tjenester selv skaber og formidler.

EU's regler giver med andre ord kun juridisk helle, når der er tale om brugergenereret indhold. Ikke indhold, som digitale tjenester selv producerer og formidler. Hvis det juridiske helle forsvinder, vil straffeloven og anden lovgivning gælde og virksomheden bag et AI-produkt vil måske kunne holdes ansvarlig ift. produktansvar, medvirkensansvar og lignende regler.

Beskyttelse mod digital vold er ikke tilstrækkelig

Digitaliseringen af vores liv og samfund er gået så hurtigt, at loven, håndhævelsen og forebyggelsen ikke er fulgt med. En stor del af de skadelige handlinger online kender vi til i forvejen. De kræver justeringer i straffeloven og håndhævelse af de regler, som gælder på nettet, men ikke nye juridiske greb. Det er fx tilfældet med ulovlig billeddeling (straffelovens § 264 d) eller digitale trusler (straffelovens § 266).

Andre skadelige handlinger er mindre velkendte og har skabt et nyt behov for beskyttelse. Det kan fx være misbrug af andres identitet. Førhen var det vanskeligere at udgive sig for at være en anden – det krævede et større setup med måske en paryk og medsammensvorne. I dag er det derimod meget nemt med en falsk social medie-profil, som giver mulighed for at få kontakt med andre på falske præmisser digitalt.

Straffeloven og kriminalisering er dog ikke svaret på alle udfordringer med digital vold. Digital vold omfatter også vold, der ikke er kriminaliseret, og hvor straf kan virke uhensigtsmæssig. Eksempelvis digital selvskade, hvor en person udøver fysisk selvskade og deler billeder af skaderne i grupper på sociale medier. Det har tydelige, mærkbare skadevirkninger for andre, som kan påvirkes til at udføre selvskade. Det taler for at kriminalisere indholdet, så det medvirker ikke til at øge selvskaden. Derimod virker det ulogisk at straffe psykisk sårbare mennesker, der deler indholdet. Her skal andre værktøj end straf tages i brug.

En anden udfordring med den digitale vold handler om, at politi og anklagemyndighed alt for ofte kommer til kort i sager om digital vold på grund af hastigheden og mængden, og fordi volden foregår på eller via digitale tjenester med hovedsæde i udlandet. Det kræver ofte en international retsanmodning, som kan tage meget lang tid at sagsbehandle, og det forudsætter, at politisamarbejdet på tværs af lande er på plads.

Straffeloven og politiindsatsen kan ikke løse alle udfordringer med digital vold og kan alene udgøre en del af værnet mod denne voldsform. Det er netop kendetegnende ved digital vold, at den foregår via en digital tjeneste, som sociale medier eller en teknologi. Derfor er der brug for at involvere og ansvarliggøre de digitale aktører – de digitale tjenester – som danner rammen om vores digitale liv. Her spiller EU-lovgivningen en hovedrolle.

De digitale aktører skal involveres og ansvarliggøres

I 1996 i USA og i 2000 i EU blev der vedtaget lovgivning, som har været med til at forme vores moderne internet og digitale tidsalder. Lovgivning giver digitale tjenester stor frihed, men meget begrænset ansvar. Hvor publicistiske massemedier har frihed til at bestemme over indhold, men samtidig har et redaktionelt ansvar for indhold, så har sociale medier og andre digitale tjenester ikke et ansvar for indholdet, og hvad der foregår på eller via deres tjenester. De digitale tjenester kan redigere eller moderere det brugergenerede indhold, men står ikke til ansvar for det.

Der er således ikke en generel forpligtelse for digitale tjenester til aktivt at undersøge forhold eller have proaktive foranstaltninger for at komme ulovligt indhold og kriminalitet til livs.

Forudsætningen for at være fri for ansvar er dog, at tjenesten ikke har noget kendskab til det ulovlige indhold eller den ulovlige aktivitet. Får digitale tjenester konkret kendskab til ulovlige aktiviteter eller ulovligt indhold, skal de dog straks tage skridt til at fjerne det pågældende indhold eller hindre adgangen hertil. Et såkaldt "notice and take down"-system. En udfordring ved det system er, at det er svært at vurdere, hvor hurtigt "straks" er, og hvad det konkret betyder "at tage skridt til".

I 2022 blev Digital Services Act (DSA) vedtaget i EU. Den nye forordning om digitale tjenester viderefører den generelle ansvarsfritagelse fra 2000 for digitale tjenester, og de store sociale mediers ansvarsfrihed er skrevet ind.

Ansvarsfriheden ændrer muligheden for at sætte ind over for den digitale vold. Straffelovens krimi-

nalpræventive effekt og mulighed for at retsforfølge bliver i udgangspunktet sat ud af kraft, da EU-reglerne skaber juridisk helle til de digitale tjenester.

Det betyder, at Danmarks ellers hårde bestemmelser om medvirken, der siger, at "alle, der ved tilskyndelse, råd eller dåd har medvirket til gerningen", i udgangspunktet ikke kan anvendes til at ansvarliggøre de digitale tjenester i sager om digital vold.

Det ville ellers være oplagt, at digitale tjenester som sociale medier kunne retsforfølges efter det brede medvirkensansvar, vi har her til lands, som eksempelvis betyder, at et trykkeri kan blive medansvarlig for indholdet af en plakat.

Udviklingen af kunstig intelligens er også et område, som EU arbejder på for at regulere. I 2021 kom Kommissionen med et udkast til en AI-forordning, der har til formål at skabe klare rammer for anvendelse af kunstig intelligens (AI). Ambitionen er, at forordningen skal forhandles færdig i 2023.

Hvor effektiv EU-reguleringen af kunstig intelligens bliver, er stadig uklart. Det faktum, at teknologien udvikles hurtigere end lovgivningen, betyder blandt andet, at EU-lovgivningen allerede er blevet overhalet inden om af generative AI-systemer som ChatGPT, der kan producere tekst, billeder og video, og som i slutningen af 2022 blev tilgængeligt for alle. EU skal med andre ord tæmme en bold, der ruller.

Udfordringen er at få skabt en lovgivningsmodel, der håndterer alle de problemstillinger relateret til digital vold, som AI og generativ AI skaber.

Det er brugerne selv, der skal reagere på digital vold

Beskyttelsen mod digital vold bygger på, at det er brugerne og ikke virksomhederne på nettet, der skal holde øje og reagere.

EU-regler stiller derudover flere krav til brugere og myndigheder, når de klager. En klage kræver en underbygget begrundelse og en nøjagtig angivelse af, hvor den digitale vold er. Det kan fx være en URL-adresse samt navn og e-mailadresse på den person eller enhed, der klager – og en erklæring om, at oplysningerne og påstandene er nøjagtige og fuldstændige.

Kravene kan have den virkning, at mange ikke klager, da det er for tidskrævende, besværligt og man ønsker at være anonym. Der er en misproportionalitet mellem den konstante strøm af stadigt nyt indhold i det digitale miljø på den ene side og langsommeligheden i klageprocessen på den anden. Især kravet om en URL-adresse, som er en unik henvisning til en bestemt placering på en hjemmeside, er svær.

Grupper og chats er lukket land

De lukkede fora på nettet som grupper på Facebook, subreddits, eller andre chatgrupper med begrænset adgang rejser et dilemma om privatlivsbeskyttelse. På den ene side vil EU-lovgivningen gerne beskytte privat kommunikation mellem privatpersoner. Samtidig har medlemsstaterne og EU en forpligtelse til at beskytte borgerne mod krænkelser af privatlivet – herunder forpligtelse til at efterforske og retsforfølge.

Når en lukket gruppe på flere hundrede medlemmer fx deler intime billeder ulovligt, fremsætter racistiske, truende eller usande påstande, deler sundhedsoplysninger uden samtykke med videre, så er gruppens kommunikation beskyttet mod indblanding af hensyn til retten til privatliv. Sociale medier er ikke forpligtet til at gribe ind og må ikke overvåge, og politiet har kun mulighed for at få adgang til grupperne, hvis der er tale om meget alvorlige forbrydelser.

Behov for en national strategi for forebyggelse og bekæmpelse af digital vold

Som beskrevet er der mange, store udfordringer, når det kommer til at forebygge, efterforske og retsforfølge digital vold, som grooming, ulovlig deling af private oplysninger, digitale trusler, stalking med videre. Derfor er der behov for en samlet strategi med målet om at nedbringe antallet af ofre, som udsættes for digital vold og sikre, at gerningspersoner retsforfølges.

Dette mål kan ikke alene opnås ved at ændre straffeloven for at kriminalisere nye fænomener eller ved at ansætte flere betjente. Målet nås heller ikke ved at lægge hele ansvaret over på brugerne på nettet, eller over på undervisere, forældre eller myndighederne, eller satse på teknologiske løsninger, som kan fjerne alt det problematiske og ulovlige.

Der er derimod brug for en samlet forpligtende strategi, som har til formål at binde de forebyggende indsatser sammen med en effektiv beskyttelse og retsforfølgelse af digital vold. Her giver det mening at skele til andre strategier på andre voldsformer, som Danmark og andre lande har forpligtet sig på at gennemføre i form af konventioner.

Danmarks forpligtelser til at sætte ind

Vold er et menneskeretligt spørgsmål, der er omfattet af både internationale og europæiske menneskerettighedskonventioner. Lande, der har tiltrådt konventionerne, er bundet af dem. Det betyder, at landet har forpligtet sig til at beskytte personer mod vold og andre overgreb fra statslige myndigheder og organer og fra andre personer i samfundet.

Beskyttelsespligten omfatter alle personers ret til liv, helbred og integritet. En særlig pligt består i forhold til bl.a. kvinder og børn ud fra en anerkendelse af, at de er særligt udsatte for kønsbetinget vold og vold i familien.

Ikke blot fysisk vold, men også psykisk, seksuel og økonomisk vold og stalking er nu anerkendt som vold i internationale konventioner. Disse former for offline vold i samfundet og familien er generelt kriminaliseret i de enkelte lande. Digital vold ligger i forlængelse af og er ofte forbundet med forskellige former for offline vold, men foregår ofte ustraffet, blandt andet fordi de involverer meget ulige aktører magtmæssigt og teknisk og ofte foregår internationalt.

Digital vold og menneskerettigheder

Europarådet, der bygger på principper om at fremme demokrati, menneskerettigheder og retsstaten, tog i 2001 fat på spørgsmålet om IT-kriminalitet med Konventionen om IT-kriminalitet. Den omtaler dog ikke digital vold. I 2018 offentliggjorde en arbejdsgruppe under Overvågningskomitéen til Konventionen om IT-kriminalitet imidlertid en kortlægning af "cyber violence," det vil sige cyber- eller digital vold.

Arbejdsgruppen definerede cybervold som "brug af computersystemer til at forårsage, fremme eller true med vold mod individer, som resulterer i eller med sandsynlighed resultater i fysisk, seksuel, psykologisk eller økonomisk skade eller lidelse, og som kan indebære udnyttelse af individets omstændigheder, karakteristika eller brug af svagheder."[12] Definitionen er ikke bindende for landene i Europarådet, men har siden præget forståelsen af digital vold i europæiske menneskeretlige sammenhænge, blandt andet i Den Europæiske Menneskerettighedsdomstol.[13]

I et menneskeretligt perspektiv har et land pligt til at forebygge og beskytte personer mod vold og at retsforfølge udøvere. Forpligtelsen kan fx opfyldes ved at gennemføre almen oplysning om digital vold, at gøre digitale krænkelser strafbare og at strafforfølge udøverne af de strafbare krænkelser. Et lands evne (og vilje) til at efterleve sine konventionsforpligtelser er selvfølgelig afgørende for at beskytte personer effektivt mod digital vold.

Det kan imidlertid være vanskeligt at opfylde pligterne i praksis. Dels spænder udøverne af digital vold fra enkeltpersoner til magtfulde internationale tech-virksomheder. Fx kan det være meget personale- og ressourcemæssigt krævende for politi og anklagemyndighed at gennemføre straffesager mod individuelle krænkere, der ulovligt deler private billeder på sociale medier. I visse tilfælde skal beskyttelsen af personers privat- og familieliv ved digital vold balanceres mod andre personers menings og- ytringsfrihed. Det kan være juridisk vanskeligt. Og i andre tilfælde er international efterforskning nødvendig for at retsforfølge de digitale voldsudøvere.

Internationale tech-virksomheders kontrol over digitale medier og tjenester betyder, at statslige aktører, herunder politiet, skal gå via dem for fx at få fjernet ulovligt billedmateriale. Derved bliver tech-virksomhederne "gatekeeper" for retshåndhævelsen. Virksomhederne udøver på grund af deres særlige position i markedet væsentlig kontrol over adgangen til en central samfundsressource.[14]

Et enkelt land kan derfor have vanskeligt ved at ansvarliggøre internationale tech-virksomheder og regulere deres adfærd. Desuden er mulighederne for at retsforfølge virksomhederne ofte begrænsede. Menneskerettigheds- og andre konventioner af betydning for at bekæmpe digital vold giver de lande, som tiltræder dem, ensartede forpligtelser og redskaber, og de involverer landene i et internationalt samarbejde om at efterforske og retsforfølge magtfulde udøvere eller formidlere af digital vold. Det er væsentligt for at fremme og styrke landenes indsats.

Staten og dens institutioner er desuden forpligtede til ikke selv at krænke borgernes familie- og privatliv og andre frihedsrettigheder. Masseovervågning med overvågningskameraer og teknologier som ansigtsgenkendelse, der er i stand til at identificere individer, kan være sådanne krænkelser. Et lands brug af logning via tele- og internetudbyderes lagre af personers kommunikationsdata og sociale mediers brug af oplysninger om enkeltpersoner kan også under konkrete omstændigheder udgøre krænkelser af menneskerettighederne.

Relevante konventioner

De konventioner, der er relevante for digital vold, har vi beskrevet i bilaget. Blandt dem er Den Europæiske Menneskerettighedskonvention (EMRK), som indeholder de centrale menneske- og frihedsrettigheder, der gælder for Europarådets medlemslande.

Den Europæiske Menneskerettighedsdomstol har afsagt to domme om digital chikane og vold.

I dommen Buturuga mod Rumænien fra 2020[15] anerkender domstolen for første gang, at digital mobning (cyber-bullying) er et aspekt af vold mod kvinder og piger, jf. artiklerne 3 og 8 i EMRK. Domstolen fastslog, at staten har en positiv pligt til at beskytte en persons fysiske og moralske integritet mod angreb fra andre, herunder mod digital mobning af en tidligere partner. Dommen er interessant, da det var første gang domstolen behandlede digital mobning som et aspekt af vold mod kvinder.

I relation til vold i hjemmet fandt domstolen, at digital overvågning ofte blev foretaget af personens partner. Den accepterede derfor, at handlinger som uberettiget overvågning, at skaffe sig adgang til eller at gemme ens partners korrespondance kunne tages i betragtning af de indenlandske myndigheder i sager om vold i hjemmet.

Domstolen har altså taget et bredt standpunkt og har set fysisk vold og digital chikane som en helhed. I en gennemgang af domstolens domme fra 2020 omtales, at vold mod kvinder og piger kan antage forskellige former som digital krænkelse af privatlivet, indtrængen i offerets computer og opsamling, deling og manipulation af data og billeder, inklusive private data.

I en senere dom fra 2021, Volodina mod Rusland (No 2)[16], fastslog domstolen, at Rusland ikke havde opfyldt sin pligt efter artikel 8 i EMRK om retten til privat- og familieliv i EMRK til at beskytte en kvinde mod vold i hjemmet. Domstolen pegede på, at den russiske stat i forbindelse med en partnervoldssag ikke havde imødekommet en kvindes ønske om at undersøge hendes eksmands gentagne indgreb i hendes computer som digital vold og ikke havde retsforfulgt manden for det.

Digital afpresning


digitalt
ansvar

2

Digital afpresning

Afpresning dækker over det, at en eller flere personer truer nogen med formålet om at opnå en gevinst.

Juridisk er afpresning en berigelsesforbrydelse, hvilket vil sige, at truslen er fremsat med henblik på økonomisk gevinst ifølge straffelovens § 281. I denne rapport indbefatter afpresning også sager, hvor gerningspersonens gevinst ikke nødvendigvis er økonomisk. Afpresning kan også have for eksempel seksuel modydelse eller privat billedmateriale som formål. Den type af afpresning straffes efter straffelovens § 260 om ulovlig tvang. Afpresses et offer til at udføre og dokumentere overgreb på sig selv, kan det fra 1. juli 2023 straffes efter straffelovens § 225 om andet seksuelt forhold end samleje.

Digital afpresning er, når digitale medier og tjenester benyttes af en gerningsperson til at afpresse et offer. Det er en underkategori til digital vold, da truslerne har konsekvenser for offerets psykisk og kan have store konsekvenser for ofrenes privatliv og omdømme.

Afpresningen kan være effektiv, hvis den bygger på en trussel om noget, som kan have skadelige konsekvenser for offeret. I en lang række sager om online afpresning trues der med at dele private oplysninger eller indhold som nøgenbilleder online eller udlevere private oplysninger om offeret på nettet. Truslen kan også bestå i at bruge AI-teknologier til at producere ulovligt materiale af et offer som falske nøgenbilleder eller skabe en falsk historie, som ved deling kan skade en persons omdømme, familie eller virksomhed.

Digital afpresning kan foregå som en del af et længerevarende chikane- eller stalkingforløb, eller det kan være en enkeltstående begivenhed. I mange tilfælde foregår alt online, men afpresningen kan også ske i et samspil mellem online- og offline interaktioner. Når afpresning foregår digitalt, behøver gerningsperson og offer ikke dele lokation. Det betyder, at gerningspersoner har fået mulighed for at nå ofre i andre dele af verden, og gerningspersoner, befinder sig i mange tilfælde i udlandet.[17]

Af de forskellige former for afpresning, der er opstået med digitale medier og tjenester, er der i daglig tale opstået særskilte betegnelser for et par af fænomenerne. Det gælder bl.a. sextortion og hurtcore.

Sextortion

Sextortion eller "sexafpresning" er afpresning eller trusler om fx deling af intimt billed- eller videomateriale af en person, hvis vedkommende ikke gør, hvad afpresseren forlanger. På trods af at sextortion griber ind i privatlivet, har sagerne ofte karakter af at være scams med økonomisk vinding som motiv.

En hyppigt benyttet fremgangsmåde består i, at en gerningsperson får kontakt til et offer, der ofte er en ung mand eller dreng. Ofte indledes kontakten på Instagram, hvorefter den rykker til SnapChat, men gerningspersonen kan også benytte sig af datingapps, andre sociale medier, online gaming-miljøer mv.[18] Efter at have udvekslet flir-

tende beskeder siger offeret ja til at videochatte eller sende intimt materiale. På den måde kan en gerningsperson indsamle intimt materiale, som gerningspersonen derefter kan bruge til at true offeret med at offentliggøre på internettet eller sende til venner, bekendte, arbejdsplads eller familie, hvis ikke offeret overfører et beløb.[19]

I medierne har der været afdækket flere sager, hvor netop denne fremgangsmåde blev fulgt. I Danmark stod Asmus på 25 år for eksempel frem i Politiken og fortalte om, hvordan han havde videochattet med en ung kvinde på Zoom, som han havde mødet på datingappen Happn. Da chatten tog en intim drejning, optog den unge kvinde en film med Asmus, som hun derefter truede med at dele med hans familie og venner, hvis ikke han overførte 6000 kr. Hans kontakter havde hun fundet på Facebook. Asmus overførte ikke pengene og blokerede kontakten med gerningspersonen, som sandsynligvis ikke var den unge kvinde, vedkommende havde givet sig ud for at være. Indtil videre ser det ikke ud til, at videoen er blevet delt.[20]

Hurtcore

Hurtcore beskriver et fænomen, hvor ofre presses til at gøre skade på sig selv via forskellige fremgangsmåder. Ofre for hurtcore oplever ofte at blive groomet og overtalt til at dele billeder, hvor gerningspersonen bruger materialet til at afpresse sit offer. Ofrene kan bl.a. opleve at blive presset til at filme dem selv, mens de udøver selvskade, drikker urin eller andre grove, nedværdigende og ufrivillige handlinger.

I 2020 blev det i Danmark afsløret, at en ung mand over en treårig periode havde udsat 169 piger og kvinder for bl.a. hurtcore. Efter at have fået kontakt til ofrene på bl.a. SnapChat, manipulerede han dem til at sende nøgenbilleder. Billederne truede han med at offentliggøre, medmindre ofrene udførte og dokumenterede handlinger af ydmygende karakter såsom at proppe forskellige genstande op i sig selv, foretage tarmrensninger på sig selv eller udsætte andre for overgreb.[21]

Metode

Rapporten bygger på tre spørgeskemaundersøgelser, Digitalt Ansvar har foretaget i samarbejde med henholdsvis Epinion i 2020 og 2022 og Voxmeter i 2023. Dertil trækker analysen på tilgængelige oplysninger fra Danmarks Statistik samt Rigspolitiet om antallet af anmeldelser og ofre. Tallene fra Rigspolitiet er behæftet med en vis usikkerhed, fordi tallene stammer fra politiets sagsstyringssystem og ikke et egentligt statistiksystem.

I 2020 og 2022 blev spørgeskemaundersøgelsen gennemført af Epinion blandt henholdsvis 1000 og 1013 danskere i alderen 18+ år, som er på internettet på deres mobil, tablet eller computer minimum én gang om ugen (f.eks. på sociale medier, mail, google-browser el. lign.). Data er indsamlet repræsentativt på køn, alder og geografi for den danske befolkning og bruttovejet, hvorefter personer, der ikke bruger internettet minimum én gang om ugen, er sorteret fra og vægtene normaliseret. Data kan således betragtes som repræsentativt for den del af den danske befolkning over 18 år, som er på internettet ugentligt. I 2020 blev data indsamlet fra 17. september til 1. oktober, og i 2022 blev data indsamlet fra 19. april til 25. april.

I 2023 blev spørgeskemaundersøgelsen gennemført af Voxmeter. Data er indsamlet efter nationalt repræsentative kvoter på køn, aldersgrupper og region, hvorefter personer, der ikke bruger internettet minimum én gang om ugen, er sorteret fra. Data blev indsamlet fra 26. maj til 1. juni 2023.

Hver 20. dansker udsat for digital afpresning

Blandt voksne danskere, der er på nettet minimum én gang ugentligt, har omkring 5% været udsat for afpresning digitalt i løbet af det seneste år. Sådan har billedet set ud siden 2020. Omregnet til danskere svarer det til i omegnen af 234.000 voksne danskere.[22]

Andelen af voksne danskere, der i løbet af det seneste år har været udsat for afpresning digitalt, har ligget nogenlunde stabilt siden 2020. Udvider man tidshorisonten og ser på anmeldelser af afpresningssager i alt – det vil sige ikke kun digitalt – er der sket en kraftig stigning siden 2016 ifølge tal fra Danmarks Statistik. Fra 2016 til 2022 er antallet af anmeldelser af afpresning og åger vokset fra 418 sager til 2106 sager. Det svarer til en stigning på 400%.

Antallet af anmeldelser toppede for perioden i 2020, hvor der var 3751 anmeldelser af afpresning og åger. Det stemmer overens med andre tal for online kriminalitet, hvor 2020 ser ud til at ligge højt på grund af bl.a. Covid-19-pandemien.[23]

Siden 2016 har også antallet af ofre i anmeldelser af ulovlig tvang vokset kraftigt. Antallet af ofre for anmeldte tilfælde af ulovlig tvang er steget fra 180 ofre i 2016 til 521 ofre i 2022. Det svarer til en stigning på knap 200%.

Andel af voksne danskere, der min. er på nettet én gang om ugen, som indenfor det seneste år har været udsat for afpresning:

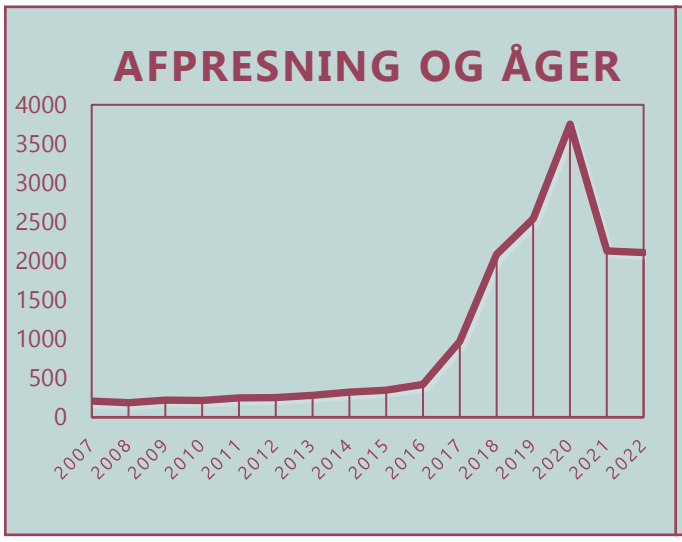
2020	2022	2023
4,7%	5,4%	5,1%

Epinion 2020, Epinion 2022, Voxmeter 2023.

400%
er anmeldelser af afpresning og åger steget fra 2016 til 2022

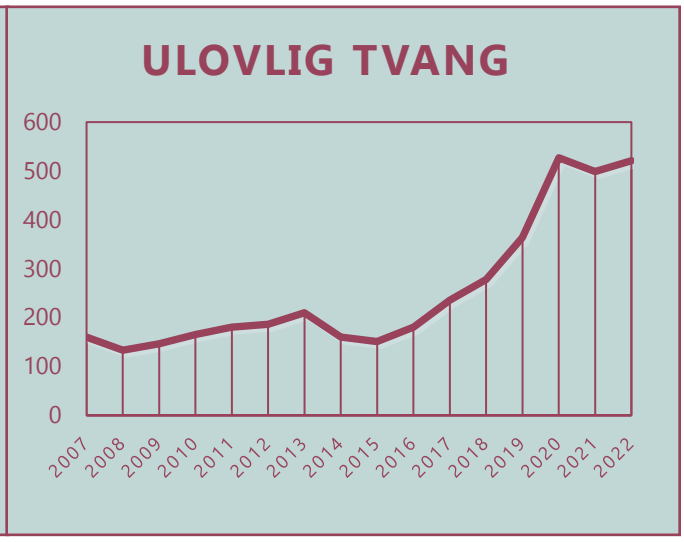
200%
er antallet af ofre i sager om ulovlig tvang steget fra 2016 til 2022

Antal anmeldelser af afpresning og åger:



Danmarks Statistik, STRAF11

Antal ofre for anmeldte tilfælde af ulovlig tvang:



Danmarks Statistik, STRAF5

Dykker vi specifikt ned i problemstillingen med sextortion, beretter tal fra politiet også om et fænomen i vækst. Fra 2019 til 2022 er anmeldelser af sextortion vokset fra 374 til 855 anmeldelser, svarende til en stigning på ca. 130%.[24] Opgørelsen er behæftet med en vis usikkerhed, fordi tallene stammer fra politiets sagsstyringssystem og ikke et egentligt statistiksystem.

Sammenholder vi anmeldelsestal fra Rigspolitiet og Danmarks Statistik med Epinion og Voxmeters undersøgelser for Digitalt Ansvar tyder det på, at der er et stort mørketal. Der er således meget stor forskel på, hvor mange der beretter, at de har været udsat for afpresning og sextortion og hvor mange, der går til politiet. Det kan skyldes flere faktorer. Det kan være, at offeret ikke har lyst til at tale med fremmede om hændelsen og helst bare vil glemme det. Det kan også være, at offeret er usikker på, om politiet kan gøre noget, eller bange for, hvad det betyder for sit omdømme, hvis andre hører om det, blandt flere andre faktorer.

Opsummering

Siden 2020 er cirka 5% af voksne danskere, der min. er på nettet én gang ugentligt, blevet udsat for online afpresning indenfor det seneste år. Det svarer til i omegnen af 234.000 danskere.

Ser man på udviklingen af anmeldte tilfælde af afpresning både offline og online, har der været en stor stigning siden 2016. Det tegner et billede af afpresning som et fænomen i vækst, der påvirker en lang række danskere.

Dertil ser der ud til at være et stort mørketal. Trods den store stigning i anmeldelser og ofre i sager om ulovlig tvang, udgør det endnu langt fra de 234.000 danskere, som Epinion og Voxmeters undersøgelser for Digitalt Ansvar viser, har været udsat for digital afpresning. Det tyder på, at mange ofre for afpresning ikke anmelder forbrydelsen.

Mænd afpresses for penge, kvinder for modydelser

Flere mænd end kvinder udsættes for afpresning. Andelen af mænd, der indenfor det seneste år har været udsat for digital afpresning, er i både 2020, 2022 og 2023 højere end andelen af kvinder, der indenfor det seneste år har været udsat for digital afpresning.

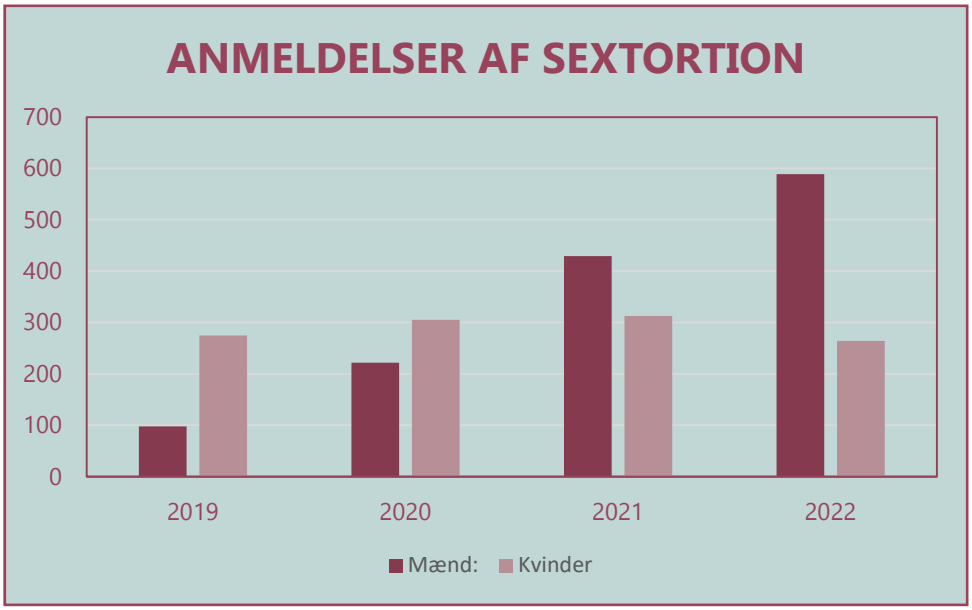
Andel af voksne danskere fordelt på køn, der min. er på nettet én gang om ugen, som indenfor det seneste år har været udsat for digital afpresning:

	2020	2022	2023
Andel af mænd i alt	7,3%	5,9%	6,2%
Andel af kvinder i alt	2,3%	4,9%	3,8%

Epinion 2020, Epinion 2022, Voxmeter 2023.

En redegørelse fra Rigspolitiet viser, at anmeldelser, hvor ordet sextortion indgår, er steget kraftigt siden 2019. Den store stigning, som politiet modtager, skyldes primært en stor stigning i sager, hvor offeret er en mand. Anmeldelser af sextortion, hvor offeret er en mand, er vokset fra 98 i 2019 til 589 i 2022. I 2022 svarer det dermed til knap 70% af anmeldelserne af sextortion.

Der tegner sig et billede af, at mænd afpresses for penge, og kvinder afpresses for modydelser. Det bekræfter både Rigspolitiet samt tal fra Danmarks Statistik.[25] I anmeldelserne af åger og afpresning for penge er der flest mænd blandt ofrene, hvor der er flest kvinder blandt ofrene i sager om ulovlig tvang.[26]



Rigspolitiet for Politiken

Opsummering

Det tyder på, at mænd og kvinder udsættes for afpresning på forskellig vis. Hvor mænd afpresses for penge, afpresses kvinder i højere grad for modydelser. Det viser både undersøgelserne af Epinion og Voxmeter for Digitalt Ansvar samt anmeldelsestal fra Rigspolitiet og Danmarks Statistik.

Afpresning ved hjælp af kunstig intelligens

Metoder til afpresning har udviklet sig i takt med udbredelsen af digitale medier og tjenester. I dag opstår kontakt mellem gerningsperson og offer ofte online, og afpresseren benytter sig af tilgængelige informationer online til at afpresse. Det kan være vennelister, arbejdsplads, uddannelsessted med videre. De muligheder har været tilgængelige siden de sociale medier for alvor har vundet indpas i samfundet.

På nuværende tidspunkt i historien står vi dog overfor en særlig udfordring. De seneste år og især fra 2022 er en lang række værktøjer blevet tilgængelige, som bruger kunstig intelligens til at producere indhold, der ikke – eller kun vanskeligt – kan skelnes fra virkeligt, menneskeskabt indhold.

Med den type værktøjer er det ikke længere nødvendigt for afpresseren at få lokket fx intimt materiale ud af et offer. Gerningspersonen kan selv producere materiale, der kan benyttes til at afpresse, uden nødvendigvis at have kontakt med offeret.

Særligt tre måder at generere materiale ved hjælp af kunstig intelligens er interessant i den henseende: Falskt billede- og videomateriale (deep fakes), stemmemanipulation og sprogmodeller.

Deepfake billede- og videomateriale

Deepfake billeder og videoer er realistiske billeder, der er skabt ved hjælp af AI.

Udtrykket "deepfake" blev skabt i 2014 af en Reddit-bruger, der anvendte deep learning-teknikker til at skabe manipuleret pornografisk indhold, og siden har deepfake-teknologien gennemgået en betydelig udvikling.

Ved hjælp af deepfake-teknologi kan gerningspersoner skabe falske pornografiske videoer, nøgenbilleder, manipulere politiske videoer mv. Disse manipulationer kan bruges til at afpresse, sprede misinformation eller have til formål at skade og ydmyge en person.

Det er ulovligt at dele manipulerede nøgenbilleder eller video uden samtykke fra den person, der er afbilledet. I Danmark har vi set sager, hvor gerningspersoner netop har hentet billeder fra unge kvinders sociale medier og manipuleret dem til at fremstå pornografisk, og i USA udsendte FBI i juni 2023 en advarsel om, at der er sket en stigning i antallet af sager, hvor deep fakes benyttes til at afpresse ofre.[27]

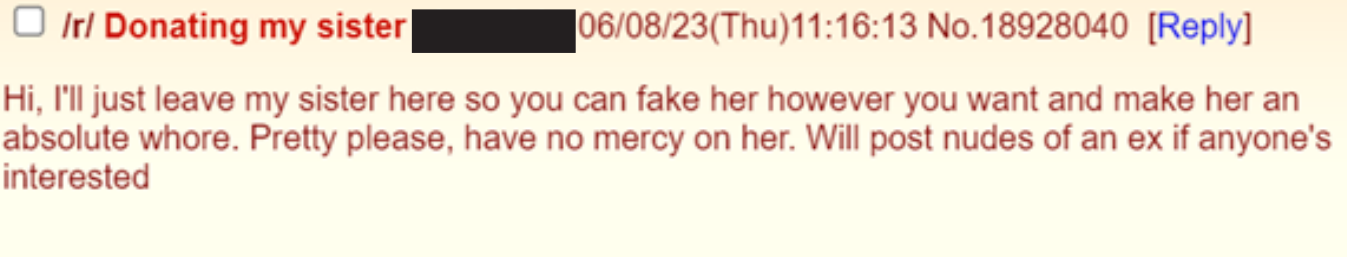
Udbredelsen af såkaldt "fake porn"-materiale kan både straffes efter bestemmelsen om blufærdighedskrænkelse (§232), udbredelse af digitalt overgrebsmateriale med børn (§235) og ulovlig billeddeling (§264d).

Hvad der engang var en ny og relativt begrænset teknologi, er blevet langt mere sofistikeret og lettilgængelig. Deepfakes er blevet mere realistiske, overbevisende og vanskeligere at opdage. Den visuelle kvalitet er forbedret, og manipulationsmulighederne er blevet mere avancerede, herunder evnen til at ændre ansigtsudtryk, bevægelser og endda generere helkropsvideoer.

En rapport fra University College London (UCL) fra 2020, rangerer deepfake-teknologi som en af de største trusler, samfundet står over for i dag.[28] Ifølge en rapport fra Europol bliver deepfake "i den oprindelige, strenge betydning" for det meste spredt med ondsindede hensigter, selvom de nu også ofte bruges til positive formål. Også ifølge Europol vurderer eksperter, at helt op til 90 % af onlineindhold i 2026 kan være syntetisk genereret[29]. Syntetiske medier refererer til medier, der er genereret eller manipuleret ved hjælp af kunstig intelligens (AI).

Det er ikke alene blevet nemmere at producere deepfake-indhold. Teknologien er også blevet mere tilgængelig ved hjælp af deepfake-markedspladser, hvor der foregår handel, udveksling eller anmodninger om deepfake-indhold. Sådanne markedspladser kan være undergrundsfora og skjulte netværk, men findes

også tilgængelige på det åbne internet. Her kan brugere anonymt anmode om at bytte eller købe forskellige former for deepfake-indhold og udveksle gode råd til, hvilke applikationer og programmer der fungerer bedst til formålet. Ofte er forespørgslerne på nøgenbilleder eller andet krænkende materiale.



AI stemmemanipulation

De seneste år er stemmeændrende teknologi blevet mere tilgængelig. I dag kan enhver med adgang til internettet downloade en app eller software, der giver dem mulighed for at manipulere deres stemme. Indtil videre fungerer det bedre på engelsk end på dansk, men udviklingen går hurtigt, og stemmeændringssoftware bliver stadig mere tilgængelig og sofistikeret. Med den nye teknologi kan man både forvrænge sin egen stemme eller reproducere andres stemmer på basis af en kort optagelse. Det giver helt nye muligheder for at udgive sig for at være en anden online.

Gerningspersoner kan udnytte dette til at efterligne en andens stemme for at narre ofre til at afsløre fortrolige oplysninger, overføre penge eller deltage i skadelige handlinger.

I USA har FBI allerede af flere omgange advaret mod virtual kidnapping.[30] Virtual kidnapping er en form for bedrag, hvor en gerningsperson forsøger at skræmme eller manipulere ofre til at tro, at en person i deres familie eller vennekreds er blevet kidnappet, selvom dette ikke er tilfældet. Ofte bruger gerningspersonerne trusler, manipulation og teknologi som telefonopkald, tekstbeskeder eller andre kommunikationsmidler for at skabe en illusion af en reel kidnappingssituation. Med kunstig intelligens har gerningspersoner fået nye muligheder for at få kidnapningen til at fremstå troværdig. Det kan for eksempel være ved hjælp af stemmeværktøjer, som på baggrund af lydoptagelser kan forfalske det påståede gidsels stemme.

Sådan foregik det i en amerikansk sag fra 2023, hvor Jennifer Destano, mor til en teenagepige på

skitur, modtog et opkald, hvor datterens stemme klart stod frem. Hun græd og bad sin mor om hjælp. Gerningspersonen krævede først 1 million dollars for at løslade datteren, hvilket hurtigt blev sænket til 50 tusind dollars. Det viste sig dog, at datteren fortsat var i sikkerhed på sin skitur, og at gerningspersonen tilsyneladende havde forfalsket hendes stemme ved hjælp af stemmeværktøjer, der benytter sig af kunstig intelligens.[31]

Da udviklingen af værktøjer går hurtigere på engelsk end dansk, er det først for nylig, stemmemanipulation er blevet mulig på dansk. I august 2023 blev stemmeværktøjet ElevenLabs tilgængeligt på dansk som det første – men flere virksomheder er på vej med lignende værktøjer.[32]

Sprogmodeller

Sproglige AI-modeller kan generere overbevisende og autentisk tekst, der kan bruges med henblik på at bedrage, narre og afpresse personer. De kan eksempelvis bruges til at producere indhold med henblik på phishing, hvor gerningspersonen forsøger at franarre internetbrugere eller virksomheder personoplysninger.

Sådanne e-mails og beskeder udgiver sig ofte for at være fra kendte virksomheder eller myndigheder, der der har brug forpersonlige oplysninger eller adgang til konti til at håndtere salg, levere ydelser eller andet, som virker uskyldigt. Men de kan også komme fra hackere, der påstår at have fået adgang til dine private oplysninger, som de truer med at dele, hvis ikke offeret betaler gerningspersonen.

De sproglige AI-modeller gør det muligt selv for folk med lidt eller ingen erfaring at skabe meget virkelighedstro indhold, der kan bruges til afpresning og svindel.

I et mindre studie sendte forskere phishing e-mails ud, som var genereret af henholdsvis mennesker og AI. Her viste det sig, at de phising e-mails, der var genereret af chatbotten, i langt højere grad blev regnet for troværdige, end de mails der var udformet af mennesker.[33] Samtidig viser et eksperiment foretaget af en journalist i 2023, at man ved hjælp af simple greb kan omgå ChatGPT's sikkerhedsforanstaltninger og få den til at forfatte phishing e-mail.[34]

Opsummering

Med udviklingen af AI er der kommet nye muligheder for at udøve afpresning. I mange sager om digital afpresning er der i dag spor, som gør det muligt at afsløre, at der er tale om falsk eller manipuleret indhold. Med udviklingen af AI bliver det dog vanskeligere og vanskeligere at skelne mellem ægte og syntetisk materiale online.

Sammenfatning og anbefalinger

3

Sammenfatning

Digital vold

Definitionen af digital vold skal bidrage til at skabe et fælles sprog og forståelse for de skadelige fænomener, der opstår på og ved hjælp af digitale medier og systemer.

Digital vold har ofte konsekvenser for vores privatliv og omdømme. Derfor er der behov for et kritisk blik på, om beskyttelsen af vores integritet, privatliv og omdømme er fulgt med den digitale udvikling. Muligheden for at sprede materiale hurtigt og gnidningsfrit betyder, at digital vold kan involvere både mange gerningspersoner, ofre og gerninger.

Digital vold er ikke nødvendigvis forårsaget af en gerningsperson – udøveren af digital vold kan også være en teknologi eller offeret selv.

Med generativ AI er der opstået nye udfordringer, som med stor sandsynlighed kommer til at accelerere i de kommende år. Afgørende bliver, hvordan domstolene anser generativ AI, samt hvordan både national lovgivere og EU regulerer kunstig intelligens og AI-virksomhedernes ansvar.

Lovgivningen, håndhævelsen og forebyggelsen er ikke fulgt med de skadelige handlinger, der forekommer online. Danmark er gennem internationale og europæiske menneskerettighedskonventioner forpligtet til at beskytte mod vold. Former af digital vold hører ind under denne beskyttelsespligt.

Digital afpresning

Digital afpresning er en form for digital vold, hvor en gerningsperson truer et offer ved hjælp af digitale medier og tjenester med henblik på at opnå en gevinst. I denne rapport medtages sager om afpresning, hvor gerningspersonens gevinst kan være både økonomisk, seksuel eller af anden karakter. Truslerne kan have store konsekvenser for offerets psyke, privatliv og omdømme.

I perioden 2020-2023 har 5% af voksne danskere, der bruger internettet minimum en gang om ugen, været udsat for digital afpresning indenfor de seneste 12 måneder.

Udvider man tidshorisonten og ser på anmeldelser af afpresningssager i alt – det vil sige ikke kun digitalt – er de dog vokset kraftigt siden 2016 ifølge tal fra Danmarks Statistik. Fra 2016 til 2022 er antallet af anmeldelser af afpresning og åger steget med 400%. I samme periode er ofre i sager om ulovlig tvang steget med 200%. Anmeldelser, der af politiet er karakteriseret som sextortion, er steget med 130% fra 2019 til 2022. Det er hovedsagligt drenge og mænd, der
Trods den store stigning i anmeldelser, ser det dog endnu ud til, at der er et stort mørketal.

Med digitale medier og tjenester er der kommet nye muligheder for at udføre afpresning. Kommer en gerningsperson i besiddelse af følsomt materiale, kan det benyttes til at true et offer med deling, hvis ikke ikke kravet om penge, modydelser eller yderligere følsomt materiale opfyldes. Mulighederne for at bruge digitale medier og tjenester til at udføre digital vold er blevet udvidet med frigivelsen af digitale værktøjer, der benytter sig af kunstig intelligens (AI) – såkaldt generativ AI.

Det har medført nye muligheder for kriminalitet. Billedgenereringsværktøjer kan benyttes til at skabe kunstigt kompromitterende materiale. Stemmeværktøjer kan benyttes til identitetsmisbrug, og med de avancerede chatbots som ChatGPT er det blevet nemmere at generere effektive trusselsmails på flere sprog.

Anbefalinger

1. Regeringen bør undersøge muligheden for at indføre et nationalt forsigtighedsprincip, indtil implementeringen af EU's AI-forordninger, der:

- Stiller krav til, at AI-genereret lyd- og visuelt indhold er tydeligt varedeklareret.

- Giver politiet mulighed for at blokere sider, apps og tjenester, der specifikt bruges til at begå kriminalitet.

2. Regeringen opretter en pulje til udvikling og implementering af digitale selvforsvarsløsninger, som er gratis, og som kan anvendes i folks dagligdag til at verificere indhold og sikre sikker deling.

3. Regeringen bør nedsætte en arbejdsgruppe eller give straffelovrådet til opgave at vurdere muligheden for at styrke indsatsen mod digital afpresning, ofres privatlivsbeskyttelse og gerningspersoners mulighed for at gemme sig bag anonymitet.

4. Regeringen bør give den nationale myndighed, som skal være koordinator og tilsynsmyndighed for digitale tjenester, jf. forordningens for digitale tjenester (DSA), mulighed for at sende strakspåbud til digitale tjenester, som sociale medier, om at fjerne ulovligt indhold eller stoppe kriminel aktivitet. Dette kunne ske via en simpel anmeldelsesportal for borgere og virksomheder og kort, standardiseret sagsbehandling hos myndigheden.

5. Regeringen bør undersøge muligheden for at gøre tech-virksomheder ansvarlige for AI-produkter, fx chatbot-svar, efter straffelovens medvirkensansvar.

6. Tech-virksomheder bør gøre det nemmere at anmelde profiler, der afpresser, på deres platforme. Dette kunne gøres ved at oprette en specifik kategori for afpresning i deres anmeldelsesprocedure.

7. Politiet gør det muligt at anmelde afpresning på politi.dk/anmeld-kriminalitet enten som selvstændig hovedkategori eller tydeligt under en af de eksisterende.

Noter

digitalt
ansvar

Noter

1 FN's højkommissær for menneskerettigheder (2021): General comment No. 25 on children's rights in relation to the digital environment. FN. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation;

Udvalget for Velfærd i Norden (2021): Udvalgsforslag om digitale krænkelser og trusler. Nordisk Råd. https://www.norden.org/sites/default/files/2021-12/A%201894_velf%C3%A6rd%20_0.pdf;

European Institute for Gender Equality (2017): Cyber violence against women and girls. EU. https://eige.europa.eu/publications/cyber-violence-against-women-and-girlsd-girls;

Se desuden: European Institute for Gender Equality (2022): Combating cyber violence against women and girls. EU. https://eige.europa.eu/publications/combating-cyber-violence-against-women-and-girls

2 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.

3 Deling af seksuelt overgrebsmateriale af børn og intime billeder uden samtykke er eksempler på privatlivskrænkelser.

4 Zuleta, L., Stefensen, T., Bahat, Y., & Kroustrup, J. (2022). DEN OFFENTLIGE DEBAT PÅ FACEBOOK. EN UNDERSØGELSE AF DANSKERNES DEBATADFÆRD. Institut for Menneskerettigheder. https://menneskeret.dk/sites/menneskeret.dk/files/media/document/Den%20offentlige%20debat%20p%C3%A5%20Facebook%2C%20analyse-notat%2C%20maj%202022_0.pdf

5 Topp, A. (2019). Politiet sigter yderligere 148 unge for at dele børneporno. DR. https://www.dr.dk/ligetil/ligetil-paa-tegnsprog/politiet-sigter-yderligere-148-unge-dele-boerneporno

6 Hagemann-Nielsen, F., Frederiksen, M. S., & Gertsen, L. (2020). Dom i brutal sag om digital afpresning og voldtægt: Ung mand afpressede og ydmygede 169 piger. DR. https://www.dr.dk/nyheder/regionale/syd/dom-i-brutal-sag-om-digital-afpresning-og-voldtaegt-ung-mand-afpressede-og

7 Whittaker, J., Looney, S., Reed, A., & Votta, F. (2021, July 3). Recommender systems and the amplification of extremist content. Internet Policy Review. https://policyreview.info/articles/analysis/recommender-systems-and-amplification-extremist-content

Se desuden: McCrosky, J., & Geurkink, B. (2021). YouTube Regrets: A crowdsourced investigation into YouTube's recommendation algorithm. Tilgængelig her: https://assets.mofoprod.net/network/documents/Mozilla_YouTube_Regrets_Report.pdf

8 Facebook's Algorithm: A Major Threat to Public Health. (2020). Avaaz. https://secure.avaaz.org/campaign/en/facebook_threat_health/

9 Larsen, N. I. (2022). Facebook prioriterer softporn og hadefuldt indhold. Her er fem hovedpunkter i de seneste afsløringer. Information. https://www.information.dk/udland/2021/10/facebook-prioriterer-softporn-hadefuldt-indhold-fem-hovedpunkter-seneste-afsloeringer

10 Roose, K. (2020). The Making of a YouTube Radical. The New York Times. https://www.nytimes.com/interactive/2019/06/08/technology/youtube-radical.html?mtrref=undefined

11 Birk, T., Frederiksen, M. S., & Heiredal, S. (2021). Stort socialt medie udbredte kendskab til krænkende foto af Lærke Bodilsen: "Det er jo fuldstændig sindssygt." DR. https://www.dr.dk/mitliv/stort-socialt-medie-udbredte-kendskab-til-kraenkende-foto-af-laerke-bodilsen-det-er-jo?cid=soc_facebook_drnyheder_post_s5ff9ud1

12 Cybercrime Convention Committee (T-CY) & Council of Europe. (2018). Mapping study on cyberviolence: with recommendations adopted by the T-CY on 9 July 2018. Council of Europe. https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914

13 European Court of Human Rights. (2022). Guide to the Case-Law of the of the European Court of Human Rights. Council of Europe. https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf

14 Jørgensen, R. F., & Akhtar, M. (2020). TECH-GIGANTERNE, YTRINGS-FRIHEDEN OG PRIVATLIVET. Institut for Menneskerettigheder. https://menneskeret.dk/sites/menneskeret.dk/files/media/document/Tech-giganterne.pdf

15 European Court of Human Rights: (2020). CASE OF BUTURUG v. ROUMANI (Application no 56867/15). .

16 European Court of Human Rights: (2021). CASE OF VOLODINA v. RUSSIA (No. 2) - Application no. 40419/19.

17 https://www.iwf.org.uk/news-media/statements/record-numbers-of-uk-men-fall-victim-to-sextortion-gangs/

18 https://protectchildren.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf

19Fremgangsmåden og at flere mænd end kvinder udsættes for sextortion, baserer sig dels på et svar til Folketinget fra Rigspolitiet, dels af beskrivelser og undersøgelser af fænomenet fra udlandet: https://www.ft.dk/samling/20222/almdel/reu/spm/111/svar/1929785/2660234.pdf Undersøgelse fra Canada: https://protectchildren.ca/pdfs/C3P_AnalysisOfFinanSextortionPostsReddit_en.pdf Tal fra USA: https://www.fbi.gov/news/press-releases/fbi-and-partners-issue-national-public-safety-alert-on-financial-sextortion-schemes Tal fra Australien: https://www.abc.net.au/news/2023-05-25/instagram-snapchat-most-used-sextortion-esafety-commissioner/102388824 Tal fra England: https://www.iwf.org.uk/news-media/statements/record-numbers-of-uk-men-fall-victim-to-sextortion-gangs/

20 https://politiken.dk/indland/art9324861/Han-blev-taget-med-bukserne-nede.-Bogstaveligt-talt.-Og-s%C3%A5-begyndte-afpresningen
21 https://www.dr.dk/nyheder/indland/piger-ned-til-11-aar-blev-brutalt-afpresset-politiet-forklarer-nu-hvorfor

22 Ifølge vores Voxmeter-undersøgelse er 2,1% af danskere over 18 år ikke på nettet ugentligt. I 2. kvartal 2023 var der i Danmark 4.787.659 danskere på 18+ jf. DST, FOLK1A. Udregningen bliver dermed: 4.787.659*0,979*0,05=234.356 danskere.

23 https://dkr.dk/it/it-kriminalitet-i-tal og https://www.europol.europa.eu/cms/sites/default/files/documents/report_beyond_the_pandemic.pdf

24 Tal fra Rigspolitiet udgivet i Politiken: https://politiken.dk/indland/art9290930/Flere-afpresses-med-intime-billeder-%E2%80%93-og-for-m%C3%A6ndene-er-det-stukket-helt-af

25 https://www.ft.dk/samling/20222/almdel/reu/spm/111/svar/1929785/2660234.pdf

26 Afpresning og åger 2022: 1551 mandlige ofre/568 kvindelige. Ulovlig tvang 2022: 174 mandlige ofre/344 kvindelige ofre (DST: STRAF5)

27 https://www.ic3.gov/Media/Y2023/PSA230605

28 https://www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat

29 https://www.europol.europa.eu/cms/sites/default/files/documents/Europol_Innovation_Lab_Facing_Reality_Law_Enforcement_And_The_Challenge_Of_Deepfakes.pdf

30 https://www.fbi.gov/contact-us/field-offices/chicago/news/press-releases/fbi-chicago-warns-public-about-virtual-kidnapping-scams, https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-public-of-virtual-kidnapping-extortion-calls

31 https://nypost.com/2023/04/12/ai-clones-teen-girls-voice-in-1m-kidnapping-scam/

32 https://www.dr.dk/nyheder/viden/teknologi/nyt-ai-vaerktoej-kan-genskabe-din-stemme-med-faa-klik-jeg-frygter-virkelig

33 https://www.wired.com/story/ai-phishing-emails/

34 https://www.cnet.com/tech/services-and-software/its-scary-easy-to-use-chatgpt-to-write-phishing-emails/

.

Bilag

digitalt
ansvar

Centrale konventioner for digital vold

I det følgende omtales en række centrale menneskerettigheds- og andre konventioner af betydning for digital vold, som Danmark har tiltrådt og er bundet af. Konventionerne anviser – med udgangspunkt i at beskytte dem enkelte persons (og persongruppers) menneskerettigheder – hvad staterne skal gøre for at forebygge og bekæmpe digital vold. Indsatserne skal være helhedsorienterede, skal gennemføres nationalt og gennem internationalt samarbejde og skal ske i nært samarbejde mellem staten og civilsamfundet.

Bilaget indeholder oversigt over:

1. Internationale menneskerettighedskonventioner

2. Europæiske menneskerettighedskonventioner

3. Andre europæiske konventioner

4. EU-rettigheder

1. Internationale menneskerettighedskonventioner

FN's Verdenserklæring om Menneskerettigheder. Vedtaget 1948.

Verdenserklæringen om Menneskerettigheder blev vedtaget for at beskytte det enkelte individ mod overgreb fra staten. Den garanterer en række fundamentale menneskerettigheder, som er udbygget og gjort bindene i senere konventioner. Erklæringen fastslår i artikel 1, at alle mennesker er født lige i værdighed og rettigheder. Artikel 2 fastslår et ikke-diskriminationsprincip , og artikel 7 hævder princippet om lighed for loven. Artikel 3 garanterer retten til liv, frihed og personlig sikkerhed, som også er grundlæggende beskyttelsesgoder i forhold til digital vold.

FN's Konvention om afskaffelse af alle former for racediskrimination. Vedtaget 1966, Tiltrådt af Danmark 1971.[35]

Formålet med konventionen er at træffe alle nødvendige foranstaltninger til hurtigst muligt at afskaffe racediskrimination i alle dens former og udslag.

Ifølge artikel 4 forpligter staten sig til at fordømme og straks at forfølge al propaganda og alle organisationer, som bygger på ideer eller teorier om overlegenhed hos en enkelt race eller persongruppe af en bestemt hudfarve eller etnisk oprindelse, eller som søger at forsvare eller fremme nogen form for racehad og racediskrimination.

Overvågningskomiteen til konventionen har i sin generelle anbefaling nr. 35 fra 2013[36] fastslået, at anbefalingen gælder racistisk hadtale, uanset hvordan det kommer til udtryk, herunder om det "udbredes via elektroniske medier, inklusive internet og sociale netværkssider."
Komiteens anbefaling er ikke direkte bindende for staterne, men er en understregning af, at digitale medier har gjort udbredelsen af racistisk hadtale lettere, og at staterne bør gribe ind mod det.

FN's Konvention om borgerlige og politiske rettigheder. Vedtaget 1966 tiltrådt af Danmark 1968.[37]

Konventionen fastslår indledningsvis, at alle folk har selvbestemmelsesret, og at de i kraft af denne frit kan bestemme deres politiske stilling og frit varetage deres egen økonomiske og sociale udvikling.

Ifølge artikel 2 skal alle personer inden for en stats område være omfattet af konventionens rettigheder uden forskelsbehandling af nogen art, jf. ovenfor om diskriminationsforbuddet. Artikel 9 beskytter enhvers ret til frihed og personlig sikkerhed. Artikel 17 beskytter mod statens vilkårlige eller ulovlige indtrængen i privatlivet, og artikel 19 fastslår retten til ytrings- og informationsfrihed med respekt for andres rettigheder eller omdømme (og statens sikkerhed, den offentlige orden, sundhed eller sædelighed). De to rettigheder er gensidigt betingede af hinanden og skal balanceres mod hinanden.

Mens staterne er forpligtede til at respektere rettighederne, gælder dette som udgangspunkt ikke tech-virksomheder.

FN's Konvention om afskaffelse af alle former for diskrimination mod kvinder (Kvindekonventionen). Vedtaget 1979. Tiltrådt af Danmark 1983.[38]

FN's Kvindekonvention sigter mod at afskaffe enhver form for diskrimination mod kvinder og sikre fuld ligestilling mellem mænd og kvinder. Vold mod kvinder omtales ikke direkte i konventionen, men kønsbetinget vold anses som diskrimination mod kvinder som defineret i artikel 1.[39]

Vold mod en kvinde, fordi hun er en kvinde, eller

som rammer kvinder uforholdsmæssigt, anses som en krænkelse af kvinders menneskerettigheder.

Digital vold fremgår ikke som omfattet af definitionen af kønsbaseret vold. Men overvågningskomiteen for konventionen omtaler, at der er sket en omdefinering af privat og offentligt gennem teknologisk medierede miljøer så som "nutidige former for vold, der forekommer online og i andre digitale miljøer." [40]

Komiteen slår fast, at i de sammenhænge, kan kønsbaseret vold mod kvinder være resultat af både staters og ikke-statslige aktørers (herunder privates) handlinger eller undladelser og være krænkelser af kvinders menneskerettigheder. (Pkt. 20 i Generel anbefaling nr. 35).[41]

Komiteen giver også konkrete anbefalinger om staternes forebyggelsesindsats over for online medier og organisationer. En generel anbefaling er dog ikke bindende for staterne, men er en anbefaling og vejledning, som komiteen følger op på i forhold til staternes rapportering.

FN's Konvention om barnets rettigheder (Børnekonventionen). Vedtaget 1989. Tiltrådt af Danmark 1991.[42]

FN's Børnekonvention har til formål at sikre børns grundlæggende rettigheder, deres ret til udvikling, ret til beskyttelse, fx mod krige, vold, misbrug og udnyttelse og deres ret til medbestemmelse.

Konventionens artikel 19 pålægger staterne at "træffe alle passende lovgivningsmæssige, administrative, sociale og uddannelsesmæssige forholdsregler til beskyttelse af barnet mod alle former for fysisk eller psykisk vold, skade eller misbrug, vanrøgt eller forsømmelig behandling, mishandling eller udnyttelse, herunder seksuel misbrug, medens barnet er i forældrenes, værgens eller andre personers varetægt."

Desuden har staten pligt til at beskytte børn mod alle former for seksuel udnyttelse og seksuelle overgreb, herunder at børn udnyttes i seksualiserede forestillinger og materialer, jf. artikel 34.
Den frivillige tillægsprotokol til konventionen om salg af børn, børneprostitution og overgrebsmateriale af børn (tiltrådt af Danmark i 2003)[43] handler, som navnet siger, om at beskytte børn mod de nævnte seksuelle overgreb.

Protokollen understreger i præamblen behovet for at imødegå den internationale udbredelse af overgrebsmateriale af børn via internettet og andre teknologier som en af begrundelserne for den.

Konventionen og tillægsprotokollen er de mest omfattende internationale instrumenter til at beskytte børn mod de nævnte overgreb og er stadig relevante og anvendelige.

Overvågningskomiteen til konventionen har dog i 2019 fundet det nødvendigt at udarbejde et sæt retningslinjer til staterne for at fortolke og gennemføre protokollens bestemmelser i lyset af den stadigt tættere kobling, der er mellem det digitale miljø og seksuelle overgreb mod børn, fx grooming og sexting og distribution af overgrebsmateriale af børn.[44]

Komiteen har også udsendt en generel kommentar nr. 25 (2021) om børns rettigheder i forhold til det digitale miljø.[45] Formålet er at forklare, hvordan staterne bør implementere Børnekonventionen i forhold til det digitale miljø og at give vejledning om relevante lovgivnings-, politiske og andre skridt for at leve op til staternes forpligtelser.

2. Europæiske menneskerettighedskonventioner

Den Europæiske Konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder (Den Europæiske Menneskerettighedskonvention). Vedtaget 1950. Inkorporeret i dansk lovgivning i 1992.[46]

Den Europæiske Menneskerettighedskonvention (EMRK) indeholder, som navnet antyder, de centrale menneske- og frihedsrettigheder, som gælder for Europarådets medlemslande. Konventionens rettigheder er inkorporeret i og er dermed en del af dansk ret.[47] EMRK fastslår i artikel 2 enhvers ret til livet. Den er, sammen med artikel 3 om forbud mod tortur og umenneskelig eller vanærende behandling og artikel 8 om retten til respekt for privat- og familieliv, relevant for beskyttelse af personer mod digital vold. Artikel 8 stk. 2 fastslår, at offentlige myndigheder som udgangspunkt ikke kan gøre indgreb i udøvelsen af denne ret – dog med en række oplistede undtagelser. Iflg. disse artikler har staten en positiv forpligtelse til at beskytte borgerne mod bl.a. vanærende behandling og deres ret til privat- og familieliv. Artikel 10 sikrer ytrings-, menings- og informationsfriheden, men pålægger også staten en pligt til at beskytte borgerne mod ulovlige ytringer og informationer som fx hate speech, der kan krænke privatlivet. Artikel 10 og artikel 8 er gensidigt afhængige, men skal balanceres mod hinanden, hvilket kan være juridisk vanskeligt. Statens begrænsninger i både ytringsfriheden og retten til privatlivet må kun ske ved lov og skal forfølge et legitimt formål og være nødvendige.[48]

Den Europæiske Menneskerettighedsdomstol har afsagt to domme om digital chikane og vold. I dommen Buturuga mod Rumænien fra 2020[49] anerkender Domstolen for første gang, at digital mobning (cyber-bullying) er et aspekt af vold mod kvinder og piger, jf. artiklerne 3 og 8 i EMRK. Domstolen fastslog, at staten har en positiv pligt til at beskytte en persons fysiske og moralske integritet mod angreb fra andre, herunder mod digital mobning af en tidligere partner.

Dommen er interessant, fordi det var første gang domstolen behandlede digital mobning som et aspekt af vold mod kvinder. I relation til vold i hjemmet fandt Domstolen, at digital overvågning ofte blev foretaget af personens partner. Den accepterede derfor, at handlinger som uberettiget overvågning og at skaffe sig adgang til eller at gemme ens partners korrespondance kunne tages i betragtning af de indenlandske myndigheder i sager om vold i hjemmet. Domstolen har altså taget et bredt standpunkt og har set fysisk vold og digital chikane som en helhed. I en gennemgang af Domstolens domme fra 2020 omtales, at vold mod kvinder og piger kan antage forskellige former som digital krænkelse af privatlivet, indtrængen i offerets computer og opsamling, deling og manipulation af data og billeder, inklusive private data.

I en senere dom fra 2021, Volodina mod Rusland (No 2),[50] fastslog Domstolen, at Rusland ikke havde opfyldt sin pligt efter artikel 8 i EMRK om retten til privat- og familieliv i EMRK til at beskytte en kvinde mod vold i hjemmet. Domstolen pegede på, at den russiske stat i forbindelse med en partnervoldssag ikke havde imødekommet en kvindes ønske om at undersøge hendes eksmands gentagne indgreb i hendes computer som digital vold (cyber violence) og ikke havde retsforfulgt manden for det.

Europarådets Konvention om forebyggelse og bekæmpelse af vold mod kvinder og vold i hjemmet. (Istanbulkonventionen) Vedtaget 2011. Tiltrådt af Danmark i 2013.[51]

Formålet med Istanbulkonventionen er iflg. artikel

1, at beskytte kvinder uanset alder mod alle former for vold og at forbygge, retsforfølge og afskaffe vold mod kvinder og vold i hjemmet.

Den bygger bl.a. på FNs Kvindekonventions generelle anbefaling nr. 19 om vold mod kvinder. Konventionen anerkender, at kønsbetinget vold mod kvinder er en form for diskrimination mod kvinder, og at både formel og reel ligestilling mellem kvinder og mænd er nøglen til at forebygge volden. Den indeholder et detaljeret sæt juridisk bindende standarder og er den nyeste og mest vidtrækkende konvention mod vold.
Artikel 3 i konventionen definerer "vold mod kvinder" og "vold i hjemmet."

"Vold mod kvinder" forstås som en overtrædelse af menneskerettighederne og en form for diskrimination af kvinder, og det omfatter alle former for kønsbetinget vold som medfører, eller som sandsynligvis medfører, fysisk, seksuel, psykisk eller økonomisk overlast eller lidelse for kvinder, herunder trusler om sådanne handlinger, tvang eller vilkårlig frihedsberøvelse, hvad enten dette sker i den offentlige eller den private sfære. Ved "vold i hjemmet" forstås alle former for fysisk, seksuel, psykologisk eller økonomisk vold som forekommer inden for familien eller i hjemmet eller mellem tidligere eller nuværende ægtefæller eller partnere, hvad enten gerningspersonen er offerets nuværende eller forhenværende sambo."

Istanbulkonventionen nævner ikke fænomenet digital vold. Men den brede formulering "alle former for vold" anses også for at omfatte digital vold. Konventionens artikler 33 om psykisk vold, 34 om stalking og artikel 40 om seksuel chikane anses også for at kunne lægges direkte til grund for online og digitalt faciliterede handlinger af den karakter.[52]

Overvågningskomiteen til konventionen (GREVIO) hilste i sin rapport om Danmarks efterlevelse af konventionen fra 2017 velkommen, at danske myndigheder engagerede sig i de nye former for vold, fx digital vold. Komiteen var også positiv over for, at undervisningsmateriale blev fokuseret på at beskytte børn mod vold, herunder digital vold. Men man mente dog, at der var behov for, at børn blev undervist i deres rettigheder, inklusive retten til at sige nej.[53]

GREVIO har i 2021 udgivet sin første generelle anbefaling om den digitale dimension af vold mod kvinder, som netop omhandler de tre nævnte artikler[54]. Den beskriver en lang række digitale handlinger, som udgør hhv. psykisk vold, stalking og seksuel chikane. Anbefalingen er ikke bindende, men har alligevel gennemslagskraft som fælles reference for staterne, fordi komiteen følger op på den i sine overvågninger.

Den generelle anbefaling definerer digital vold mod kvinder som "den digitale dimension af vold mod kvinder" og beskriver hvilke digitale handlinger og handlemåder, der udgør digital vold. GREVIO finder definitionen tilstrækkelig omfattende til både at dække online voldshandlinger og handlinger begået via teknologi, inklusive fremtidig teknologi.

Endelig giver den staterne anbefalinger om, hvordan de kan implementere konventionens krav til forebyggelse og beskyttelse af kvinder og retsforfølgning af voldsudøvere samt koordinerede politikker mod vold mod kvinder, ("de fire p'er" – prevention, protection, prosecution og coordinated policies).

3. Andre europæiske konventioner

Flere europæiske konventioner er væsentlige i beskyttelsen af personer mod digital vold. Fælles for dem er, at der i lyset af deres beskyttelsesområder og karakter lægges stor vægt på internationalt samarbejde i håndhævelsen, og konventionerne er derfor åbne for, at også lande uden for Europarådet kan tiltræde dem, hvilket mange lande har gjort.

Konventionen om IT-kriminalitet (Budapestkonventionen).

Vedtaget 2001. Tiltrådt af Danmark i 2005.[55]

Ud fra en erkendelse af at informationsteknologien har ændret samfundet fundamentalt, vedtog Europarådet i 2001 Konventionen om IT-kriminalitet (Budapestkonventionen). Formålet med konventionen er at "hindre handlinger rettet mod fortroligheden, integriteten og tilgængeligheden af edb-systemer og -netværk og elektroniske data samt misbrug af sådanne systemer, netværk og data."[56]

Konventionen har til formål at harmonisere landenes straffelovgivning om "cyber-crime" (digital kriminalitet) og at være model for den samt at etablere et hurtigt og effektivt internationalt samarbejde mod digital kriminalitet. Udover at kræve, at staterne skal kriminalisere de ovennævnte handlinger mod fortroligheden, integriteten og tilgængeligheden af edb-systemer og -netværk, skal de kriminalisere edb-relateret dokumentfalsk og databedrageri.[57]

I relation til digital vold kræver konventionen, at staterne skal kriminalisere i hvert tilfælde digital fremstilling, udbud, distribution eller overførsel og besiddelse af overgrebsmateriale af børn, jf. artikel 9. De skal desuden vedtage lovgivning eller andre foranstaltninger, så juridiske personer, herunder tech-virksomheder, kan gøres strafansvarlige for krænkelser af konventionen, jf. artikel 12, og den indeholder bestemmelser om staternes ret til at foretage hurtig sikring og give pålæg om udlevering af elektroniske data og om ransagning og beslaglæggelse af elektroniske oplysninger.

Overvågningskomiteen til Budapestkonventionen har senest fulgt op på landenes efterlevelse af artikel 31 i konventionen om "Gensidig retshjælp vedrørende adgang til lagrede elektroniske data," og nævner i den sammenhæng bl.a. det danske Cyber Crime Center som et eksempel på en god praksis.[58]

Tillægsprotokol til Konventionen om IT-kriminalitet vedrørerende kriminalisering af handlinger af racistisk eller fremmedfjendsk karakter begået gennem EDB-systemer.

Vedtaget 2003. Tiltrådt af Danmark i 2007.[59]

Tillægsprotokollen forpligter staterne til at bekæmpe racistisk og fremmedfjendsk materiale og beskytte enkeltpersoner og persongrupper mod udbredelse af sådant materiale via edb-systemer. Ved racistisk og fremmedfjendsk materiale forstås iflg. artikel 1 "skriftligt materiale, billeder eller anden fremstilling af ideer eller teorier af enhver art, der forfægter, fremmer eller tilskynder til had, forskelsbehandling eller vold rettet mod en person eller en gruppe af personer på grund af race, hudfarve, herkomst eller national eller etnisk oprindelse eller religion, hvis denne anvendes som påskud for en af disse faktorer."

Det kan fx være tale om fremmedfjendske og racistiske trusler og fornærmelser, og det kan være benægtelse, grov bagatellisering eller billigelse af eller forsvar for folkedrab eller forbrydelser mod menneskeheden, der udbredes via edb systemer.

Anden Tillægsprotokol til Konventionen om digital kriminalitet om forbedret samarbejde og oplysning om elektronisk bevismateriale. Åben for underskrift 12/5 2022.

Tillægsprotokol 2 til Budapestkonventionen giver retligt grundlag for forbedret internationalt samarbejde, både mellem stater og mellem stater og private tech-firmaer, om at indsamle bevismateriale og at opklare digital kriminalitet. Tillægsprotokollen skal på den ene side skabe effektive vilkår og sikkerhedsgarantier for at beskytte menneskerettigheder og fundamentale friheder gennem samarbejdet. På den anden side skal den balancere dette op mod, at bevisindsamling til strafforfølgning ofte angår persondata og kræver beskyttelse af privatlivet og persondata. Danmark har endnu ikke underskrevet tillægsprotokollen.

Europarådets Konvention om beskyttelse af børn mod seksuel udnyttelse og seksuelt misbrug. (Lanzarotekonventionen). Vedtaget 2007. Tiltrådt af Danmark i 2009.[60]

Lanzarotekonventionen indeholder detaljerede garantier, der har til formål at forebygge og bekæmpe seksuel udnyttelse og misbrug af børn og at beskytte børn, der er ofre for sådanne overgreb. Den knytter sig til FN's Børnekonvention og sigter mod af styrke beskyttelsen og at udvikle og supplere standarderne i den. I præamblen til konventionen bemærkes, at seksuel udnyttelse og misbrug af børn både på nationalt og internationalt plan har fået et "betænkeligt omfang" som følge af både børns og gerningspersoners øgede brug af informations- og kommunikationsteknologi. Derfor lægges der vægt på at fremme det nationale og internationale samarbejde mod seksuelle overgreb på børn.

Iflg. artikel 9 stk. 2 skal staterne "opfordre den private sektor, herunder især IKT-sektoren" til at deltage i at udarbejde en politik til at forebygge seksuel udnyttelse af børn og implementere nationale standarder gennem selvregulering eller delt regulering." IKT-sektoren omfatter ikke blot tech-virksomheder, men også mobiltelefoner, netværksudbydere og søgemaskiner. Ansvarliggørelsen af sådanne virksomheder for at begrænse udbredelse af overgrebsmateriale af børn medfører dog ikke en pligt for dem til at medvirke.

Artiklerne 18 – 23 definerer de handlinger, som staterne skal kriminalisere: Seksuelt misbrug og handlinger som fx rekruttering til børneprostitution (Artikler 18 0g 19). Artikel 19. handler om fremstilling, udbud, distribution eller overførsel og besiddelse af overgrebsmateriale af børn, handlinger i forbindelse med børns deltagelse i eller overværelse af seksualiserede forestillinger og grooming. Staterne skal iflg. artikel 23 vedtage lovgivning om "forlokkelse" (grooming) af børn til seksuelle formål ved brug af informations- og kommunikationsteknologi. Den Europæiske Menneskerettighedsdomstol har desuden udviklet en betydelig retspraksis om beskyttelse af børn mod vold i enhver sammenhæng.[61]

Overvågningskomiteen til konventionen fremlagde i marts 2022 sin anden tematiske evalueringsrunde. Temaet var beskyttelsen af børn mod seksuel udnyttelse og misbrug via informations- og kommunikationsteknologier, og rapporten handlede om de udfordringer, der rejser sig ved seksuelle billeder og videoer, som børn selv lægger på nettet.[62] Komiteen refererede landenes svar uden bemærkninger og kom med nogle generelle anbefalinger til implementeringen af konventionen.

4. EU-rettigheder

Den Europæiske Unions charter om grundlæggende rettigheder. (EU Charteret). Vedtaget 2009.[63]

EU's Charter om grundlæggende rettigheder bygger dels på FN's Verdenserklæring om Menneskerettigheder og dels - i vid udstrækning - på Den Europæiske Menneskerettighedskonvention.

Den menneskelige værdighed ses, som i Verdenserklæringen, ikke blot som en grundlæggende rettighed i sig selv, men som selve fundamentet for de grundlæggende rettigheder. Charteret beskytter ligesom EMRK den enkelte persons grundlæggende ret til livet, menneskelig værdighed, respekt for menneskelig integritet og forbyder tortur og umenneskelig og nedværdigende behandling. Artikel 7 fastslår retten til respekt for privatliv og familieliv, hjem og kommunikation. Det omfatter som væsentlige elementer respekt for privatlivets fred i forbindelse med kommunikation og beskyttelse af brugerens terminaludstyr.

Ytrings- og informationsfriheden er beskyttet i artikel 11, ligesom beskyttelsen af persondata også ses som en grundlæggende rettighed, jf. artikel 8. Chartrets artikel 21 indeholder et forbud mod forskelsbehandling af beskyttede persongrupper inden for EU-lovgivningens område, jf. nedenfor.

EU-forordninger

I 2022 har EU vedtaget to væsentlige forordninger for den digitale sektor: Digital Markets Act (DMA) og Digital Services Act (DSA), som har til formål at regulere tech-giganterne. Formålet med DMA er at sikre et velfungerende indre marked med åbenhed og fair konkurrence blandt tech-giganterne, især blandt dem, der har position som gatekeepere.

Formålet med DSA er at beskytte borgernes rettigheder online og dermed skærpe kontrollen med tech-giganterne. Særligt meget store onlineplatforme vil blive pålagt en række krav, herunder pligt til at have mekanismer til at anmelde og fjerne ulovligt indhold, til at give begrundelser til brugere om, hvorfor opslag er blevet fjernet og at give klageadgang.

Derudover bliver de største onlineplatforme pålagt en rapporteringspligt om hvor meget indhold, der er blevet fjernet og redigeret mm. og at samarbejde med håndhævelsesmyndigheder. De allerstørste platforme skal desuden bl.a. udarbejde risikovurderinger ift. systemiske trusler mod samfundet samt dele data med myndigheder og forskere.

Endelig er der i marts 2022 fremsat et direktivforslag om bekæmpelse af vold mod kvinder og vold i hjemmet.[64] Direktivforslaget omfatter også "cypervold". Af forslaget fremgår, at cybervold har været stigende i kølvandet på brugen af digitale medier og internettet, og at cybervold ofte er en udvidelse af den vold, ofre udsættes for offline og derfor skal behandles i lighed med offline vold. Det vedtagne direktiv vil ikke være umiddelbart bindende for Danmark på grund af retsforbeholdet, men ventes alligevel at blive anerkendt.

Ikke-diskrimination

Fælles for Europarådets konventioner, som fastslår personers grundlæggende menneske- og frihedsrettigheder er, at de hviler på princippet om ikke-diskrimination. Det betyder, at ingen personer eller grupper må udsættes for forskelsbehandling, hverken direkte eller indirekte, på grundlag af særlige karakteristika eller tilhørsforhold. Det gælder også i forhold til at beskytte personers liv, helbred og integritet mod digital vold.

Diskriminationsforbuddets områder og beskyttelsesfelt har udviklet sig i konventionerne. Den Europæiske Menneskerettighedskonvention fra 1950 indeholder i artikel 14 et forbud mod diskrimination i forhold til konventionens rettigheder og friheder. I lyset af samfundsudviklingen i de mellemliggende 50 år, vedtog staterne i Europarådet imidlertid i år 2000 Protokol nr. 12 til EMRK[65]. Pro-

tokollen udvider anvendelsesområdet til at være et generelt forbud mod diskrimination og sikrer ligebehandling i forhold til alle (også nationale) rettigheder. Protokollen er bindende for staterne.

"Artikel 1. Nydelsen af enhver i loven forudset ret skal sikres uden nogen diskrimination, navnlig på grund af køn, race, hudfarve, sprog, religion, politiske meninger eller enhver anden mening, national eller social herkomst, tilhørighed til et nationalt mindretal, formue, fødsel eller enhver anden situation. 2. Ingen kan blive til genstand for diskrimination fra en offentlig myndighed, uanset hvilken, navnlig på grund af de i paragraf 1 nævnte motiver."

Også EU's menneskerettighedsdokument, Den Europæiske Unions charter om grundlæggende rettigheder (EU's Charter), indeholder et diskriminationsforbud. Det bygger i vid udstrækning på EMRK's artikel 14. Bestemmelserne i de to systemer supplerer og styrker hinanden i vid udstrækning, om end der også er forskelle.[66]

Artikel 21 i EU's Charter forbyder i stk. 1 "enhver forskelsbehandling på grund af køn, race, farve, etnisk eller social oprindelse, genetiske anlæg, sprog, religion eller tro, politiske eller andre anskuelser, tilhørsforhold til et nationalt mindretal, formueforhold, fødsel, handicap, alder, seksuel orientering eller ethvert andet forhold."
Bestemmelsen er fulgt op af EU direktiver om ligebehandling med hensyn til beskæftigelse og direktivet om racelighed og direktivet om ligebehandling af kvinder og mænd, der i forskelligt omfang forbyder forskelsbehandling og forpligter medlemsstaterne.

Forbud mod diskrimination har også betydning i forhold til digital vold. Direkte diskrimination[67] kan i visse tilfælde i sig selv udgøre digital vold, fx chikane af LGBT+personer på internettet, tilskyndelse til race- eller religiøst had eller incel gruppers hadske opslag mod kvinder og piger. Indirekte forskelsbehandling[68] forekommer bl.a. i forbindelse med digital diskrimination. Den digitale diskrimination kan være vanskelig at afdække, fordi den kan forekomme uafhængigt af, om nogen har haft til hensigt til at diskriminere eller ej. Der kan fx være tale om, at fordomme i samfundet ubevidst videreføres i online sagsbehandling. Der kan også være tale om biased design af algoritmer, men også "neutrale" algoritmer, der er blevet fodret med biased data kan medføre diskriminerende resultater. Staten er, som det fremgår, forpligtede til både at forebygge og bekæmpe ulovlig og usaglig forskelsbehandling af enkeltpersoner og persongrupper online såvel som offline.

Som det fremgår, arbejdes der både i europæiske menneskeretlige sammenhænge og i EU-regi med at bekæmpe digital vold og andre krænkelser uden forskelsbehandling. Den menneskeretlige tilgang til bekæmpelsen af digital vold bygger – bredt sagt – på at beskytte det enkelte menneskes liv, integritet og privat- og familieliv og kræver en helhedsorienteret indsats med forebyggelse, beskyttelse af ofre og retsforfølgning af udøvere. EU's forordninger om den digitale sektor indeholder også bestemmelser om beskyttelse af individet mod digitale krænkelser, men sigter – også bredt sagt – i højere grad på at regulere tech-giganternes virksomhed og status inden for det indre marked. Danmark er allerede forpligtet af de europæiske menneskerettigheder og vil, når EU-forordningerne træder i kraft, skulle indrette sin lovgivning og implementeringen af den efter begge retsordener.

Noter

35 Bekendtgørelse af international konvention af 21. december 1965 om afskaffelse af alle former for racediskrimination.

36 General recommendation No. 35 82013) on combating racist hate speech. CERD/C/GC/35. II 7

37 Bekendtgørelse af international konvention af 16. december 1966 om borgerlige og politiske rettigheder med tilhørende valgfri protokol.

38 Bekendtgørelse af konvention af 18. december 1979 om afskaffelse af alle former for diskrimination imod kvinder.

39 THE COMMITTEE ON THE ELIMINATION OF DISCRIMINATION AGAINST WOMEN Eleventh session (1992).

General recommendation No. 19: Violence against women. The Convention in article 1 defines discrimination against women. The definition of discrimination includes gender-based violence, that is, violence that is directed against a woman because she is a woman or that affects women disproportionately. It includes acts that inflict physical, mental or sexual harm or suffering, threats of such acts, coercion and other deprivations of liberty. Gender-based violence may breach specific provisions of the Convention, regardless of whether those provisions expressly mention violence.

40 Report of the Secretary-General entitled "In-depth study on all forms of violence against women" (A/61/122/ Add.1 and Corr.1). 2006.

41 General recommendation No. 35 (2017) on gender-based violence against women, updating general recommendation No. 19 (1992). 26 July 2017. CEDAW/C/GC/35.

42 BKI nr 6 af 16/01/1992Bekendtgørelse af FN-konvention af 20. november 1989 om Barnets Rettigheder.

43 Bekendtgørelse af valgfri protokol af 25. maj 2000 til FN-konventionen om barnets rettigheder. vedrørende salg af børn, børneprostitution og børnepornografi.

44 Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.10. September 2019.

45 General comment No. 25 (2021) on children's rights in relation to the digital environment.

46 Danmarks ratifikation af konvention til beskyttelse af Menneskerettigheder og grundlæggende Frihedsrettigheder, undertegnet i Rom den 4. november 1950 med tilhørende tillægsprotokol, undertegnet i Paris den 20. marts 1952.

47 LBK nr 138 af 26/01/2022 Bekendtgørelse af lov om Den Europæiske Menneskerettighedskonvention (Inkorporeringsloven).

48 LBK nr 138 af 26/01/2022 Bekendtgørelse af lov om Den Europæiske Menneskerettighedskonvention (Inkorporeringsloven).

49 AFFAIRE BUTURUG c. ROUMANI (Requête no 56867/15) 11/06/2020.

50 CASE OF VOLODINA v. RUSSIA (No. 2) (Application no. 40419/19) 14/12/2021

51 BKI nr 11 af 01/08/2014 Bekendtgørelse af konvention af 11. maj 2011 til forebyggelse og bekæmpelse af vold mod kvinder og vold i hjemmet.

52 Adriane van der Wilk: Protecting Women and Girls from Violence in the Digital Age. The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women. December 2021.

53 GREVIO Baseline Evaluation Report of Denmark. Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO). November 2017.

54 GREVIO General Recommendation No. 1 on digital dimensions of violence against women adopted on 20 October 2021.

55 BKI nr 12 af 15/03/2007 Bekendtgørelse af konvention af 23. november 2001 om IT-kriminalitet

56 Præamblen til konventionen.

57 Cybercrime Convention Committee (T-CY). Working Group on cyberbullying and other forms of online violence, especially against women and children. Mapping study on cyberviolence with recommendations adopted by the T-CY on 9 July 2018.

58 Ibid.

59 BKI nr 17 af 10/05/2007. Bekendtgørelse til tillægsprotokol af 28. januar 2003 til konventionen af 23. november 2001 om IT-kriminalitet.

60 BKI nr 57 af 15/10/2010. Bekendtgørelse af konvention af 25. oktober 2007 om beskyttelse af børn mod seksuel udnyttelse og seksuelt misbrug.

61 Håndbog om europæisk lovgivning om børns rettigheder. Den Europæiske Unions Agentur for Grundlæggende Rettigheder og Europarådet, 2015

62 Lanzarote Committee. Committee of the Parties to the Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse. Implementation report. The protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTS) addressing the challenges raised by child self-generated sexual images and/or videos.. T-ES(2022)02_en final (subject to editing) 10 March 2022.

63 Den Europæiske Unions Charter om Grundlæggende Rettigheder (2010/C 83/02)

64 Forslag til Europa-Parlamentets og Rådets direktiv om bekæmpelse af vold mod kvinder og vold i hjemmet (Fremsat 8. marts 2022).

65 Protokol nr. 12 til Konventionen for beskyttelse af menneskerettighederne og de grundlæggende frihedsrettigheder Rom, 4.XI.2000

66 Håndbog om europæisk lovgivning om ikke-forskelsbehandling. Den Europæiske Unions Agentur for Grundlæggende Rettigheder. 2010. Europarådet.

67 Direkte forskelsbehandling er, når en person på grund af en særlig (beskyttet) egenskab bliver behandlet ringere sammenlignet med, hvordan andre, der er er i en tilsvarende situation, er blevet eller ville blive.

68 Indirekte forskelsbehandling er, når en tilsyneladende neutral regel, betingelse eller praksis rammer stiller en beskyttet gruppe ringere end andre personer.

digitalt
ansvar

digitalt
ansvar