KOMMERSIELL UTNYTTING AV BARN OG UNGE PÅ NETT

Slik sikrer
vi en tryggere
digital oppvekst

FORBRUKERRÅDET

November 2024
Forside: VON Kommunikasjon
Oversettelse: NTB Arkitekst

Innhold

Oppsummering

Mange deler av barn og unges liv er tett knyttet til digitale tjenester. Internett har gitt oss nye metoder for å kommunisere og bygge relasjoner, uttrykke oss kreativt og politisk, oppsøke kunnskap og mye mer. I takt med at bruk av internett har blitt stadig mer utbredt og normalisert, har imidlertid de mørke sidene vokst seg større. Små barn utsettes for skremmende og destruktivt innhold, ungdom bombarderes av kommersielle budskap som utnytter sårbarheten deres, og skjermtid kan gå på bekostning av andre deler av livet.

Myndighetene har et ansvar for å beskytte borgerne, uansett alder. Virksomheter er også forpliktet til å respektere barns rettigheter. Likevel har ikke de skadelige sidene ved digitalisering blitt tatt ordentlig tak i de siste 20 årene. Etter hvert som bevisstheten om de skadelige sidene ved sosiale plattformer øker, begynner imidlertid lovgivere og tilsynsmyndigheter å se etter løsninger.

Målet med denne rapporten er å kartlegge de viktigste skadevirkningene for barn og unge på nettet, med et særlig fokus på bruken av sosiale medier. Slik ønsker vi å legge et grunnlag for videre diskusjon om hvilke tiltak som kan og bør innføres. Rapporten tar hovedsakelig for seg skadevirkningene fra et forbrukerperspektiv, men andre risikofaktorer blir drøftet når det er nødvendig for å få en mer helhetlig oversikt over de risikoene barn og unge står overfor.

Det er mange pågående diskusjoner blant politikere, myndigheter og tilsyn om å introdusere tekniske sperrer for å blokkere eller fjerne barn og unge fra visse digitale tjenester. Denne rapporten gir en oversikt over de viktigste begrensningene ved en slik tilnærming og risikoene som introduksjonen av ID-basert aldersverifisering kan føre til for både barn og voksne.

I rapporten foreslås en rekke politiske, juridiske og tekniske tiltak som kan motvirke skadevirkningene. Vi mener at disse kan bidra til et tryggere og bedre internett for alle, uten å måtte ty til invaderende og ekskluderende tiltak.

Tiltakene kan oppsummeres i følgende fem punkter:

1. **Holde selskapene ansvarlige**, slik at de fjerner avhengighetsskapende mekanismer, bruker anbefalingsalgoritmer som styrker brukernes autonomi og rettigheter istedenfor å forsterke destruktivt innhold og stopper all ulovlig markedsføringspraksis.

2. Streng, koordinert og avskrekkende **håndheving av regelverk nasjonalt og internasjonalt**.

3. **Oppdatere forbrukerlovgivningen** der eksisterende regler og håndheving ikke er tilstrekkelige. Dette inkluderer horisontal beskyttelse

for alle forbrukere, når det er den mest effektive måten å beskytte barn, i tillegg til konkrete tiltak for barn.

4. **Eventuell aldersverifisering må bare brukes i tråd med en rekke grunnprinsipper**, som blant annet skal sikre at det ivaretar retten til personvern, informasjon og deltakelse.

5. **Få på plass tydelige veiledninger** for foreldre, omsorgspersoner og barn, inkludert veiledning om anbefalte aldersgrenser for sosiale medier.

Rapporten ble ferdigstilt 1. november 2024.

1. Innledning

Internett generelt og digitale plattformer spesielt, har hatt stor betydning for forbrukere, enkeltpersoner og samfunnet som helhet. For forbrukere er plattformer som sosiale medier en viktig del av dagliglivet. Her organiserer vi livene våre, kommuniserer med venner og familie, shopper, holder oss oppdatert på nyheter og arrangementer og mye mer.

Samtidig bruker mange teknologiselskaper plattformene sine til å hente ut «verdi» fra brukerne. Digitale tjenester, slik som sosiale medier, tjener penger gjennom reklame, salg og innsamling av personopplysninger. For å holde folk aktive på plattformene så lenge som mulig, tas ulike metoder i bruk for å engasjere og holde på brukerne. Dette har skapt en dypt problematisk situasjon, der teknologigigantene støtter seg på team av teknologer, designere, psykologer, samfunnsvitere og advokater[1] for å utvikle avhengighetsskapende opplevelser som spiller på, og ofte forsterker, følelser som sinne, frykt, usikkerhet og hat.

Disse avhengighetsdrevne raserimaskinene, som mange nettplattformer har utviklet seg til å bli, har en betydelig negativ innvirkning på brukerne. Skadevirkningene blir imidlertid spesielt alvorlige når sluttbrukerne er barn. Barns opplevelser på nett har ofte gått under radaren, til dels på grunn av personaliserte digitale tjenester og små skjermer, som gjør det vanskelig for foreldre og andre voksne å følge med. Det økende antallet barn og unge som er aktive på det som i bunn og grunn er digitale reklameplattformer, er til stor bekymring for foreldre, omsorgspersoner, politikere, samfunnet og i mange tilfeller for barna selv.[2]

Det finnes talløse eksempler på at små barn utsettes for skadelig innhold, slik som idealisering av selvmord, brutal vold, aggressiv reklame for produkter knyttet til vektnedgang, kosmetisk kirurgi og en rekke andre dypt problematiske praksiser.[3] Digitale tjenester er utformet for å skape oppmerksomhet uten hensyn til hvordan dette rammer brukernes autonomi, rettigheter, selvtillit og

[1] «Ex-Google CEO says successful AI startups can steal IP and hire lawyers to 'clean up the mess'», Alex Heath, The Verge (2024). https://www.theverge.com/2024/8/14/24220658/google-eric-schmidt-stanford-talk-ai-startups-openai

[2] «Pathways: How digital design puts children at risk», 5Rights Foundation (2021). https://5rightsfoundation.com/wp-content/uploads/2021/09/Pathways-how-digital-design-puts-children-at-risk.pdf.

[3] Se for eksempel BEUCs klage mot TikTok fra 2021: «BEUC files complaint against TikTok for multiple EU consumer law breaches», https://www.beuc.eu/press-releases/beuc-files-complaint-against-tiktok-multiple-eu-consumer-law-breaches og posisjonsnotatet deres om influensermarkedsføring: «From influence to responsibility - Time to regulate influencer marketing» (2023), https://www.beuc.eu/position-papers/influence-responsibility-time-regulate-influencer-marketing.

psykiske velvære.[4] Barn mangler ofte evner og ferdigheter til å bearbeide og håndtere mange av disse problemene. De brede, systemiske og komplekse mekanismene som er i spill, gjør at foreldre og omsorgspersoner ofte også føler seg hjelpeløse i kampen mot de store teknologiselskapene.

Denne rapporten fremhever hvordan mange av skadevirkningene barn utsettes for på digitale tjenester er nært knyttet til de dominerende forretningsmodellene på nett. Disse modellene inkluderer bruk av avhengighetsskapende mekanismer, manipulerende design, samt utnyttelse og forsterkning av psykisk uhelse og destruktivt innhold. Noen av risikoene barn møter på nett ligger utenfor et rent forbrukerperspektiv, selv om plattformenes forretningsmodeller fortsatt er relevante i disse sammenhengene. Dette gjelder blant annet nettmobbing, uønsket kontakt med fremmede og seksuell utnyttelse. Rapporten tar opp disse utfordringene, men går ikke i dybden, ettersom Forbrukerrådets mandat er begrenset til forbrukerspørsmål.

1.1. Et bedre internett for unge

Den offentlige debatten om beskyttelse av barn og unge på nettet, dreier seg ofte om hvordan vi kan holde de unge fullstendig borte fra tjenester som sosiale medier. Det er et viktig og prisverdig mål å sørge for at barn og unge er trygge. Det er også et faktum at ikke alle plattformer bør være tilgjengelige for barn. Samtidig er denne tilnærmingen svært begrensende og fører med seg en rekke ulemper.

Vi mener det finnes alternative tilnærminger for å håndtere skadevirkningene fra nettplattformer, som ikke ekskluderer unge fra deltakelse. Utgangspunktet for dette er oppfatningen om at internett og tjenester som sosiale medier ikke er skadelige i seg selv. Det er både mulig og ønskelig å jobbe mot en bedre digital verden.

Barn og unge har rett til tilgang til teknologier som gjør det mulig for dem å samhandle, engasjere seg i viktige temaer og finne informasjon som er relevant for dem. Dessverre har teknologiselskapene gjort disse mulighetene avhengige av at brukerne godtar omfattende kommersiell overvåking, anbefalingsalgoritmer som utnytter sårbarheter og aggressive markedsføringsstrategier. I praksis blir barn brukt som prøvekaniner for store atferdseksperimenter utført av Silicon Valley og lignende aktører.

Selv om de dominerende nettplattformene i dag er preget av destruktive algoritmer, inngripende overvåking og sporing, manipulerende design og ulovlig innhold, er ikke disse negative egenskapene grunnleggende kvaliteter ved

[4] «Disrupted Childhood. The cost of persuasive design», 5Rights Foundation (2023). https://5rightsfoundation.com/wp-content/uploads/2024/08/5rights_DisruptedChildhood_G.pdf

tjenestene. Vi mener at selskaper kan tvinges til å utforme plattformene – eller deler av dem – på måter som fremmer positive, trygge og styrkende opplevelser for barn og unge.

Et bedre digitalt miljø for barn og unge betyr ikke at de må utestenges totalt fra sosiale medier og andre digitale tjenester. Istedenfor å fokusere på hvordan noen kan forhindres fra å få tilgang til digitale tjenester, bør selskaper pålegges et større ansvar for tjenestene de tilbyr. Historien har gjentatte ganger vist at dette ikke kommer til å skje uten betydelige rettslige pålegg og effektiv håndheving.

Mange av de problematiske aspektene som vanligvis knyttes til barns internettbruk, er ikke utelukkende et problem ved digitale sfærer. Fenomener slik som mobbing, psykisk uhelse og oppmerksomhetsproblemer er komplekse og mangefasetterte utfordringer som ikke utelukkende kan tilskrives bruken av teknologi. Det blir for enkelt å anta at løsningen på sosiale og strukturelle problemer kan eller bør ligge i rene teknologiske tiltak, slik som aldersverifisering. Visse teknologiske tiltak kan bidra til å lindre symptomene på mer vidtfavnende problemer, men disse bør ikke vurderes i et vakuum.

I stedet for å fokusere på tilsynelatende enkle løsninger og «mirakelkurer», er det et presserende behov for å iverksette tiltak som til sammen sikrer bedre og tryggere opplevelser på nettet for alle. Digitale tjenestetilbydere bør pålegges å utforme tjenestene sine i samsvar med menneskerettighetsforpliktelser og gjeldende lovgivning. Forbrukere i alle aldre bør gis mer kontroll over hvilket innhold de utsettes for og når og hvor mye de bruker digitale tjenester. Ingen selskaper bør utnytte barns sårbarheter til å målrette kommersielle budskap mot dem.

Digitale tjenester bør understøtte barn i mange ulike aldre. Det forutsetter at tjenestene har grunnleggende rettigheter som utgangspunkt for både utforming og drift. I tillegg er det behov for alderstilpasset design, som kan ta høyde for at unge mennesker har varierende egenskaper og behov for beskyttelse. Selvregulering og individualiserte selvhjelpstiltak har vist seg å være utilstrekkelig, og må erstattes av et sterkt regelverk, politiske tiltak og robust håndheving.

1.2. Om forfatterne

Forbrukerrådet er en offentlig finansiert, uavhengig interesseorganisasjon som representerer forbrukere. Vi mottar ingen finansiering fra private selskaper.

Denne rapporten ble skrevet med bidrag fra BEUC, EDRi, 5Rights Foundation, Anja Salzmann (postdok på Centre for the Science of Learning and Technology (SLATE) på Universitet i Bergen), Jürgen Bering (Head of Center for User Rights at Gesellschaft für Freiheitsrechte) og Jon Worth.

2. Hvordan arter barns rettigheter seg i det digitale miljøet?

Alle personer under 18 år regnes som barn og har rettigheter etter FNs konvensjon om barnets rettigheter (Barnekonvensjonen).[5] Alle EU- og EØS-medlemsland har ratifisert konvensjonen, som betyr at de må sørge for at barn har tilstrekkelig beskyttelse og rettigheter i tråd med konvensjonen, både på nett og ellers. Dette kan myndighetene for eksempel sikre gjennom å innføre lovbestemmelser eller politiske tiltak. Barnekonvensjonens rettigheter er utdypet spesifikt for den digitale sfæren i FNs generelle kommentar nr. 25 om barns rettigheter relatert til det digitale miljøet.[6]

Stater skal ikke tillate kommersielle aktører å utnytte eller i urimelig grad påvirke barn,[7] for eksempel gjennom markedsføring, målrettet kommersielt innhold basert på profilering eller kommersiell sporing og profilering av barn. Dette omfatter beskyttelse mot manipulerende design, for eksempel design som kan skape en falsk opplevelse av tillit og tilknytning,[8] eller design som presser barn til å bruke mer tid eller penger enn de egentlig ønsker. Beskyttelse mot kommersiell påvirkning er avgjørende for å styrke barns rettigheter på ulike områder, for å støtte deres selvstendighet, ytrings- og tankefrihet, rett til fritid og lek, samt rett til utdanning.

I praksis må digitale tjenester utformes og administreres med hensyn til barns beste, både individuelle barn og grupper av barn.[9] Dette er spesielt viktig hvis digitale tjenester innebærer konflikt mellom barns ulike rettigheter, eller dersom det er et motsetningsforhold mellom barns og andre aktørers interesser. Dersom det for eksempel oppstår konflikt mellom selskapers kommersielle interesser og barnets beste, skal barnets beste prioriteres.[10] Å ivareta barnets beste innebærer blant annet alderstilpassede og ikke-manipulerende tiltak som tar hensyn til barnets alder og utvikling. Innebygd personvern og trygghet er viktige tiltak for dette formålet.[11]

Barn har rett til vern mot diskriminering, som omfatter lik og effektiv tilgang til digitale miljøer på måter som er meningsfulle for dem. Stater er forpliktet til å

---

[5] «Convention on the Rights of the Child», FN (1989). https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child
[6] «General comment nr. 25 (2021) 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
[7] Generell kommentar nr. 25 (2021) avsnitt 40–42.
[8] «Dark Patterns of Cuteness: Popular Learning App Design as a Risk to Children's Autonomy» i «Children, Young People and Online Harms», Stockman, Nottingham (2024). https://link.springer.com/chapter/10.1007/978-3-031-46053-1_5.
[9] Generell kommentar nr. 25 (2021) avsnitt 12.
[10] For en grundig analyse av barnas beste, se «The best interests of the child in the digital environment», Livingstone, Cantwell, Özkul, Shekhawat, Kidron (2024). https://www.digital-futures-for-children.net/digitalfutures-assets/digitalfutures-documents/Best-Interests-of-the-Child-FINAL.pdf.
[11] Generell kommentar nr. 25 (2021) avsnitt 110.

iverksette 'alle nødvendige tiltak for å forhindre digital ekskludering'.[12] Diskriminering kan også oppstå i form av nettmobbing, eller dersom algoritmebaserte systemer basert på skjeve data, kode eller profilering brukes til å ta beslutninger som angår barnet.

Barn har også rett til privatliv og personvern, som kan sikres ved å bygge inn personvern i tjenester de bruker.[13] For eksempel har de rett til beskyttelse mot overvåking og inngripende sporing både fra kommersielle og statlige aktører. Etter hvert som barn blir eldre, skal foreldre eller omsorgspersoner også gi dem en økende grad av autonomi og privatliv.[14] Retten til privatliv er nært knyttet til retten til tankefrihet og meningsfrihet. Barn må kunne lære, utvikle seg og leke i miljøer som ikke samler inn data om dem for å utnytte følelsene og sårbarheten deres for kommersielle formål.[15]

FNs barnekonvensjon anerkjenner barnets rett til en høyest mulig helsestandard. Digital markedsføring av produkter som har en klar innvirkning på barns helse (usunn mat, alkohol, pengespill osv.), har store konsekvenser for innfrielsen av denne rettigheten. Retten til helse innebærer også at barn ikke bør utsettes for handlinger som kan skade den mentale helsen deres, slik som usunn deltakelse i digitale spill eller på sosiale medier.[16]

Statene som har ratifisert konvensjonen er pålagt å holde selskaper ansvarlige. For eksempel må statene sørge for at ingen selskaper krenker barns rettigheter, tilby barn, foreldre og omsorgspersoner effektive rettsmidler, samt oppmuntre til at selskaper legger ut offentlig og tilgjengelig informasjon i rett tid for å støtte opp om trygg og sunn bruk av digitale tjenester.[17] Selskaper skal også pålegges å gjennomføre og offentliggjøre barnerettighetsvurderinger.[18]

Barn har rett til beskyttelse i digitale sammenhenger. FNs generelle kommentar om barns rettigheter i det digitale miljøet understreker samtidig at bruken av digitale tjenester kan være svært viktig for barn, blant annet for sosial samhandling og utvikling, utdanning, autonomi, for å bli hørt og for å få hjelp i kriser. Stater oppfordres til å rådføre seg med barn, for eksempel i forbindelse med utarbeidelse av lover og politikk som påvirker barns rettigheter.[19]

---

[12] Generell kommentar nr. 25 (2021) avsnitt 9.
[13] Generell kommentar nr. 25 (2021) avsnitt 70.
[14] Generell kommentar nr. 25 (2021) avsnitt 85.
[15] Generell kommentar nr. 25 (2021) avsnitt 62.
[16] Generell kommentar nr. 25 (2021) avsnitt 96.
[17] Generell kommentar nr. 25 (2021) avsnitt 36.
[18] Generell kommentar nr. 25 (2021) avsnitt 38, se også følgende eksempel: «Wikimedia Foundation Child Rights Impact Assessment», Wikimedia Foundation (2023). (https://upload.wikimedia.org/wikipedia/commons/d/d8/ArticleOne_-_WMF_Child_Rights_Impact_Assessment_Report_2023.pdf).
[19] Generell kommentar nr. 25 (2021) avsnitt 16.

2.1. Det må tas hensyn til mangfoldet blant barn og unge

Mange av skadevirkningene som skisseres i denne rapporten, er dypt problematiske ikke bare for barn, men også for voksne. Likevel er det mange grunner til at barns rettigheter fortjener et særlig vern og oppmerksomhet.

Barn er i en fase av livet der personligheten, meningene og oppfatningene deres formes. Når selskaper retter kommersielle budskap mot dem eller utsetter dem for destruktivt innhold, kan barn være spesielt påvirkelige. Barn kan for eksempel ha problemer med å skille reklame fra annen, ikke-kommersiell kommunikasjon.[20] Dette gjør det spesielt viktig å beskytte dem mot uakseptabel kommersiell påvirkning.

Barns evne til å forandre seg raskt og mye gjør dessuten brudd på personvernet deres spesielt alvorlig. Etter hvert som de blir eldre, utforsker og prøver barn ut ulike stiler, meninger og interesser. Dette må være mulig, uten at en logg over alle handlingene deres på nett forfølger dem resten av livet og senere kan påvirke dem på måter vi ennå ikke kjenner til eller forstår omfanget av. Barns mulighet å utforske og forandre seg utfordres når selskaper utsetter dem for konstant digital overvåking.

Selv om barn har visse fellestrekk som gjør dem spesielt sårbare, må det tas hensyn til mangfoldet blant barn. Akkurat som voksne er barn forskjellige, både innenfor og på tvers av aldersgrupper. Evnene deres utvikler seg i ulik takt,[21] og de kan også være sårbare på ulike måter avhengig av sosioøkonomisk bakgrunn, kjønn, nasjonalitet, emosjonell stabilitet, interesser, hjemmesituasjon med mer.[22] Skadelige effekter ved bruk av sosiale medier varierer også mellom individuelle ungdommer.[23] Enkelte barn og unge står overfor ytterligere risikoer fordi de tilhører marginaliserte grupper, for eksempel dersom de er skeive.

Noen beskyttende tiltak kan ha positiv innvirkning på alle barns rettigheter, slik som tiltak for å styrke personvernet. Selskaper som tilbyr tjenester til barn, skal overholde personvernprinsippene. For eksempel skal de kun behandle barns personopplysninger på en rettferdig og lovlig måte, for spesifikke formål og minimere personopplysningene som brukes til disse formålene.[24] I praksis vil

---

[20] «Comparing children's and adults' cognitive advertising competences in the Netherlands», Rozendaal, Buijzen, Valkenburg (2010). https://www.researchgate.net/publication/232995879_Comparing_Children's_and_Adults'_Cognitive_Advertising_Competences_in_the_Netherlands.

[21] Generell kommentar nr. 25 (2021) avsnitt 19.

[22] «Changing the odds for vulnerable children», OECD (2019). https://www.oecd-ilibrary.org/docserver/23101e74-en.pdf?expires=1725998095&id=id&accname=guest&checksum=D473DA5CB7A96677F7A56AD6A5103CB6

[23] «The effect of social media on well-being differs from adolescent to adolescent», Beyens, Pouwels, Driel, Keijsers, Valkenburg (2020). https://www.nature.com/articles/s41598-020-67727-7

[24] Personvernforordningen art. 5.

overholdelse av personvernprinsippene sikre at barns personopplysninger brukes på en svært begrenset måte. Dette bidrar til å beskytte viktige rettigheter som beskyttelse av privatlivet, friheten til å tenke og danne seg oppfatninger uten urimelig påvirkning, samt at risikoen for at personopplysningene deres faller i hendene på aktører med onde hensikter begrenses betraktelig.

På den annen side viser tiltak som innholdsmoderering utfordringene med å tilby én standardløsning for å beskytte alle barn på nett. Det er betydelige forskjeller mellom et barn på fem, ti, tolv eller fjorten år, for ikke å snakke om at det kan være stor variasjon på barn innad i samme aldersgruppe. Selv om foreldre eller omsorgspersoner kan ønske å unngå at egne, unge barn skal se nyhetsinnhold som kan være opprørende, er det utvilsomt en viktig del av ungdommers utvikling at de utsettes for informasjon om verden som kan gjøre dem opprørt eller lei seg, for eksempel når de leser eller ser på nyheter.

Skadene som beskrives i denne rapporten, varierer i alvorlighetsgrad avhengig av aldersgruppe, kontekst, individuelle faktorer som modenhetsnivå, med mer. Små barn kan for eksempel være mer sårbare enn eldre ungdommer i visse sammenhenger og derfor trenge sterkere beskyttelse mot visse typer innhold. På den annen side er ungdom spesielt påvirkelige for tilbakemeldinger, oppmerksomhet og bekreftelse fra venner,[25] og er mer risikosøkende.[26] Dette kan kreve sterkere beskyttelse av ungdom mot innebygde funksjoner i sosiale medier som utnytter menneskers bekreftelsesbehov. Både barnas behov og metodene for å beskytte dem endrer seg etter hvert som de blir eldre.

Foreldreveiledning og -tilsyn kan være et viktig tiltak for å beskytte unge barn, men blir stadig mer komplisert etter hvert som barna blir eldre. Det er for eksempel enklere for foreldre eller omsorgspersoner å forhindre at en fireåring bruker digitale tjenester, enn en fjortenåring. Barna får også sterkere individuelle rettigheter overfor foreldre eller omsorgspersoner når de blir eldre, for eksempel når det gjelder selvbestemmelse og privatliv.[27] Siden det generelt er mer gjennomførbart, både juridisk og praktisk, å beskytte små barn mot skader på nettet gjennom individuelle tiltak og oppfølging fra foreldre, fokuserer denne rapporten på barn og unge fra og med skolealder.

Tiltak for å beskytte barn og unge må uansett ta hensyn til den store variasjonen innad i denne gruppen. Dette betyr at barn i ulike aldre kan ha behov for ulike beskyttelsestiltak på nett og at tiltakene for å beskytte flertallet av barn ikke bør gå på bekostning av særlig utsatte eller sårbare grupper av barn. Følgelig bør

---

[25] «Health advisory on social media use in adolescence», American Psychological Association (2023), https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use

[26] «Adolescents' heightened risk-seeking in a probabilistic gambling task», Burnett, Bault, Coricelli, Blakemore (2010). https://www.sciencedirect.com/science/article/pii/S0885201410000201

[27] Generell kommentar nr. 25 avsnitt 85.

barn og unge ha tilgang til alderstilpassede opplevelser på nettet.[28] Det er også viktig å gi selskaper og tilsynsmyndigheter tilstrekkelig rom for skjønn, for å analysere og redusere risikoer for mindre, mer spissede grupper av barn, heller enn å kreve tiltak som skjærer alle over én kam.

3. Hvordan skades barn og unge på internett?

I de senere år har det pågått en diskusjon blant forskere om hvorvidt bruk av sosiale medier skader unge menneskers psykiske helse.[29] Samtidig finnes det imidlertid utstrakt belegg for at bruken av sosiale medier er knyttet til psykiske helseutfordringer, for eksempel gjennom opplevelse av utestenging, normalisering av selvskading og spiseforstyrrelser.[30]

Sett i lys av føre-var-prinsippet er det helt klart at politiske tiltak er berettiget for å risikere risiko og skadevirkninger. I dag er det bred enighet om at barn står overfor en rekke former for risiko på nettet, ofte oppsummert i fem kategorier – innhold, kontakt, atferd, kontrakt og tverrgående aspekter. Til sammen omfatter de alle potensielle risikoer for barns rettigheter i det digitale miljøet.[31]

Alle de store sosiale mediene er aggressivt kommersialiserte, de er utformet på en måte som forsterker destruktivt innhold og holder brukerne på tjenestene så lenge som mulig og de er basert på svært invaderende sporing og profilering av enkeltpersoner. Ettersom barn endrer seg og vokser opp raskt, har forsinkede eller neglisjerte tiltak et enormt skadepotensial for svært mange barn. Som samfunn svikter vi barna dersom vi ikke treffer umiddelbare tiltak for å ivareta deres sikkerhet og rettigheter i den digitale sfæren.

Selv om alle digitale tjenester har aspekter som vil kunne være skadelige for barn og unge, dreier den offentlige debatten seg ofte om sosiale medier. Denne rapporten vil derfor i hovedsak ta opp ulike aspekter ved «tradisjonelle» sosiale medier som Facebook, SnapChat og TikTok. Som beskrevet i kapittel 4.2, mangler imidlertid begrepet 'sosiale medier' en klar definisjon og kan også overlappe med andre tjenester, slik som videoplattformer, e-handelstjenester, dataspill, osv. I resten av denne rapporten vil begrepet «sosiale medier» brukes bredt og omfatte alle tjenester som tilrettelegger for samhandling gjennom digitale plattformer, med mindre noe annet er uttrykkelig angitt.

---

[28] «Child Rights by Design», Digital Futures Commission, 5Rights Foundation. https://childrightsbydesign.digitalfuturescommission.org.uk/
[29] «Inside the debate over The Anxious Generation», Schiffer (2024). https://www.platformer.news/anxious-generation-jonathan-haidt-debate-critique/
[30] «Social Media and Youth Mental Health», the U.S. Surgeon General (2023). https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf
[31] «The 4Cs: Classifying Online Risk to Children», Livingstone, Stoilova (2021). https://www.ssoar.info/ssoar/bitstream/handle/document/71817/ssoar-2021-livingstone_et_al-The_4Cs_Classifying_Online_Risk.pdf?sequence=4&isAllowed=y&lnkname=ssoar-2021-livingstone_et_al-The_4Cs_Classifying_Online_Risk.pdf

I dette kapittelet beskriver vi hvordan barns rettigheter utfordres på dagens digitale tjenester. Tiltakene for å redusere eller fjerne disse risikoene er beskrevet i kapittel 5 og omfatter for eksempel håndheving av eksisterende regelverk, nye regler for å tette rettslige smutthull og mykere virkemidler som politiske føringer for offentlig sektor, samt retningslinjer og bedre foreldrekontroller.

3.1. En forretningsmodell som baserer seg på utnytting

Barns rett til å ikke bli utnyttet kommersielt, stopper ikke selskaper fra å forsøke å tjene penger på dem. Forskere har funnet ut at sosiale medier tjener milliarder i reklameinntekter på innhold rettet mot brukere under 18 år.[32] Ifølge Metas interne dokumenter fra 2021, anser selskapet yngre undergrupper av barn, såkalte «tweens» (8–12 år) som et «verdifullt, men uutnyttet publikum».[33] Beskyttelse av barn på nettet krever derfor en granskning av plattformenes og de digitale tjenestenes forretningsmodeller.

Alle de dominerende sosiale medieselskapene har forretningsmodeller som belønner maksimalt «engasjement», som hovedsakelig betyr å få brukerne til å fortsette å samhandle med plattformen. Sporing av brukernes atferd og salg av annonseplasser, er de viktigste inntektskildene til mange tjenestetilbydere. Tjenestetilbyderen lover annonsørene at reklamen kan målrettes mot rett person til rett tid, noe som vil øke sannsynligheten for at annonsen er effektiv. For å oppnå dette samler tjenestetilbyderen vanligvis inn store mengder data om brukeren, både data som brukeren aktivt gir fra seg (f.eks. alder, kjønn, interesser) og de som innhentes passivt (f.eks. avledede interesser, atferd). Det finnes også datameglere som selger personopplysninger om enkeltpersoner.

De samme opplysningene benyttes for å skreddersy informasjon som vises til den enkelte bruker. Under dekke av å tilby en persontilpasset brukeropplevelse, finjusteres anbefalingsalgoritmer for å maksimere brukerens tidsbruk og engasjement med plattformen, noe som gir plattformtilbyderen mulighet for å vise flere annonser. Engasjement og tidsbruk på plattformen øker når brukere eksponeres for innhold som fremkaller en sterk emosjonell respons, noe som kan føre til at algoritmene favoriserer støtende eller voldelig innhold. Kort sagt skaper forretningsmodellen en ond sirkel, der brukerne kontinuerlig blir fôret med avhengighetsskapende og destruktivt innhold, slik at de kan bli presentert for overvåkingsbasert reklame og legge igjen flere dataspor, noe som igjen gjør algoritmene mer effektive.

---

[32] «Targeting kids generates billions in ad revenue for social media», Raffoul, Ward, Santoso, Kavanaugh, Austin (2024). https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0295337.

[33] «Facebook's Effort to Attract Preteens Goes Beyond Instagram Kids, Documents Show», Wells, Horwitz (2021). https://www.wsj.com/articles/facebook-instagram-kids-tweens-attract-11632849667

Omfattende profiler av enkeltbarn kan videre brukes til en lang rekke andre kommersielle formål og så snart slik informasjon er tilgjengelig fra datameglere eller lignende aktører, er det i praksis umulig å vite hvem som vil ha tilgang til profilene eller hvordan de kan bli misbrukt.[34] I de senere år har en rekke teknologiselskaper for eksempel begynt å tråle internett etter innhold som kan brukes til å lære opp modeller for kunstig intelligens (KI-modeller). Bilder fra sosiale medier, personlige blogger, innlegg på internettfora og mye annet blir samlet inn og brukt som treningsdata. Når en KI-modell først har blitt trent, er det umulig å fjerne informasjonen som inngikk i treningsdataene og det er ofte vanskelig eller umulig å protestere mot å være en del av treningsmaterialet.[35]

Den kontinuerlige innsamlingen av barns data på tvers av digitale tjenester utgjør ikke bare en trussel mot deres personvern, men også mot deres autonomi og tankefrihet. Store mengder data om atferd og andre forhold som blir samlet inn over lange tidsperioder, gjør det mulig å spore det meste av et barns liv: fra den første gangen foreldrene eller omsorgsgiverne deres legger ut et bilde av dem på nettet, gjennom de appene de bruker på skolen,[36] og når de bruker digitale tjenester på fritiden. Dersom disse dataene brukes til å trene prediksjonssystemer, kan det også ha alvorlige implikasjoner for barnets utvikling. Prediksjoner er i sin natur basert på statistiske gjetninger ut fra tidligere observert atferd, noe som betyr at de snevrer inn omfanget av fremtidige muligheter.

Undersøkelser har vist at kommersiell overvåking gjør at barn føler seg ukomfortable og utsatt, men også at de føler seg maktesløse til å gjøre noe med det.[37] Dette kan ha betydelige «nedkjølingseffekter» på barns autonomi og ytringsfrihet, for eksempel hvis de avstår fra å søke etter informasjon fordi de er bekymret for hvordan søkehistorikken deres kan bli brukt mot dem. Etter hvert som barn vokser og modnes, bør de slippe å risikere at deres atferd og interesser i barndommen blir brukt mot dem senere i livet.

Det er en betydelig makt- og kunnskapsasymmetri mellom store teknologiselskaper som sysselsetter et enormt antall ingeniører, jurister, designere og atferdspsykologer på den ene siden og barn, foreldre og

---

[34] Mer informasjon om datameglerindustrien finnes på «Time to ban surveillance-based advertising», Forbrukerrådet (2021) https://www.forbrukerradet.no/side/new-report-details-threats-to-consumers-from-surveillance-based-advertising/

[35] En detaljert oversikt over skadevirkningene av generativ KI finnes på «Ghost in the machine – Forbrukerutfordringer ved generativ kunstig intelligens», Forbrukerrådet (2023) https://storage02.forbrukerradet.no/media/2023/08/fr-generative-ai-rapport-web-no-mindre.pdf.

[36] «'How dare they peep into my private life?' – Children's rights violations by governments that endorsed online learning during the Covid 19 Pandemic», Human Rights Watch (2022). https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

[37] «'I Feel Exposed': Caught In TikTok's Surveillance Web», Amnesty International (2023). https://www.amnesty.org/en/documents/POL40/7349/2023/en/

omsorgsgivere på den andre. Plattformenes mulighet til å trekke på kompetansen til tusenvis av høyt kvalifiserte fagfolk og bruke dette til å kontinuerlig endre innhold og utforming av tjenestene basert på barnas personopplysninger, gjør barn spesielt sårbare for kommersiell utnyttelse i den digitale sfæren.[38]

Som vi beskriver i de følgende avsnittene, ligger den dataintensive forretningsmodellen – som Amnesty International beskriver som en alvorlig trussel mot personvernet, ytringsfriheten, tankefriheten og retten til likebehandling og frihet fra diskriminering for alle brukere[39] – til grunn for mange av de sosiale medienes skadevirkninger.

3.1.1. Overvåkingsbasert markedsføring og kommersielt press

Digitale tjenester, som for eksempel sosiale medier, samler vanligvis inn store mengder data om alle sine brukere, for eksempel stedsdata, biometriske data, identitetsinformasjon og data om atferd. Slike atferdsdata blir brukt til å utnytte sårbarheter gjennom målretting av reklame og annet innhold.[40] Dersom en tenåring for eksempel engasjerer seg med plattformen på en måte som tyder på at vedkommende føler seg usikker på eget utseende, kan plattformen prioritere å vise innhold som forsterker denne usikkerheten og vise annonser for produkter som for eksempel slankepreparater, kosttilskudd eller kosmetisk kirurgi.[41]

Den reklamedrevne forretningsmodellen til sosiale medier og selskaper som annonserer for og selger produkter og tjenester, har også ført til en økende kommersialisering av så godt som all aktivitet på plattformene. Det er alltid noen som forsøker å selge deg noe eller tjene penger på deg i de digitale flatene, gjennom alt fra nyhetsstrømmer som er fulle av reklame, til influensere som utnytter den parasosiale relasjonen til sine følgere for å markedsføre produkter.

For barn og unge er det konstante kommersielle presset på digitale flater spesielt lumskt. Det påvirker alle deler av barns liv, fra lekerommet til soverommet og klasserommet. Grensene mellom markedsføring og annet innhold blir stadig mindre tydelige, noe som gjør det vanskelig å forstå om noen prøver å selge noe eller bare lager underholdning eller annet innhold. Selskaper og influensere utnytter unge menneskers iboende tillit og naivitet til å selge

---

[38] BEUC kaller dette «digital sårbarhet», eller *digital vulnerability*: «EU Consumer Protection 2.0. Protecting fairness and consumer choice in a digital economy», BEUC (2022).https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-015_protecting_fairness_and_consumer_choice_in_a_digital_economy.pdf.

[39] «Surveillance Giants: How the business model of Google and Facebook threaten human rights», Amnesty International (2019). https://www.amnesty.org/en/documents/pol30/1404/2019/en/

[40] «Time to ban surveillance-based advertising», Forbrukerrådet (2021). https://storage02.forbrukerradet.no/media/2021/06/20210622-final-report-time-to-ban-surveillance-based-advertising.pdf

[41] «Utsettes for ny type kroppspress», Teigen, Steinnes (2019). https://www.oslomet.no/forskning/forskningsnyheter/ny-type-kroppspress.

produkter,[42] for eksempel ved å blande sammen oppfordringer til innholdsproduksjon, spill og annen underholdning med markedsføring.[43] Gjennom lansering av såkalte «utfordringer» kan varemerker få med seg barn til å opptre som digitale reklameplakater.[44] For eksempel kan barn uforvarende komme til å reklamere for produkter – herunder for usunn mat,[45] alkohol,[46] pengespill[47] og liknende – eller oppfordre andre barn til risikofylt atferd.[48]

Det finnes lovverk som regulerer markedsføring som påvirker barn, inkludert på digitale tjenester.[49] De nåværende håndhevingsregimene for mye av denne lovgivningen har imidlertid havnet bakpå i forhold til omfanget av ulovlig reklame på nett og er både utilstrekkelig og har for liten grad av avskrekkende effekt. Noen håndhevingsregimer er basert på selvreguleringsordninger med bransjerepresentanter, som har liten eller ingen makt til å pålegge sanksjoner for overtredelser.[50]

I den digitale sfæren kan det derfor fremstå som at det er fritt fram for enhver som ønsker å tjene penger på å målrette kommersielt innhold mot unge mennesker. Det er også dokumentert at store teknologiselskaper finner omveier for å målrette innhold mot barn, ved å målrette innhold mot kategorier av brukere med «ukjent» alder, selv om de vet at disse brukergruppene først og fremst består av barn.[51]

---

[42] «From influence to responsibility. Time to regulate influencer marketing», BEUC (2023). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-093_From_influence_to_responsibility_Time_to_regulate_influencer-marketing.pdf

[43] «How children are being targeted with hidden ads on social media», Rossi, Nairn, The Conversation (2021). https://theconversation.com/how-children-are-being-targeted-with-hidden-ads-on-social-media-170502.

[44] «TikTok without filters», BEUC (2021): https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-012_tiktok_without_filters.pdf.

[45] «Food marketing to children needs rules with teeth», BEUC (2021). https://www.beuc.eu/reports/food-marketing-children-needs-rules-teeth

[46] «Picture me drinking: alcohol-related posts by Instagram influencers popular among adolescents and young adults», Hendriks, Wilmsen, Dalen, Gebhardt (2020). https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2019.02991/full

[47] «Gambling operators' use of advertising strategies on social media their effects: a systematic review», Singer, Wöhr, Otterbach (2024). https://link.springer.com/article/10.1007/s40429-024-00560-4

[48] «Under the influence of (alcohol)influencers? A qualitative study examining Belgian adolescents' evaluations of alcohol-related Instagram images from influencers», Vranken, Beullenes, Geyskens, Matthes (2021). https://www.tandfonline.com/doi/full/10.1080/17482798.2022.2157457 og «Young and exposed to unhealthy marketing», Forbrukerrådet (2019) https://storage02.forbrukerradet.no/media/2019/02/young-and-exposed-to-unhealthy-marketing-digital-food-marketing-using-influencers-report-february-2019.pdf.

[49] Se mer om disse reglene i kapittel 5.1.

[50] Se for eksempel problemer med denne tilnærmingen på EU-nivå: («Food marketing to children needs rules with teeth», BEUC (2021), https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-084_food_marketing_to_children_needs_rules_with_teeth.pdf) og i Norge: («Krever bedre regulering av markedsføring på nett mot unge», Forbrukerrådet (2020). https://www.forbrukerradet.no/siste-nytt/krever-bedre-regulering-av-markedsforing-pa-nett-mot-unge/).

[51] «Google and Meta struck secret ads deal to target teenagers», Morris, Murphy, Financial Times (2024). https://www.ft.com/content/b3bb80f4-4e01-4ce6-8358-f4f8638790f8

Det er et sterkt behov for omfattende tiltak for å sette en stopper for ulovlig markedsføring på digitale flater, som må rette seg mot annonsører, plattformene som selger annonseplasser og influensere som markedsfører produkter og tjenester til barn og unge. Dette forutsetter sterkere håndheving av det eksisterende lovverket som gjelder for reklame og markedsføring. I tillegg er det nødvendig med målrettede oppdateringer av handelspraksisdirektivet (Unfair Commercial Practices Directive), for å innføre forbud mot visse typer markedsføring mot barn og for å sikre at selskapene ikke kan finne måter å omgå regelverket. Disse og flere andre tiltak er beskrevet nærmere i kapittel 5.1.

3.1.2. Forsterking av destruktivt innhold

På sosiale medier florerer det med ekstremt og destruktivt innhold, slik som videoer av selvmord, vold og narkotikamisbruk. Det er to sider ved dette problemet: dels handler det om hvordan anbefalingsalgoritmer prioriterer innholdet til brukerne, dels om hvorvidt innholdet er tillatt på plattformen i det hele tatt.

For både ungdommer og voksne er det en viktig forskjell på å bli overrumplet av opprørende innhold som blir anbefalt av en algoritme og å aktivt søke etter slikt innhold. Å kreve at selskapene endrer algoritmene sine kan ha en viktig effekt på hvilke typer innhold som anbefales til enkeltpersoner og i hvilke sammenhenger enkeltpersoner blir eksponert for innholdet.

Anbefalingsalgoritmer

Som beskrevet i forrige kapittel, er sosiale medier ofte finansiert gjennom salg av annonseplass. Når brukere skroller gjennom nyhetsstrømmen eller ser på endeløse serier av videoer, kan plattformen vise annonser som resulterer i inntekter. Dette har skapt et økonomisk insentiv til å holde brukerne aktive på plattformen så lenge som mulig. Innhold som fremkaller sinne, frykt, sorg og hat blir forsterket fremfor alt annet, fordi det bidrar til engasjement med plattformen.[52] Sosiale medieselskaper har aktivt motsatt seg tiltak for å forbedre situasjonen.[53]

Anbefalingsalgoritmene som kontrollerer hva den enkelte ser på plattformen, «lærer» ved å observere brukeren, noe som betyr at brukere som oppsøker bestemte former for innhold, vil bli vist mer av det samme – eller mer ekstreme

[52] «Facebook under fire – Five points for anger, one for a 'like': How Facebook's formula fostered rage and misinformation», Merrill, Oremus, The Washington Post (2021). https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/

[53] «Facebook executives shut down efforts to make the site less divisive», Horwitz, Seetharaman, The Wall Stress Journal (2020). https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499

versjoner av – innholdet.[54] Dette er også kjent som «kaninhull-effekten», der brukere som opprinnelig engasjerte seg med eller så på relativt ufarlig innhold, blir presentert for stadig mer ekstremt innhold, helt til de har blitt «trukket ned i kaninhullet». Praksisen knyttes ofte til radikalisering.[55]

Det finnes talløse eksempler på barn og unge som har falt ned i slike kaninhull, for eksempel deprimerte tenåringsjenter som blir eksponert for stadig grovere og mer støtende innhold, som til og med kan inkludere videoer av mennesker som begår selvmord.[56] Tilsvarende er barn og unge i sine formative år er spesielt mottakelige for innhold som utnytter deres usikkerhet, slik som innhold om slanking, vold og pengespill.[57]

Selv om anbefalingsalgoritmer i dag er utformet for å maksimere tiden og oppmerksomheten folk bruker på plattformen, er ikke dette en nødvendig egenskap ved teknologien. Da sosiale medier som fenomen først begynte å vokse fram i samfunnet, ble brukere i hovedsak vist innhold fra personer og organisasjoner som de selv aktivt valgte å følge.[58] Dagens sosiale medier anbefaler i hovedsak tvert imot innhold og videoer basert på sponset innhold og «innhold som kan være av interesse for deg». Sluttbrukere har liten kontroll over hva de blir vist, fordi dette ville vært mindre lukrativt for plattformene.

Skadevirkninger som stammer fra anbefalingsalgoritmer, kan motvirkes og begrenses ved å kreve at selskapene reduserer bruken av personopplysninger til å anbefale innhold. I tillegg må brukerne få mer kontroll over hvilket innhold de ønsker å se, tryggere standardinnstillinger og alderstilpasset design. Det finnes allerede lovverk som kan benyttes til å håndheve slike tiltak, som beskrives nærmere i kapittel 5.1.

---

[54] Se for eksempel «Recommender systems and the amplification of extremist content», Whittaker, Looney, Reed, Votta (2021) https://policyreview.info/articles/analysis/recommender-systems-and-amplification-extremist-content, «Fixing recommender systems», Panoptykon, Irish Council for Civil Liberties, People vs. Big Tech (2023) og «When my dad was sick, I started Googling grief. Then I couldn't escape it», Ryan-Mosley (2023). https://www.technologyreview.com/2023/02/06/1067794/escape-grief-content-unsubscribe-facebook-instagram-amazon-recommendation-algorithms/.

[55] «YouTube Regrets: A crowdsourced investigation into YouTube's recommendation algorithm», Mozilla (2021). https://assets.mofoprod.net/network/documents/Mozilla_YouTube_Regrets_Report.pdf

[56] «Driven Into Darkness: How TikTok encourages self-harm and suicidal ideation», Amnesty International (2023). https://www.amnesty.org/en/latest/news/2023/11/tiktok-risks-pushing-children-towards-harmful-content/

[57] «Pathways: How digital design puts children at risk», 5Rights Foundation (2021). https://5rightsfoundation.com/uploads/Pathways-how-digital-design-puts-children-at-risk.pdf

[58] «Social Quitting», Doctorow (2023). https://pluralistic.net/2023/01/08/watch-the-surpluses/

Innholdsmoderering

Forekomsten av destruktivt innhold må også håndteres gjennom innholdsmoderering på plattformene. Innholdsmoderering er imidlertid svært vanskelig å gjøre på en god måte – det er i bunn og grunn et forsøk på å benytte en teknologisk løsning på en rekke kompliserte og sammensatte utfordringer.[59]

Manglende moderering innebærer at destruktivt innhold sprer seg. Samtidig kan for mye moderering gå på bekostning av viktige rettigheter som ytringsfrihet og tilgang til informasjon. Dette gjelder spesielt for automatisert innholdsmoderering, der effektiviteten av innholdsmodereringen måles basert på omfang og kvantitet, snarere enn nøyaktighet.

Enkelte typer innhold, for eksempel TikTok-videoer som idealiserer og romantiserer selvskading, kan virke åpenbart skadelige og dermed noe som ingen bør se, særlig ikke mindreårige. Selv i slike tilfeller kan det imidlertid være ekstremt vanskelig å skille mellom hvilke typer innhold som er skadelige eller ikke, fordi konteksten for innholdet er viktig – å spre kunnskap om psykiske lidelser er ikke det samme som å fremme selvskading. Tilsvarende finnes det ingen klar juridisk definisjon av begrepet «skadelig innhold».[60]

Å betegne noe som skadelig innhold er kulturelt og politisk betinget. I enkelte deler av verden blir informasjon om temaer som seksualitet og kjønnsuttrykk betraktet som kontroversielt og upassende for mindreårige, mens det i andre land anses som absolutt nødvendig for spesielt sårbare grupper og inkluderes som del av utdanningsløpet.

Det pågår politiske debatter om hvorvidt bilder som viser krigsforbrytelser og andre grusomheter bør være tillatt på sosiale medier.[61] Selv om slike bilder uten tvil er opprørende, er bildene ofte også avgjørende for å spre bevissthet i samfunnet. Selv om det synes klart at en åtteåring ikke bør bli utsatt for slikt innhold, er det usikkert om en fjortenåring trenger det samme nivået av beskyttelse.

Videre vil aggressiv innholdsmoderering uten tilstrekkelig innsyn og effektive klagemekanismer uunngåelig føre til situasjoner der legitimt innhold blir fjernet, eller kontoer blir stengt uten tilstrekkelig forklaring eller klagemuligheter. Manglende åpenhet rundt modereringspraksis reduserer også muligheten forskere har til å vurdere hvor effektivt innholdsmodereringen fungerer.

---

[59] «Treating the symptoms or the disease? Analysing the UK Online Safety Act's Approach to digital regulation», Nash, Felton (2024). https://onlinelibrary.wiley.com/doi/pdf/10.1002/poi3.404
[60] «The perils of legally defining disinformation», Fathaig, Helberger, Appelman (2021). https://policyreview.info/articles/analysis/perils-legally-defining-disinformation
[61] «Meta's Broken Promises: Systematic Censorship of Palestine Content on Instagram and Facebook», Human Rights Watch (2023). https://www.hrw.org/report/2023/12/21/metas-broken-promises/systemic-censorship-palestine-content-instagram-and

De skadevirkningene som stammer fra destruktivt innhold, kan reduseres ved å bremse anbefalingsalgoritmenes spredning og forsterkning av ulovlig og destruktivt innhold, som skissert ovenfor. Det er viktig å skille mellom tiltak som forhindrer brukere fra å få tilgang til bestemte typer innhold i det hele tatt, og som forhindrer plattformen i å aktivt fremme og spre innholdet. Dette må suppleres av en sterkere, mer robust, menneskekontrollert og transparent praksis for innholdsmoderering fra plattformtilbydernes side, samt alderstilpasset design og merking av innhold som kan være opprørende. Tiltakene er nærmere beskrevet i kapittel 5.1.

3.1.3. Avhengighetsskapende mekanismer og overdreven skjermbruk

En av de største bekymringene rundt unge menneskers bruk av internett, er at de tilbringer for mye tid foran skjermen. Det diskuteres for eksempel hvordan bruken av mobiltelefon kan komme i veien for andre viktige deler av barns liv, som skole, fysisk aktivitet, fri lek, utvikling av sosiale ferdigheter og søvn, og kan føre til øyeskader.[62] Selv om dette også kan hevdes å være et problem blant voksne, er skjermtidens virkning på barn og unge spesielt problematisk dersom den påvirker andre vesentlige deler av livet deres mens de formes og vokser opp.

Som beskrevet i de foregående kapitlene, har forretningsmodellen bak sosiale medier skapt et sterkt insentiv til å holde brukerne fanget (eller «engasjert») så lenge som mulig, til enhver pris. Anbefalingsalgoritmene optimerer kontinuerlig innhold etter hva som skaper mest engasjement med plattformen, og som derfor er både avhengighetsskapende og dopaminutløsende. Brukerne blir kontinuerlig bombardert med innhold som algoritmen har regnet ut at vil få brukeren til å fortsette å skrolle, klikke og se.[63]

Plattformene oppmuntrer også innholdsprodusenter til å lage innhold som får brukere til å fortsette å skrolle, klikke og se, for eksempel gjennom økonomiske insentiver for innholdsprodusenter som laster opp innhold som fører til engasjement med plattformen.[64] De mest vellykkede innholdsprodusentene er eksperter i å utnytte anbefalingsalgoritmene og skreddersyr innhold for å maksimere antall visninger og delinger.[65] Dette kan for eksempel resultere i at kunstig intelligens brukes til å lage og spre innhold i hurtig tempo.[66]

---

[62] «Digital Screen Use and Dry Eye: A Review» Mehra, Galor (2020). https://www.sciencedirect.com/science/article/pii/S216209892300155X

[63] «What Makes TikTok so Addictive?: An Analysis of the Mechanisms Underlying the World's Latest Social Media Craze», Petrillo (2021). https://sites.brown.edu/publichealthjournal/2021/12/13/tiktok/

[64] «Facebook Content Monetization Beta», Meta. https://creators.facebook.com/programs/bonuses/?locale=en_US

[65] «Playing the visibility game: How digital influencers and algorithms negotiate influence on Instagram», Cotter (2019). https://pure.psu.edu/en/publications/playing-the-visibility-game-how-digital-influencers-and-algorithm

[66] «Where Facebook's AI Slop Comes From», Koebler, 404Media (2024). https://www.404media.co/where-facebooks-ai-slop-comes-from/

For å sikre at brukerne fortsetter å komme tilbake til plattformene benytter tjenestetilbyderne ofte mekanismer som varslinger eller «streaks». Andre triks brukes deretter for å holde brukeren limt fast til skjermen. For eksempel anvender mange plattformer for deling av videoer en automatisk avspillingsfunksjon, som viser brukerne en ny video uten at de trenger å aktivt be om det. Slike avhengighetsskapende mekanismer blir bevisst benyttet for å fremskynde vanedannende atferd hos brukerne.[67] Mekanismene utvikles også kontinuerlig.

Innføringen av tjenester for generativ kunstig intelligens har ført til at selskaper kan automatisere og skreddersy engasjement hos enkeltbrukere. Samtaleroboter markedsføres som virtuelle venner og åpner nye muligheter for parasosiale relasjoner, mens simulerte følelser og tilgjengelighet døgnet rundt legger grunnlag for potensiell avhengighet og manipulering.[68] Det er spesielt problematisk at KI-tjenester rulles ut og presses på barn og unge som kan ha vansker med å forstå at KI-systemet ikke er en person og ikke har noen følelser.

Ettersom bekymringene rundt overdreven skjermtid har økt, har flere teknologiselskaper innført tiltak for å redusere skjermtid. Disse tiltakene må vurderes kritisk. Interne dokumenter fra TikTok viser for eksempel at deres verktøy for å begrense tidsbruk har minimal effekt på skjermtid.[69] Formålet fra selskapets side er primært å skape talepunkter i politiske sammenhenger og å øke tilliten i befolkningen. Istedenfor å faktisk endre de avhengighetsskapende mekanismene, innfører plattformene altså ineffektive verktøy, som gir et falskt inntrykk av ansvarlighet.

Avhengighetsskapende mekanismer kan motvirkes gjennom sterk og ambisiøs håndheving av eksisterende lovverk, samtidig som det er nødvendig å innføre nye regler som stiller krav til å redusere eller fjerne avhengighetsskapende mekanismer og manipulerende design. Tjenestetilbydere bør pålegges å utforme sine plattformer på en rettferdig og trygg måte og bør også tilby fungerende foreldrekontroller med alderstilpassede standardinnstillinger for skjermtid. I tillegg bør myndighetene publisere faktabaserte, tydelige og lett forståelige retningslinjer som kan hjelpe foreldre og omsorgsgivere med å sette grenser for sine barns skjermbruk. Disse tiltakene er videre beskrevet i kapittel 5.

---

[67] «EU lawmaker points to mental health risks for online services' addictive design», Tar, Euractiv (2023). https://www.euractiv.com/section/platforms/news/eu-lawmaker-points-to-mental-health-risks-for-online-services-addictive-design/

[68] «One is the loneliest number... Two can be as bad as one. The influence of AI Friendship Apps on users' well-being and addiction», Marriott, Pitardi (2023). https://onlinelibrary.wiley.com/doi/10.1002/mar.21899

[69] «TikTok executives know about app's effect on teens, lawsuit documents allege», Allyn, Goodman, Kerr, NPR.(2024). https://www.npr.org/2024/10/11/g-s1-27676/tiktok-redacted-documents-in-teen-safety-lawsuit-revealed

3.2. Andre alvorlige utfordringer

Så langt har denne rapporten gjennomgått en rekke risikoer barn møter på nett. Ikke alle skadevirkninger av digitale tjenester kan eller bør imidlertid forstås i lys av forbrukerperspektivet.

Derfor beskriver vi i det følgende kort noen av de mest diskuterte skadevirkningene, nærmere bestemt psykisk uhelse, nettmobbing og uønsket kontakt med fremmede. Flere av disse kan likevel være tett forbundet med forretningsmodellen som er beskrevet ovenfor.

3.2.1. Psykisk uhelse

I de senere år har det skjedd en drastisk negativ utvikling i unge menneskers psykiske helse. Lekkasjer fra Facebook har vist at selskapet var klar over hvilken negativ virkning plattformen hadde på tenåringer og barn,[70] og i 2023 utga USAs helsedirektør («general surgeon») en urovekkende rapport om sosiale mediers og barns psykiske helse og livskvalitet.[71]

Sosiale medier kan påvirke brukernes selvbilde negativt på ulike måter og barn og unge er spesielt sårbare for dette. «Liker»-funksjoner er for eksempel et tilsynelatende klart og kvantifiserbart mål på sosial anerkjennelse eller fordømmelse. Dette utnytter ungdommers behov for bekreftelse og frykten for å gå glipp av noe og kan skape eller forsterke eksisterende følelser av usikkerhet og dermed føre til stress, depresjon og andre psykiske helseproblemer.[72]

Det finnes en rekke influensere og andre kommersielle aktører som publiserer innhold som kan ha en negativ virkning på barns og ungdommers selvbilde. Dette kan utspille seg i form av videoer om selvutvikling, pornografisk materiale,[73] problematiske kostholdsråd og treningsprogrammer forkledd som velværeprogrammer, eller markedsføring for kosmetisk kirurgi og produkter som motvirker aldringssymptomer,[74] alkohol, pengespill, risikofylte finansielle

---

[70] «Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show», Wells, Horwitz, Seetharaman, The Wall Street Journal (2021). https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739

[71] «Surgeon General Issues New Advisory About Effects Social Media Use Has on Youth Mental Health», U.S. Department of Health and Human Services (2024). https://www.hhs.gov/about/news/2023/05/23/surgeon-general-issues-new-advisory-about-effects-social-media-use-has-youth-mental-health.html

[72] «Fear of missing out and social networking sites use and abuse: A meta-analysis», Giulia Fioravanti, Silvia Casale, Sara Bocci Benucci, Alfonso Prostamo, Andrea Falone, Valdo Ricca, Francesco Rotella, Computers in Human Behavior, Volume 122 (2021). https://doi.org/10.1016/j.chb.2021.106839

[73] «Undress or fail: Instagram's algorithm strong-arms users into showing skin», Algorithm Watch, European Data Journalism Network (2020). https://algorithmwatch.org/en/instagram-algorithm-nudity/

[74] «Young girls are using anti-aging products they see on social media. The harm is more than skin deep», Gecker, The Associated Press (2024). https://apnews.com/article/influenced-skincare-routine-mental-health-f59bb09114ab93323e3a47197a1ad914

produkter osv. Anbefalingsalgoritmer kan også stilles inn til å prioritere innhold med konvensjonelt vakre mennesker og apper kan inneholde «skjønnhetsfiltre», som begge kan påvirke kroppsbilde.[75]

Selv om problemer knyttet til barns mentale helse og livskvalitet ikke utelukkende kan forstås i lys av digitalisering og sosiale medier, finnes det viktige tiltak som kan innføres i den digitale sfæren for å redusere den psykiske belastningen hos barn og unge. Mange av problemene forverres av den aggressive kommersialiseringen, forsterkingen av destruktivt innhold og de avhengighetsskapende mekanismene nevnt tidligere i denne rapporten.

Det bør derfor innføres sterkere regulering av markedsføring, inkludert forbud mot bestemte typer markedsføring rettet mot barn og unge, slik det blir beskrevet i kapittel 5.1.1 og 5.1.2. Videre kan håndheving av regler som reduserer eller fjerner avhengighetsskapende mekanismer, design som leder til forsterking av destruktivt innhold og annen inngripende profileringspraksis også være viktige verktøy for å bekjempe psykiske skadevirkninger av digitalt innhold.

3.2.2. Nettmobbing

Selv om sosialt press og mobbing også finnes andre steder enn på nettet, har utbredelsen av sosiale medier intensivert og utvidet negative situasjoner. Det kan ha sterkt negative følger, både når situasjonene oppstår i møte med personer fra barnet eller ungdommens egen sosiale krets, eller i uoppfordret kontakt med fremmede.

Sosiale medier skaper nye utfordringer med sosial ekskludering og andre former for mobbing. Stadige statusoppdateringer fra venner skaper et inntrykk av at alle andre lever et bedre og mer meningsfylt liv, er mer populære og så videre. Apper sender varsler fortløpende, hele dagen for å «minne» brukerne på at alle andre alltid har det hyggelig. Deling av stedsdata, slik som SnapMap, kan få barn og unge til å føle seg ekskludert ved å vise andre personer som er på samme fest, går på konsert sammen, osv. I andre tilfeller har barn brukt anonyme meldingsapper[76] og funksjoner som får meldinger til å bli borte,[77] til å trakassere og mobbe andre barn.

---

[75] «TikTok executives know about app's effect on teens, lawsuit documents allege», Allyn, Goodman, Kerr, NPR (2024). https://www.npr.org/2024/10/11/g-s1-27676/tiktok-redacted-documents-in-teen-safety-lawsuit-revealed

[76] «Millions of teens are using a new app to post anonymous thoughts, and most parents have no idea», Balingit (2015). https://www.washingtonpost.com/local/education/millions-of-teens-are-using-a-new-app-to-post-anonymous-thoughts-and-most-parents-have-no-idea/2015/12/08/1532a98c-9907-11e5-8917-653b65c809eb_story.html

[77] «Gone in a Flash: How Disappearing Messages Can Impact Your Child's Online Safety», Mobicip (2024). https://www.mobicip.com/blog/gone-flash-how-disappearing-messages-can-impact-your-childs-online-safety

Deling av brukergenerert innhold kan også ha spesielt skadelige virkninger på unge mennesker. Innhold slik som bilder kan raskt bli spredt utenfor barnets kontroll, selv når det i utgangspunktet blir delt frivillig. Problemet kan videre forverres dersom foreldre, omsorgsgivere eller andre uforvarende deler bilder av barnet. Måten internett fungerer på betyr at det er så godt som umulig å fjerne innhold etter at det har blitt spredd og kan derfor ha svært negative konsekvenser for personen innholdet gjelder. De negative konsekvensene kan vende tilbake over tid og i nye sammenhenger.

Nettmobbing, inkludert uønsket deling av bilder, er en del av et bredere sosialt problem, selv om internett har gitt dette fenomenet ekstra kraft. Problemet kan følgelig ikke løses fullstendig med teknologiske eller juridiske tiltak. Utdanning og opplæring av unge mennesker til å bli digitale borgere er for eksempel sentralt, sammen med andre typer tiltak.[78]

Nettmobbing er et alvorlig problem, men det ligger utenfor Forbrukerrådets mandat og derfor denne rapporten. Samtidig kan skadevirkninger fra nettmobbing reduseres ved at plattformene fjerner eller endrer designelementer som kan legge til rette for nettmobbing. Noen av disse er knyttet til plattformenes forretningsmodell. Våre anbefalinger for å skape en digital sfære som støtter opp under barns rettigheter er beskrevet i kapittel 5.

3.2.3. Uønsket kontakt med fremmede

Uønsket kontakt med fremmede er også en vesentlig bekymring når barn bruker sosiale medier, på grunn av risikoen for seksuell utnyttelse av barn på nettet.[79] Det er mulig å redusere dette problemet ved å innføre funksjoner som blokkerer meldinger fra fremmede til profiler som tilhører barn og unge og at barns kontoer ikke anbefales til fremmede.[80] Selv om kontakt med fremmede er et alvorlig problem, ligger dette utenfor Forbrukerrådets mandat og derfor denne rapporten.

Det finnes ulike hjelpelinjer som barn, deres foreldre og omsorgsgivere kan bruke i tilfeller av nettmobbing, uønsket kontakt med fremmede eller andre ubehagelige situasjoner. Disse vil vanligvis variere fra land til land.[81]

---

[78] «Ending the torment: tackling bullying from the schoolyard to cyberspace», UNICEF (2016). https://www.unicef.org/media/66536/file/Ending-the-torment.pdf

[79] «Child Sexual Exploitation», EUROPOL. https://www.europol.europa.eu/crime-areas/child-sexual-exploitation

[80] «Risky-by-Design. Case study: Friend suggestions», 5Rights Foundation. https://www.riskyby.design/friend-suggestions

[81] For Norge finnes denne her: «Barn, ungdom og voksne – her kan du snakke, chatte og få hjelp», Redd Barna. https://www.reddbarna.no/her-kan-du-fa-hjelp/

4. Utfordringer ved teknisk blokkering av digitale tjenester

Å stanse barn fra å få tilgang til digitale tjenester blir ofte trukket fram som et av de viktigste tiltakene for å beskytte dem mot de skadevirkningene som er skissert ovenfor. Tiltaket dukker opp i ulike sammenhenger, som i politiske debatter,[82] eller tilsynsavgjørelser.[83]

Selv om de negative virkningene av sosiale medier ikke skal undervurderes, finnes det også betydelige risikoer knyttet til å stenge barn, og særlig ungdommer, ute. Dette kan begrense deres evne til å få ivaretatt sine øvrige rettigheter på nettet, som beskrevet i kapittel 2.

De tekniske løsningene for å sperre barn og unge ute kan også introdusere en rekke nye utfordringer og risikoer. Mange av disse risikoene påvirker ikke bare barn og unge, men også voksne. For eksempel vil et krav om fremlegging av identitetspapirer på sosiale medier nødvendigvis innebære at også alle voksne må identifisere seg.

Som vi beskriver i de følgende underkapitlene vil tiltak som retter seg mot bestemte plattformer (slik som TikTok, Snapchat eller Instagram), etterlate seg store blindsoner. Det er også fare for at tekniske løsninger for utestengelse av barn og unge fra digitale tjenester, både er ineffektive for å beskytte dem på nettet, og til og med kan forverre situasjonen. Et viktig bakteppe for diskusjonen er også at flere rapporter har konkludert med at det per dags dato ikke finnes noen tekniske løsninger som i tilstrekkelig grad ivaretar brukernes grunnleggende rettigheter.[84]

4.1. Bør barn og unge utestenges fra sosiale medier?

Når politikere og andre vurderer å innføre harde tekniske sperrer for sosiale medier, bør de også ta hensyn til de legitime årsakene til at barn er på nettet i utgangspunktet. Dette er viktig, fordi det kan tilsi at andre, effektive tiltak bør prioriteres dersom de reduserer de skadevirkningene barn er utsatt for på nettet uten å begrense barns øvrige rettigheter.

---

[82] Debatt i EU («European authorities press on with digital wallets for social media age verification», Gkritsi, Euractiv (2024). https://www.euractiv.com/section/tech/news/european-authorities-press-on-with-digital-wallets-for-social-media-age-verification/) og i Norge («Støre vil ha aldersgrense for sosiale medier», Jobling, NRK (2024). https://www.nrk.no/norge/store-vil-ha-aldersgrense-for-sosiale-medier-1.16944311).

[83] «Vulnerable Individuals. Tools for Online Protection. Children and Age Verification – Spring Conference 2023», Garante per la Protezione dei Dati Personali (2023). https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9965235

[84] Se for eksempel «Trustworthy Age Assurance?», Sas, Mühlberg, Greens/EFA (2024) https://extranet.greens-efa.eu/public/media/file/1/8760 og «Online age verification: balancing privacy and the protection of minors», CNIL (2022). https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors.

Det finnes svært legitime grunner til at barn over en bestemt alder trenger tilgang til mange av de plattformene som politikerne i dag vurderer å innføre aldersspærrer på. Mange barn og unge, særlig fra tidlig i tenårene, bruker for eksempel sosiale medier til å delta i samfunnet, holde seg oppdatert og mobilisere for saker de er opptatte av. Dette kan være alt fra lokale ungdomsgrupper og aktiviteter, til globale kampanjer som for eksempel Fridays for Future.[85]

Sosiale medier har vært viktige mobiliseringsverktøy for grasrotkampanjer over hele verden og for barn er dette én av få muligheter til å gjøre sin stemme hørt. Dersom ungdommer blir nektet tilgang til sosiale medier og lignende digitale tjenester, kan de miste et viktig talerør.

Etter hvert som politisk debatt i økende grad forflytter seg til digitale arenaer, medfører utestengelse fra disse plattformene at unge mennesker risikerer å bli fratatt en betydelig del av sin utdanning til å bli samfunnsborgere. Deltakelse i digitale fora kan dem mulighet til å lære om verden, bli eksponert for ulike kulturer og meninger, og hjelpe dem med å utvikle egenskaper som kritisk tenkning, beslutningsevne og autonomi.

Selv om sosiale medier kan bidra til konflikt og splittelse, fungerer tjenestene også som møteplass, og de kan være livsviktige for mange unge mennesker. Ulike nettsamfunn kan for eksempel gi barn og unge som føler seg alene mulighet til å finne likesinnede. Dette kan være spesielt viktig for skeive barn og unge, for eksempel hvis de føler seg isolert fordi de vokser opp i en liten bygd. Barn og unge med funksjonshemminger kan også bruke digitale tjenester til å få kontakt og omgås med andre barn, for eksempel gjennom nettbaserte dataspill.[86]

4.2. Å definere sosiale medier er komplisert

I den offentlige debatten betraktes sosiale medier ofte som en bestemt type digital tjeneste som skader barn og unge mennesker. Det finnes imidlertid ingen bred enighet om hva «sosial medier» faktisk er. Tjenester som Facebook, Instagram og TikTok faller kanskje åpenbart inn under begrepet. Etter hvert som man forsøker å definere «sosiale medier», blir grensene imidlertid mindre tydelige. Dette påvirker vurderingen av proporsjonalitet for aldersspærrer i sosiale medier.

---

[85] «Gen Z: How young people are changing activism», Carnegie, BBC (2022). https://www.bbc.com/worklife/article/20220803-gen-z-how-young-people-are-changing-activism

[86] «Først da Mats var død, forsto foreldrene verdien av gamingen hans», Schaubert, NRK (2019). https://www.nrk.no/dokumentar/xl/forst-da-mats-var-dod_-forsto-foreldrene-verdien-av-gamingen-hans-1.14197198

Sosial nettverksbygging er ofte et element i tjenester som vanligvis ikke betraktes som sosiale medier. Dette kan for eksempel omfatte tjenester som meldingsapper (iMessage, Whatsapp, Signal), nettbaserte dataspill (Roblox, Fortnite), diskusjonsfora (Reddit, Discord) og praktisk talt alle tjenester som inkluderer kommentarfelt eller lignende funksjoner, slik som videoplattformer (YouTube) og nyhetstjenester.

Wikipedia definerer sosiale medier som «tjenester på Internett som ikke skiller mellom produsenter og konsumenter av innhold – innholdet lages i stor grad av brukerne selv – og som legger til rette for 'mange til mange-kommunikasjon'».[87] Dette omfatter vanligvis funksjoner som sosial nettverksbygging, brukerskapt innhold og profiler, og algoritmebaserte nyhetsstrømmer.

EU-forordningen om digitale tjenester (DSA) inneholder også en henvisning til sosiale medier: «internettbaserte plattformer, slik som sosiale nettverk [...], skal defineres som tilbydere av hosting-tjenester som ikke bare lagrer informasjon som er stilt til disposisjon av mottakerne av tjenesten på deres oppfordring, men som også formidler denne informasjonen til offentligheten på oppfordring fra mottakerne av tjenesten».[88] I praksis betyr formidling av informasjon til offentligheten at informasjonen skal være tilgjengelig for et ubegrenset antall personer.[89] Selv om denne definisjonen kan synes å utelate meldingsapper, vil den for eksempel kunne omfatte alle typer diskusjonsfora.

Når man skal innføre tiltak for å beskytte barn og unge mot sosiale mediers skadevirkninger, er det viktig å ha tydelig for seg hvilke forebyggende tiltak som er nødvendige og relevante og hvilke typer plattformer som skal iverksette de aktuelle forebyggende tiltakene. Mange av de skadelige virkningene som er beskrevet i forrige kapittel, er ikke begrenset til de «tradisjonelle» sosiale mediene, men kan være like utbredt innenfor andre typer tjenester, som læringsplattformer, e-handelstjenester og dataspill. En smal definisjon av sosiale medier kan resultere i at skadevirkningene som barn og unge må beskyttes mot, fortsetter på øvrige plattformer og tjenester.

4.3. Ekskludering av barn under en bestemt alder beskytter ikke barn som er over aldersgrensen

Som beskrevet i kapittel 3 kjennetegnes mange digitale plattformer av en forretningsmodell som er basert på utnytting, hvilket resulterer i aggressiv kommersialisering, omfattende brudd på personvernet, forsterking av destruktivt innhold og avhengighetsskapende mekanismer. Tiltak som ekskluderer barn under en bestemt alder fra sosiale medier, påvirker ikke

[87] «Sosiale medier», Wikipedia. https://no.wikipedia.org/wiki/Sosiale_medier
[88] DSA fortalepunkt 13, uoffisiell oversettelse.
[89] DSA fortalepunkt 14.

hvordan plattformene ellers utformer tjenestene sine. Dette betyr at alle som er over aldersgrensen, inkludert personer som har juridisk status som barn fordi de er under 18 år, vil fortsette å bli utsatt for svært problematiske og skadelige forretningsmodeller.

Innføring av en hard, teknisk aldersspærre – som betyr at alle som ikke innfrir verifikasjonskravet, blir stengt ute – vil være både tidkrevende og kostbart, selv om det bare innføres på de mest populære digitale tjenestene. Dessuten vil det sannsynligvis gå på bekostning av andre initiativer, som for eksempel målrettede tiltak for å forhindre skadevirkningene som oppstår på grunn av plattformenes innretning. Dette betyr at selskapene kan fortsette å utsette barn som er over en gitt aldersgrense (for eksempel 13 eller 15 år), for destruktivt innhold som meningsløs vold og idealisering av spiseforstyrrelser og selvmord. På samme måte vil de avhengighetsskapende mekanismene på plattformene fortsette uhindret, og selskaper kan fortsette å utnytte barns sårbarheter til å målrette innhold og reklame mot dem.

Dersom innsatsen rettes mot harde, tekniske aldersspærrer for digitale tjenester, vil det også kunne føre til en vekst i markedet for alderskontrollsystemer, som kan gå på bekostning av markedet for alderstilpassede digitale tjenester. Digitale tjenester kan brukes til barns beste på mange måter, forutsatt at tjenestene er utformet på en måte som respekterer deres rettigheter. Dette kan for eksempel være digitale tjenester som kan brukes til å koordinere aktiviteter blant ti- til tolvåringer, eller som gir unge mennesker mulighet til å få sin stemme hørt om politiske saker som angår dem. Generelt bør barn beskyttes gjennom å legge til rette for utøvelse av deres rettigheter, ikke utestenging.

4.4. Tekniske løsninger er risikofylte og ikke uten feil

Dersom man anser utestenging av barn og unge fra noen typer tjenester som nødvendig, må man håndtere spørsmålet om hvordan en aldersgrense skal gjennomføres i praksis. Dette krever at digitale tjenestetilbydere vet om en bruker er et barn eller ikke.

Samlebetegnelsen for metoder som kan brukes for å anslå en persons alder er «aldersbekreftelse», eller *age assurance* på enelgesk. Dette omfatter metoder for å fastslå en persons nøyaktige alder («aldersverifisering», eller *age verification* på engelsk) og metoder for å utlede tilnærmet alder eller aldersspennet til en person («aldersestimering», eller *age estimation* på engelsk).

Selv om tiltak som teknologi for aldersbekreftelse kan være ment å forhindre barn fra å få tilgang til bestemte tjenester, vil slike tiltak uunngåelig kreve at *alle* bekrefter alderen sin. Det inkluderer universitetsstudenter, personer med funksjonshemminger, innvandrere, eldre, andre tenåringer og voksne som er

over aldersgrensen. Aldersbekreftelse legger derfor et ekstra lag mellom alle medlemmer av samfunnet og det som kan være viktige digitale tjenester, noe som gjør slik teknologi mer inngripende enn det umiddelbart kan synes. Ulike grupper i samfunnet kan også ha ulik forutsetning for å bruke digitale tjenester, tilgang til identitetspapirer og liknende.

Tidspunktet og hyppigheten av aldersbekreftelse er også viktig. Aldersbekreftelse kan for eksempel bli brukt den første gangen noen får tilgang til en tjeneste, når noen oppretter en profil eller en konto, eller hver gang noen benytter en tjeneste. Jo oftere aldersbekreftelsen gjennomføres, jo vanskeligere er det å omgå tiltaket over tid. Samtidig øker hyppig bruk av alderskontroll de risikoene som er forbundet med den aktuelle metoden for aldersbekreftelse.

Aldersbekreftelsesmetoden som oftest blir drøftet på EU-nivå og i norsk sammenheng, er aldersverifisering basert på ulike former for elektroniske ID-løsninger.[90] På EU-nivå kan det for eksempel være aktuelt å basere aldersverifisering på den kommende EU-forordningen eIDAS, som oppstiller en liste med krav til et teknisk system for identitetskontroll.[91] Siden ID-basert aldersverifisering er den metoden som diskuteres mest, både politisk og regulatorisk, vier vi betydelig plass i rapporten til de risikoene denne bestemte løsningen innebærer.

4.4.1. ID-basert aldersverifisering

ID-basert aldersverifisering baserer seg på et offisielt aldersbevis. Slike offisielle dokumenter fungerer ofte også som identitetsbevis, slik som pass, nasjonale ID-kort eller elektronisk identifikasjon basert på nasjonale identitetsdokumenter (eID).

Det er mange grunner til at ID-basert aldersverifisering kan være spesielt risikofylt for barn og for forbrukere generelt. De viktigste risikoene kan kategoriseres som digital og sosial utestenging, personvern og sikkerhet.

Utestenging

ID-basert verifisering betyr at *alle, uansett alder*, vil måtte identifisere seg og innebærer derfor en betydelig risiko for ekskludering. Uansett hvilken type teknologisk tiltak som blir innført, vil enkeltpersoner ha behov for tilgang til et

[90] Se for eksempel «Støre vil ha aldersgrense for sosiale medier», Jobling, NRK (2024) https://www.nrk.no/norge/store-vil-ha-aldersgrense-for-sosiale-medier-1.16944311, «Unreleased document: DSA, identity wallets take spotlight on protection of minors online», Gkritsi, Euractiv (2024). https://www.euractiv.com/section/digital/news/unreleased-document-dsa-identity-wallets-take-spotlight-on-protection-of-minors-online/

[91] «eIDAS Regulation», European Commission. https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

relevant identitetsbevis for å kunne benytte sosiale medietjenester og eventuelt andre tjenester som innfører aldersverifisering. Personer som ikke har tilgang til det nødvendige identitetsbeviset, vil heller ikke ha tilgang til tjenestene.

Det er mange grunner til at enkeltpersoner ikke har tilgang til et identitetsbevis. Dette kan også variere mellom ulike land. Selv om Norge er et meget digitalisert land etter enhver målestokk, har for eksempel om lag 400 000 innbyggere (eller 7 % av befolkningen) ikke tilgang til, eller er ikke brukere av, en elektronisk ID.[92] Dersom en elektronisk ID blir gjort til et krav for tilgang til ulike digitale tjenester, vil disse forbrukerne i praksis være utestengt fra de aktuelle tjenestene.

Siden sosiale medier nå er en vesentlig del av hverdagen, kan utestenging ha betydelige negative konsekvenser for mange forbrukere som allerede er marginaliserte. For eksempel kan det stanse eldre og pensjonister fra å kommunisere med sine familier, eller innvandrere fra å benytte plattformer som ellers kan sette dem i kontakt med nye naboer eller potensielle arbeidsgivere.

Personvern og anonymitet på nettet

Det er mange helt legitime grunner til å ønske å være anonym på nettet. Grunnleggende sett kan dette handle om at man ønsker å unngå å bli sporet og profilert for kommersielle formål. For eksempel kan forbrukere ønske å unngå at søkehistorikken deres om et mulig helseproblem brukes til markedsføringsformål eller blir solgt til tredjeparter.

Anonymitet på nettet er spesielt viktig for å beskytte sårbare grupper eller enkeltpersoner. Politiske dissidenter eller aktivister som frykter forfølgelse for sine meninger, er ett slikt eksempel. Menneskerettsaktivister som organiserer seg for å avsløre og/eller protestere mot undertrykking kan være avhengige av anonymitet for å unngå trakassering eller represalier. Etter at retten til abort ble opphevet i mange delstater i USA, ble det også rapportert om kvinner som ble straffeforfulgt fordi de krysset delstatsgrenser for å oppsøke reproduktive helsetjenester.[93] Uten anonymitet hadde ikke disse kvinnene noen trygg måte å søke hjelp på.

Hvis digitale tjenester pålegges å ha systemer for ID-basert aldersverifisering, kan muligheten til å forbli anonym bli sterkt begrenset. Som skissert nedenfor finnes det verktøy som kan benyttes til å omgå slike verifiseringssystemer, men for sårbare grupper som mangler kunnskap eller evne til å gjøre dette, kan mangelen på anonymitet bli farlig. Selv om man tviler på at ID-basert

[92] «Outsiderness in the consumer markets», Forbrukerrådet (2023) s. 10. https://storage02.forbrukerradet.no/media/2023/01/forbrukerradet--outsiderness-in-the-consumer-markets-en.pdf

[93] «Location Data Tracks Abortion Clinic Visits. Here's What to Know», Electronic Frontier Foundation (2024). https://www.eff.org/deeplinks/2024/03/location-data-tracks-abortion-clinic-visits-heres-what-know

aldersverifisering ville blitt misbrukt i norsk sammenheng, bør man ikke undervurdere signaleffekten overfor andre, mer repressive regimer.

Personvernutfordringer ved innføring av ID-basert aldersverifisering må også forstås i kontekst av dagens dominerende forretningsmodell, nemlig overvåkningsbasert markedsføring. Å koble ekte identiteter til digitale profiler er en gyllen mulighet for selskaper som driver med sporing og profilering av forbrukere for kommersielle formål. Sporing på tvers av enheter og tjenester er ekstremt attraktivt for disse selskapene, fordi det gir dem mulighet til å skape enda mer detaljerte og finmaskede profiler om den enkelte forbruker. Et system for ID-basert aldersvertifisering som «garanterer» at brukerprofiler på ulike tjenester tilhører samme enkeltperson, er en permanent identifikator som kan brukes til å undergrave forbrukernes personvern ytterligere.

Selv om personvernforordningen (GDPR) trådte i kraft i EU i 2016, har talløse selskaper fortsatt å kontinuerlig bryte loven fordi overvåking er ekstremt lønnsomt – for eksempel for markedsføringsformål, men også for å trene opp dataintensive KI-modeller. Med mindre det blir teknisk umulig å knytte informasjon om *hvem* som benytter en tjeneste, til *hvilken type tjeneste eller innhold* de har tilgang til, bør det forventes at selskaper vil forsøke å omgå eventuelle tekniske, juridiske eller organisatorisk hindringer. Dette kalles gjerne «nullkunnskapsbevis» (eller *zero-knowledge proof* på engelsk) med «dobbel blinding» (eller *double blind* på engelsk). Manglende tekniske beskyttelser vil gjøre både voksne og barn enda mer sårbare for invaderende sporingspraksis enn de allerede er i dag.

En ID-basert løsning for aldersverifisering med «dobbel blinding» og som derfor ikke sporer enkeltpersoner, kan likevel være problematisk i et personvernperspektiv. Når personer føler at de blir observert, endrer de ofte atferd (gjerne kalt «nedkjølingseffekten»). Dette kan for eksempel innebære at man avstår fra å søke etter temaer og tjenester som oppfattes som sensitive, slik som informasjon om seksuell orientering eller hjelpelinjer for mobbeofre. Nedkjølingseffekten forutsetter ikke at noen faktisk observerer hva du gjør, bare at det føles slik. En ID-basert løsning for aldersverifisering risikerer å gi et slikt inntrykk, uavhengig av om personopplysninger blir lagret og brukt til nye formål, eller ikke.

Ethvert obligatorisk aldersverifiseringssystem må innføres i overensstemmelse med de strenge kravene i personvernforordningen. Det er uakseptabelt dersom verifiseringsmekanismen brukes til noe annet formål enn å fastslå personens alder. Bruken av verifiseringssystemet må ikke innebære loggføring eller registrering utover det som er nødvendig for å verifisere personens alder. I tillegg må aldersverifisering ikke pålegges dersom dette kan ha en nedkjølingseffekt, spesielt når det gjelder informasjon, oppslagstavler eller nettverk som omhandler temaer som kan oppleves sensitive for barn.

Sikkerhetsrisiko

Dersom tjenestetilbydere blir pålagt eller på annen måte får insentiver til å verifisere sine brukeres alder og/eller identitet, vil dette sannsynligvis involvere mer innsamling av personopplysninger. Verifisering kan lede til sentralisering av verdifull informasjon og gjør det med attraktivt å skaffe seg identitetspapirer på svartebørser.[94] Når store mengder informasjon blir samlet og lagret, kan selskapene som sitter på informasjonen også bli attraktive mål for aktører med onde hensikter.

Hvis en database som inneholder store mengder personopplysninger blir utsatt for innbrudd eller kompromittert på andre måter, kan dette ha mange skadelige konsekvenser, inkludert identitetstyveri, utpressing, angrep med løsepengevirus og svindel. Tiltak som skanning og opplasting av pass, eller biometriske identifiseringsløsninger, er spesielt alvorlig. Dersom slik informasjon ender opp i feil hender, kan skaden være uopprettelig. Risikoen for at dette skal skje øker med antallet tilbydere av aldersverifiseringssystemer på markedet, som kan ha ulike tilnærminger til sikkerhet.

Det finnes allerede en overflod av eksempler på sikkerhetsbrudd. I 2024 ble det avslørt at en tredjepartstilbyder av ID-basert aldersverifisering for tjenester som TikTok og X hadde blitt utsatt for datainnbrudd, der førerkortene til sluttbrukere som hadde verifisert sin identitet, ble kompromittert.[95] Tilsvarende ble det amerikanske teleselskapet AT&T utsatt for et datainnbrudd i 2024, der komplette datasett av kundenes telefon- og SMS-logger kom på avveie.[96]

Det er viktig at myndighetene krever tilstrekkelig sterke sikkerhetstiltak gjennom forskrifter og standarder. Det tekniske referansedokumentet for en eID-løsning for hele EU[97] ble nylig publisert og har blitt kritisert av en bredt sammensatt gruppe med sivilsamfunnsorganisasjoner og forskere for å bare kreve gammeldagse og utdaterte krypteringsmekanismer.[98]

---

[94] «Age against the machine: the race to make online spaces age-appropriate», EDRi (2024). https://edri.org/our-work/age-against-the-machine-the-race-to-make-online-spaces-age-appropriate/

[95] «ID Verification Service for TikTok, Uber, X Exposed Driver Licenses», Cox, 404Media (2024). https://www.404media.co/id-verification-service-for-tiktok-uber-x-exposed-driver-licenses-au10tix/

[96] «The Sweeping Danger of the AT&T Phone Records Breach», Newman, WIRED (2024). https://www.wired.com/story/att-phone-records-breach-110-million/

[97] Slik som eIDAS-forordningen krever.

[98] «Euopean eID Implementation, Open Letter», epicenter.works et al. (2024). https://epicenter.works/fileadmin/medienspiegel/user_upload/eIDAS_-_European_eID_Implementation_Open_Letter.pdf

Enkel omgåelse

Selv dersom det stills krav til bruk av ID-basert aldersverifisering for enkelte digitale tjenester og plattformer, er det betydelig risiko for at unge vil være i stand til å omgå harde tekniske sperrer, slik at disse blir ineffektive. Dette kan gjøres ved å bruke alternative tjenester, eller ved å finne måter å omgå den tekniske aldersverifiseringen.

Bytte til alternative tjenester

Selv om de store sosiale medieplattformene er dominerende aktører på nett, er de ikke de eneste tilgjengelige tjenestetilbyderne. Unge mennesker som blir stengt ute fra de største plattformene, vil enkelt kunne flytte seg til mindre, alternative plattformer som ikke har innført aldersverifisering.[99]

Nettverkseffekter gjør det utfordrende for voksne å flytte vekk fra de store nettplattformene. Hvis slektninger, venner fra skoletiden, kolleger og barnas fritidsaktiviteter alle er samlet på Facebook, er det ikke realistisk at du bytter til en annen plattform. Ulempene ved å bytte er ganske enkelt for store. For barn og unge er disse ulempene mindre, siden unge mennesker generelt har færre sosiale forbindelser og kan være mer nysgjerrige på hva andre tjenester har å by på. Dette illustreres for eksempel av hvordan nye apper og tjenester stadig dukker opp og blir svært populære over en kort periode, når yngre brukere kaster seg over «den nye greia». For eksempel hadde meldingstjenesten BeReal en plutselig økning i popularitet i 2022 og ble fort en av de mest nedlastede appene på verdensbasis. Etter under ett år skrumpet antallet brukere inn, og andre tjenester tok over plassen.[100]

Dersom de store plattformene blir pålagt å innføre aldersverifisering, vil dette kunne bety at mange unge personer holdes vekk fra dem. Dette vil imidlertid ikke hindre de samme personene i å flytte seg til en annen plattform som ikke har innført aldersverifisering. Med andre ord, hvis de store sosiale mediene begynner å stenge yngre brukere ute, kan de unge svært enkelt flytte seg til et mindre alternativ, der de ikke blir utestengt.

Hvis yngre brukere begynner å flytte til alternative plattformer uten aldersverifisering, kan dette skape nye eller forverre eksisterende skadelige virkninger. De fleste store plattformene har i det minste innført en viss grad av innholdsmoderering og sikkerhetstiltak, om ikke annet fordi de kan bli gransket av tilsynsmyndigheter eller offentligheten. Mindre aktører vil ha mindre penger å bruke på risikoreduserende tiltak, de blir i mindre grad gransket, og i mange

[99] «A booming industry of AI age scanners, aimed at children's faces», Harwell, The Washington Post (2024). https://www.washingtonpost.com/technology/2024/08/07/face-scanning-kids-online-privacy/
[100] «They're Over Being Real», Holtermann, The New York Times (2023). https://www.nytimes.com/2023/04/13/style/bereal-app.html

tilfeller mangler de insentiver til å investere i sikkerhet, personvern, trygghet og innholdsmoderering. Dette betyr at tekniske tiltak for å stenge unge mennesker ute vil kunne skyve dem over mot andre tjenester som er enda verre enn dagens dominerende plattformer.

Det eneste som kan forhindre at barn og unge flytter over til alternative plattformer og tjenester, er å innføre alderssperrer på hele internett. Dette vil kreve at politikere og tilsynsmyndigheter finner en måte å sikre at tjenester som ikke overholder reglene for hard aldersverifisering, ikke er tilgjengelige for barn på andre måter. I teorien kan dette innebære et krav til internettleverandører om å blokkere tilgangen til bestemte tjenester på nettverksnivå. Vi har allerede beskrevet hvor utfordrende det kan være å definere sosiale medier, og lovgivere vil derfor måtte gi tilsynsmyndigheter mandat til å blokkere eller stenge ned en bred gruppe plattformer og tjenester.

I et slikt scenario ville tilsynsmyndighetene også trenge fullmakt til å handle raskt for å fange opp og blokkere nye tjenestetilbydere etter hvert som de kommer inn på markedet. Slike raske vedtak er urealistisk med tanke på tidshorisonten for andre vedtak i den digitale sfæren, der tilsynsmyndighetene kan bruke mange år på å fatte ett vedtak – som i praksis er en stor del av et barns liv. Alternativet er at internettleverandører bare tillater tilgang til nettsteder og apper som er forhåndsgodkjent i Norge eller EU. Dette vil utgjøre en nasjonal brannmur, eller også en bred sensur av internett, noe som er uakseptabelt i demokratiske samfunn.

Obligatoriske aldersverifiseringssystemer kan ikke medføre filtrering av internett på nettverksnivå eller lignende invaderende tiltak for å hindre omgåelse. Slike tiltak ville i praksis bety fullstendig sensur av internett.

Tekniske omgåelser

Nasjonale eller regionale blokkeringer eller restriksjoner på bestemte tjenester eller plattformer kan omgås ved hjelp av tekniske hjelpemidler. Verktøy som virtuelle private nettverk (VPN) lar brukere rute internettrafikken sin via en tredjepart, slik at det ser ut som om brukeren er plassert et annet sted - for eksempel et land som ikke blokkerer mindreårige fra sosiale medier. Aldersverifiseringssystemer som er innført på nasjonalt eller regionalt nivå, kan derfor lett omgås ved å installere den rette programvaren, noe mange ungdommer allerede er flinke til. Den eneste måten å unngå omgåelse på er et verdensomspennende krav om aldersverifisering.

Hvis barn får tilgang til disse tjenestene gjennom en VPN som er rutet utenfor EU (eller lignende teknologi), vil de også bli dårligere beskyttet. For eksempel har ikke USA noen føderal personvernlovgivning og barn som bruker TikTok eller Instagram fra USA, vil derfor ha svakere personvernbeskyttelser enn voksne europeere.

Barn og unge kan også finne andre metoder for å omgå aldersverifisering ved å lure den tekniske implementeringen. De kan for eksempel benytte falsk ID, låne en ID fra venner eller familiemedlemmer, eller kjøpe selfievideoer eller bilder dersom tilbyderen av aldersverifiseringen krever ytterligere bevis.[101] Når barn først har funnet metoder for å omgå aldersverifiseringen, kan metodene spre seg raskt blant jevnaldrende.

Man kan også se for seg at ondsinnede aktører omgår aldersverifiseringsverktøy motsatt vei. De kan utgi seg for å være barn ved å bruke falsk ID, og komme seg uhindret inn i det som anses som trygge rom, ved å utnytte den falske tryggheten som aldersverifiseringssystemene kan skape.

I praksis er det så godt som umulig å skape et vanntett system for aldersverifisering. Dette er et rent teknisk virkemiddel for å løse en kombinasjon av mange sammensatte tekniske og sosiale problemer som barn opplever på nettet. Hvis løsningen utelukkende handler om å holde barn unna tjenesten, vil de forsøke å omgå systemet. Tilbydere av aldersverifisering vil måtte øke sine kontroll- og overvåkingstiltak for å motvirke nye omgåelsesmetoder etter hvert som de blir avdekket og spredd blant barn og unge.

4.4.2. Risikable teknikker for aldersestimering

I tillegg til de ovennevnte teknikkene for ID-basert aldersverifisering finnes det flere metoder for aldersbekreftelse som er basert på aldersestimering, altså metoder for å finne den tilnærmede alderen eller aldersspennet til en person. Disse fører med seg mange av de samme risikoene som ID-basert løsninger, i tillegg til noen risikoer som er spesifikke for disse metodene.

Det er verdt å merke seg at aldersestimering er iboende problematisk dersom dette brukes til å avgjøre om enkeltpersoner skal gis tilgang til tjenester, fordi aldersgrenser er binære – enten er du gammel nok til å få tilgang til tjenesten, ellers blir du stengt ute. Dersom aldersestimering blir brukt til å avgjøre om noen skal få tilgang til tjenesten, vil tilgangen i bunn og grunn være vilkårlig, basert på kvalifisert gjetning. Alternativet er å kombinere aldersestimering med aldersverifisering hver gang noen blir flagget av aldersestimeringssystemet. Dette vil innebære alle de risikoene aldersverifiseringssystemer fører med seg, som beskrevet tidligere i denne rapporten.

[101] «A booming industry of AI age scanners, aimed at children's faces», Harwell, The Washington Post (2024). https://www.washingtonpost.com/technology/2024/08/07/face-scanning-kids-online-privacy/

Profilering av brukere

Det er mulig å anslå brukeres alder gjennom profilering, som innebærer innsamling og analyse av personopplysninger om enkeltpersoners atferd. Denne typen løsning kan synes fristende, siden mange digitale tjenestetilbydere allerede lager omfattende profiler av sine brukere for kommersielle formål. Å gjenbruke slike datapunkter for å avdekke om det er barn på en tjeneste, er imidlertid dypt problematisk.

Som beskrevet i kapittel 3.1, innebærer den nåværende forretningsmodellen med innsamling og gjenbruk av personopplysninger at selskaper kan utlede barns sårbarheter, samtidig som den fyrer opp under utformingen og spredningen av avhengighetsskapende mekanismer, forsterking av destruktivt innhold og trening av KI-modeller. Dersom man krever at selskaper skal lage profiler av sine brukere for å estimere alderen deres, vil politikerne i praksis legitimere dypt invaderende overvåking som har møtt omfattende kritikk fra sivilsamfunnsorganisasjoner.[102]

Å bruke profileringsteknikker som et grunnlag for alderskontroll øker også risikoen for ekskludering for alle med en atferd som ligger utenfor det som anses «normalt», slik som personer med psykisk eller annen utviklingshemming.[103] Dette kan føre til at de blir feilaktig flagget som under aldersgrensen.

Biometri

Aldersverifisering kan være basert på å benytte biometri til å anslå en persons alder. Dette kan for eksempel være ansiktsanalyse av et opplastet bilde eller en video.

Biometriske data er ekstremt sensitiv informasjon. Det er ikke bare å endre egne biometriske kjennetegn, og dersom biometriske data blir lekket eller utsatt for et datainnbrudd, oppstår det derfor en dyptgripende risiko for misbruk. Dersom enkeltpersons atferd på nettet kobles til en egenskap som ikke kan endres, er dette også et alvorlig brudd på personvernet.

Biometrisk ansiktsanalyse er også notorisk unøyaktig og utsatt for feil. Slike systemer kan ha problemer med å verifisere alderen til barn eller voksne som er nær aldersgrensen, ved at algoritmenes nøyaktighet i beste fall ligger innenfor et

[102] «International coalition calls for action against surveillance-based advertising», Forbrukerrådet (2021). https://www.forbrukerradet.no/side/new-report-details-threats-to-consumers-from-surveillance-based-advertising/
[103] «Invisible No More: The Impact of Facial Recognition On People with Disabilities», eticas. https://eticas.ai/invisible-no-more-the-impact-of-facial-recognition-on-people-with-disabilities-2/

spenn på 2–4 år.[104] Dette betyr at noen barn som skulle hatt tilgang, blir stengt ute fra plattformen, mens barn som er under aldersgrensen, vil kunne få tilgang. I tillegg vil mangelen på nøyaktighet kunne ha en diskriminerende slagside, fordi algoritmene ofte er mindre nøyaktige når de analyserer ansiktene til personer med mørkere hud, spesielt kvinner.[105]

4.4.3. Alderserklæring

Alderserklæring innebærer å be en person om å oppgi sin alder, for eksempel i forbindelse med registrering av en konto hos en tjenestetilbyder eller når man går inn på en tjeneste eller nettside. Dette anvendes i dag av mange digitale tjenestetilbydere og er en av de minst inngripende formene for aldersbekreftelse. Det skyldes at alderserklæring ikke krever overvåking av brukere over tid og heller ikke øker risikoen for utestenging.

Et alderserklæringssystem signaliserer til barn og deres foreldre eller omsorgsgivere at innholdet og utformingen av en tjeneste ikke er ment for barn under aldersgrensen. Dette kan avskrekke barn fra å bruke tjenesten. Selv om de skulle gå inn på tjenesten på tross av aldersgrensen, vil de kunne være bedre mentalt forberedt, fordi de vet at de befinner seg i et utrygt rom.

At alderserklæring er enkelt å omgå, er en av de viktigste innvendingene mot slike systemer i dag. Barna, deres foreldre eller omsorgsgivere kan enkelt erklære at barnet er eldre enn de er og dermed omgå aldersspersen eller andre tiltak spesielt rettet mot barn.

Selv om alderserklæringssystemer er ganske lett å omgå, kan teknologien likevel være nyttig for å beskytte barn og unge på nettet. For eksempel bruker 20 % av norske barn i alderen 9-12 år YouTube selv om de ikke får lov til det av sine foreldre eller omsorgsgivere.[106] Én av fem er ganske mange, men for TikTok, Instagram og Snapchat, som i offentlig debatt ofte fremstilles som de mest problematiske tjenestene, er denne andelen nede på 1–2 %. Samtidig får 90% av barn i alderen 9-12 år lov til å bruke YouTube av foreldrene sine, mens tallene er

---

[104] «Online age verification and children's rights», EDRi et al. (2023). https://edri.org/wp-content/uploads/2023/10/Online-age-verification-and-childrens-rights-EDRi-position-paper.pdf og «Mandatory age verification for pornography access: Why it can't and won't 'save the children'», Stardust, Obeid, McKee, Angus (2024). https://journals.sagepub.com/doi/epub/10.1177/20539517241252129

[105] «Ban Biometric Mass Surveillance», EDRi (2020). https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

[106] «Foreldre og medier 2024: Delrapport: Foreldres regulering av barnas mediebruk», Medietilsynet, s. 28. https://www.medietilsynet.no/globalassets/publikasjoner/foreldre-og-medier-undersokelser/2024/delrapport-2-foreldreregulering-av-barnas-mediebruk-med-uttak-fra-fom-og-bom.pdf

noe lavere for andre tjenester som Snapchat (42%), TikTok (32%) og Instagram (12%).[107]

Dette illustrerer at de fleste barn som omgår alderserklæringen, gjør dette med sine foreldres eller omsorgsgiveres godkjenning. Løsningen ligger derfor ikke nødvendigvis i å øke de tekniske hindringene for barna, men heller i å redusere det sosiale presset til å være til stede på nettet og foreldrenes eller omsorgsgivernes tilbøyelighet til å gi godkjenning. Det er mangefasetterte grunner til at foreldre lar barna bruke sosiale medier til tross for aldersgrensene, blant annet knyttet til en frykt for sosial utestenging. Foreldrekontroller, legitime aldersgrenser og andre metoder for å bistå foreldre og omsorgsgivere i å sørge for at barn er trygge på nettet, blir mer inngående drøftet i kapittel 5.2.

Mer forskning kan være nødvendig for å forstå hvordan metoder for alderserklæring kan presenteres for familier på en måte som reduserer sannsynligheten for at barna omgår dem. Mange barn ønsker å være trygge på nettet og det er kanskje mulig å dra nytte av dette for å øke sjansen for at de opptrer sannferdig. Når alderserklæring blir kombinert med andre tiltak, slik som innebygd personvern og trygghet, kombinert med hensiktsmessig tilsyn fra foreldre og omsorgsgivere, kan dette bli et effektivt og lite inngripende tiltak.

4.5. Prinsipper for legitim alderskontroll

Politikere må ha en helhetlig tilnærming til beskyttelse av barns rettigheter på nettet. Dette omfatter betraktninger om *hvorvidt* barn skal stenges ute fra digitale rom, noe som er et komplisert og mangefasettert spørsmål. Det omfatter også betraktninger om *hvordan* dette skal gjøres, dersom man finner at det faktisk er nødvendig å stenge barn ute fra digitale rom.

Aldersbekreftelse kan anvendes på mange måter. Det er verdt å merke seg at jo vanskeligere en metode for aldersbekreftelse er å omgå, desto flere risikoer utgjør gjerne denne metoden for barns og forbrukeres rettigheter. Dette har viktige implikasjoner for når ulike metoder er nødvendige og proporsjonale. De hardeste metodene for aldersbekreftelse bør bare vurderes dersom andre metoder har blitt vurdert, utprøvd og funnet mangelfulle.

Det finnes en rekke aspekter som må vurderes når det gjelder nødvendigheten og proporsjonaliteten ved å innføre ulike metoder for aldersbekreftelse. For eksempel er det verdt å ha i mente at metoder for aldersbekreftelse ikke kan begrenses til bare å gjelde barn. Tiltaket krever at alle er gjenstand for den

[107] «Foreldre og medier 2024: Delrapport: Foreldres regulering av barnas mediebruk», Medietilsynet, s. 26. https://www.medietilsynet.no/globalassets/publikasjoner/foreldre-og-medier-undersokelser/2024/delrapport-2-foreldreregulering-av-barnas-mediebruk-med-uttak-fra-fom-og-bom.pdf

samme aldersbekreftelsen med medfølgende risikoer, noe som øker terskelen for at tiltaket er proporsjonalt.

Vurderingen av nødvendighet og proporsjonalitet påvirkes også av hvordan tjenester er utformet. Målrettede tiltak for å håndtere konkrete risikoer, slik som å redusere bruken av avhengighetsskapende mekanismer og overvåkingsbasert markedsføring, vil redusere risikoene på tjenesten. Slike tiltak bør anvendes bredt og gjelde i samme utstrekning overalt, for eksempel for opplæringsplattformer og internettilkoblede leketøy, istedenfor å være begrenset til tradisjonelle sosiale medier. Når risikoene forbundet med tjenestene reduseres, endres også vurderingen av om ulike former for aldersbekreftelse er et proporsjonalt tiltak.

Det er også viktig å ha i mente hvilke problemer man ønsker å ta tak i ved å innføre invaderende tekniske tiltak. Dersom de teknologiske verktøyene som vurderes, ikke er egnet for å løse det angitte problemet, eller etterlater betydelige muligheter til å omgå aldersverifiseringen, må andre løsninger vurderes i stedet.

Med unntak av alderserklæring introduserer alle de eksisterende metodene for aldersbekreftelse i det minste en viss risiko for barns og andre forbrukeres rettigheter. Aldersbekreftelsen bør bare brukes i overensstemmelse med gjeldende lovverk. Lovverket fastsetter et rammeverk for legitim aldersbekreftelse, med en risiko- og rettighetsbasert tilnærming som tar grundig hensyn til barnets rettigheter.

For å være akseptabel må enhver verifiseringsmekanisme:

- Brukes bare der det er strengt nødvendig og proporsjonalt.
- Være tilgjengelig for alle, slik at enkeltpersoner og grupper over aldersgrensen ikke stenges ute fra tjenester de kan være avhengige av. Dette inkluderer å sørge for at alle beholder retten til en fysisk ID og at de som er over aldersgrensen, men mangler en elektronisk ID, ikke blir utestengt.
- Ikke være altfor byrdefull for de som ikke ønsker eller har midler til å verifisere sin identitet.
- Unngå nedkjølingseffekter, slik som å avskrekke eller forhindre barn og unge fra å søke informasjon relatert til utdanning, helse, osv.

- Være i tråd med lover og tekniske standarder,[108] slik som de strenge kravene som er fastsatt i personvernforordningen.

- Ikke gi annen informasjon til tjenestetilbyderen enn ja eller nei, og ikke legge til rette for deling med tredjeparter (inkludert foreldre og omsorgsgivere).

- Ikke loggføre eller på annen måte registrere bruk utover det som er nødvendig for å verifisere brukerens alder, og ikke koble informasjon om for eksempel internettaktivitet til brukerens identitet.

- Ikke tillate behandling av biometriske data eller data basert på biometri.

- Være underlagt strenge sikkerhetskrav og revisjoner utført av uavhengige tredjeparter.

- Ikke omfatte filtrering av internett på nettverksnivå eller lignende inngripende tiltak for å motvirke omgåelse.

- Ikke føre til innføring av stadig sterkere overvåkingstiltak for å motvirke omgåelsestaktikker.

- Inkludere lett tilgjengelige og effektive klagemekanismer for tilfeller der en persons alder, enten det er et barn eller en voksen, har blitt feilaktig fastsatt eller anslått.

- Omfatte risikovurderinger og risikoreduserende tiltak med tanke på mulige virkninger i form av utestenging eller diskriminering, med spesielt fokus på sårbare personer og grupper.

5. Nødvendige tiltak for å beskytte barn på internett

Denne rapporten har gitt en oversikt over de risikoene barn står overfor på nett i dag, som samlet sett er uakseptabelt. Barn bør ikke utnyttes for kommersielle formål på noe tidspunkt i sin hverdag, slik som når de leker, har kontakt med venner, deltar i politiske eller andre diskusjoner på nettet, eller får undervisning.

Det er imidlertid viktig å huske på at de skadelige trekkene som i dag gjennomsyrer det digitale miljøet, ikke er iboende trekk ved sosiale medier eller internett som sådan. Som samfunn kan vi velge å forandre disse trekkene, og gi

[108] Se for eksempel «Workshop Agreement: Age appropriate digital services framework», CEN and CENELEC (2023). https://www.cencenelec.eu/media/CEN-CENELEC/CWAs/ICT/cwa18016_2023.pdf.

barn og unge tilgang til tjenester som respekterer deres rettigheter – eller sågar forsterker disse rettighetene.

Det finnes ingen enkel løsning på hvordan barn kan beskyttes i den digitale sfæren. Myndighetene må i stedet ta en helhetlig og kumulativ tilnærming til beskyttelsen av barns rettigheter på nettet. Dette omfatter bruk av juridiske tiltak, men også mykere styringstiltak som retningslinjer. I det følgende gir vi en rekke anbefalinger.

5.1. Krev et digitalt miljø der rettigheter blir respektert

Det digitale miljøet er for øyeblikket i dårlig forfatning, der forbrukere og barn blir utnyttet for kommersielle formål. Det positive er at mange av de skadelige praksisene som er skissert gjennom denne rapporten, allerede er regulert i eksisterende lover og regler. På EU-nivå omfatter dette for eksempel personvernforordningen (GDPR),[109] handelspraksisdirektivet (UCPD),[110] forordningen om digitale tjenester (DSA)[111] og direktivet for audiovisuelle medietjenester (AMT-direktivet).[112] Barn er også beskyttet av sektorspesifikke lover på nasjonalt nivå, slik som den norske opplæringsloven.[113]

Lovene gjelder for ulike virksomheter og kontekster. For eksempel gjelder direktivet om urimelig handelspraksis for næringsdrivendes handelspraksiser overfor forbrukere, personvernforordningen gjelder all behandling av personopplysninger, mens DSA har noen regler for alle nettplattformer og noen som bare gjelder veldig store nettplattformer (eller *very large online platforms* på engelsk). Alle de ulike lovene må derfor håndheves på sine felter, for å håndtere de totale skadevirkningene i ulike kontekster og fra ulike virksomheter. Der DSA ikke gjelder, kan personvernforordningen og direktivet om urimelig handelspraksis fungere som sikkerhetsnett. Et av de viktigste tiltakene er derfor å sørge for at de relevante tilsynsmyndighetene håndhever eksisterende lovverk aktivt og besluttsomt.

---

[109] EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) (GDPR).
[110] Europaparlaments- og rådsdirektiv 2005/29/EF av 11. mai 2005 om foretaks urimelige handelspraksis overfor forbrukere på det indre marked og om endring av rådsdirektiv 84/450/EØF, europaparlaments- og rådsdirektiv 97/7/EF, 98/27/EF og 2002/65/EF og europaparlaments- og rådsforordning (EF) nr. 2006/2004 («direktivet om urimelig handelspraksis») [Handelspraksisdirektivet].
[111] REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 000/31/EC (Digital Services Act).
[112] Europaparlaments- og rådsdirektiv 2010/13/EU av 10. mars 2010 om samordning av visse bestemmelser om tilbud av audiovisuelle medietjenester, fastsatt ved lov eller forskrift i medlemsstatene (direktivet om audiovisuelle medietjenester) [AMT-direktivet]
[113] Lov om grunnskoleopplæringa og den vidaregåande opplæringa (opplæringslova), LOV-2023-06-09-30. https://lovdata.no/lov/2023-06-09-30.

Det er i dag store begrensninger i mange av de eksisterende håndhevingsregimene. Håndhevingen av personvernforordningen går notorisk sakte, spesielt i grenseoverskridende tilfeller. For mange selskaper er det lønnsomt å bryte både personvernforordningen og direktivet om urimelig handelspraksis, fordi bøtene kommer for sent og er for små til å ha en avskrekkende virkning. Å bryte loven oppfattes som en driftskostnad. I tillegg er samarbeidet mellom tilsynsmyndighetene for dårlig, slik at saker der barns rettigheter utfordres kan falle mellom ulike tilsyn. Forbedring og styrking av håndhevingsapparatet bør derfor stå i forreste linje i enhver strategi for å styrke rettigheter i det digitale miljøet.

Selv om mange av de risikoene barn står overfor på nettet kan bli redusert eller dempet ved å sørge for stabil, avskrekkende og resolutt håndheving av eksisterende lovverk, finnes det fortsatt enkelte juridiske blindsoner. For eksempel tar ikke forbrukerlovgivningen tilstrekkelig hensyn til forbrukeres og barns sårbarheter når de bruker digitale tjenester. Ursula von der Leyen, leder av EU-kommisjonen, har gitt den neste kommissæren med ansvar for forbrukersaker i oppdrag å utvikle en «Digital Fairness Act» som kan regulere manipulerende design, influensermarkedsføring, avhengighetsskapende mekanismer og profilering på nett.[114] Et oppdatert forbrukerregelverk bør gi den endelige sikkerheten barna trenger, ved å innføre horisontale regler med et bredere nedslagsfelt enn konkret, digital lovgivning som DSA – som bare gjelder for nettplattformer, og der enkelte bestemmelser bare gjelder for nettplattformer med flere enn 45 millioner brukere i EU.

I de følgende kapitlene skisserer vi hvordan digitale tjenester kan endres slik at de respekterer forbrukere og barns rettigheter. Vi vil peke på hvilke lover som bør håndheves bedre for å styrke barns beskyttelse på nett, og der det finnes juridiske blindsoner, foreslår vi målrettede oppdateringer av lovverket. Vi kommer også med anbefalinger for å forbedre håndhevingsregimene.

5.1.1. Digitale tjenester som respekterer rettighetene til alle forbrukere

Mange av de skadevirkningene som drøftes i denne rapporten, rammer alle forbrukere, ikke bare barn og unge. Verken barn eller voksne bør utsettes for forretningsmodeller som utnytter dem i form av aggressiv kommersialisering, destruktivt innhold eller avhengighetsskapende mekanismer.

Når skadelig praksis endres for alle som bruker en tjeneste, istedenfor å bare endres for brukere som er under 18 år, kan ikke selskapene utsette barn for skadelig praksis ved å hevde at de ikke vet (eller bare ignorerer) at brukeren er et barn. Digitale miljøer der alle brukeres rettigheter blir respektert, gir derfor også

[114] «Mission Letter», Ursula von der Leyen, Europakommisjonens president (2024). https://commission.europa.eu/document/download/907fd6b6-0474-47d7-99da-47007ca30d02_en?filename=Mission%20letter%20-%20McGRATH.pdf

barn den beste beskyttelsen. For å oppnå dette må det iverksettes en rekke tiltak på digitale tjenester, gjennom ambisiøs håndheving av eksisterende lovverk.

Ansvarlighet og risikoreduserende tiltak

Veldig store nettplattformer[115] må identifisere, vurdere og redusere risikoer tjenestene deres innebærer for forbrukeres grunnleggende rettigheter. Dette bør inkludere uavhengige revisjoner og åpenhetskrav, for å sikre ansvarlighet og interessentinvolvering. Det er flere bestemmelser i DSA som er relevante:

- Risikovurderinger er lovpålagt i DSA art. 34, og bør basere seg på den beste informasjonen som er tilgjengelig, samt involvering av sivilsamfunnsorganisasjoner.[116] Risikovurderingene til sosiale medieplattformer bør inkludere risikoene som er gjennomgått i denne rapporten.

- Risikoreduserende tiltak er lovpålagt i DSA art. 35 og skal basere seg på risikoene som er identifisert og vurdert i DSA art. 34. Tiltakene skal redusere risikoene plattformene innebærer for forbrukernes grunnleggende rettigheter. Det er de veldig store nettplattformene som er nødt til å identifisere risikoreduserende tiltak, men denne rapporten introduserer en rekke risikoreduserende tiltak som bør vurderes.

- Uavhengige revisjoner av risikovurderingene og de risikoreduserende tiltakene er lovpålagt i DSA art. 37(1)(a). [117]

- Offentliggjøring av revisjonsrapportene er lovpålagt i DSA art. 42(4), og skal inkludere resultatene av risikovurderingene og de risikoreduserende tiltakene som er iverksatt. En tilstrekkelig detaljert offentlig rapport er sentralt for at sivilsamfunnsorganisasjoner kan identifisere mangler i risikovurderingene som er gjennomført av de veldig store plattformene.

Avhengighetsskapende design og anbefalingsalgoritmer

Denne rapporten har beskrevet en rekke risikoer knyttet til måten digitale tjenester er utformet i dag. Det finnes mange eksisterende regelverk som kan brukes for å redusere skadene knyttet til avhengighetsskapende og destruktive anbefalingsalgoritmer.

---

[115] Listen over veldig store nettplattformer er tilgjengelig her: «Supervision of the designated very large online platforms and search engines under DSA», EU-kommisjonen. https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses.
[116] DSA fortalepunkt 90.
[117] Se også «Youtube Regrets», Mozilla Foundation (2024). https://assets.mofoprod.net/network/documents/Mozilla_YouTube_Regrets_Report.pdf

Ambisiøs håndheving av DSA art. 35 kan pålegge veldig store nettplattformer å gjennomføre en rekke risikoreduserende tiltak. Som beskrevet i kapittel 3, ligger anbefalingsalgoritmene helt i kjernen av mange av risikoene mange unge mennesker utsettes for på nett i dag. Sosiale medier bør derfor gjøre grunnleggende endringer i sine anbefalingsalgoritmer. I praksis betyr dette at:

- Standardinnstillingene bør ikke benytte anbefalingsalgoritmer som er basert på overvåking og profilering.[118] Personvernforordningens prinsipper om dataminimering og innebygd personvern kan også håndheves for å redusere skadevirkningene av personaliserte anbefalingsalgoritmer betraktelig.[119]

- Plattformene bør tilby alternative anbefalingsalgoritmer som ikke er basert på profilering, slik DSA art. 38 også pålegger dem.

- Anbefalingsalgoritmene bør ikke være optimalisert for engasjement,[120] og kan istedenfor optimaliseres for kvalitet og innhold.

- Brukere bør kunne velge hva slags type innhold de ønsker å se.[121]

- Standardinnstillingene bør ikke inkludere avhengighetsskapende mekanismer. Avhengighetsskapende mekanismer kan også regnes som en urimelig handelspraksis etter handelspraksisdirektivet.[122]

- Brukerkontroller må være lett tilgjengelige og nyttige. Dette inkluderer foreldrekontroller.

- Innholdsprodusenter bør ha mulighet til å markere innhold som kan virke støtende, slik at det kan skjules bak innholdsvarsler. Noen personer kan også ønske å filtrere vekk slikt innhold.

- Det må være tilstrekkelige ressurser til menneskekontrollert innholdsmoderering, jevnt fordelt på alle språkene plattformen tilbyr

---

[118] «Ending artificial amplification of hate & hysteria», Irish Council for Civil Liberties (2023). https://www.iccl.ie/wp-content/uploads/2023/12/Ending-artificail-amplification-of-hate-and-hysteria.pdf
[119] GDPR art. 5(1)(c) og 25.
[120] «Safe by Default», Panoptykon Foundation, People vs. Big Tech (2024). https://en.panoptykon.org/safe-default-panoptykon-foundation-and-people-vs-bigtechs-briefing
[121] «Safe by Default», Panoptykon Foundation, People vs. Big Tech (2024). https://en.panoptykon.org/safe-default-panoptykon-foundation-and-people-vs-bigtechs-briefing
[122] UCPD art. 5 og 8, jf. «Addictive Design as an Unfair Commercial Practice: The Case of Hyper-Engaging Dark Patterns», Esposito, Ferreira (2024). https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/addictive-design-as-an-unfair-commercial-practice-the-case-of-hyperengaging-dark-patterns/038CED800E0CAD86EC5B5216E0AA88DD.

tjenesten sin på,[123] for å fjerne ulovlig innhold fra plattformene. Dette kan også håndheves gjennom DSA art. 6(1)(b).

I tillegg til å introdusere risikoreduserende tiltak, må veldig store nettplattformer gi forskere tilgang til data fra anbefalingsalgoritmene sine, slik at de kan bidra til å avdekke, identifisere og forstå risikoene anbefalingsalgoritmene utgjør for forbrukere, herunder spesielt barn. Dette kan håndheves gjennom DSA art. 40.

Plattformene bør ha innebygd personvern, blant annet basert på prinsippene om formålsbegrensning, dataminimering, og rettferdig og lovlig behandling av personopplysninger. Dette krever sterk og ambisiøs håndheving av personvernforordningen, særlig art. 5, 6 og 25.

Manipulerende design og overvåkningsbasert markedsføring

Rapporten har vist at det er store utfordringer knyttet til manipulerende utforming av digitale tjenester og bruk av personopplysninger for å målrette markedsføring mot enkeltindivider og grupper. Regelverkene som skal beskytte forbrukere, er ikke tilstrekkelige. Derfor bør forbrukerregelverket oppdateres, på en måte som tydeliggjør grensene for lovlig og ulovlig praksis, for eksempel gjennom å:

- Tydeliggjøre samspillet mellom personvernforordningen, direktivet om urimelig handelspraksis og DSA, som alle regulerer manipulerende design på ulike måter.[124]

- Introdusere et horisontalt forbud mot manipulerende design i direktivet om urimelig handelspraksis, for å sørge for forbrukerbeskyttelse i tilfeller som faller utenfor sektorspesifikke bestemmelser.[125]

- Introdusere preskriptive bestemmelser som er enkelt for tilsynsmyndighetene å håndheve, som forbyr konkrete typer manipulerende design.

- Overvåkingsbasert markedsføring bør forbys,[126] utover eksisterende forbud i DSA mot målretting av markedsføring basert på særlige

[123] «How Big Tech platforms are neglecting their non-English language users», Global Witness (2023). https://www.globalwitness.org/en/campaigns/digital-threats/how-big-tech-platforms-are-neglecting-their-non-english-language-users/

[124] Om enn med den begrensning at DSA kun gjelder for design som ikke allerede er omfattet av GDPR og UCPD, jf. DSA art. 25(2). Det gjenstår derfor å se hvilke, om noen, typer design som omfattes av DSA.

[125] «Towards European digital fairness», BEUC (2023). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-020_Consultation_paper_REFIT_consumer_law_digital_fairness.pdf

[126] Time to ban surveillance-based advertising», Forbrukerrådet (2021). https://storage02.forbrukerradet.no/media/2021/06/20210622-final-report-time-to-ban-surveillance-based-advertising.pdf

kategorier av personopplysninger og barns personopplysninger. Et generelt forbud er den beste måten å beskytte barn på.[127]

Innføre nye lovbestemmelser med horisontal beskyttelse

Den digitale sfæren er preget av grunnleggende strukturelle asymmetrier mellom forbrukere og de næringsdrivende, noe som gjør forbrukere spesielt sårbare.[128] Lovgivere må derfor også innføre følgende krav i lovgivningen, for eksempel gjennom målrettede oppdateringer av direktivet om urimelig handelspraksis:

- Næringsdrivendes[129] aktsomhetsplikt bør ta hensyn til digital forbrukersårbarhet. Det betyr at de bør sørge for et høyt nivå av forbrukervern og sikre at tjenestene deres ikke er utformet på en måte som kan påvirke forbrukernes autonomi.[130]

- Næringsdrivende bør utforme sine tjenester med innebygd rettferdighet (eller *fairness by design* på engelsk).[131] Standardinnstillingene må gi forbrukere det høyeste nivået av forbrukerbeskyttelse.

- Bevisbyrden for at den digitale tjenesten er trygg og respekterer forbrukernes rettigheter, bør ligge på den næringsdrivende.[132]

- Det bør innføres felles regler for avhengighetsskapende mekanismer i hele EU og EØS, med spesiell vekt på hvordan slike mekanismer påvirker barn.[133] Det innebærer å:

    - Sikre horisontal beskyttelse mot slike mekanismer, også for tilfeller som faller utenfor sektorspesifikke bestemmelser.

    - Introdusere preskriptive bestemmelser som er enkelt for tilsynsmyndighetene å håndheve, som forbyr konkrete typer avhengighetsskapende mekanismer.

---

[127] «I-SPY: The billion-dollar business of surveillance advertising to kids», McCann, New Economics (2021). https://neweconomics.org/2021/05/i-spy
[128] «EU CONSUMER PROTECTION 2.0 - Structural asymmetries in digital consumer markets», Helberger, Lynskey, Rott, Sax, Strycharz (2021). https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf
[129] Direktivet om urimelig handelspraksis art. 2(b).
[130] «Towards European digital fairness», BEUC (2023). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-020_Consultation_paper_REFIT_consumer_law_digital_fairness.pdf
[131] Ibid.
[132] Ibid.
[133] «Addictive design of online services and consumer protection», European Parliament (2024). https://www.europarl.europa.eu/committees/en/addictive-design-of-online-services-and-/product-details/20230908CDT12141

5.1.2. Krev at barns rettigheter blir ivaretatt

I tillegg til tiltak som bør innføres for å forbedre internett generelt, finnes det mange lover som gir barn ekstra beskyttelse. For eksempel skal ikke næringsdrivende målrette direkte kjøpsoppfordringer til barn,[134] og veldig store nettplattformer har plikt til å redusere risikoer for barn på sine tjenester.[135]

Tjenestetilbydere må sørge for å iverksette nødvendige tiltak for å beskytte og styrke barns rettigheter, og må holdes til ansvar hvis de bryter loven. I mange tilfeller bør tjenestetilbyderne gå enda lenger enn det loven krever, for eksempel ved å tilby tjenester som er laget for å bli brukt av og støtte opp under barn og deres rettigheter.

Når lover inneholder regler som beskytter barn spesielt, må tjenestetilbyderne vite om brukere som benytter deres tjenester, er barn. Som vi har beskrevet i detalj i denne rapporten, må alle metoder for aldersbekreftelse overholde en rekke krav for å være lovlige, nødvendige og proporsjonale. Dette innebærer blant annet å ivareta brukernes personvern, digital inkludering og sikkerhet.

Alderserklæring er forbundet med få risikoer og kan være et viktig verktøy for aldersbekreftelse dersom det brukes i kombinasjon med andre tiltak. For eksempel legger operativsystemtilbydere vanligvis til rette for at enheter kan settes opp som en «barnevennlig enhet», med tilhørende foreldrekontroller. Dette er grunnleggende sett basert på alderserklæring, der et barn, barnets forelder eller barnets omsorgsgiver erklærer at brukeren av enheten er et barn.

Når en enhet er knyttet til et barn, kan man tenke seg at tilbyderen av operativsystemet deler denne informasjonen med tilbydere av apper og tjenester på enheten ved å sende ut et signal. Dette signalet ville utløst de lovbestemte beskyttelsestiltakene andre tjenestetilbydere må iverksette for barn, og samtidig redusert byrden på foreldre og omsorgsgivere med å endre og detaljstyre innstillingene i hver enkelt app eller tjeneste.

Hvis slike tekniske alderssignaler blir implementert galt, kan de imidlertid ha en negativ virkning på barns rettigheter. Hvis signalet for eksempel i praksis utestenger ungdommer fra de fleste apper eller tjenester, eller skjuler bestemte typer innhold, vil dette kunne påvirke barnets rett til informasjon og ytringsfrihet. For å unngå at alderssignalet gjør operativsystemtilbyderen til en portvokter, med makt til å velge for eksempel hvordan signalet fungerer og hvem det deles med, må alderssignalet utvikles som en åpen, teknisk standard, uten lisensieringsbegrensninger. Det må også være basert på tilgjengelig og åpen kildekode som kan brukes av alle.

---

[134] Direktiv om urimelig handelspraksis vedlegg I, punkt 28.
[135] DSA art. 34 og 35.

Det er viktig at alderssignaler blir implementert som myke tekniske tiltak, gir muligheter for detaljerte innstillinger, og at de kan slås av eller endres i samsvar med barnets situasjon og behov. Videre er det verdt å ha i mente at alle tiltak som gjøres på en enhet, slik som alderssignaler, ikke vil ha noen effekt dersom barna benytter digitale tjenester på en enhet som ikke er spesifikt angitt som deres, for eksempel en enhet som tilhører en forelder eller omsorgsgiver.

I tillegg til endringene som må gjøres for alle forbrukere, må leverandører av digitale tjenester i alle fall iverksette en rekke målrettede tiltak mot barn og unge, for å styrke deres rettigheter og autonomi på nett. Dette forutsetter ambisiøs håndheving av eksisterende lovverk.

Alderstilpassede tjenester

Veldig store nettplattformer må vurdere og redusere risikoer som plattformene deres utgjør for barn, i tråd med DSA art. 34 og 35.[136]

I tillegg til tiltakene som må iverksettes av de veldig store nettplattformene, må *alle* nettplattformer som er tilgjengelige for barn iverksette tiltak for å sikre et høyt nivå av personvern, trygghet og sikkerhet for barn på sine tjenester, jf. DSA art. 28(1). En streng tolkning av dette kravet kan være essensielt for å få bukt med destruktive anbefalingsalgoritmer og markedsføring basert på profilering og personopplysninger, samt avhengighetsskapende teknikker.

Nettplattformer bør på denne bakgrunn iverksette en rekke tiltak:

- Alderstilpassede verktøy, informasjon og standardinnstillinger.
- Anbefalingsalgoritmene bør ikke være optimalisert for engasjement,[137] og kan istedenfor optimaliseres for kvalitet og barns tilbakemelding og eksplisitte signaler.[138]
- Avhengighetsskapende mekanismer som uendelig skrolling, autoavspilling og «streaks», bør ikke brukes for barnekontoer.
- Barns personopplysninger bør ikke utnyttes til kommersielle formål, for eksempel til å trene KI-modeller. Dette kan også håndheves gjennom personvernforordningen art. 5(1), som krever formålsbegrensning og dataminimering.

[136] Se mer om dette i kapittel 5.1.1.
[137] «Safe by Default», Panoptykon Foundation and People vs. Big Tech (2024). https://en.panoptykon.org/safe-default-panoptykon-foundation-and-people-vs-bigtechs-briefing
[138] «Towards a safer, more private and secure internet for children in online platforms», BEUC (2024). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2024-074_Submission_to_the_Call_for_Evidence_on_Article_28_DSA.pdf

- Tilgjengelige og brukervennlige verktøy for å slette barns digitale fotspor.[139]

- Klage- og varslingsmekanismer bør være alderstilpassede og tilgjengelige for barn og unge. DSA art.16 krever også at varslingsmekanismer skal være «enkelt å få tilgang til og brukervennlig».

- Det må være mange nok ansatte som har fått opplæring i å behandle klager og interagere med barn unge, slik at de kan svare på spørsmål og gi annen hjelp, for eksempel hvis barn opplever uønsket kontakt eller innhold.

I tillegg bør nettplattformer benytte standardinnstillinger som beskytter barns personvern, trygghet og sikkerhet:

- Alderstilpasset «sikkert søk»-filter.

- Private barnekontoer, slik at innholdet de lager for eksempel ikke blir åpent tilgjengelige for offentligheten.

- Varsler bør være redusert til et minimumsnivå.

- Ingen sporing av barns atferd, hverken analogt eller digitalt, for kommersielle formål.[140]

- Ingen anbefalingsalgoritmer som er basert på overvåking og profilering.[141] Personvernforordningens prinsipper om dataminimering og innebygd personvern kan også håndheves for å redusere skadevirkningene ved av individuelt målrettede anbefalingsalgoritmer betraktelig.[142]

- Ingen funksjoner som er basert på signaler om sosial anerkjennelse (slik som knappen for «liker» / «liker ikke»).[143]

Alle tilbydere av digitale tjenester bør også gjennomføre personvernkonsekvens-vurderinger når det er sannsynlig at barn benytter tjenestene deres, jf.

---

[139] Se flere tiltak her: «Towards a safer, more private and secure internet for children in online platforms», BEUC (2024). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2024-074_Submission_to_the_Call_for_Evidence_on_Article_28_DSA.pdf
[140] Ibid.
[141] «Ending artificial amplification of hate & hysteria», Irish Council for Civil Liberties (2023). https://www.iccl.ie/wp-content/uploads/2023/12/Ending-artificail-amplification-of-hate-and-hysteria.pdf
[142] Se art. 5(1)(c) og 25.
[143] «Safe by Default», Panoptykon Foundation and People vs. Big Tech (2024). https://panoptykon.org/sites/default/files/2024-03/panoptykon_peoplevsbigtech_safe-by-default_briefing_03032024.pdf

personvernforordningen art. 35.[144] Dette inkluderer å implementere risikoreduserende tiltak for enhver risiko for barns personvern.

Markedsføring

For å begrense utbredelsen av ulovlig handelspraksis og markedsføring på digitale tjenester bør det treffes en rekke tiltak:

- Næringsdrivende skal ikke målrette direkte kjøpsoppfordringer til barn. Dette kan håndheves gjennom vedlegg 1 i direktivet om urimelig handelspraksis, og må inkludere bruk av avskrekkende bøter.

- Digitale tjenester bør ikke benytte manipulerende design mot barn. Dette kan håndheves gjennom DSA art. 25, personvernforordningen og direktivet om urimelig handelspraksis, alt etter hvilket regelverk som egner seg best.[145] For eksempel bør ikke digitale tjenester manipulere barn til å velge innstillinger som leder til dårligere personvern.

- Digitale plattformer bør ikke målrette annonser basert på profilering mot barn. Dette kan håndheves gjennom DSA art. 28(2).

Influensermarkedsføring

For influensermarkedsføring bør innhold og markedsføring være mer tydelig atskilt enn de er i dag. Skjult markedsføring er ulovlig, jf. direktivet om urimelig handelspraksis art. 7(2). For å operasjonalisere forbudet mot skjult markedsføring, bør det utarbeides felles standarder for merking i hele EU. Standardene bør ta utgangspunkt i DSA art. 26(2),[146] og bør inkludere:

- Større og mer visuelt fremtredende merking, som for eksempel kan ta opp halve skjermen i videoer.

- Klare skiller mellom influenseres betalte og ubetalte innhold, for eksempel ved å ta tydelige «reklamepauser» i videoer når de reklamerer for et produkt.[147]

---

[144] Se ICO's retningslinjer: «Data protection impact assessments», https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/2-data-protection-impact-assessments/

[145] Som nevnt i kapittel 5.1.1 er det behov for å utrede hvordan disse regelverkene må forstås i sammenheng.

[146] «From influence to responsibility: Time to regulate influencer marketing», BEUC (2023). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-093_From_influence_to_responsibility_Time_to_regulate_influencer-marketing.pdf.

[147] Influensere kan også risikere å bryte for eksempel UCPD vedlegg 1 punkt 11, hvis det ikke kommer tydelig nok fram at det er snakk om et kommersielt budskap.

Influensermarkedsføring må også reguleres strengere i et oppdatert forbrukerregelverk, for eksempel ved å stille krav til:

- Ytterligere åpenhet om hvem som betaler for sponset innhold. Dette kan bygge på DSA art. 26(2).

- Felles regler på EU-nivå om delt ansvar mellom influensere, deres byråer og næringsdrivende, for å etablere ansvarlighet gjennom hele influenserverdikjeden.[148]

Innføre nye lovbestemmelser med horisontal beskyttelse for barn

Barn bør ha horisontal beskyttelse utover det å være ansett som sårbare forbrukere, slik som nå er tilfelle i direktivet om urimelig handelspraksis.[149] Lovgivere må derfor også innføre noen nye lovbestemmelser gjennom målrettede oppdateringer av direktivet om urimelig handelspraksis, som for eksempel:

- Et krav om at alle næringsdrivende må vurdere om tjenestene deres appellerer til barn. Hvis tjenestene deres appellerer til barn, må de identifisere og redusere risikoer for barn. Dette bør være en del av de næringsdrivendes aktsomhetsplikt.[150]

- Bestemmelser som beskytter barn mot uakseptabel markedsføring bør generelt beskytte dem mot reklame de eksponeres for, snarere enn reklame som er målrettet mot dem. Dette senker terskelen for håndheving og styrker beskyttelsen av barn på nett.

- Terskelen for at noe blir ansett som «målrettet» mot barn må være lav, for å sikre at barn får den beskyttelsen de har krav på gjennom lover som for eksempel direktivet om urimelig handelspraksis.

Direktivet om urimelig handelspraksis må utvides til å gjelde flere handelspraksiser som alltid skal regnes som urimelige. Dette vil gjøre det enklere for selskapene å trekke opp klare grenser for egen handelspraksis og for tilsynsmyndigheter å sanksjonere selskaper som bryter loven. Urimelige

---

[148] «From influence to responsibility: Time to regulate influencer marketing», BEUC (2023). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-093_From_influence_to_responsibility_Time_to_regulate_influencer-marketing.pdf. I Norge er dette allerede gjeldende: «Forbrukertilsynets veiledning om reklame i sosiale medier», Forbrukertilsynet (2024). https://www.forbrukertilsynet.no/lov-og-rett/veiledninger-og-retningslinjer/someveiledning#hvordanmerke

[149] «Towards European digital fairness», BEUC (2023). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-020_Consultation_paper_REFIT_consumer_law_digital_fairness.pdf

[150] UCPD art. 2(h).

handelspraksiser bør omfatte:

- Et generelt forbud mot målretting av reklame mot barn under 16 år, eller som vises til mange barn under 16 år,

- Et generelt forbud mot markedsføring av mat som inneholder mye fett, sukker eller salt,[151]

- Et forbud på EU-nivå mot influensermarkedsføring av pengespill, alkoholholdige produkter, medisinske produkter, kosmetiske inngrep og andre produkter som kan ha en negativ påvirkning på barns mentale helse eller velvære.[152]

5.1.3. Forbedre og styrke håndhevingsapparatet

Som vi har bemerket på flere steder i denne rapporten, er hverken internett generelt, eller sosiale medier spesielt, lovløse rom. Det finnes en rekke gjeldende lovbestemmelser både på nasjonalt og europeisk nivå. Mange av disse lovene blir imidlertid ikke håndhevet i tilstrekkelig grad, noe som gir dårlig beskyttelse for både barn og voksne på nettet.

I løpet av DSAs første måneder med håndheving, har EU-kommisjonen allerede utnyttet sin adgang til å be om informasjon fra selskaper en rekke ganger, for eksempel om anbefalingsalgoritmene til YouTube, TikTok og SnapChat.[153] EU-kommisjonen har også åpnet flere formelle saker, og forpliktet for eksempel TikTok til å trekke tilbake tjenesten «TikTok Lite Rewards», som inneholdt avhengighetsskapende mekanismer.[154] Forhåpentligvis vil EU-kommisjonen fortsette den grundige håndhevingen av DSA, inkludert ved å ilegge avskrekkende overtredelsesgebyrer.

Samtidig er det nødvendig med sterkere og mer effektiv håndheving av andre lover som regulerer digitale tjenester, som personvernforordningen, handelspraksisdirektivet, og AMT-direktivet. Håndhevingsapparatet kan styrkes og forbedres på mange ulike måter.

---

[151] «Food marketing to children needs rules with teeth», BEUC (2021). https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-084_food_marketing_to_children_needs_rules_with_teeth.pdf

[152] «From influence to responsibility: Time to regulate influencer marketing», BEUC (2023). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-093_From_influence_to_responsibility_Time_to_regulate_influencer-marketing.pdf

[153] «Commission questions YouTube, TikTok, and Snapchat over recommender algorithms», Gkritsi, Eurativ (2024). https://www.euractiv.com/section/tech/news/commission-questions-youtube-tiktok-and-snapchat-over-recommender-algorithms/

[154] «TikTok commits to permanently withdraw TikTok Lite Rewards programme from the EU to comply with the Digital Services Act», EU-kommisjonen (2024). https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4161

Tverrsektoriell og grenseoverskridende håndheving

Barns rettigheter er spredd over mange ulike lover.[155] Tilsynene som håndhever disse lovene, må ha klart definerte ansvarsområder, slik at ulovlig praksis rettet mot barn ikke «faller mellom stoler».[156]

Tilsynsmyndigheter må samarbeide på tvers av sektorer. Dette bør omfatte:

- Å sørge for at barn enkelt kan klage på ulovlig praksis. Hvis en klage blir sendt til feil tilsynsmyndighet, må tilsynet sørge for at klagen blir sendt videre til rett instans.
- Regelmessige koordinerte tilsyn på tvers av sektorer.
- Plikt til å informere andre tilsynsmyndigheter hvis de oppdager lovbrudd som ligger innenfor noen andres mandat.

Håndheving av barns rettigheter forutsetter samarbeid på tvers av landegrenser. Dette betyr at nasjonale tilsynsmyndigheter må samarbeide med andre tilsyn i av EU og EØS.[157] Europeiske tilsynsmyndigheter bør også samarbeide med tilsyn i andre land, som for eksempel Federal Trade Commission (FTC) i USA og Ofcom i Storbritannia.

Sikre at barn kan representeres i rettssystemet

Mange av handelspraksisene som har blitt skissert i denne rapporten, er svært invaderende, foregår i det skjulte, og er både teknisk og juridisk komplekse. Barn bør ikke overlates til seg selv. Istedenfor bør de kunne la seg representere av organisasjoner som ikke har profitt for øye i klagesaker mot selskaper som bryter deres grunnleggende rettigheter. Det inkluderer:

- Rett til å la seg representere i gruppesøksmål under direktivet om beskyttelse av forbrukernes kollektive interesser.[158]
- Rett til å la seg representere av en organisasjon i klagesaker som gjelder brudd på deres personvern, jf. personvernforordningen art. 80(1).

---

[155] I Norge er disse spredd over minst ti ulike lover: «Nødvendig å styrke barns forbrukervern i digitale medier», Barneombudet, Forbrukerrådet (2022). forbrukervern-i-digtale-medier.pdf.
[156] «Too much or too little? Assessing the Consumer Protection Cooperation (CPC) network in the protection of consumers and children on TikTok», Gamito, Micklitz, BEUC (2023). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-018_Assessing_CPC_Network_in_the_protection_of_consumers_and_children_on_TikTok-Report.pdf
[157] Consumer Protection Cooperation Network (CPC) og Det europeiske personvernrådet (EDPB) er eksempler på dette.
[158] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (Text with EEA relevance).

Den rådende forretningsmodellen påvirker millioner av barns rettigheter hver dag. Ingen enkeltbarn bør pålegges å sende inn klager på noen av verdens største selskaper, på vegne av barn som gruppe.

Organisasjoner som oppfyller visse kriterier, inkludert å ikke ha profitt for øye, må derfor kunne klage inn selskaper som opererer på måter som leder til systematiske og dyptgripende brudd på barns personvern, uten enkeltbarns mandat. Dette er mulig etter personvernforordningen art. 80(2), men forutsetter nasjonal lovhjemmel.

Sanksjoner

Tilsynsmyndigheter må ha mandat til å bruke avskrekkende håndhevingsmidler overfor selskaper som bryter loven, inkludert gjennom overtredelsesgebyrer, ødeleggelse av modeller («algorithmic digorgement»),[159] og å kreve umiddelbar stans av enhver ulovlig praksis. Dette er sentralt for å avskrekke selskapene som er gjenstand for vedtaket. Å bryte loven skal ikke være lønnsomt eller bli betraktet som en «driftskostnad».[160]

Samtidig bør sanksjoner også bidra til å avskrekke andre selskaper som opererer på tilsvarende måter. I dag er det for mange næringsdrivende som opererer i strid med loven til at håndheving kan basere seg på privat dialog mellom tilsyn og enkeltaktører. Hvis håndhevingsmidlene ikke virker avskrekkende, vil tilsynene aldri lykkes i å få stanset alle overtrampene.

Ressurser til tilsynsmyndigheter

Håndheving av eksisterende lover er et svært viktig grep for å forbedre barns opplevelser og rettigheter på nett. Det forutsetter at tilsynsmyndighetene har tilstrekkelig ressurser, inkludert tilgang til nødvendig ekspertise innenfor for eksempel design og teknologi. Tilsynsmyndigheter må også bruke teknologi på en måte som gjør det mulig å skalere håndheving.

Selvreguleringsordninger har vist seg å være utilstrekkelige i den digitale sfæren og skaper en uoversiktlig håndhevingsstruktur for barn, foreldre og omsorgsgivere. Det ansvaret som er plassert hos selvreguleringsordninger, bør overføres til uavhengige tilsynsmyndigheter.

---

[159] «Explaining model disgorgement», IAPP (2023). https://iapp.org/news/a/explaining-model-disgorgement

[160] «Big Tech has already made enough money in 2024 to pay all its 2023 fines», Proton (2024). https://proton.me/blog/big-tech-2023-fines-vs-revenue

Revisjon av lovene som regulerer samarbeid på tvers av landegrenser

Det pågår en lovgivningsprosess for å forbedre håndhevingen av personvernforordningen i grenseoverskridende saker. Slike saker tar i dag svært lang tid, og handler i mange tilfeller om noen av de aller største teknologiselskapene. Sakene har derfor konsekvenser for personvernet til nært sagt alle forbrukere i EU og EØS.

Lovgivere bør utnytte muligheten til å sikre:[161]

- Enklere og tilrettelagte klageordninger. Enkeltindivider, herunder barn, kan ikke pålegges å underbygge sin klage med en foreløpig juridisk analyse for at klagen skal anses som gyldig.

- Rimelige og proporsjonale tidsfrister, slik at håndhevingsprosessen ikke tar mer enn 12–18 måneder.

- Partsrettigheter, slik at den som klager inn et forhold blir hørt på en meningsfull måte.

Samtidig bør EU-kommisjonen revidere Consumer Protection Cooperation Network-forordningen,[162] som regulerer samarbeidet mellom europeiske forbrukertilsynsmyndigheter, for eksempel om håndheving av direktivet om urimelig handelspraksis.

En oppdatert forordning bør omfatte:[163]

- En håndhevingsrolle for EU-kommisjonen i saker som gjelder i hele EU. EU-kommisjonen må i så fall også ha adgang til å ilegge overtredelsesgebyrer.

- Et krav om at koordinerte aksjoner ikke kan avsluttes før de næringsdrivende har gjennomført alle tiltakene de har forpliktet seg til.

- Prosessuelle rettigheter for organisasjoner som sender inn eksterne varsler om systematiske brudd.

---

[161] «GDPR Cross-Border Enforcement Regulation – BEUC's Position Paper», BEUC (2023). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-162_Cross-Border_Enforcement_Regulation.pdf

[162] Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 (Text with EEA relevance)

[163] Se flere tiltak her: «Strengthening the coordinated enforcement of consumer protection rules», BEUC (2022). https://www.beuc.eu/sites/default/files/publications/BEUC-X-2022-135_Strengthening_the_coordinated_enforcement_of_consumer_protection_rules.pdf

5.2. Sørge for at familier og offentlige myndigheter er rustet til å tilby barn alderstilpassede opplevelser på nettet

Ettersom det er ekstremt lønnsomt for digitale tjenestetilbydere å utnytte barn, er det urealistisk å forvente at de endrer sine handelspraksiser basert på ikke-bindende tiltak som retningslinjer og anbefalinger. Familier, foreldre, omsorgsgivere og offentlige myndigheter har imidlertid ingen kommersielle insentiver til å utsette barn for fare. Våre anbefalinger omfatter derfor en rekke mykere tiltak som er rettet mot dem, som for eksempel retningslinjer, aldersgrenser og styringsdokumenter.

5.2.1. Reduser antallet barn som benytter digitale tjenester til tross for at de er under aldersgrensen

Den offentlige debatten om beskyttelse av barn på nett fokuserer ofte på bruk av tekniske sperrer for å holde barn og unge unna bestemte digitale tjenester. Denne rapporten har vist at innføring av aldersverifisering på digitale tjenester er et komplisert og risikofylt tiltak. Det skyldes de negative virkningene aldersverifisering kan ha på barns øvrige rettigheter, risikoene forbundet med de fleste av de tekniske løsningene som er tilgjengelige i dag, og sannsynligheten for at barn vil bruke alternative tjenester som innebærer en enda større risiko.

Selv om aldersverifisering ikke nødvendigvis er den «perfekte» løsningen mange politikere og tilsynsmyndigheter håper på, er det åpenbart at en del digitale tjenester ikke er ment for barn under en viss alder. Myndigheter og selskaper må derfor iverksette tiltak som reduserer antallet barn som skaffer seg tilgang til og bruker slike tjenester, selv om de er under aldersgrensen.

I Norge bruker rundt 50 % av alle niåringer allerede sosiale medier, til tross for plattformenes selvpålagte aldersgrense på 13 år og bruk av alderserklæring.[164] Allerede fra en svært ung alder, omgår med andre ord mange barn plattformenes aldersbekreftelsesmekanismer. Dette har overbevist mange politikere om at harde, tekniske tiltak er en absolutt nødvendighet, spesielt sett i lys av de mange risikoene barn og unge står overfor på plattformene.

Det hender at barn omgår aldersbekreftelsesmekanismene på sosiale medier uten at foreldre eller omsorgsgivere vet om det. For disse barna kan en hardere teknisk sperre redusere muligheten for å få tilgang til tjenester.[165] Som beskrevet i kapittel 4.4.1, er det imidlertid vanligst at barn under aldersgrensen bare bruker

[164] «Barn og Medier 2024: Delrapport: Barn og unges medievaner og tilgang til teknologi», Medietilsynet (2024) s.15. https://www.medietilsynet.no/globalassets/publikasjoner/barn-og-medier-undersokelser/2024/delrapport-1_bom_barn-og-unges-medievaner-og-tilgang-til-teknologi.pdf

[165] Likevel med forbehold om mulige omgåelsestaktikker.

sosiale medier dersom de har fått tillatelse til det fra foreldre eller omsorgspersoner, eller til og med deres hjelp. Et viktig tiltak er derfor å redusere antallet foreldre eller omsorgspersoner som tillater at barna sine omgår aldersgrensen.

Mange foreldre og omsorgsgivere opplyser at grunnen til at de tillater sine barn å bruke digitale plattformer selv om de er under aldersgrensen, er at de er redde for at barna vil kunne bli sosialt utestengt hvis de ikke er til stede på nettet.[166] For eksempel er det vanlig at skoleklasser allerede fra tidligere alderstrinn oppretter digitale grupper på sosiale medier. Den åpenbare og umiddelbare risikoen for sosial eksklusjon betraktes som større enn den risikoen plattformene i seg selv representerer. Mangelen på koordinering og fellesføringer blant foreldre og omsorgsgivere fører til det minste felles multiplum og dermed den laveste beskyttelsen for enkeltbarn.

Når foreldre og omsorgsgivere mener at barna deres trenger å bruke sosiale medier av sosiale årsaker, er det stor risiko for at de vil fortsette å tillate barna å omgå eventuelle hardere tekniske aldersspærrer. Dette problemet forsterkes ved at mange barn som er under aldersgrensen, men likevel bruker sosiale medier fordi de har fått tillatelse til det av foreldre eller omsorgsgivere, vil miste tilgangen til plattformene dersom de innfører aldersverifisering. Det er derfor ikke nok å innføre hardere tekniske sperrer; det sosiale presset om å være til stede på plattformene må først reduseres. Dette forutsetter at samfunnet som helhet, herunder foreldre, omsorgsgivere og barna selv, oppfatter aldersgrensen for sosiale medier som både legitim og nødvendig.

Så langt er det i hovedsak tjenestetilbyderne selv som har fått velge aldersgrensen på sosiale medier. Selv om personvernforordningen krever at barn må være mellom 13 og 16 år før de kan samtykke til behandling av sine personopplysninger på sosiale medietjenester,[167] er ikke dette en aldersgrense for tjenestene som sådan, bare en aldersgrense for å samtykke til behandling av personopplysninger om seg selv. Det betyr at foreldre kan samtykke til at barn under aldersgrensen for samtykke bruker sosiale medier. I tillegg kan selskaper argumentere for at de bruker andre rettslige grunnlag enn samtykke når de behandler barns personopplysninger,[168] slik de for eksempel har gjort etter at Danmark økte sine aldersgrenser for samtykke tidligere i 2024.[169]

---

[166] «Digitale dilemmaer – en undersøkelse om barns debut på mobil og sosiale medier», Medietilsynet (2023). s. 50. https://www.medietilsynet.no/globalassets/publikasjoner/barn-og-medier-undersokelser/2022/230206_digitale-dilemmaer.pdf

[167] Medlemslandene står fritt til å bestemme en nøyaktig aldersgrense på nasjonalt nivå.

[168] «Annex C: Lawful basis for processing», ICO. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/annex-c-lawful-basis-for-processing/.

[169] «Hvert andet barn i Danmark er på sociale medier, før de fylder ti år», Medierådet for Børn & Unge (2024). https://medieraadet.dk/aktuelt-fra-medieraadet/2024/maj/hvert-andet-barn-i-danmark-er-paa-sociale-medier-foer-de-fylder-ti-aar

Personvernforordningens aldersgrense for samtykke kan med andre ord gi en indikasjon om at slike tjenester ikke bør brukes av barn under denne alderen, men er langt fra noen tydelig grense for bruk av sosiale medier.

Mens dagens aldersgrenser for sosiale medier enten er uklare eller basert på selskapenes selvpålagte regler, er det også en mangel på klare og faktabaserte retningslinjer fra myndighetene om når barn bør bruke sosiale medier. Et bidrag som er verdt å merke seg fra den siste tiden, er retningslinjene svenske myndigheter publiserte i 2024.[170] Selv om de ikke fastsetter noen nye aldersgrenser, er de eksplisitte og klare på at barn under aldersgrensen ikke bør bruke sosiale medier.

Norske myndigheter, derimot, oppfordrer foreldre og omsorgsgivere til å vurdere individuelt hvorvidt barna deres er gamle og modne nok til å bruke sosiale medier.[171] Samtidig har ikke myndighetene formidlet risikoene ved digitale tjenester i tilstrekkelig grad. Risikoen for sosial ekskludering som følge av å ikke bruke sosiale medier er umiddelbar, mens risikoene ved bruk av sosiale medier ofte er mye mindre håndgripelige. Det er derfor nødvendig at myndigheter, skoler og andre offentlige institusjoner formidler disse risikoene tydelig til barn, foreldre og omsorgsgivere gjennom kanaler slik som helsestasjoner, barnehager, skoler og biblioteker.

En legitim aldersgrense forutsetter at myndighetene finner den rette balansen mellom barnas mange rettigheter og interesser. Etter å ha fastsatt en slik aldersgrense, må myndighetene også begrunne aldersgrensen og gi tydelig veiledning til familier, skoler og andre institusjoner med ansvar for og overfor barn. Dette kan bane vei for kollektive avgjørelser blant foreldre og omsorgsgivere om at yngre barn ikke skal bruke sosiale medier. Sprikende kommunikasjon fra myndighetene om hvor gamle barna bør være før foreldre og omsorgsgivere gir dem tilgang til sosiale medier, svekker aldersgrensens legitimitet og bør unngås.

En legitim aldersgrense må suppleres med praktiske og funksjonelle foreldrekontroller, alderstilpasset design og standardinnstillinger som respekterer barnas rettigheter.

Myndighetene må gi familier:

- Legitime aldersgrenser, tydelige råd og fungerende verktøy. For eksempel kan ikke foreldre gis ansvar for å utføre individuelle

[170] «Rekommendationer för en balanserad skärmanvändning bland barn», Folkhälsomyndigheten (2024). https://www.folkhalsomyndigheten.se/nyheter-och-press/nyhetsarkiv/2024/september/rekommendationer-for-en-balanserad-skarmanvandning-bland-barn

[171] Per 15. oktober 2024. Se for eksempel Bufdirs veiledning: «Barn og sosiale medier». https://www.bufdir.no/foreldrehverdag/skolebarn/digital-hverdag/barn-og-sosiale-medier/.

risikovurderinger av konkrete digitale tjenester, da disse er juridisk, sosialt, kommersielt og teknisk komplekse.

- Alderstilpasset veiledning om bruk av digitale tjenester, basert på føre-var-prinsippet, der det tas hensyn til barnets alder. Det kan omfatte elementer som:
    - Generelle råd om å følge aldersgrenser.
    - Hvilke typer digitale tjenester barn under en viss alder ikke skal bruke.
    - Den maksimale tiden barn i ulike aldre bør tilbringe på sosiale medier eller andre digitale tjenester.[172]
    - Råd om innstillinger for «sikkert søk» og andre innstillinger som er relativt effektive og enkle å bruke.

5.2.2. Foreldreansvar bør kun supplere andre tiltak

Selv om det er viktig at foreldre og omsorgsgivere regulerer barns bruk av smarttelefoner og digitale tjenester, er det urettferdig å skyve hele ansvaret over på hver enkelt familie. Det er mange grunner til dette.

Foreldrekontroller blir mindre og mindre effektive, etter hvert som barna blir eldre. Når de blir tenåringer, er de svært begrensede. Digital kompetanse er heller ikke jevnt fordelt blant foreldre og omsorgsgivere – og noen barn har ikke foreldre eller omsorgsgivere i det hele tatt. Det er høyst problematisk dersom barn med digitalt kompetente foreldre eller omsorgsgivere er de eneste som får beskyttelse i den digitale sfæren.

Foreldreansvar kan derfor bare fungere som supplement til andre systemiske tiltak, for eksempel iverksatt av myndigheter, skoler og tjenestetilbydere. Politikerne må derimot prioritere å kreve at selskaper endrer sine digitale tjenester slik at de grunnleggende sett respekterer barns rettigheter, med tiltakene vi beskrev i kapittel 5.1. Samtidig vil det ta tid å få de store teknologigantene til å endre måtene de opererer på. I mellomtiden vil det å redusere bruken av de mest skadelige digitale tjenestene være det mest effektive tiltaket for å beskytte yngre barn. Tekniske foreldrekontroller kan være et nyttig verktøy for dette formålet.

[172] Se for eksempel «Till dig som har barn i åldern 6–12 år», Folkhälsomyndigheten (2024). https://www.folkhalsomyndigheten.se/livsvillkor-levnadsvanor/digitala-medier-och-halsa/till-dig-som-har-barn-i-aldern-612-ar/ (kun tilgjengelig på svensk).

Det er viktig å ha i mente at tekniske foreldrekontroller også kan misbrukes, for eksempel ved at de åpner for muligheten for å spionere på barna eller fjerne tilgangen til innhold og apper som er nødvendig for ungdommers og tenåringers velvære. Det kan for eksempel være snakk om hjelpetelefoner eller informasjon om seksualitet, kjønn eller religion. Hjemmesituasjonen til barn og unge kan også variere, og i voldelige hjem kan foreldrekontroller volde mer skade enn nytte.

Tiltak for å beskytte barn gjennom foreldreansvar må ikke føre til uakseptable kontrolltiltak mot barn, spesielt etter hvert som de blir eldre. Barnet bør være fullt informert om funksjoner for foreldrekontroll og foreldres eller omsorgsgiveres tilgang og kontroll bør gradvis reduseres etter hvert som barnet blir eldre.

Foreldre og omsorgsgivere kan prøve å beskytte sine unge barn gjennom alderstilpassede innstillinger, men mange av funksjonene de trenger, må tilbys av de relevante digitale tjenestetilbyderne.[173]

Når foreldrekontroller tilbys, bør de:

- Inneholde alderstilpassede standardinnstillinger og anbefalinger,
- Være tilgjengelige og enkle å bruke.
- Fungere på tvers av operativsystemer og enheter.
- Fungere etter sin hensikt.
- Tillate foreldre og omsorgsgivere å opprette separate alderstilpassede profiler og kontoer for barna sine, der standardinnstillingene gir barna den beskyttelsen de har krav på.
- Ikke forutsette at foreldre og omsorgsgivere må ha fullstendig oversikt over og detaljstyre innstillinger for en rekke apper, tjenester og nettsider, da dette er en enorm og tilnærmet umulig oppgave for de fleste foreldre.
- Sikre at barn får informasjon om hvordan foreldrekontroller fungerer, på en alderstilpasset og lett tilgjengelig måte.

Som beskrevet ovenfor, er tydelig veiledning og hjelp fra offentlige virksomheter også viktig for å sette foreldre eller omsorgsgivere i stand til, individuelt og som gruppe, å ta tak i barns og ungdoms bruk av sosiale medier på en ansvarlig måte.

---

[173] Dette kan være ett av flere tiltak for å sikre barns personvern, trygghet og sikkerhet på digitale tjenester, jf. DSA art. 28(1), eller et risikoreduserende tiltak, jf. DSA art. 35. Se mer om dette i avsnitt 5.1.

5.2.3. Offentlig sektor må gå foran med et godt eksempel

Denne rapporten har hovedsakelig tatt for seg digitale tjenestetilbydere, men det er også viktige tiltak som må gjennomføres i offentlig sektor. De siste 20 årene har offentlig sektor rullet ut digitale tjenester på skoler og andre institusjoner. Dette har ofte skjedd uten tilstrekkelig oversikt over hvem som får tilgang til barnas personopplysninger og oppmerksomhet. Utviklingen skjøt fart under pandemien.[174]

I praksis utsettes barn derfor ikke bare for kynisk kommersiell praksis på fritiden, men det er også en stor del av skolehverdagen deres. For eksempel utsettes 12 år gamle jenter for reklame for slankepiller på skoleenhetens kalkulator, og elevenes personopplysninger gjenbrukes for uspesifiserte formål gjennom «gratis» apper.[175] En rapport fra Human Rights Watch i 2022 avdekket at 145 av 163 produkter for utdanningsteknologi (89 prosent), tilsynelatende behandlet personopplysninger på måter som setter barns rettigheter i fare.[176]

Den svake beskyttelse barna får på skolen, har minst to viktige følger: Barna utsettes for uakseptabel risiko når de er på skolen, og skolene har en signaleffekt overfor foreldre og omsorgsgivere. Så lenge skolene ukritisk tilbyr iPad-er og PCer, uten at det legges inn sikkerhetsmekanismer, er det lite sannsynlig at foreldre og omsorgsgivere vil anse tilbakeholdenhet som et viktig tiltak for å redusere risikoer for yngre barn på nettet.

Det er mange tiltak offentlig sektor kan iverksette for å redusere barns eksponering for uakseptabel kommersiell påvirkning og misbruk av personopplysninger. Myndighetene bør for eksempel gi skoler og andre institusjoner i offentlig sektor som tilbyr digitale tjenester til barn:

- En katalog over digitale tjenester der personvern og sikkerhet er ivaretatt i tilstrekkelig grad, og som ikke bidrar til kommersielt press. Det er urealistisk å kreve at hver enkelt skole skal ha den nødvendige tekniske kompetansen til å gjøre dette selv.

- En personvernnorm i skolesektoren.[177]

---

[174] «An ed-tech tragedy? Educational technologies and school closures in the time of COVID-19», UNESCO (2023). https://www.unesco.org/en/articles/ed-tech-tragedy-educational-technologies-and-school-closures-time-covid-19

[175] «Ditt personvern – vårt felles ansvar», NOU 2022:11, Personvernkommisjonen (2022) https://www.regjeringen.no/contentassets/e4c60a6c51b147628b2c2e55db7e08e3/no/pdfs/nou20222022002011000dddpdfs.pdf

[176] «How Dare They Peep into My Private Life?», Human Rights Watch (2022). https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

[177] «Læring, hvor ble det av deg i alt mylderet?», NOU 2023:19, Ekspertgruppen for digital læringsanalyse (2023). https://www.regjeringen.no/no/dokumenter/nou-2023-19/id2982722/?ch=5#kap13

Myndighetene bør samtidig kreve at skoleeiere og andre institusjoner i offentlig sektor som tilbyr digitale tjenester til barn:

- Tilbyr innholdsfiltre på skolens enheter og skolenettverket. Dette tiltaket er spesielt relevant for yngre barn. Ved filtrering av innhold må skoler eller filtertilbyder være oppmerksomme på barns rett til informasjon, spesielt etter hvert som de blir eldre.

- Installerer annonseblokkere på skolens enheter, og sørger for at reklame ikke blir vist på digitale tjenester som tilbys til barna via skolen eller andre offentlige institusjoner. Annonseblokkerne må fungere både på skolens område og hjemme, dersom barna forventes å ta enhetene med seg hjem. Dette vil redusere kommersialiseringen av tjenestene og personvernrisikoene knyttet til salg av annonseplasser. Barn skal ikke behandles som forbrukere mens de er på skolen eller når de bruker andre tjenester tilbudt av myndighetene.

- Tilrettelegger for diskusjoner, tydelige retningslinjer og regler til elever og foreldre om bruken av digitale teknologier.

5.2.4. Styrke barn og unges forståelse av digitale utfordringer

Avslutningsvis er det også viktig at barn og unge selv får de verktøyene som kan forberede dem best mulig på de utfordringene de møter på nettet, for eksempel i form av opplæring. Så langt har dette ofte vært den eneste løsningen politikere og beslutningstakere har fokusert på, slik at barn og unge selv har måttet ta ansvar for å håndtere de enorme utfordringene digitale tjenester kan innebære. Tilnærmingen har vært mislykket og utilstrekkelig.

Hvis politikere og andre beslutningstakere imidlertid klarer å ha en helhetlig tilnærming til å håndtere utfordringene på digitale tjenester, slik vi har beskrevet i denne rapporten, taler mye for at også digital kompetanse og myndiggjøring bør være en del av de totale virkemidlene. En bred tilnærming til undervisning i mediekunnskap bør omfatte kunnskap om forretningsmodellene på nettet, personvern, sikkerhet, handelspraksiser, mobbing, psykisk helse, uønsket oppmerksomhet, uriktig informasjon, desinformasjon med mer. Involvering og undervisning bør starte fra en tidlig alder, og være alderstilpasset. Skoler og offentlige institusjoner spiller en sentral rolle.

forbrukerradet.no

FOR MER INFORMASJON:
Finn Lützow-Holm Myrstad, fagdirektør
Forbrukerrådet
finn.myrstad@forbrukerradet.no