

Til: Barne- og familiedepartementet og Digitaliserings- og
forvaltningsdepartementet

7. oktober 2025

Høringssvar – forslag til lov om aldersgrense for bruk av sosiale medier

Fra The Norwegian Chapter of Internet Society (ISOC Norge)

Med vennlig hilsen

Joar Rasmussen
Styremedlem
ISOC Norge

Med vennlig hilsen

Tom Fredrik Blenning
Styremedlem
ISOC Norge

Innledende sammendrag

ISOC Norge støtter regjeringens mål om å beskytte barn mot skadevirkningene av sosiale medier, men mener det foreslåtte virkemiddelet – en absolutt aldersgrense med krav til aldersverifisering – er teknisk og rettslig uegnet. Tiltaket vil ikke adressere de underliggende utfordringene ved dagens sosiale medier, og risikerer i stedet å svekke personvern, interoperabilitet og tillit til digitale tjenester.

ISOC Norge deler bekymringen for hvordan sosiale medier utnytter barns oppmerksomhet gjennom algoritmisk styrte forretningsmodeller. Det er imidlertid disse mekanismene som må reguleres, ikke barns tilgang til internett. En nasjonal aldersgrense basert på identitetskontroll vil i praksis skape en form for digital legitimasjonsplikt, med konsekvenser langt utover målgruppen.

Erfaringene fra andre europeiske land viser at aldersverifisering uten felles standarder fører til teknologisk fragmentering, svekket personvern og uforenlige systemer på tvers av landegrenser. EU-kommisjonen har derfor bedt medlemsland som Frankrike og Danmark om å utsette sine nasjonale prosjekter i påvente av en felles europeisk tilnærming. ISOC Norge mener Norge bør gjøre det samme: delta aktivt i det pågående arbeidet med europeiske og internasjonale standarder, i stedet for å utvikle en særnorsk løsning.

Forslaget står dessuten i spenningsforhold til eksisterende regelverk som Digital Services Act (DSA), General Data Protection Regulation (GDPR) og eIDAS, som allerede gir rammer for å beskytte barn på nett og regulere plattformenes ansvar. En ny nasjonal lov vil overlappe og potensielt kollidere med disse prosessene, og dermed svekke både rettssikkerhet og teknologisk harmonisering.

ISOC Norge anbefaler derfor at arbeidet med barns vern på nett forankres i europeisk koordinering, åpne standarder og prinsippene om privacy by design og zero knowledge. Slike løsninger kan gi effektiv aldersverifisering uten å kompromittere anonymitet, ytringsfrihet eller personvern.

Norge bør ta en aktiv rolle i å fremme slike løsninger internasjonalt – ikke innføre et system som bryter med dem.



Innholdsfortegnelse

Innledende sammendrag.....	1
Innledning.....	4
Overordnet vurdering.....	4
Infrastrukturmessige konsekvenser.....	5
Tap av interoperabilitet.....	5
Økt sentralisering og maktkonsentrasjon.....	6
Reidentifisering og metadata-risiko.....	6
Kostnader, kompleksitet og innovasjonsbarrierer.....	7
Digital suverenitet og avhengighet.....	7
Konklusjon.....	7
Standarder og teknologisk realisme.....	8
Privacy by Design.....	8
Zero-Knowledge Proof (ZKP).....	8
Åpne standarder.....	9
Distribuert tillit.....	9
Risiko for fragmentering og pågående internasjonalt arbeid.....	10
W3C Verifiable Credentials.....	10
IETF Privacy Pass og OPAQUE.....	11
OpenID4VP og Self-Sovereign Identity (SSI).....	11
Nasjonale initiativ og europeisk koordinering.....	12
Frankrike og Kommisjonens inngripen.....	12
Spania og utfordringene i praksis.....	12
Behovet for europeisk koordinering.....	13
Modenhetsvurdering.....	13
Barns digitale deltakelse og læring.....	15
Barns rett til deltakelse.....	15
Læring og teknologisk kompetanse.....	15
Risiko for forsterket digitalt utenforskap.....	16
En rettighetsbasert tilnærming.....	16
Konklusjon.....	17
Forholdsmessighet og rettssikkerhet.....	17
Prinsippet om forholdsmessighet.....	17
Risikoen ved strukturell kontroll.....	18

Rettssikkerhet og etterprøvbarehet.....	18
Helhetsvurdering.....	18
Vurdering.....	19
Konklusjon.....	19

Innledning

Norway Chapter of the Internet Society (ISOC Norge) takker for muligheten til å gi innspill til forslaget til lov om aldersgrense for bruk av sosiale medier.

The Internet Society (ISOC) er en global organisasjon som arbeider for å fremme et åpent, globalt sammenkoblet og sikkert internett. Siden etableringen i 1992 har ISOC vært sivilsamfunnets organisasjon i arbeidet med internettstyring, og hatt en sentral rolle i å utvikle prinsippene for åpenhet, interoperabilitet og brukerstyrke.

Gjennom sitt internasjonale nettverk av medlemmer, kapitler og partnere har ISOC bidratt til å forme både tekniske standarder og politiske prosesser, og vært en drivkraft i å gjøre internett til en global ressurs for alle. ISOC regnes i dag som en av de mest innflytelsesrike aktørene i internettets utvikling – en organisasjon som ikke bare forsvarer et åpent internett, men aktivt bygger det.

ISOC Norge er den norske avdelingen, og deltar i nasjonale prosesser der digitale rettigheter, tekniske prinsipper og samfunnsmessige konsekvenser av internettregulering står i sentrum.

Dette høringssvaret kompletterer Elektronisk Forpost Norge (EFN) sitt. Der EFN hovedsakelig fokuserer på de menneskerettslige og juridiske sidene av forslaget, retter ISOC Norge sitt fokus mot de tekniske og infrastrukturelle konsekvensene av aldersverifisering, samt de implikasjonene dette har for internettets åpenhet, interoperabilitet og barns faktiske deltakelse i det digitale samfunnet.

Overordnet vurdering

ISOC Norge deler regjeringens mål om å beskytte barn og unge mot skadevirkninger på digitale plattformer. Samtidig mener vi at tiltak som griper inn i den grunnleggende infrastrukturen for internett må vurderes med særlig varsomhet.

Aldersverifisering slik det foreslås vil i praksis innebære et identitetslag på tvers av alle sosiale medier, og dermed et strukturelt inngrep i hvordan internett fungerer. Det skaper ikke bare utfordringer for personvern og rettigheter, men også for interoperabilitet, sikkerhet og tillit – tre av de bærende prinsippene som har gjort internett globalt og åpent.

Forslaget legger opp til at tilbydere av sosiale medier skal stå ansvarlig for å implementere «effektiv aldersverifisering». Dette innebærer et teknisk krav uten klar definisjon, standard eller rammeverk. Resultatet vil være fragmenterte løsninger, proprietære systemer og økt avhengighet av store internasjonale aktører som allerede dominerer autentiseringsmarkedet.

Slike løsninger kan i verste fall føre til splinternet – et internett delt opp etter nasjonale og kommersielle grenser. For et lite land som Norge vil dette svekke både innovasjon og deltakelse, og kunne begrense barns tilgang til læring og fellesskap på tvers av landegrenser.

Effektive tiltak mot skade på nett må bygge på internasjonalt samarbeid, åpne standarder og “privacy by design”. Uten dette risikerer vi å erstatte dagens utfordringer med nye, langt mer inngripende problemer – der løsningen blir verre enn problemet.

ISOC Norge mener derfor at det fremlagte lovforslaget, i sin nåværende form, ikke oppfyller grunnleggende krav til teknisk realisme og internasjonal samordning, og at det må utredes nærmere før eventuelle tiltak iverksettes.

Infrastrukturmessige konsekvenser

Kravet om aldersverifisering reiser ikke bare spørsmål om personvern og lovgivning – det griper direkte inn i internettets tekniske arkitektur og prinsippene som gjør internett åpent, sikkert og sammenkoblet. Internett er ikke designet som et kontrollert miljø, men som et nettverk av nettverk, der interoperabilitet, desentralisering og tillitsbaserte protokoller danner grunnmuren.

Å innføre et krav om obligatorisk identitets- eller aldersverifisering innebærer å bygge et nytt, statlig eller kommersielt identitetslag over denne infrastrukturen. Et slikt lag vil nødvendigvis kreve integrasjon mellom hver enkelt tjeneste og en sentralisert eller delvis sentralisert verifikasjonsmekanisme, enten nasjonal eller global. Dette er et systemskifte som får konsekvenser langt utover sosiale medier alene.

Tap av interoperabilitet

Internettets styrke ligger i at alle aktører – store og små – kan bruke de samme åpne protokollene (for eksempel TCP/IP, HTTP, TLS, DNS) uten særnorske

eller proprietære krav. Dersom Norge innfører egne aldersverifiseringsmekanismer uten internasjonal standardisering, vil det bryte med prinsippet om protokollnøytralitet.

Tjenester som ønsker å operere i Norge, må da tilpasse seg særnorske krav. Dette kan føre til at:

- mindre utenlandske tjenester velger å stenge norske brukere ute
- globale plattformer innfører regionbasert differensiering (geo-fencing)
- åpne fellesskapstjenester som Mastodon, Wikipedia eller åpne forum mister teknisk kompatibilitet med norske brukere

Dette er den praktiske inngangsporten til splinternett – et internett der nasjonale regler og tekniske sperrer bryter opp den globale helheten.

Økt sentralisering og maktkonsentrasjon

Et universelt krav om aldersverifisering kan i praksis bare oppfylles av aktører med tilgang til omfattende identitetsdata. Det betyr at store teknologiselskaper, betalingsleverandører eller statlige ID-løsninger vil bli de faktiske portvokterne for digital deltakelse.

Dette øker risikoen for maktkonsentrasjon og svekket konkurranse. Plattformene som allerede dominerer markedet for identitet (Google, Apple, Meta, Microsoft) vil kunne tilby «ferdige» løsninger for aldersverifisering og dermed styrke sin posisjon ytterligere. Små, åpne eller desentraliserte tjenester – inkludert norske start-ups og ideelle plattformer – vil derimot stå uten realistiske alternativer.

Dermed risikerer tiltaket å redusere mangfoldet i det digitale økosystemet, samtidig som kontrollen over brukernes digitale identitet flyttes fra individet til store institusjoner.

Reidentifisering og metadata-risiko

Selv løsninger som hevder å være personvernvennlige, innebærer en risiko for reidentifisering. Når en bruker må bevise sin alder via en tredjepart, etterlater dette tekniske spor: IP-adresser, tidsstempler, kryptografiske nøkler, token-ID-er, transaksjonslogger og metadata om enhet og plattform.

Kobles disse over tid – for eksempel mellom ulike tjenester eller med andre datakilder – kan det i praksis rekonstruere brukerens identitet, selv om det aldri ble utlevert navn eller fødselsnummer. Dette er en kjent utfordring i systemer som ikke bygger på zero-knowledge proof (ZKP)-prinsipper.

Uten et helhetlig rammeverk for «privacy by design» og dataminimering vil slike systemer i realiteten føre til en ny form for digital sporing, bare under dekke av barns beskyttelse.

Kostnader, kompleksitet og innovasjonsbarrierer

Krav om integrert aldersverifisering vil også ha betydelige økonomiske og tekniske konsekvenser for tilbydere.

For små og mellomstore aktører, som i dag utgjør mye av innovasjonen i sosiale og kommunikative tjenester, vil det kreve både juridisk og teknisk omstilling: utvikling av grensesnitt, avtaler med verifikasjonstjenester, logging, og dokumentasjon av etterlevelse.

De store globale plattformene vil kunne absorbere slike kostnader uten vesentlig endring, mens mindre aktører risikerer å falle ut av markedet. Resultatet blir et mindre mangfoldig og mer sentralisert internett, i strid med både norske næringsinteresser og ISOCs globale prinsipper om åpen innovasjon.

Digital suverenitet og avhengighet

For et land som Norge, som er sterkt integrert i europeisk digital infrastruktur, innebærer dette en strategisk risiko:

Enten må vi basere oss på utenlandske løsninger for verifisering, og dermed avgi teknologisk kontroll,

eller vi må bygge nasjonale systemer som bryter interoperabilitet med resten av verden.

Begge alternativer undergraver digital suverenitet og prinsippet om et globalt, sammenkoblet internett.

Konklusjon

ISOC Norge mener at enhver vurdering av aldersverifisering må inkludere en systemisk analyse av dens arkitektoniske konsekvenser. Å bygge

kontrollmekanismer på infrastruktur-nivå uten global standardisering er i strid med internettets grunnprinsipper.

Tiltaket må derfor vurderes ikke bare som et juridisk eller etisk spørsmål, men som et inngrep i internettets arkitektur med potensielt irreversible følger.

Standarder og teknologisk realisme

For at et krav om aldersverifisering skal kunne gjennomføres uten å skade internettets grunnstruktur, må det bygge på åpne, internasjonalt anerkjente standarder og tekniske prinsipper som ivaretar både personvern og interoperabilitet.

Per i dag eksisterer ingen slike standarder som kan implementeres på tvers av jurisdiksjoner og tjenestetyper uten å skape nye risikoer. De løsningene som finnes, spenner fra enkle selvrapporderingsmekanismer til avanserte systemer for digital identitet og biometrisk verifikasjon – men ingen av dem oppfyller samtidig kravene til personvern, sikkerhet, skalerbarhet og åpenhet.

Privacy by Design

Et system for aldersverifisering må konstrueres slik at det teknisk sett hindrer unødvendig datainnsamling. Dette prinsippet innebærer at personvern ikke kan legges til som et juridisk vedlegg eller en funksjon på toppen av systemet, men må være innebygd i selve arkitekturen.

All behandling av data må være nødvendig, forholdsmessig og dokumenterbart begrenset. I praksis betyr dette at aldersverifisering må kunne utføres uten lagring av identitetsdata, logger eller koblingsnøkler som kan brukes til å gjenkjenne enkeltbrukere på tvers av tjenester.

Dette utelukker bruk av mekanismer som kontinuerlig autentisering via fødselsnummer, biometriske identifikatorer eller IP-baserte profiler. Løsninger som bryter med dette prinsippet, undergraver ikke bare personvernet, men også tilliten til infrastrukturen.

Zero-Knowledge Proof (ZKP)

Et reelt personvernvennlig system må baseres på kryptografiske metoder som gjør det mulig å bevise alder uten å avsløre identitet. Dette er kjent som «zero-knowledge proof».

ZKP-løsninger lar en bruker bevise et forhold – for eksempel at vedkommende er over 15 år – uten at noen får vite når eller hvor personen ble født, eller hvem vedkommende er.

Teknologien er allerede i bruk i enkelte digitale identitetsprosjekter, men krever koordinert standardisering og bred implementasjon for å kunne fungere i stor skala.

Bruk av ZKP er den eneste kjente tekniske metoden som kan balansere kravene til alderskontroll, personvern og anonymitet på en måte som er forenlig med menneskerettigheter og GDPRs prinsipper om dataminimering.

Åpne standarder

Et bærekraftig system må bygge på åpne og interoperable spesifikasjoner utviklet i internasjonale fora som IETF, W3C eller ISO. Dette sikrer transparens, etterprøvbarehet og teknologisk nøytralitet.

Lukkede, proprietære løsninger – som kommersielle ID-tjenester eller plattformspesifikke API-er – bryter med internettets arkitektur og øker risikoen for låsing (vendor lock-in).

Åpne standarder gjør det mulig for ulike aktører å implementere kompatible systemer, slik at brukere kan bevege seg fritt mellom tjenester uten å måtte gi fra seg mer informasjon enn nødvendig.

Distribuert tillit

Internettets grunnmodell er bygget på desentralisert tillit – ingen enkeltaktør kontrollerer hele systemet. Aldersverifisering må følge samme prinsipp.

Hvis én aktør – enten statlig eller kommersiell – gis kontroll over aldersverifisering for alle brukere, skaper det både sikkerhetsrisiko og demokratisk ubalanse.

Distribuert tillit kan etableres ved bruk av flere uavhengige attestutstedere, der hver part bare har begrenset informasjon og ingen enkeltaktør kan overvåke eller spore brukere på tvers av tjenester.

Dette forhindrer sentralisering og gjør det teknisk mulig å kombinere sikkerhet med personvern.

Risiko for fragmentering og pågående internasjonalt arbeid

Internasjonale standardiseringsorganer har de siste årene arbeidet med å utvikle tekniske rammeverk som kan balansere behovet for autentisering med personvern og interoperabilitet. Selv om ingen av disse løsningene foreløpig er modne nok til å dekke et nasjonalt krav om aldersverifisering, representerer de et viktig utgangspunkt for fremtidige standarder.

Samtidig viser erfaringene fra flere europeiske land at nasjonale særordninger på dette området raskt fører til fragmentering, både teknisk og rettslig.

Når hvert land utvikler egne løsninger for aldersverifisering, uten felles standarder for personvern, identitetsforvaltning og interoperabilitet, oppstår et uensartet digitalt indre marked.

Dette svekker både sikkerheten, personvernet og tilliten til digitale tjenester, og undergraver i praksis de mål som tiltaket var ment å oppnå.

ISOC Norge mener derfor at norsk politikk på området må forankres i de pågående internasjonale prosessene, fremfor å etablere særnorske ordninger som bryter med europeisk og global harmonisering.

Et slikt samarbeid er avgjørende for å unngå teknologisk isolasjon og sikre at norske brukere og tjenester forblir en del av det åpne, sammenkoblede internettet.

W3C Verifiable Credentials

World Wide Web Consortium (W3C) har utviklet Verifiable Credentials (VC) – et åpent rammeverk for digitale attestasjoner, der en bruker kan motta, lagre og presentere verifiserbar informasjon uten å avsløre mer enn nødvendig.

Et VC kan for eksempel si at en bruker er «over 15 år» uten å oppgi fødselsdato eller identitet. Dette oppnås ved hjelp av kryptografisk signering og selektiv deling av data, der brukeren selv kontrollerer hvem som får tilgang til hvilke opplysninger.

Teknologien er allerede implementert i flere pilotprosjekter i EU og Asia, men er fortsatt under standardisering. W3C-rammeverket er imidlertid den mest lovende veien mot interoperabel og personvernvennlig aldersverifisering, nettopp fordi det bygger på åpne prinsipper, brukerens kontroll og internasjonal forankring.

IETF Privacy Pass og OPAQUE

Internet Engineering Task Force (IETF) arbeider parallelt med flere tekniske mekanismer som kan understøtte anonyme eller delvise autentiseringssystemer.

To av de mest relevante er Privacy Pass og OPAQUE (Password-Authenticated Key Exchange).

Privacy Pass gjør det mulig å bevise at en bruker tidligere er validert av en tredjepart – uten at tjenesten vet hvem brukeren er. Det fungerer som et anonymt «bevis på autoritet» som kan brukes i forbindelse med f.eks. spam-forebygging eller adgangskontroll.

OPAQUE håndterer sikker autentisering uten at passord eller identitetsdata noensinne overføres i klartekst, og kan brukes som byggestein i systemer som ønsker distribuert tillit.

Disse teknologiene er fortsatt på eksperimentelt stadium, men de representerer en fremvoksende standard for personvernvennlig autentisering på internett, i tråd med ISOCs prinsipper om åpne protokoller og desentralisert sikkerhet.

OpenID4VP og Self-Sovereign Identity (SSI)

Et annet initiativ som er relevant for fremtidig aldersverifisering, er Self-Sovereign Identity (SSI) og den tilhørende spesifikasjonen OpenID for Verifiable Presentations (OpenID4VP).

SSI bygger på prinsippet om at individet skal ha full kontroll over sine digitale identitetsdata. I stedet for å stole på en sentral aktør, kan brukeren selv bevise utvalgte attributter – for eksempel «jeg er over 15 år» – ved hjelp av kryptografiske bevis.

Dette gir både sikkerhet og fleksibilitet: informasjonen kan verifiseres uten å avsløre personens øvrige data, og uten at en sentral database kan misbrukes eller kompromitteres.

Flere europeiske og internasjonale prosjekter, blant annet EUDI Wallet (EU Digital Identity), benytter SSI-prinsipper som del av et bredere identitetsøkosystem.

Teknologien har foreløpig utfordringer knyttet til interoperabilitet og brukervennlighet, men representerer den langsiktige retningen for personvernvennlige digitale identiteter i Europa.

Nasjonale initiativ og europeisk koordinering

Flere EU-land har de siste årene forsøkt å innføre nasjonale systemer for aldersverifisering, men disse forsøkene viser tydelig hvor krevende dette er – både teknisk, rettslig og politisk.

De mest profilerte eksemplene er fra Frankrike og Spania, der ulike modeller er prøvd ut for å kontrollere tilgangen til sosiale medier og pornografisk innhold.

Frankrike og Kommisjonens inngripen

I 2023 varslet EU-kommisjonen at Frankrikes forslag til nasjonal aldersverifisering ikke kunne settes i kraft uten ytterligere vurdering av forholdet til personvern og digitalt indre marked. Kommisjonen pekte spesielt på risikoen for fragmentering og ulike standarder mellom medlemsland, som kan undergrave den felles europeiske tilnærmingen til digitale tjenester.

Frankrike ble bedt om å stanse implementeringen i påvente av en felles europeisk løsning.

Dette viser at EU betrakter aldersverifisering som et spørsmål som krever koordinerte standarder og harmonisering, ikke nasjonale særordninger.

Spania og utfordringene i praksis

Den spanske regjeringen har valgt å gå videre med en pilot for aldersverifisering der brukeren må legitimere seg mot en sentral database før tilgang til visse nettjenester gis.

Modellen innebærer at en statlig mellomtjeneste verifiserer brukerens identitet før godkjennelse videresendes til den aktuelle plattformen.

Selv om systemet er ment å beskytte brukernes personvern gjennom mellomledd, innebærer det i praksis en sentralisert autentiseringsinfrastruktur som kan brukes til å spore brukere på tvers av tjenester.

Ekspertene, inkludert EDRi og ISOCs europeiske nettverk, har advart mot at en slik modell bryter med prinsippene for Privacy by Design og Zero-Knowledge, og kan bli en de facto overvåkningsmekanisme hvis den tas i bruk uten omfattende sikkerhetsgarantier.

Spania har også møtt betydelig teknisk motstand fra både kommersielle aktører og sivilsamfunn, som peker på at løsningen ikke er interoperabel og at den ikke lar seg integrere med eksisterende EU-ID-systemer (EUDI Wallet).

Behovet for europeisk koordinering

Disse eksemplene illustrerer hvorfor nasjonale løsninger ikke kan fungere isolert. Aldersverifisering er teknisk og juridisk tett knyttet til spørsmål om identitet, sikkerhet og interoperabilitet – områder som i EU er underlagt felles regelverk som DSA, eIDAS og GDPR.

Uten samordnet standardisering risikerer hvert land å utvikle egen teknologi og egen praksis, med uforenlige sikkerhetsnivåer og gjensidig ekskluderende systemer.

ISOC Norge mener Norge bør vente på og delta i den europeiske standardprosessen som nå pågår i regi av Kommisjonen, i samarbeid med W3C, IETF og EDRi. Dette er den eneste realistiske veien til varig og rettighetsforankret implementering.

Modenhetsvurdering

Selv om de tekniske og organisatoriske initiativene som beskrives ovenfor viser betydelig fremgang, befinner feltet for aldersverifisering seg fremdeles på et utviklings- og eksperimentstadium. Ingen av de eksisterende modellene oppfyller i dag de krav som kreves for nasjonal implementering – verken med hensyn til sikkerhet, interoperabilitet eller personvern.

For det første finnes det ingen etablerte internasjonale standarder som definerer hvordan aldersverifisering skal utføres på en måte som samtidig ivaretar anonymitet, minimal databehandling og brukerkontroll.

Både W3C, IETF og ISO har pågående arbeid, men prosessene er uferdige og delvis overlappende. Å basere et lovpålagt nasjonalt system på slike uferdige standarder vil tvinge Norge til å velge teknologi før prinsippene er ferdig definert.

For det andre er implementasjonskostnadene og infrastrukturen for slike systemer fortsatt uklare. Et reelt Zero-Knowledge-basert system krever kryptografisk modenhet, infrastruktur for nøkkelforvaltning og et økosystem av uavhengige attestutstedere. Dette eksisterer ikke i dag i praktisk eller operativ form.

Et forsøk på å etablere et nasjonalt system nå vil derfor nødvendigvis innebære en eller annen form for sentralisert mellomløsning, slik vi har sett i Spania – med de personvernmessige og sikkerhetsmessige konsekvensene det medfører.

For det tredje mangler det rettslig og institusjonell avklaring på europeisk nivå. EU-kommisjonen har eksplisitt signalisert at medlemsstatene bør avvente felles retningslinjer før egne systemer etableres. En norsk særordning nå vil derfor ikke bare kunne stride mot harmoniseringsprinsippet, men også skape teknisk inkompatibilitet mot EUs kommende EUDI-rammeverk.

På bakgrunn av dette vurderer ISOC Norge modenheten som for lav til at et påbud kan forsvares politisk, juridisk eller teknisk.

Det er nødvendig med minst tre parallelle utviklingsløp før aldersverifisering kan gjennomføres i samsvar med internasjonale prinsipper:

1. Standardisering: Fullføring av W3C- og IETF-arbeidet for Verifiable Credentials, Privacy Pass og relaterte teknologier.
2. Pilotering: Småskala, frivillige piloter i samarbeid med sivilsamfunn, akademia og teknologimiljøer for å validere løsninger i praksis.
3. Governance-modell: Utvikling av et uavhengig, distribuert tillitssystem som sikrer at ingen enkeltaktør – verken statlig eller kommersiell – kan overvåke eller spore brukere.

Inntil disse forutsetningene er oppfylt, vil ethvert lovpålagt krav til aldersverifisering innebære høy risiko for fragmentering, svekket sikkerhet og utilsiktet masseinnsamling av data.

Norsk politikk bør derfor ta sikte på å bidra til standardiseringsarbeidet snarere enn å innføre særnorske tekniske krav.

Barns digitale deltakelse og læring

Internett er ikke bare en sosial arena – det er en grunnleggende lærings- og deltakelsesplattform.

Barn og unge utvikler både teknologisk forståelse, kritisk tenkning og samfunnsengasjement gjennom sin digitale tilstedeværelse.

Et regelverk som innfører et generelt forbud mot bruk av sosiale medier under 15 år, risikerer derfor å redusere barns faktiske handlingsrom i det digitale samfunnet og svekke deres rett til utvikling.

Barns rett til deltakelse

FNs barnekonvensjon artikkel 12 og 13 slår fast barns rett til å bli hørt, ytre seg og delta i samfunnslivet.

I et moderne samfunn skjer store deler av denne deltakelsen digitalt – gjennom kommunikasjon, læring, samarbeid og uttrykk.

Aldersbaserte forbud vil i praksis ekskludere barn fra en rekke arenaer der samfunnsdebatt, nyhetsformidling og kulturutveksling foregår.

Særlig i et lite språksamfunn som Norge, der innhold for barn og unge i økende grad produseres og deles digitalt, vil et slikt forbud føre til at norske barn mister deltakelse i sin egen kulturkrets.

For mange vil konsekvensen være at de oppsøker uoffisielle eller utrygge plattformer, uten moderasjon og sikkerhetsmekanismer – det stikk motsatte av lovens formål.

Læring og teknologisk kompetanse

Digital kompetanse er ikke en ferdighet som kan tilegnes i et vakuum. Den utvikles gjennom praktisk erfaring, feiltrinn, og sosial læring.

Å nekte barn tilgang til sentrale digitale verktøy i formative år, er å frata dem muligheten til å lære ansvarlig og kritisk bruk av teknologi under trygge rammer.

ISOC Norge mener at barns digitale trygghet ikke oppnås gjennom isolasjon, men gjennom gradvis myndiggjøring og teknologiforståelse.

Dette innebærer at barn får delta under veiledning, og at foreldre, lærere og samfunn får verktøy til å støtte utviklingen av digital dømmekraft.

En slik tilnærming er i tråd med EU Kids Online-rammeverket, som viser at barn som lærer aktiv bruk av digitale medier under trygge forhold, både klarer seg bedre og er mindre utsatt for risiko senere.

Risiko for forsterket digitalt utenforskap

Et absolutt forbud rammer ikke alle barn likt.

Barn fra familier med høy digital kompetanse vil i praksis finne veier rundt forbudet, mens barn fra ressurssvake eller lavteknologiske hjem vil bli stående uten tilgang til digitale læringsarenaer.

Dette vil føre til økende digital ulikhet, der de som allerede står svakest sosialt og økonomisk også mister de digitale ferdighetene som kreves for framtidig utdanning og arbeid.

Digitalt utenforskap er ikke bare et sosialt problem, men et demokratisk.

Når tilgangen til ytringsrom og informasjon blir differensiert etter sosioøkonomisk bakgrunn, svekkes grunnlaget for likeverdig deltakelse i samfunnsdebatten.

En rettighetsbasert tilnærming

I stedet for aldersbaserte forbud bør politikkutviklingen bygge på retten til trygg og meningsfull deltakelse.

Dette krever tiltak som:

- styrker digital opplæring i skole og hjem,
- regulerer plattformenes design og kommersielle praksis,
- og støtter utviklingen av nasjonale verktøy og fellesskap som gir barn reell kompetanse og trygghet.

Et slikt rammeverk er i tråd med både FNs barnekonvensjon og EUs strategier for empowerment over restriction – og gjenspeiler internasjonal beste praksis.

Konklusjon

ISOC Norge understreker at barns behov for beskyttelse ikke må forstås som et behov for ekskludering.

Barn må beskyttes gjennom deltakelse, ikke fra den.

Lovforslagets foreslåtte aldersgrense kan gi en falsk trygghet, mens den reelle effekten blir økt utenforskap, svekket læring og redusert deltakelse i nettbaserte fellesskap.

Et fremtidsrettet regelverk må derfor ta utgangspunkt i barns rett til teknologi – ikke bare deres risiko ved den.

Forholdsmessighet og rettssikkerhet

Et demokratisk samfunn må kunne beskytte barn uten å undergrave de prinsipper som beskytter alle.

Et lovpålagt krav om aldersverifisering for bruk av sosiale medier representerer et inngrep i den digitale grunnstrukturen som går langt utover formålet det skal tjene.

Prinsippet om forholdsmessighet

Etter både Grunnloven § 113 og menneskerettighetene skal ethvert inngrep i borgernes frihet og privatliv være nødvendig, egnet og forholdsmessig.

Et tiltak som griper inn i hele befolkningens digitale handlefrihet, må derfor vurderes opp mot både nytteverdi og risiko.

Det foreligger ingen dokumentasjon som tilsier at en absolutt aldersgrense på 15 år gir bedre beskyttelse enn eksisterende regler kombinert med opplæring og tilsyn.

Tiltaket vil tvert imot påføre alle brukere et identifikasjonskrav og etablere en teknisk infrastruktur som i praksis åpner for kontinuerlig overvåkning og profilering.

Når et virkemiddel er massivt og lite treffsikkert, står det i strid med proporsjonalitetsprinsippet, uavhengig av hvor legitimt formålet måtte være.

Risikoen ved strukturell kontroll

Aldersverifisering kan ikke gjennomføres uten at staten eller private aktører får tilgang til og kontroll over identitetsdata.

Dette innebærer en overgang fra dagens modell, der brukerne har reell autonomi over sin nettbruk, til en modell der enhver digital handling må autoriseres gjennom en tredjepart.

En slik struktur flytter tillit fra brukeren til systemet, og innfører et nytt lag av digital kontroll i samfunnets kommunikasjonssystem.

Det bryter med internettets opprinnelige prinsipper om desentralisert tillit, og skaper en presedens der teknologisk infrastruktur brukes som forvaltningsverktøy.

Erfaringer fra andre land viser at slike systemer, selv når de er etablert for å beskytte barn, gradvis får utvidet bruksområde – for eksempel til alderssjekk ved netthandel, videoinnhold eller deltakelse i debattfora.

Det som begynner som et smalt tiltak, kan raskt bli et infrastrukturkrav for tilgang til hele internett.

Rettssikkerhet og etterprøvbarehet

Rettssikkerhet krever at borgere kan forstå, etterprøve og bestride statens inngrep.

Et aldersverifiseringssystem som baserer seg på proprietære løsninger, algoritmisk vurdering eller kommersielle verifiseringstjenester, vil i praksis være ugjennomsiktig og utestet rettslig.

Verken brukere eller tilsynsmyndigheter vil kunne kontrollere hvordan data behandles, hvem som har tilgang, eller hvilke algoritmer som brukes.

Dette bryter med prinsippet om forutberegnelighet i Grunnloven § 113 og EUs rettspraksis om «foreseeability of law».

Helhetsvurdering

ISOC Norge deler EFNs vurdering av at lovforslaget, slik det nå foreligger, ikke oppfyller kravene til nødvendighet og forholdsmessighet.

Teknisk sett finnes det ingen implementerbar løsning som ikke samtidig innebærer alvorlige inngrep i privatliv, ytringsfrihet og strukturell tillit.

Juridisk sett mangler det dokumentasjon på at tiltaket er nødvendig eller effektivt.

Vurdering

Forholdsmessighet er ikke et spørsmål om vilje, men om virkemidler.

Å beskytte barn er et legitimt formål, men midlene må stå i rimelig forhold til formålet og være i samsvar med rettsstaten og internettets åpne arkitektur.

ISOC Norge mener derfor at forslaget, i sin nåværende form, ikke kan gjennomføres uten å undergrave både rettssikkerhet og tillit til internettets infrastruktur.

Regulering bør i stedet rettes mot plattformenes praksis, innholdsmoderering og algoritmisk styring – ikke mot brukernes identitet.

Konklusjon

ISOC Norge støtter regjeringens mål om å beskytte barn på nett, men mener at foreslåtte virkemidler må bygge på åpne standarder, internasjonal samordning og teknisk realisme.

Et krav om aldersverifisering slik det nå foreligger, vil medføre alvorlige inngrep i internettets arkitektur, svekke interoperabilitet, skape nye sikkerhetsrisikoer og forsterke digitalt utenforskap.

Effektiv beskyttelse av barn oppnås ikke gjennom sentralisert kontroll, men gjennom tiltak som fremmer digital kompetanse, styrker personvernbydesign-prinsipper og stiller krav til plattformenes forretningsmodeller.

Teknologien for personvernvennlig aldersverifisering er foreløpig umoden, og Norge bør derfor bidra til det europeiske standardiseringsarbeidet fremfor å etablere særnorske løsninger.

ISOC Norge anbefaler at lovforslaget sendes tilbake for videre utredning med særlig vekt på:

- forholdet til EUs pågående arbeid med EUDI Wallet og aldersverifisering,

- tekniske og rettslige krav til «zero-knowledge»-baserte løsninger,
- og konsekvensene for barns rett til digital deltakelse og læring.

Bare gjennom internasjonal koordinering, åpenhet og desentralisert tillit kan vi sikre et internett som både beskytter og frigjør.