Straks weten ze niet alleen wat je zegt, maar ook wat je denkt. Waarom dit verbod voor kinderen uitmondt in censuur voor iedereen

Posted on 27 juni 2026 by John Knieriem

Er is iets eigenaardigs aan hoe democratieën reageren op nieuwe technologie. Het begint met negeren. Dan worden de gevaren zichtbaar en slaat de stemming om. Dan volgen wetten. En verder gaat het. We zitten met sociale media nu al in fase vier.

Australië ging in december 2025 als eerste over: een verbod op sociale media voor iedereen onder de 16. Het Verenigd Koninkrijk kondigde vorige week soortgelijke plannen aan.

Dichter bij huis. Het Europees Parlement nam in november 2025 met grote meerderheid een (niet-bindende) resolutie aan die pleit voor een EU-brede minimumleeftijd van 16. Tegelijkertijd werkt de Europese Commissie aan

leeftijdsverificatie via de Europese digitale *identiteitswallet*. Nederland wil een minimumleeftijd van 15, bij voorkeur Europees geregeld. Wie al deze bewegingen naast elkaar legt, ziet een patroon waarbij de ene maatregel de infrastructuur legt voor de volgende.

Onschuldig zijn Facebook en TikTok niet

Nu hebben de grote social-media platforms inderdaad ernstige schade aangericht. Ze zijn ontworpen om zoveel mogelijk verslaving te veroorzaken. Interne Facebook-documenten toonden dat het bedrijf wist dat Instagram voor een deel van de tienermeisjes schadelijk kon zijn. Zij hield deze bevindingen geheim. Onderzoek liet zien dat TikTok kwetsbare jongeren binnen minuten naar schadelijke content over zelfbeschadiging kon leiden.

Het is dus evident dat deze platforms een probleem zijn. Maar de vraag is of de maatregel die nu wordt ingevoerd dat probleem oplost, of dat ze er gebruik van maakt om iets anders te regelen.

Om te controleren of iemand geen 15-jarige is, moet je iedereen controleren. Er is geen andere manier. Anoniem een account aanmaken is daarmee structureel onmogelijk. Het is de basis van het systeem. Besproken verificatiemethoden kunnen zijn: gezichtsscans, digitale ID en bankchecks.

De Europese Commissie werkt aan *zero-knowledge proofs*, waarbij je je leeftijdsrange bewijst zonder je geboortedatum te tonen. Natuurlijk is dit eleganter maar ook daarvoor is ergens een autoriteit noodzakelijk die weet wie jij bent. De infrastructuur die nu in Europa wordt gebouwd, is die van een geïdentificeerd internet. Bij het kopen van bier eindigt de verificatie bij de kassa. Bij platformregistratie begint ze en alles wat je daarna doet is daardoor in principe permanent aan je identiteit gekoppeld. Deelname aan het publieke debat is een grondrecht, verankerd in artikel 7 van de Grondwet. Deze marktplaats van ideeën is de afgelopen decennia grotendeels naar sociale media verplaatst.

Fluisteren wordt het nieuwe spreken

Het eigenlijke gevaar zit in wat er met mensen gebeurt als ze weten dat hun naam aan hun woorden hangt. Een ambtenaar die zijn minister wil aanspreken. Een

werknemer die zijn werkgever wil bekritiseren. Ze zeggen het zachter, voorzichtiger, of helemaal niet. Dit is het zogenaamde *chilling effec*t waarin een samenleving zichzelf begint te filteren.

'Ben je dan voor *grooming*?' zo zou je kunnen tegenwerpen. Nee natuurlijk niet. De vraag is ronduit oneerlijk maar begrijpelijk, want hij werkt. De vraag is niet of kinderen beschermd moeten worden. De vraag is of dit werkt.

De kwetsbaarsten worden het minst beschermd

Technisch slimme kinderen omzeilen het verbod via de beveiligde internetverbinding VPN en blijven verder ongemoeid. De kinderen die dat niet kunnen of durven – bijvoorbeeld LGBTQ+-jongeren die online hun enige veilige gemeenschap hebben of kinderen die anoniem hulp zoeken – verliezen precies die toegang. Het verbod treft het zwaarst degenen waarvan het beleid zegt dat het hen wil beschermen.

De *grooming gangs* in Rotherham en Rochdale in het V.K. misbruikten meer dan 1.400 kinderen terwijl de overheid het wist en zweeg. Wat de beerput opende, waren niet de mainstream media maar sociale media, klokkenluiders en burgeractivisten. Begin juni 2026 zwegen de Nederlandse mainstream media dagenlang over een zware mesaanval in Belfast. Sociale media niet. NU.nl erkende achteraf: 'We waren te voorzichtig' uit vrees dat het bericht zou worden ingezet in het immigratiedebat. De politieke conclusie was niet: geef die informatiestroom meer ruimte. De conclusie was: controleer sociale media beter.

De staatsgreep op de sociale media, in vijf stadia

De stap van 'sociale media zijn schadelijk voor kinderen' naar 'de overheid bepaalt wat er op sociale media staat' wordt al gezet, *in fasen*.

Fase één: kinderbescherming. Leeftijdsverificatie, het argument dat niemand kan weerleggen.

Fase twee: desinformatiebestrijding. De EU verbood in 2022 de televisiezender RT (Russia Today) wegens staatspropaganda. Breed gesteund maar de precedentwaarde is enorm. Wie bepaalt voortaan wat propaganda is? Zouden we niet in staat zijn om dat zelf uit te kunnen maken?

Fase drie: de *Digital Services Act*, al van kracht. Waarom wordt de verantwoordelijkheid voor wat verwijderd moet worden, neergelegd bij een commercieel platform? In een rechtsstaat doet een rechter dat. De DSA verplaatst die beslissing naar platforms onder boetedreiging van zes procent van de wereldwijde omzet. De rationele keuze van *Big Tech*: ruim modereren, snel verwijderen. Het is risicomanagement, geen rechtspraak. En dan is er nog de tweede laag: platforms moeten zogenoemde 'systeemrisico's' aanpakken: content die een bedreiging vormt voor maatschappelijk debat, verkiezingen of volksgezondheid.

Dat klinkt redelijk. Maar die formulering omvat vrijwel elke boodschap die een overheid onwelgevallig vindt. Het is de logica van het ministerie van Pre-Crime uit de film *Minority Report*: je wordt niet aangepakt voor wat je deed, maar voor wat je straks misschien veroorzaakt. In de eerste helft van 2025 werden meer dan 1.800 platformbeslissingen gereviewed; in 52% van de afgesloten zaken werd de verwijdering teruggedraaid. Platforms verwijderen structureel te veel.

Fase vier: identiteitsregistratie nu voor kinderen, structureel voor iedereen.

Fase vijf: de combinatie. Als de overheid weet wie iedereen is, en platforms verplicht zijn bepaalde content te verwijderen, is het systeem compleet. Niet door een wet die zegt 'dit mag je niet zeggen' maar door een architectuur waarin elke uiting herleidbaar is en elke leeskeuze wordt geregistreerd. De overheid weet dan in potentie niet alleen wat je zegt maar ook wat je leest, welke kanalen je volgt, welke ideeën je tot je neemt.

Identificatie normaliseert herleidbaarheid. Zodra platformgebruik aan een echte identiteit is gekoppeld, kan een politiek profiel worden gebouwd van mensen die nooit iets hebben gepubliceerd: puur op basis van wat ze lezen. Dat is het wezenlijke verschil met traditionele censuur: klassieke censuur verbiedt wat je zegt. Dit systeem registreert wat je denkt.

Camera's zijn het klassieke voorbeeld van *functiecreep*: opgehangen om de verkeersstromen te optimaliseren, later ingezet voor gezichtsherkenning en demonstratiemonitoring en verkeersboetes.

Dezelfde logica geldt hier. De infrastructuur voor leeftijdsverificatie kan later worden ingezet tegen desinformatie, extremisme of maatschappelijke onrust. Elk

doel klinkt redelijk. De optelsom is een internet waarop anonimiteit een uitzondering is waarvoor je toestemming nodig hebt.

Wie nu de infrastructuur bouwt voor 'geïdentificeerd platformgebruik', bouwt die ook voor de volgende regering en de regering daarna. Welke partij er ook aan de macht is, de sleutels liggen er al. Infrastructuur is politiek neutraal. De handen die haar bedienen zijn dat nooit.

Beter zijn maatregelen die de manipulatie bij de bron aanpakken. Het Europees Parlement stelde in bovenstaande resolutie ook voor: een verbod voor minderjarigen op engagement-algoritmes, *infinite scrolling, auto-play* en *loot boxes* (betaalde digitale verrassingspakketten in games waarbij je niet weet wat je krijgt. Het gokprincipe, verpakt als speelgoed).

Dit zijn ontwerpkeuzes die uitsluitend aanwezig zijn omdat ze verslaving genereren. Een verbod hierop pakt de manipulatie aan zonder de identiteit van elke volwassene te registreren. Dat die maatregelen in de marge verdwijnen terwijl leeftijdsverificatie domineert, is niet toevallig. Verboden op verslavende ontwerpen raken de verdienmodellen van de grootste techbedrijven. Leeftijdsverificatie raakt die modellen niet maar bouwt de registratie-infrastructuur die overheden al langer willen.

Ik ben voor kinderbescherming. En precies daarom ben ik kritisch op beleid dat die doelen als schild gebruikt voor maatregelen die ze niet halen.

De infrastructuur die nu wordt gebouwd kent geen leeftijdsgrens. Die geldt voor iedereen.

Het gevaar is niet dat morgen een ambtenaar elk bericht meeleest. Het gevaar is subtieler: deelname aan het digitale publieke debat verandert van een vrij vertrekpunt in een toegangsrecht waarvoor eerst identiteit en betrouwbaarheid moeten worden bewezen en waarvoor de spelregels worden bepaald door wie op dat moment de infrastructuur beheert.

Wynia's Week *zit als een bok op de haverkist, als het gaat om inperking van rechten en vrijheden van burgers.* ***Steunt u deze onmisbare journalistiek? Hartelijk dank!***