

VEDLEGG



Stortinget - Justiskomiteen
Stortinget
0026 OSLO

Deres ref.

Vår ref.
24/1727

Dato
22.04.2024

Dokument 8:127 S (2023-2024) – Representantforslag om krav om nedslag i kinesiske TikTok

Jeg viser til oversendelse av 4. april i år til et representantforslag fra stortingsrepresentantene Kjell Ingolf Ropstad, Olaug Vervik Bollestad og Dag Inge Ulstein om nedslag i kinesiske TikTok (jfr. dok. 8:127 S (2023-2024)).

Justiskomiteen har bedt om min vurdering av forslaget: «Stortinget ber regjeringen fremme forslag som innebærer krav til at sosiale medier som TikTok kun kan eies av ikke-kinesiske selskaper som tilfredsstillers nasjonale sikkerhetshensyn, for å kunne operere i Norge.»

Generelt om bruken av sosiale medier

Sosiale medier brukes mer og mer av trusselaktører som ønsker å påvirke gjennom desinformasjon og falske nyheter. Dette er urovekkende og gjelder de fleste plattformer, inkludert TikTok.

Det er viktig at vi er bevisst disse utfordringene, og følger gode sikkerhetsråd. Nasjonal sikkerhetsmyndighets (NSM) sine råd om hvordan vi bør forholde oss for å beskytte skjermingsverdige verdier er sentrale. Eksempelvis er en vanlig mobiltelefon ikke godkjent for gradert tale. Vi bør også være svært varsomme med å snakke eller lagre sensitiv informasjon på en slik telefon. NSM har uttalt at TikTok ikke bør installeres på offentlig ansattes tjenesteenheter som er tilknyttet virksomhetens interne digitale infrastrukturer eller tjenester. Dersom det er tjenstlige behov for TikTok, anbefaler NSM at applikasjonen installeres og benyttes på en separat enhet forbeholdt denne typen formål og som ikke er tilknyttet virksomhetens interne systemer.

Regjeringen oppfordrer til å vise aktsomhet ved bruk av sosiale medieapper. Vårt mål er likevel ikke å forby tjenester som mange finner glede i, men i stedet oppfordre til bevissthet om bruk, og sørge for at tjenesten er så trygg som mulig og følger norske lover og regler.

Jeg forventer at TikTok, som alle andre, følger de lover og regler vi har i samfunnet. Både her i Norge og i EU. Et viktig tiltak for å trygge brukerne er å føre tilsyn med at tjenester som tilbys i Norge tilfredsstiller vårt regelverk, slik Datatilsynet har ført tilsyn med tjenestene fra Meta. Vi jobber nå med regler som vil innføre forbud mot systemer som har til hensikt å manipulere brukerne. Nettopp for å hindre at apper skal kunne brukes til å lure folk til å ta beslutninger de egentlig ikke ønsker, kjøpe ting de ikke trenger eller gi fra seg personopplysninger de ikke ønsker. Plattformene skal særlig beskytte mindreåriges personopplysninger, mental og fysisk helse – bl.a. ved å ikke målrette reklame særskilt mot barn og unge.

I tillegg er vi i ferd med å innføre regler som skal bidra til å redusere og forebygge ulovlig og skadelig aktivitet på nett. Dette regelverket stiller særlige krav til at de aller største plattformene må sikre at tjenestene ikke kan misbrukes til spredning av innhold som kan skade et stort antall personer og samfunnet som sådan. Dette skjer gjennom arbeidet med AI-forordningen og DSA. Digitaliserings- og forvaltningsministeren har vært tydelig på at dette regelverket skal innføres raskt.

Kultur- og likestillingsdepartementet har igangsatt et arbeid med en strategi for å styrke motstandskraften mot desinformasjon. I Norge er vi i utgangspunktet godt rustet til å stå imot påvirkningsforsøk. Vi har et bredt mediemangfold, høy tillit til mediene og en høyt utdannet befolkning. Spredning av misledende og feilaktig informasjon kan imidlertid bidra til å svekke tilliten. Utbredelsen av sosiale medier, endrede medievaner, økt uro i verden og utviklingen innenfor generativ kunstig intelligens gjør det nødvendig å vurdere hvorvidt dagens virkemiddelapparat er tilpasset den nye virkeligheten.

NSM har råd på hvordan vi bør forholde oss for å beskytte skjermingsverdige verdier. Retningslinjene peker ikke på spesielle apper eller sosiale media som ikke bør brukes, men er anbefalinger som hver enkelt må vurdere ut i fra egen situasjon.

Forhold knyttet eierskap av sosiale medier

På generelt grunnlag vil det alltid være en risiko for at informasjon fra apper, sosiale medier og andre digitale tjenester kan samles inn og brukes til formål som ikke er ønskelige. NSM pekte i sin åpne risikovurdering «Risiko 2023» på at fremmede etterretningstjenester kan benytte det store volumet av kommersielt tilgjengelige brukerdata for å manipulere og utpresse personer som sitter på verdifull informasjon. Brukerdata kan bl.a. understøtte cyberoperasjoner, innsidevirksomhet og påvirkningsoperasjoner.

Applikasjoner som kan lastes ned til norske mobiltelefoner, kan ha opprinnelse eller eierskap knyttet til land vi ikke har sikkerhetssamarbeid med. En fellesnevner for flere

utbredte applikasjoner er at de samler inn til dels omfattende data om brukeren. Det bør derfor utøves varsomhet ved bruk av slike applikasjoner og at nødvendige vurderinger gjøres i tråd med anbefalinger fra myndighetene.

Det vil alltid være viktig å vurdere nasjonale sikkerhetshensyn på ulike områder hvor det er relevant, blant annet knyttet til påvirkning, desinformasjon og annen sammensatt virkemiddelbruk. Det er imidlertid ikke ønskelig med et generelt forbud for selskaper med eierinteresser fra ett land å tilby tjenester i Norge, ei heller land vi ikke har et sikkerhetsmessig samarbeid med.

Med hilsen

Emilie Mehl

Dokumentet er elektronisk godkjent og sendes uten signatur.