

Kommunal- og moderniseringsdepartementet
v/Nils Ø. Gulbrandsen

Kongens gate 14
0153 Oslo, Norway
T: +47 23 31 83 00
www.teknologiradet.no

Vår ref.: 2020/37
Dato: 09.09.2020

Innspill til EUs høring om Digital Services Act

Teknologirådet ønsker med dette å fremme to konkrete innspill som Norge kan fremme for EU i høringen om Digital Services Act.

- 1) EU bør utvikle et system for algoritmerevisjon
- 2) EU bør begrense målretting av politiske annonser i sosiale medier

Algoritmerevisjon

I dag er det slik at bedrifter over en viss størrelse må levere regnskapet sitt til revisjon. I dataøkonomien mener vi det bør være like naturlig med *algoritme*-revisjon.

Så å si alle tjenester er i ferd med å bli digitale. Om du skal ha vaskehjelp hjemme, kontormøbler til jobben eller globale advokattjenester vil dette i stadig større grad formidles via digitale plattformer.

Plattformer er igjen basert på algoritmer og maskinlæring, eller det vi enkelt sagt kaller kunstig intelligens. Det er nettopp fordi denne teknologien har kommet så langt at plattformene lykkes så godt.

Algoritmene skaper imidlertid nye utfordringer:

- Det kan være vanskelig eller umulig for brukerne eller kundene å forstå hvordan et system kom frem til et svar, en anbefaling eller en rangering.
- Algoritmer kan være kan være diskriminerende, for eksempel fordi de er trent opp på datasett med historiske beslutninger som igjen har vært diskriminerende.
- Algoritmene kan i en del tilfeller ta beslutninger som er meningsløse eller til og med farlige, fordi de støter på en situasjon de ikke er trent for.

Jo større og mer dominerende plattformene er, jo viktigere er det at algoritmene er ansvarlige, trygge og rettferdige. I Teknologirådets rapport [Kunstig intelligens – muligheter, utfordringer og en plan for Norge](#) fra 2018 anbefalte vi at maskinlæringsalgoritmer som brukes av det offentlige skal være åpne for innsyn og kontroll.

Men dette er ikke alltid mulig, blant annet av hensyn til forretningshemmeligheter, personvern eller sikkerhet. Algoritmene bør likevel bli gjenstand for en vurdering dersom de skal anvendes i større skala i samfunnet.

Hva kan algoritmerevisjon innebære?

Vår anbefaling er at EU setter opp et rammeverk for algoritmerevisjon. Det viktigste prinsippet er at ansvarlige tredjeparter får ansvar for å gjennomgå algoritmene som er sentrale for de digitale tjenestene, for å sikre at både kunder, brukere og samfunnet ellers kan ha tillit til tjenestene.

I Teknologirådets rapport om kunstig intelligens peker vi på at det blant annet bør vurderes om algoritmene er rettferdige, korrekte, forklarbare og etterprøvbare, og at det er synliggjort hvordan man kan klage på uønskede effekter. Andre kriterier kan være at algoritmene ikke innebærer misbruk av markedsmakt, og at de er trygge for brukere av plattformen.

En revisjon gir plattformeieren mulighet til å bevise for omverdenen at deres plattform oppfyller disse kriteriene, uten at de behøver å avsløre sine forretningshemmeligheter. Dette kan gi både kundevekst og tilgang på finansiering. Derfor ser vi også eksempler på [frivillig algoritmerevisjon](#). Vi foreslår *ikke* at vi skal ha et system hvor all bruk av algoritmer i digitale plattformer krever forhåndsgodkjenning. Dette vil strupe utvikling og nødvendig effektivisering som de bidrar til.

I stedet kan EU se til sitt eget [White Paper om kunstig intelligens](#), der de anbefaler en *risikobasert* tilnærming, hvor høyere risiko bør medføre krav til grundigere revisjon:

- Risiko i sektoren (høyere i helse eller justis enn i kreative næringer)
- Risiko ved bruksområdet (høyere ved robotkirurgi enn timeplanlegging i helse)
- Risiko ut fra markedssituasjonen: Jo mer dominerende en plattform er i sitt marked, jo høyere risiko utgjør dette for enkeltindividene og de små aktørene som er prisgitt denne plattformen.

Det er mange muligheter for hva en slik revisjon kan omfatte, og dette bør altså igjen variere ut fra risiko. Noen eksempler til hva revisjonen kan innebære, er:

- Inspeksjon av hvordan systemet er bygget opp i detalj, inkludert innsyn i koden. Et eksempel er hvordan kildekoden i den norske Smittestopp-appen ble undersøkt av en gruppe eksperter.
- Inspeksjon av dataene systemet trenes opp på, for å avklare om de inneholder historisk slagside eller andre skjevheter, og hvilke situasjoner systemet kan forventes å virke godt eller mindre godt i.
- Test av robusthet mot feil, eller mot angrep der noen [bevisst prøver å manipulere algoritmen](#). Et eksempel fra kunstig intelligens i medisin er å [utsette systemet for et bilde med forstyrrelser](#), for å se hvordan resultatet blir påvirket.

Finansiell revisjon bidrar til at aktørene i et marked kan ha tillit til hverandre, også der det er informasjonsasymmetri mellom partene. På samme måte kan algoritmerevisjon bidra til at denne tilliten består i den digitale plattformøkonomien, og dermed bidra til et bedre fungerende marked.

Målretting av politiske annonser

Sosiale medier kan bli så kraftfulle verktøy for politisk kommunikasjon at de kan skade demokratiet. EU bør derfor begrense hvor individuelt målrettet politisk reklame kan

være. Dette er en av anbefalingene i Teknologirådets rapport «[Valg, teknologi og politisk påvirkning](#)».

Sosiale medieplattformer har snudd opp ned på politisk valgkamp. Budskap kan spisses og tilpasses mot individer langt mer effektivt enn tidligere, samtidig som potensialet for å nå store velgergrupper er enormt. Annonseverktøyene gjør det mulig å følge responsen i sanntid. Dette gjør det mulig å teste ulike budskap på ulike grupper, og deretter spre videre de annonsene som treffer best.

I den forrige amerikanske presidentvalgkampen publiserte Trump-kampanjen [5,9 millioner ulike annonser på Facebook](#), og det finnes [over 250 selskaper](#) som spesialiserer seg på persontilpasset politisk markedsføring. Målrettet markedsføring gjør det mulig å publisere såkalte «[Dark ads](#)» — annonser som kun vises til målgruppen. Det vil si at partier og politikere kan velge hvilke budskap de vil fremme til hvilke personer, uten at andre har innsyn i hva som skjer. Ulike personer og grupper kan dermed få ulike inntrykk av et partis budskap.

I tillegg til at politiske aktører bruker disse verktøyene, kan de også [brukes av utenforstående](#) for å manipulere velgere i det skjulte, og spre falske nyheter og villedende informasjon.

De aller fleste politiske aktører bruker nå sosiale medieplattformer og deres annonseverktøy for å spre og markedsføre sitt budskap. Kraften i disse verktøyene tilsier at vi bør regulere hvordan de skal kunne brukes. [Teknologirådet](#) har ved flere anledninger pekt på paradokset at politisk reklame er forbudt på TV, mens vi fullstendig mangler felles spilleregler for den digitale valgkampen.

Hva innebærer forslaget om begrenset målretting?

Det har vist seg svært vanskelig å fjerne eller merke innhold som sprer villedende informasjon hurtig nok. Et eksempel er hvordan [manipulerte eller bevisst villedende videoer spres i den amerikanske valgkampen](#).

Vårt forslag er i stedet å legge begrensninger på hvor målrettede politiske annonser kan være. Det vil gjøre verktøyene mindre effektive for politiske aktører, men også mindre attraktive for de som ønsker å spre desinformasjon.

I dag er det slik at [Twitter](#) har valgt å forby politisk reklame, mens [Google](#) har gått inn for å begrense målrettingen til noen få kriterier som kjønn og bosted. **Facebook** tillater derimot fortsatt at annonsene målrettes etter demografisk informasjon, interesser, politisk tilhørighet med mer.

Dette er et område hvor EU kan gå foran og lage tydelige, felles regler, slik at ingen tjener på å være den mest skruppelløse aktøren i markedet.

Med vennlig hilsen

Tore Tennø
Direktør

Anne Siri Koksrud Bekkelund
Senior prosjektleder