Teknologirådet

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

Justiskomiteen
Stortinget
Postboks 1700 Sentrum
0026 Oslo

Vår ref.: 2022/35
Dato: 01.11.2022

Innspill fra Teknologirådet til Dokument 8:167 S (2021-2022) – Bedre personvern på sosiale medier.

Dagens digitale økonomi er dominert av store, internasjonale teknologiselskaper. Vi kan si med sikkerhet at disse selskapene samler inn store mengder personopplysninger om norske innbyggere, men det er vanskelig å gi et fullstendig bilde av hva slags informasjon som samles inn om oss, hvem den deles med og hvordan den brukes.

Sosiale medier er spesielt viktige i denne sammenhengen, siden data herfra gjerne er knyttet til identifiserbare enkeltpersoner, og forretningsmodellen baserer seg på å bygge omfattende profiler som kan brukes til å påvirke eller manipulere brukerne ved hjelp av avansert algoritmer.

EU har innført strengere krav til sosiale medieplattformer, gjennom to nye lover. Digital Services Act (DSA) skal ansvarliggjøre nettselskaper for ulovlig og skadelig innhold, og Digital Markets Act (DMA) skal bidra til mer rettferdig digital konkurranse, og gi brukerne mer valgfrihet. Begge disse vil bli norsk lov. Flere av punktene i representantforslaget vil trolig dekkes av DSA og DMA. Det er likevel noe handlingsrom for nasjonale tilpasninger, og en viktig jobb fremover vil være å definere hva dette kan og bør være.

Forslag 1: Utrede forbud mot overvåkingsbasert reklame

Et av de mest omstridte spørsmålene i forhandlingene om DSA var reglene knyttet til atferdsbasert markedsføring. Det ble ikke enighet om å forby denne type reklamepraksis generelt. Kompromisset ble å forby atferdsbasert reklame mot barn, og reklame basert på sensitive personopplysninger som for eksempel opplysninger om seksualitet, etnisitet og religiøs tilhørighet. Teknologirådet er blant flere aktører som har tatt til orde for at norske myndigheter bør vurdere et forbud. En utredning av et forbud er også en av anbefalingene fra Personvernkommisjonens flertall.

Det finnes allerede alternative metoder for digital annonsering som kan erstatte bruken av persondata til markedsføring. Såkalt kontekstuell annonsering innebærer at annonser plasseres basert på innholdet på en nettside, ikke hvem brukeren er. Et forbud mot å bruke persondata i annonser kan også bidra til å bedre konkurransesituasjonen i annonseindustrien. Ved å frata selskaper som Google og Facebook deres største fordel (persondata), kan andre selskaper konkurrere på likere vilkår. Det kan også gi selskapene insentiv til å innovere.

Forslag 3: Etablere et algoritmetilsyn under Datatilsynet

Den kraftige utviklingen innen kunstig intelligens og algoritmer er en av grunnene til at de digitale 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 diskriminerende, for eksempel fordi de er trent opp på datasett med historiske beslutninger som igjen har vært diskriminerende.
- Algoritmene kan i den del tilfeller ta beslutninger dom er meningsløse eller til og med farlige, fordi de støter på en situasjon de ikke er trent for.

I Teknologirådets rapport om kunstig intelligens peker vi på at en revisjon blant annet bør vurdere 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 tjenesten.

Vi tror derimot ikke det er en god ide med et system hvor all bruk av algoritmer i digitale plattformer krever forhåndsgodkjennelse. Dette vil strupe utvikling og nødvendig effektivisering som de bidrar til.

DSA innebærer at forskere og tilsynsmyndigheter skal få innsyn i designet, logikken og funksjonen til algoritmene til de største nettplattformene og søkemotorene. Mer tilgang på data om plattformenes virksomhet og algoritmer skal bidra til å bygge kunnskap om hvordan plattformene operer og hvordan tjenestene påvirker mennesker og samfunn. Det er foreløpig uavklart hvem som skal føre tilsyn av loven i Norge, men det vil være nødvendig med tilstrekkelige ressurser og kompetanse for å sikre en effektiv håndheving.

For bruk av algoritmer i offentlig sektor har Teknologirådet tidligere anbefalt at disse bør være åpne for innsyn og kontroll. I Norge er det Riksrevisjonen som kontrollerer at statsforvaltningen anvender fellesskapets midler og verdier slik Stortinget har bestemt. Forvaltningsrevisjonen vurderer om grunnleggende verdier som likebehandling og offentlighet i tjenestene er oppfylt, og i fremtiden kan dette også inkludere tilsyn med algoritmene i offentlig forvaltning.

EU forhandler nå om en ny lov for å regulere kunstig intelligens. Artificial Intelligence Act (AI Act) skal sikre en ansvarlig bruk av teknologien, også i offentlig sektor. Loven vil trolig ferdigforhandles i 2023, og deretter bli norsk lov. Et eventuelt nasjonalt algoritmetilsyn og revisjon av algoritmer bør vurderes i lys av dette.

Forslag 5: Innføre rett til å kunne bruke digitale tjenester uten at innsamlet data deles på tvers av plattformer eid av ett og samme selskap.

Gjennom å dele innsamlet data om brukere på tvers av tjenester eid av ett og samme selskap, kan selskapene sammenstille data til detaljerte profiler på brukerne. Profilene brukes til å selge og vise brukerne atferdsbasert reklame på nett. Muligheten til å koble sammen data på denne måten gir de store selskapene et stort konkurransefortrinn, sammenliknet med selskaper som tilbyr færre tjenester.

DMA går stykke på vei i å forby denne praksisen. DMA forbyr portvokterne fra å koble personopplysninger om brukerne på tvers av tjenestene uten samtykke fra brukerne selv. Det innføres derimot ikke noe generelt forbud mot å koble på tvers av plattformer, så lenge dette ikke er personopplysninger. Det blir heller ikke forbudt å koble personopplysninger sammen, dersom brukeren samtykker til det.

Det er verdt å merke seg at DMA bare gjelder for såkalte «portvoktere» i den digitale økonomien. Portvoktere er selskaper som har € 7,5 milliarder i omsetning, 45 millioner brukere og 10 000 forretningskunder i Europa av minst én sentral plattformtjeneste man tilbyr. Både Meta, Google, Apple, Microsoft og Amazon møter kriteriene i dag.

Det er i tillegg kun kobling av data mellom såkalte «sentrale plattformtjenester» som blir forbudt. Dette er definert i DMA som søkemotorer, sosiale medie-plattformer, plattformer for videodeling, meldingstjenester, operativsystemer, skylagringstjenester, reklametjenester, nettlesere, digitale assistenter og digitale formidlingstjenester. Det er uklart hvor langt forbudet vil gå. For eksempel er det usikkert om det blir forbudt for Google å koble sammen personopplysninger mellom e-post-tjenesten Gmail og Google Analytics, et verktøy for nettanalyse.

For å styrke brukernes personvern og bedre konkurransesituasjonen, kan det vurderes om kobling av persondata mellom tjenester skal forbys, uavhengig om brukeren samtykker eller ikke. Det kan også vurderes om et slikt forbud bør gjelde for flere tjenester enn det DMA regulerer.

Forslag 6: Utrede omfanget av og utfordringene rundt lagring av biometriske data på sosiale medieplattformer.

Sosiale medier og digitale tjenester samler stadig inn mer biometrisk data. Alt fra fingeravtrykk til stemmeidentifikasjon og ansiktsgjenkjenningsverktøy regnes som biometrisk data. Gjennom DSA blir det forbudt å målrette reklame basert på sensitive opplysninger, slik som biometrisk data. Dette er et steg i riktig retning, men det er fremdeles store personvernutfordringer knyttet til denne type innsamling og bruk, som også Personvernkommisjonen fremhever i sin NOU.

Selskapet Clearview har for eksempel brukt alle åpne kilder på internett som grunnlag for å bygge sin bildebase. Dette vil si at potensielt alle som er avbildet på internett, vil kunne gjenkjennes ved bruk av Clearviews teknologi. Selskapet selger tilgang til databasen til private selskaper og politimyndigheter. Flere datatilsyn i Europa, inkludert det italienske og britiske, har gitt rekordstore bøter til selskapet for brudd på GDPR.

Biometrisk fjernidentifikasjon, som for eksempel bruk av ansiktsgjenkjenning på offentlige steder, kan også være svært inngripende. Det åpner opp for masseovervåkning uten at innbyggerne er klar over det, og vil kunne være en trussel mot retten til forsamlingsfrihet. I de pågående forhandlingene om AI Act i EU diskuteres det om bruken av ansiktsgjenkjenning på offentlige steder i sanntid skal forbys. Teknologirådet har også tatt til orde for at et forbud mot bruk av ansiktsgjenkjenning bør vurderes.

Ser vi fremover, er det klart at bruk av biometri vil øke kraftig, og bør utredes. Vi vil peke på to eksempler – taleteknologi og metaverset.

Økt tilgang på taleopptak, regnekraft og maskinlæring, har ført til hurtig utvikling innen språkteknologi. Taleteknologi kan gi et enormt løft for universell utfordring, frigjøre ressurser brukt på transkribering og være en livline for utsatte språk. Samtidig øker risikoen for diskriminering og misbruk. På grunn av skjevheter i treningsgrunnlaget, forstår teknologien noen dialekter, aldersgrupper og kjønn bedre enn andre. Samtidig brukes stemmeanalyse til å persontilpasse kundebehandling og reklame. Et patent fra Amazon viser hvordan Alexa kan høre om noen er forkjølet, for så å kjøpe hostemedisin. Et Google-patent viser at Assistent kan gjette kjønn og alder på alle i en familie, høre hva de bruker tid på, og lage statistikk for å gjøre den effektiv.

«Deepfakes» er bilder, videoer og lydklipp manipulert ved hjelp av kunstig intelligens, og de blir stadig bedre. I mars 2022 sirkulerte en falsk video av Ukrainas president Volodymyr Zelenskyj der han ber ukrainske styrker overgi seg. Zelenskyj måtte selv gå ut og avkrefte videoen som falsk. I Norge har svindlere lurt folk til å tro at de snakker med familien ved hjelp av stemmekloning, og i Hong Kong overførte en bankansatt 35 millioner dollar til svindlere, etter at en stemmeklonet versjon av sjefen ringte og ba om transaksjonen.

Hvis vi i framtiden ikke bare skal logge oss på nettet, men leve interaktive liv i et slags altomsluttende internett av verdener og tjenester – ofte referert til som metaverset – så vil datainnsamlingen og personvernutfordringene bli langt mer omfattende enn i dag. Utstyret du har på deg vil kunne samle inn blodtrykk, pusterytme og ansiktsuttrykk, og registrere hva du gjør, hvor du går, hva du ser på, og hvordan du reagerer på det du ser. Forskning viser at kun 5-minutters bruk av VR-briller gir et godt nok datagrunnlag til å kunne identifisere et menneske med 95 % sikkerhet. I virtuelle verdener kan det også bli vanskeligere å beskytte seg mot manipulasjon, trakassering og hets.

Det er dermed behov for å utrede både omfanget og utfordringer knyttet til innsamling og bruk av biometrisk data.

Forslag 7: Strengere krav til personvern i forbindelse med offentlige anskaffelser som involverer sosiale medier

I Digital agenda for Norge, slås det fast at offentlig sektor har et særlig ansvar for å gå foran som gode bestillere av personvernvennlig teknologi og innebygd personvern.

Likevel spores innbyggerne av kommersielle aktører som Alphabet og Facebook på de fleste offentlige nettsteder. I rapporten «Kommersiell sporing i offentlig sektor» har Teknologirådet kartlagt den utstrakte bruken av sporingsverktøy på offentlige nettsider. Bruken av gratistjenester som Google Analytics og Facebook Pixel brukes på over 80% av de offentlige nettstedene som er undersøkt, og innebærer at data om innbyggernes kontakt med det offentlige deles med Google og andre aktører i den digitale annonseindustrien.

Slike verktøy bør erstattes av personvernvennlige løsninger som samler inn langt mindre informasjon om norske innbyggere. I andre land, som for eksempel Danmark, er bruken av slike verktøy langt lavere. Det tyske datatilsynet har anbefalt at bruken av Google Analytics fases ut. I Norge kan for eksempel digitaliseringsrundskrivet brukes til å styre bruken av verktøy som ikke tar hensyn til innbyggernes personvern.

Det bør være et prinsipp at det offentlige skal betale for tjenestene de bruker med penger, ikke innbyggernes data. Dette kan også føre til stimulering av markedet, ved at personvernvennlige løsninger etterspørres i større grad.

Med hilsen

Tore Tennøe
Direktør