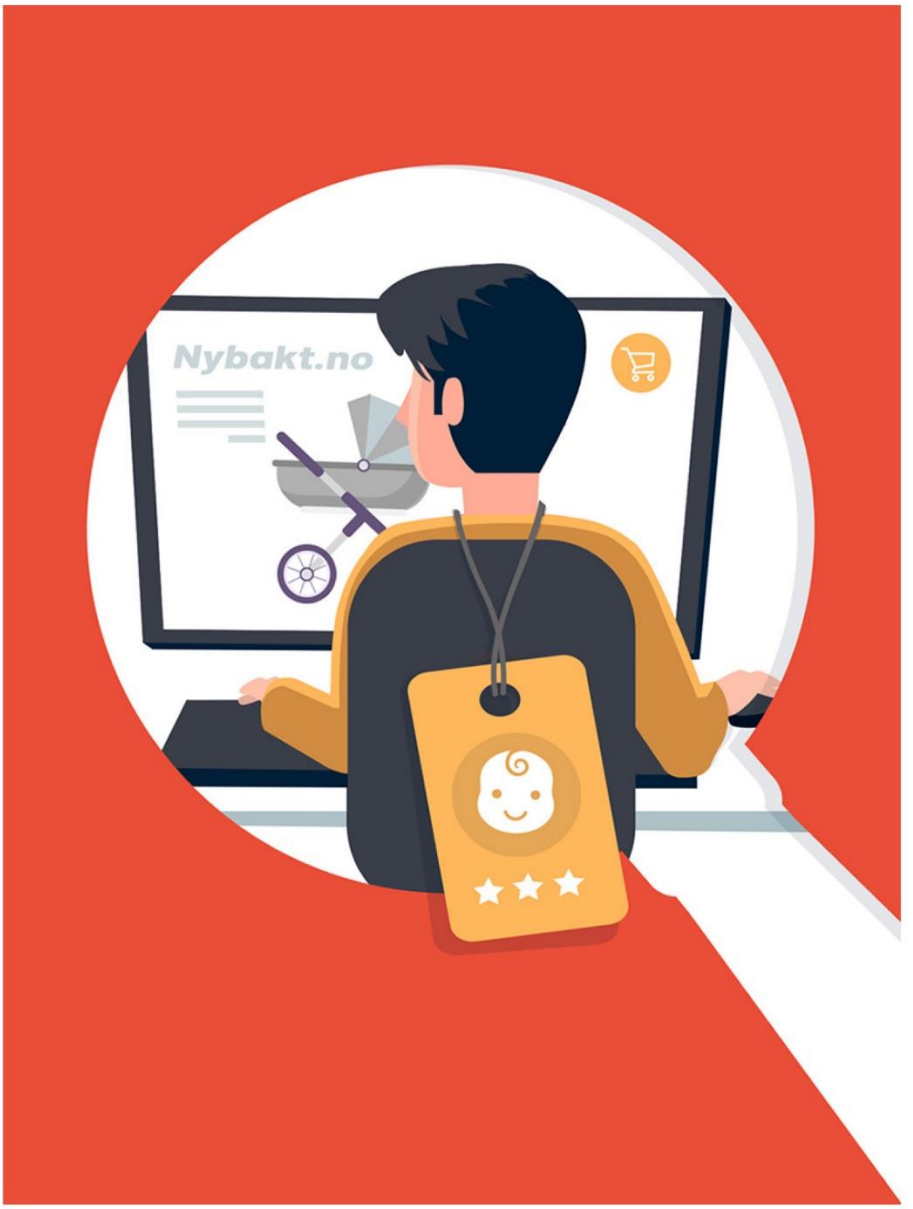


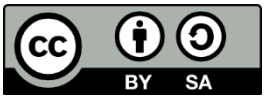
KOMMERSIELL SPORING I OFFENTLIG SEKTOR

Teknologirådet

KOMMERSIELL SPORING I OFFENTLIG SEKTOR

ISBN 978-82-8400-011-4

Utgitt: Oslo, mars 2021
Forsideillustrasjon: Birgitte Blandhoel
Elektronisk publisert på: www.teknologiradet.no



FORORD

«If something is free, you're not the customer, you are the product»

Dette sitatet fra Bruce Schneier beskriver det som kalles overvåkingsøkonomien – hvordan digitale tjenester tilbys gratis, mot at det samles inn enorme mengder data om brukerne. Disse dataene brukes deretter videre i annonseindustrien, for å påvirke din og min adferd gjennom persontilpasset reklame.

Med denne rapporten ønsker vi å sette søkelys på hvordan overvåkingsøkonomien og sporing på internett har inntatt offentlig sektor. Gjennom å bruke gratis tilgjengelige verktøy fra de store internettselskapene, inviterer offentlige nettsteder kommersielle aktører inn i de innerste sfærene av våre liv.

Denne utviklingen er problematisk fordi offentlige tjenester kommer tett på oss og våre privatliv, og det ikke finnes noen alternative tjenestetilbydere. Offentlig sektor bør derfor ta et særlig ansvar for å ikke dele data om oss med kommersielle aktører.

Teknologirådet skal gi uavhengige råd til Stortinget og regjeringen om ny teknologi og bidra til en åpen, offentlig debatt. Vi håper rapporten kan bidra til en opplysende diskusjon om hvordan offentlig sektor kan ta innbyggernes personvern på alvor – også når tjenestene digitaliseres.

Tore Tennøe

Direktør, Teknologirådet

INNHOLD

SAMMENDRAG

Offentlig sektor bidrar i dag til at informasjon om innbyggerne samles inn og deles med de største aktørene i overvåkingsøkonomien. Dette er et demokratisk problem fordi man ikke kan velge bort overvåkningen, og et konkurransepolitisk problem fordi det styrker de digitale monopolene.

DEN DIGITALE ØKONOMIEN ER BASERT PÅ OVERVÅKING

Når man bruker internett er det en rekke aktører som følger med på hva man gjør. Informasjon om hvilke nettsider som besøkes, hvem man følger på sosiale medier eller hvilke filmer man ser, er verdifull informasjon for annonseindustrien. Dette har ført til en utvikling hvor mange digitale tjenester tilbys gratis, mot at det samles inn store mengder data om brukerne. Dette er for eksempel grunnlaget for tjenester fra Google og Facebook, samt en lang rekker apper og spill.

Fordi man kan spores på tvers av ulike nettsteder og enheter, får selskapene i annonseindustrien mulighet til å lage digitale profiler. Ved å analysere adferd på nett, bevegelsesmønstre og vaner, kan disse digitale profilene bli svært detaljerte, og danne et komplekst og nærgående bilde av brukerne. Profilene kan blant annet inneholde informasjon om personlighetstype, nære relasjoner og seksuelle preferanser, i tillegg til kjønn og alder, bosted, arbeidssted, språk og interesser.

DE STORE DOMINERER MARKEDET

Det digitale annonsemarkedet er stort og komplekst, med mange ulike aktører. De store internettselskapene som Google og Facebook dominerer markedet, og man antar at disse to mottar over halvparten av pengene som brukes på digital markedsføring i verden.

Det at disse selskapene allerede sitter på store mengder data gjør det vanskelig for konkurrenter å etablere seg eller utfordre deres posisjoner. I tillegg sitter Google og Facebook på flere sider av bordet samtidig – de kjøper og selger både annonser og annonseplass.

ULIKE VERKTØY SPORER NESTEN ALL NETT-AKTIVITET

Det finnes mange ulike metoder og teknikker for sporing på nettsider.

Informasjonskapsler, sporingsbilder og **digitale fingeravtrykk** er alle teknikker som gjør at nettleseren samler inn og deler informasjon om nettaktivitet. Dersom en aktør sporer mange forskjellige nettsteder, blir det også mulig å følge brukeren på tvers av disse. Fordi disse teknikkene er så utbredt, fører det til at noen selskaper etter hvert sitter på enorme mengder informasjon om hver enkelt sin aktivitet på nett.

Mange nettlesere gjør det mulig å blokkere bruk av informasjonskapsler, mens bruken av sporingsbilder er vanskeligere både å oppdage og blokkere.

Opptak av nettsidebesøk og **tastelogging** er to andre typer teknikker for sporing av aktivitet. Opptak av nettsidebesøk kan sammenliknes med at noen står bak ryggen din og følger med på hvert minste klikk, musebevegelse eller scrolling. Dette kan deretter spilles av i etterkant av besøket på nettsiden. Tastelogging innebærer at all tekst som skrives inn i skjemaer, chat eller annet registreres – også før man har trykket på send eller lagre.

Begge disse teknikken har stor risiko for at sensitiv informasjon blir samlet inn og delt med uvedkommende, for eksempel hvis man sender inn kredittkortinformasjon, helseopplysninger eller kontaktinformasjon i et skjema.

Google og **Facebook** har egne sporingsverktøy som er svært utbredt. Google Analytics er et gratis verktøy for analyse av nettsidebesøk, og antas å være i bruk

på over halvparten av alle nettsider i verden. Detaljert informasjon om bruk av nettsiden deles som regel med Google.

Facebook Pixel brukes for å få innsikt i hvordan brukere reagerer på annonser publisert gjennom Facebook. Dette betyr at man kan følge en brukers aktivitet når en klikker på en Facebook-annonse, eller mer generelt på nettsteder som har Pixel installert. Her kan aktivitet kobles til navngitte brukere hvis de er logget inn på Facebook.

Samlet sett gjør disse verktøyene at tilnærmet all aktivitet på nett blir sporet, lagret og delt med aktører i annonseindustrien. Fordi Google og Facebook allerede sitter på store datamengder og eier noen av de mest utbredte verktøyene, bidrar dette til at deres markedsposisjon styrkes ytterligere.

KOMMERSIELL SPORING I OFFENTLIG SEKTOR

Digitaliseringen av offentlig sektor er i full gang. Prinsippet om digitalt førstevalg innebærer at kommunikasjon mellom innbygger og forvaltning i hovedsak skal foregå på nett.

I denne rapporten har Teknologirådet undersøkt 41 offentlig nettsteder ved å bruke verktøyet Blacklight. Blacklight undersøker hvilke sporingsteknologier som er aktive på nettstedene og hvilke aktører som mottar informasjon om brukernes aktivitet. I tillegg har vi lest sidenes personvernerklæringer for å se hvordan de selv beskriver sporingen som skjer på nettstedet.

Hele 36 av nettstedene bruker Google Analytics, og mange bruker i tillegg flere andre verktøy fra Google. Hotjar, et verktøy for opptak av nettsidebesøk, er også utbredt. Facebook Pixel er mindre vanlig, og er bare tatt i bruk på fire av nettstedene.

Demokratisk problem

38 av nettstedene deler data med kommersielle aktører. Offentlige tjenester kan ikke velges bort av innbyggerne, og kan innebære deling av informasjon knyttet til helse, familieliv eller privatøkonomi.

Informasjon om at en innbygger søker om foreldrepermisjon eller barnehageplass, er for eksempel attraktiv informasjon på de digitale annonsebørsene, og kan bli brukt for å selge annonser for barnevogn eller nye vintersko. Da er det betenkelig at NAV bruker tre ulike analyseverktøy fra Google, og opplyser om at hvis man stopper informasjonskapsler, vil sidene ikke lenger fungere som de skal.

Et annet eksempel er Bufdir, som er åpne om at de sporer personer som har vært inne på deres nettsider om fosterhjem for senere å kunne vise dem reklame på Facebook om det å være fosterforeldre.

Ofte finnes det ingen alternative tjenestetilbydere. Derfor bør offentlig sektor ta et særskilt stort ansvar når det kommer til sikkerhet og beskyttelse av persondata.

Vanskelig å forstå

Mange selskaper gir inntrykk av at brukerne har kontroll over hvordan data samles inn og brukes. I mange tilfeller er dette kun en overfladisk prosess, da alternativet til å ikke godkjenne sporing er å ikke bruke nettsiden i det hele tatt.

I tillegg er personvernerklæringer vanskelige å lese. Med mindre man har kjennskap til og forståelse for sporingsteknologien som brukes, er det så å si umulig å forstå hva som egentlig skjer. Mange av personvernerklæringene er i tillegg mangelfulle eller uforståelige.

Styrker allerede dominerende aktører

I tillegg til å bruke informasjonen til å påvirke brukernes adferd med reklame, fører den utstrakte sporingen til å bygge opp særlig Google og Facebooks markedsdominans. Den store tilgangen disse selskapene har på data er en vesentlig årsak til denne dominansen.

Både globalt og i Norge jobbes det nå aktivt politisk for å unngå slik markedsdominans, særlig i den digitale økonomien. At offentlig sektor, deriblant Forbrukertilsynet, Forskningsrådet og Innovasjon Norge, bidrar til dette gjennom å bruke gratisverktøy fra de store internettselskapene, er derfor problematisk.

HVA KAN GJØRES?

Offentlig sektor bør gå foran og ta et særskilt ansvar for å gi innbyggerne gode digitale tjenester – uten at kommersielle aktører får være med på lasset. Det er særlig tre grep som kan bidra til å gjøre overvåkingsøkonomien en mindre attraktiv forretningsmodell.

Minimer datainnsamling og gi bedre informasjon

Flere av nettstedene begrunner sporingen med viktigheten av brukervennlighet, og veier dermed dette tyngre enn brukernes personvern. Vi mener dette kan oppnås på andre måter, uten at kommersielle aktører involveres. Offentlig sektor bør velge løsninger og verktøy som følger personvernprinsippene, og dermed samler inn minimalt med data til helt spesifikke formål.

Hvis en først skal samle inn data, må man kunne forklare formålet med sporingen på en enkel og tydelig måte.

Betal med penger, ikke data

Når Google tilbyr sine analysetjenester gratis, er det ikke fordi de ønsker å være snille, men fordi de ser en verdi i dataene som samles inn gjennom verktøyet. Offentlig sektor bør ta et aktivt valg om å ikke delta i overvåkingsøkonomien, og betale for verktøyene de bruker med penger – ikke med innbyggernes data.

Vurder et forbud mot mikromålretting

En av grunnene til at det samles inn data, er fordi det brukes til mikromålretting av annonser. Det finnes allerede mange eksempler på hvordan slike teknikker for persontilpassing er med på å påvirke demokratier og samfunnsstrukturer i hele verden. Mikromålretting av reklame bør derfor forbys, noe som også vil gi likere konkurransevilkår fordi persondata blir mindre viktig.

OVERVÅKINGSØKONOMIEN

Forretningsmodellen i den digitale økonomien er i stor grad basert på overvåking av brukerne. Opplysninger om hva vi gjør, våre vaner og interesser brukes for å vise oss persontilpasset reklame.

Når man bruker nettet, følger en rekke selskaper med på hva man gjør. Informasjon om hvilke nettsider som besøkes, hvem man følger på sosiale medier eller hvilke filmer man ser på, er verdifull informasjon for annonseindustrien. Jo mer de vet, jo mer presist kan de målrette reklame. Data om brukere blir dermed et verdifullt element av annonsemarkedet.

TEKNOLOGIEN SOM DRIVER UTVIKLINGEN

Det er særlig fire utviklingstrekk som har bidratt til at overvåkingsøkonomien er blitt så omfattende:[1]

- **Tingenes internett:** Stadig flere ting rundt oss utstyres med sensorer og kobles til nett. I tillegg bæres stadig mer teknologi direkte på kroppen gjennom utviklingen av smartklokker, pulsebelter og annen kroppsnær teknologi.

[1] Teknologirådet (2016)

- **Data og metadata:** Alle datamaskiner produserer store mengder data. Når samfunnet rundt oss digitaliseres blir livene våre også dokumentert i større grad. I tillegg blir metadata stadig viktigere – data som beskriver omstendighetene rundt vår aktivitet på nett.
- **Billig lagring:** Datamaskinene får stadig større og rimeligere lagringsplass. Dermed kan det lagres mer og mer data.
- **Store data, rimelig regnekraft og maskinlæring viser nye sammenhenger:** Utviklingen av kunstig intelligens gjør det mulig å stadig oppdage nye sammenhenger i store datasett. Nesten alle typer data kan komme til nytte, og analyseres på måter man tidligere ikke trodde var mulig.

OVERVÅKNING SOM FORRETNINGSMODELL

I begynnelsen var det få kommersielle interesser på internett. Da selskaper etter hvert etablerte seg på nett mot slutten av 1990-tallet, jaktet de en måte å tjene penger på. Siden brukerne hadde blitt vant til at tjenestene var gratis, ble brukerbetaling utelukket. Det fantes heller ingen etablert infrastruktur for mikrobetalinger. Annonser, for eksempel i form av bannere, ble lansert som et alternativ.

For å tiltrekke seg annonsører måtte imidlertid nettreklamen tilby noe man ikke kunne få andre steder.[2] Fordi det allerede var mulig å analysere brukernes adferd på nett, ble dette tatt i bruk for å tilby målrettet reklame.[3]

Utviklingen av Google er et godt eksempel på dette. Da grunnleggerne Larry Page og Sergey Brin lanserte sin søkemotor i 1998 ville de unngå å koble sammen søkeresultater og annonsering. Søkeresultatene skulle ikke være påvirket av kommersielle interesser, men være transparente og basert på en rangeringsordning inspirert av akademisk henvisningspraksis.[4] I begynnelsen tjente de derfor penger på å selge lisenser, blant annet til Yahoo!.

[2] Zuckerman, Ethan (2014)
[3] Se også oppsummering av utviklingen her https://www.digi.no/artikler/debatt-nordmenn-til-salgs-overvaknings-okonomien-er-fortsatt-ute-av-kontroll/503821
[4] Brin, Sergey og Lawrence Page (1998)

Etter hvert endret imidlertid forretningsmodellen seg, spesielt etter at den såkalte dotcom-boblen sprakk og investorene forsvant etter 10. mars 2000.[5] I oktober 2000 lanserte Google verktøyet AdWords slik at annonsører kunne kjøpe seg plass øverst i søkeresultatene. Basert på søkeord og store mengder data om brukernes netthistorikk kunne Google tilby målrettet annonsering, der kundene betalte for klikk i stedet for visninger. Dette gjorde selskapet til en dominerende aktør på annonsemarkedet og en enestående kommersiell suksess, selv om søkemotoren fortsatt ikke koster penger for brukerne.

Dette har etter hvert blitt den dominerende modellen for digitale tjenester: de aller fleste tjenester tilbys gratis, mot at det samles inn enorme mengder data om brukerne for å fange oppmerksomheten deres og selge annonser. I dag er dette grunnlaget for populære tjenester fra Facebook og Google, samt en rekke populære apper og spill.

DIGITALE PROFILER

Fordi man kan spores på tvers av ulike nettsteder og enheter, får selskapene i annonseindustrien mulighet til å lage digitale profiler om brukerne. Informasjonen som samles inn, er sammensatt. En type er informasjon om innholdet man interagerer med: hvilke nettsider og apper som brukes, hvem man er venner mer på sosiale medier og hva man søker etter. I tillegg samles det inn metadata – for eksempel hvilket utstyr som brukes, hvor brukeren befinner seg eller hvilke tidspunkt man er mest på nett. Basert på denne informasjonen kan digitale profiler også inneholde *utledet informasjon*. Dette innebærer at selskaper som Facebook antar en rekke ting, basert på informasjonen de har, for eksempel etnisitet, interesser og økonomiske forhold.

Ved å analysere vår adferd på nett, bevegelsesmønstre og vaner, kan disse digitale profilene bli svært detaljerte, og danne et komplekst og nærgående bilde av oss som individer. Profilene kan blant annet inneholde informasjon som personlighetstype, nære relasjoner og seksuelle preferanser, i tillegg til kjønn alder og interesser, bosted, arbeidssted og språk.

Disse profilene danner grunnlaget for målrettingen av reklame på nett. Basert på våre interesser, preferanser og økonomi kan annonsørene persontilpasse

[5] Foroohar, Rana (2019)

budskapet sitt, og til og med forutsi hvilke behov vi kommer til å få i fremtiden.[6] Målet er å få og holde på oppmerksomheten vår, og etter hvert få oss til å gjøre ting som å reagere på innholdet og klikke på annonser. På Yotube er 70 prosent av innholdet som brukerne ser på, valgt på bakgrunn av anbefalingsalgoritmene til videoplattformen.[7] Det er dermed plattformene selv som i stor grad styrer hvilket innhold brukerne ser og reagerer på.

Det er økende bevissthet om at informasjon om nettaktivitet brukes til å målrette reklame. At informasjonen lagres i komplekse digitale profiler er mer overraskende for mange.[8] Når målretting skjer åpent og tydelig, for eksempel i anbefalinger på Netflix eller Spotify, synes mange dette er positivt. Imidlertid brukes data også i stor grad til å tilpasse søkeresultater, reklame og tjenester på måter som er mindre synlige.

En fersk undersøkelse fra USA viser at hele 81 prosent er bekymret for at data som samles inn om dem brukes til å lage komplekse digitale forbrukerprofiler.[9]

KJØP OG SALG PÅ ANNONSEBØRSER

Det digitale annonsemarkedet er stort og komplekst, med mange ulike aktører. Helt generelt kan aktørene deles inn i fire kategorier:[10]

- **Publisister** selger tilgang til flater hvor ulike annonsører kan kjøpe annonseplass. Eksempler på publisister er nettaviser, blogger, mobilspill og sosiale medier.
- **Annonsører** inkluderer alle selskaper, virksomheter og organisasjoner som ønsker å nå nye og eksisterende kunder gjennom digitale annonser.
- **Tredjeparts-leverandører** er en stor gruppe ulike selskaper som selger tjenester til publisister, markedsførere eller andre leverandører. Disse selskapene kan for eksempel være analyseselskaper eller datameglere.

[6] Christl, Wolfie (2017)
[7] Solsmann (2018)
[8] Which? (2018)
[9] Consumer Reports (2020)
[10] Forbrukerrådet (2020)

- **De store plattformene** som Facebook og Google har fått dominerende posisjoner, blant annet fordi de sitter på store mengder data. De har gjerne flere roller samtidig og kontrollerer flere ledd av markedet.

Når man besøker nettstedet til en publisist settes det i gang en auksjon hvor ulike annonsører konkurrerer om å kjøpe reklameplass. I løpet av millisekunder blir brukerens digitale profil presentert for mulige annonsører. Den som er villig til å betale mest, vinner, og det er denne aktørens annonser brukeren ser på nettsiden. Hele denne helautomatiske prosessen foregår på den tiden det tar å laste inn nettstedet.

Prisen som betales for hver enkelt reklame er lav. Imidlertid er det visse typer informasjon som kan føre til at verdien øker.[11] Store livshendelser som giftemål, flytting eller graviditet fører ofte til endringer i innkjøpsmønstre, og for annonsører gir dette mulighet for å tjene penger. Derfor vil informasjon om slike hendelser innebære at man blir et langt mer attraktivt objekt på annonsemarkedet. Helseopplysninger, særlig om legemiddelbruk, er det aller mest attraktive, og kan nesten doble prisen annonsørene er villige til å betale.

MARKEDET DOMINERES AV GOOGLE OG FACEBOOK

Estimater anslår at Google og Facebook til sammen mottar over halvparten av pengene som brukes på digital markedsføring i verden.[12] I Norge anslås annonsemarkedet til omtrent 20 milliarder, hvor Facebook og Googles andel er seks milliarder.[13] For mange land er andelen langt høyere. I USA er det anslått at de to selskapene fikk nær 70 prosent av de digitale annonseinntektene i 2019, og i Storbritannia er andelen anslått til hele 80 prosent. Google og Facebook er de største selskapene i overvåkingsøkonomien, og er rangert som de henholdsvis femte og sjette mest verdifulle selskapene i verden.[14]

Google

Google startet opp med nettsøk, men har i tillegg blitt en dominerende aktør på svært mange områder i den digitale økonomien. Nettleseren Chrome er den mest brukte på verdensbasis, og Google Maps dekker 80 prosent av digital

[11] Steel, Emely (2013)
[12] eMarketer (2020)
[13] Ekeberg (2019)
[14] Statista (2020)

kartbruk.[15] Sammen med tjenester som YouTube, Google Translate, Gmail, Google Workplace, hjemmeassistentene Home og Nest, og operativsystemet Android, har selskapet skapt et helt eget produktunivers med datainnsamling som grunnlag.

Mindre kjent for mange er kanskje Google Analytics, en gratis tjeneste for analyse av nettbesøk. Dette er det mest utbredte verktøyet globalt, og det anslås at over halvparten av alle nettsteder i verden bruker Google Analytics.[16] Ved å installere en liten kode på nettsiden, kan man bruke Google Analytics til å følge med på aktivitet på egen nettside, som hvor brukerne kommer fra, hvilke sider de besøker mm. Den som eier nettsiden får dermed et gratis verktøy for å analysere trafikken, samtidig som Google får tilgang til den informasjon som samles inn.

Tilgangen Google har til data gjennom alle sine tjenester gjør at de kan diktere store deler av mekanismene i annonsemarkedet. Google eier DoubleClick, den største annonsebørsen, samtidig som de selger og kjøper både annonser og annonseplass. De innehar altså roller som publisist, markedsfører og tredjepartsleverandør samtidig.

Google var et av de første selskapene som drev med persontilpasset reklame, basert på tilgang til persondata om brukerne. Og det er fortsatt her hovedinntekten til selskapet ligger. I 2019 tjente de nesten 135 milliarder dollar bare på annonser.[17]

Facebook

Facebook er verdens største sosiale nettsted med nærmere 3 milliarder brukere. I tillegg eier selskapet de svært populære tjenestene Instagram, Messenger og WhatsApp. Disse fire tjenestene var de mest nedlastede appene på 2010-tallet.[18] Deres forretningsmodell baserer seg på å samle inn data om både brukere og ikke-brukere gjennom å følge deres nettaktivitet både på og utenfor Facebook. Deretter selger de tilgang til denne informasjonen via sine annonseverktøy. Utfra denne forretningsmodellen er Facebook primært en annonseplattform, som samler inn data om brukerne gjennom deres deltakelse i grupper og nettverk.

[15] Subcommittee on antitrust, commercial and administrative law of the committee on the judiciary (2020)
[16] W³Techs (2020)
[17] Véliz, Carissa (2020)
[18] Shead (2019)

Gjennom de siste årene har Facebook stadig utviklet produktene sine, og beholdt en dominerende markedsposisjon med langt flere brukere enn noen av konkurrentene innen sosiale medier. Faktisk er flere av de viktigste konkurrentene til Facebook eid av selskapet selv.

Den dominerende markedsposisjonen gjør Facebook attraktiv som annonseplattform. En annen fordel er muligheten til å målrette annonsene sine til faktiske, navngitte personer, ikke bare digitale profiler av brukerne.[19] Slik individuell målretting skjer for eksempel ved at et selskap kan laste opp sin kundeliste til Facebook, koble disse navnene til kundenes Facebook-profiler, og målrette reklame direkte til dem.

Det store antallet brukere gir annonsørene et stort publikum, og de får også tilgang til komplekse verktøy for å målrette, teste og forbedre annonsene sine. Et av disse verktøyene er Facebook Pixel. Når noen har klikket på en reklame, gjør Pixel det mulig å følge med på hva brukeren gjør på siden – for eksempel om de kjøper noe eller ikke.[20]

Et av de mest populære verktøyene man kan bruke via Pixel, er å målrette reklame mot brukere som tidligere har vært på siden din. Istedenfor å bruke målgrupper basert på alder, kjønn eller bosted, kan du vise annonser til dem som allerede har vist interesse for det du har å selge.

Facebook sitter på enorme mengder data om oss, uavhengig av om vi er brukere eller ikke. Det er informasjon hentet gjennom brukerprofiler, kundelister lastet opp til annonseverktøyene, eller data samlet inn gjennom Pixel på utallige nettsider. I tillegg har Facebook et rufsete rykte når det kommer til hvordan data deles og behandles, blant annet etter Cambridge Analytica-saken i 2016.[21]

[19] Subcommittee on antitrust, commercial and administrative law of the committee on the judiciary (2020)
[20] Facebook (udatert)
[21] Wired (udatert)

SLIK BLIR VI SPORET

Det finnes stadig flere måter å spore oss på nettet. Informasjonskapsler har fått selskap av sporingsbilder, tastelogging og video – og ikke minst analyseverktøy fra Facebook og Google.

Det finnes flere ulike verktøy og metoder for å spore nettaktivitet. I tillegg har både Facebook og Google egne tjenester som samler inn data på tvers av et enormt antall nettsider.

Tradisjonelt har sporing på nett stort sett vært gjort med informasjonskapsler. Økt bevissthet rundt slik sporing har blant annet ført til at flere nettlesere, som Firefox, Edge og Safari, nå blokkerer tredjeparts informasjonskapsler for å beskytte brukernes personvern. Informasjon om brukerne er så sentralt for internettøkonomien at annen sporingsteknologi nå brukes i større grad enn tidligere for å omgå disse blokkeringene.

I dag skjer stadig mer av vår nettaktivitet via mobilen og apper. Også her utvikles det egne sporingsteknologier og teknikker for å kunne identifisere brukere. I den digitale annonseindustrien er det for eksempel vanlig med annonse- eller enhets-ID. Ved å tillegge hver bruker eller enhet et unikt nummer, kan man følge med på hva brukeren gjør på tvers av tjenester og enheter.[22] Dermed kan de også bygge opp komplekse profiler knyttet til hvert enkelt ID-nummer.

[22] Forbrukerrådet (2020)

I denne rapporten fokuserer vi på sporing på nettsider, og beskriver sporingsteknikker som hovedsakelig brukes i en nettleser. Nedenfor omtales de viktigste.

INFORMASJONSKAPSLER

Informasjonskapsler, eller «cookies», har tradisjonelt være den mest utbredte formen for sporing på nett. Når man besøker en nettside, lagres det en liten kode i nettleseren, som gjør at man blir gjenkjent ved et senere besøk. Filen sørger for at eieren av nettstedet får informasjon om hva brukerne foretar seg på sidene.

Det finnes flere typer informasjonskapsler. Førstehånds informasjonskapsler er når eieren av en nettside selv tar i bruk informasjonskapsler for å få informasjon om hva brukeren foretar seg, for eksempel til statistikkformål. Dette gjør det også mulig å lagre innloggingsinformasjon eller språkinnstillinger til et senere besøk.

Tredjeparts informasjonskapsler plasseres ut av andre enn dem som eier nettsiden, og slike selskaper har ofte informasjonskapsler installert på mange ulike nettsider. Det blir dermed mulig å identifisere og kartlegge brukernes aktivitet på tvers av alle disse nettstedene. Dette er vanlig innenfor annonseindustrien, og gjør at man kan persontilpasse reklame basert på den enkeltes nettaktivitet.

SPORINGSBILDER

Sporingsbilder er en usynlig bildefil som plasseres på nettsider, enten i kombinasjon med eller istedenfor informasjonskapsler.

Nettsider som inneholder bilder, har alltid disse bildene lagret på en server. Når man besøker en nettside, laster nettleseren ned disse bildene for å vise dem til deg. Når en nettside bruker sporingsbilder skjer akkurat det samme: nettleseren laster ned sporingsbildet. Når bildet lastes ned sendes det en rekke

datapunkter tilbake til den som eier nettsiden, inkludert IP-adresse, tekniske innstillinger og hva man gjør på siden.[23]

Sporingsbilder brukes til å samle inn informasjon om brukernes aktiviteter på nettstedet, på samme måte som informasjonskapsler. Selv om nettleseren ikke aksepterer informasjonskapsler, vil sporingsbilder fortsatt samle opplysninger om brukerens aktivitet.

Sporingsbilder brukes ofte for å innhente informasjon til persontilpassing av reklame, og er også vanlige å bruke i nyhetsbrev for å samle informasjon og analysere brukeratferd, for eksempel om hvor mange som klikker på lenker i et nyhetsbrev.[24]

DIGITALE FINGERAVTRYKK

Et digitalt fingeravtrykk er en metode for å identifisere brukere, basert på sammenstilling av ulike informasjonsbiter og det tekniske utstyret som brukes.

For at en nettside skal vises korrekt, deler nettleseren en mengde informasjon med nettsidens eier – som skjermoppløsning, språkvalg og operativsystem. Når slike detaljer settes sammen, skapes det det et unikt digitalt fingeravtrykk som gjør brukeren identifiserbar. På denne måten kan nettsteder kjenne deg igjen hver gang du besøker nettsiden.

Teknikken ble utviklet for sikkerhetsformål, og brukes fortsatt til dette for å avsløre piratkopiering av programvare, identitetstyveri eller kredittkortsvindel.[25] Digitale fingeravtrykk er vanskelige å oppdage og slette, fordi teknikken ikke baserer seg på installasjon av programvare (slik som for eksempel informasjonskapsler) eller registrering av IP-adresse.

Digitale fingeravtrykk brukes særlig av tredjeparts aktører i annonseindustrien, for eksempel datameglere. Fordi disse aktørene er aktive på store deler av nettet, kan brukernes aktivitet følges også på tvers av ulike nettsider.

[23] The Verge (2019)
[24] Whatagraph (2019)
[25] Briz, Nock (2018)

Teknikken ble utviklet rundt 2010, men har ikke vært særlig utbredt. I 2019 ble den brukt på rundt 3,5 prosent av de mest populære nettsidene. Dette var likevel en økning fra rundt 1,6 prosent i 2016. I tillegg brukes det i en rekke ulike apper.[26] Fordi mange nettlesere nå blokkerer informasjonskapsler, blir alternative metoder stadig mer populære.

TASTELOGGING

Tastelogging innebærer at et nettsted eller en tredjepart registrerer hva man skriver inn i et skjema, også før man trykker «send» eller «lagre». Det kan også innebære å samle metadata – hvor fort man skriver eller hvor hardt man trykker på tastene.[27]

Tastelogging kan brukes på flere måter. Et eksempel mange er kjent med, er når man begynner å skrive tekst inn i et søkefelt, og det kommer opp forslag til tekst. Det kan også brukes i sikkerhetsarbeid, for eksempel for å oppdage uautorisert aktivitet på en server. Metadata om tasting viser seg å være nyttig til å gjenkjenne personer. Da er det ikke *hva* man skriver, men *hvordan* man skriver som blir analysert.[28]

Fordi de fleste digitale tjenester har tekstbaserte elementer, kan tastelogging føre til at man avslører sensitiv informasjon uten at man er klar over det. Dette kan for eksempel være kredittkortinformasjon, passord eller personnummer. Hvis man skriver dette inn i et skjema og det brukes tastelogging, kan denne informasjonen bli tilgjengelig for andre enn den den var tiltenkt i etterkant.

Denne informasjonen kan deretter brukes videre, både til målretting av reklame, men også i ulike typer svindel.

[26] Chen, Brian X. (2019)
[27] Kaspersky (udatert)
[28] Baisotti, Valentina (2019)

OPPTAK AV NETTSIDEBESØK

Opptak av nettsidebesøk innebærer at hele besøk på en nettside registreres og lagres som på et videoopptak.

Dette inkluderer alle små og store aktiviteter, som hvilke bevegelser man gjør med musepekeren, hvilke sider som besøkes og når man scroller opp og ned. Teknologien fungerer altså som om noen stod bak deg og fulgte med på alle dine bevegelser.

Når man kan se opptak av hvordan brukerne navigerer på siden, får man innsikt i om det er vanskelig å finne frem eller utføre de oppgavene brukerne kom til nettsiden for å gjøre. Dermed kan dette være et nyttig verktøy for å gjøre sider mer brukervennlige. Samtidig utfordrer dette personvernet. Å analysere slike opptak innebærer for eksempel at informasjon man har skrevet inn i skjemaer kan bli synlig, som navn, adresse, passord eller helseinformasjon.

Hotjar er et populært verktøy for opptak av nettsidebesøk. Av de 41 nettstedene Teknologirådet har undersøkt, delte 14 av dem informasjon med Hotjar.

GOOGLE ANALYTICS

Google Analytics er et gratis analyseverktøy for nettbesøk. Det er svært utbredt, og antas å være i bruk på over halvparten av alle nettsider.[29]

For å ta i bruk verktøyet installeres det en liten kodebit på nettsiden. Den registrerer alt brukerne foretar seg. Eieren av nettsiden får dermed tilgang til informasjon om blant annet hvor brukeren er, hvilke sider som besøkes, hvordan brukeren kom til siden osv. Den samme informasjon deles også ofte med Google.[30]

Data fra Google Analytics kan kobles sammen med data fra Googles annonsetjenester, noe som gjør det mulig å følge med på hvordan brukere interagerer med annonser i tillegg til selve nettsiden. Dette legger til rette for persontilpasset reklame. Verktøyet *Remarketing audiences* innebærer for eksempel at man

[29] W³Techs (2020)
[30] Google (udatert)

kan målrette reklame mot brukere som tidligere har besøkt en nettside, for å få dem til å komme tilbake.

Google Tag Manager er et annet vanlig verktøy. Dette brukes til å sette opp og holde oversikt over ulike aktiviteter på et nettsted. For eksempel kan man sette opp «tags» for å spore konkrete aktiviteter som et gjennomført kjøp i nettbutikken, nedlasting av et dokument eller utfylling av et skjema.[31]

Som beskrevet i forrige kapittel, har Google flere ulike roller i annonsemarkedet. De mange tjenestene Google driver, og det store antallet nettsteder som bruker Google Analytics, gjør at Google har tilgang til informasjon om en svært stor andel av den globale nettaktiviteten.

FACEBOOK PIXEL

Facebook Pixel er et gratis verktøy fra Facebook, som analyserer interaksjon med annonser på Facebooks annonseplattform, og besøk på nettsider som har Pixel installert.

På samme måte som Google Analytics, tas Pixel i bruk ved at en liten kodebit installeres på nettsiden. Denne registrerer brukernes aktivitet.

Facebook Pixel er koblet mot Facebooks annonsetjenester. Det gir innsikt i hvordan annonser på Facebook fungerer, fordi man kan følge brukernes handlinger når de har klikket på en annonse. Hvorvidt brukeren ender opp med å kjøpe et produkt eller ikke, eller hvilke andre varer vedkommende ser på, er informasjon man får ved å bruke Pixel. Slik legges det også til rette for persontilpasset reklame, basert på aktivitet på sider og apper utenfor Facebook.

Pixel undersøker også om besøkende til siden er logget inn på Facebook, Instagram aller Whatsapp. Hvis de er det, kobles informasjon om nettsideaktiviteten mot den konkrete Facebook-brukeren. Dette betyr at Facebook kan følge brukerne utenfor sine egne plattformer, på mange ulike nettsteder. Fordi mange er logget inn på Facebook både på mobil og pc, kan de også spores på tvers av enheter. Facebook Pixel samler også informasjon om personer som ikke

[31] Fedorovicius, Julius (2020)

har Facebook-konto. Dette vil ikke kunne kobles til en navngitt person, men likevel samle data som brukes til å bygge videre på en digital profil.

PERSONVERNUTFORDRINGENE

Bruken av informasjonskapsler, sporingsbilder og digitale fingeravtrykk er i utgangspunktet ganske lik. Teknikkene brukes for å samle inn informasjon om hvordan man bruker og beveger seg mellom ulike nettsider. Mange leverandører til annonseindustrien er bredt representert på nett, noe som gjør at de kan følge oss på tvers av mange ulike nettsteder.

Der man etter hvert har fått relativt gode muligheter til å blokkere for informasjonskapsler, tar sporingsbilder og digitale fingeravtrykk over – og disse er mye vanskeligere å både identifisere og slette.

Tastelogging og opptak av nettsidebesøk er en litt annen type teknologi. En personvernutfordring ved opptak av nettsidebesøk er at sensitiv informasjon kan bli tatt opp og lagret.[32] Dette kan være identifiserbar informasjon som navn og adresse, eller helseopplysninger eller kredittkortinformasjon. Tastelogging har liknende utfordringer, men her kan man også risikere at et nettsted samler inn informasjon som er skrevet inn i et skjema, men aldri sendt. Man kan dermed si at teknikken kan samle inn informasjon om hva vi tenker, ikke bare hva vi faktisk gjør.

Omfanget av bruken av verktøy fra Google og Facebook er problematisk i seg selv. Det betyr at disse to selskapene har oversikt over store deler av dagens internettbruk. De kan dermed også følge brukerne på tvers av ulike nettsteder og enheter.

Selv om hver enkelt lille bit av informasjon ikke sier så mye om hver enkelt bruker, vil en større sammenstilling av nettbruk gi et detaljert og nærgående bilde av vaner, preferanser, nettverk og aktiviteter.

[32] Kassner, Michael (2017)

KOMMERSIELL SPORING I OFFENTLIG SEKTOR

Offentlig sektor utfører en rekke oppgaver og tjenester som innbyggerne er avhengige av og ikke kan velge vekk. Da blir det ekstra viktig at personvernet ivaretas.

Digitaliseringen av offentlig sektor er i full gang. Prinsippet om digitalt førstevalg innebærer at kommunikasjon mellom innbyggere og forvaltning i hovedsak skal foregå digitalt.[33]

Offentlige tjenester kommer ofte svært tett på innbyggerne, og kan innebære deling av personinformasjon knyttet til helse, familieliv eller privatøkonomi. Ofte finnes det ingen alternative tjenestetilbydere. Derfor bør offentlig sektor ta et særskilt stort ansvar når det kommer til sikkerhet og beskyttelse av persondata når tjenestene digitaliseres. Dette innebærer å sikre at det ikke samles inn mer data enn det som er ytterst nødvendig.

I 2016 undersøkte Forbrukerrådet nettsidene til norske kommuner, med nedslående resultater.[34] Mange kommuner delte informasjon om brukerne sine med et stort antall tredjeparter, mange knyttet til annonseindustrien. I tillegg manglet mange av sidene personvernerklæringer.

[33] Digitaliseringsdirektoratet (udatert)
[34] Forbrukerrådet (2016a)

ER DET LOV?

ANALYSE AV NETT-TRAFIKK

Bruk av tjenester som Google Analytics kan innebære innsamling og analyse av persondata. IP-adresser er for eksempel definert som en personopplysning, fordi de kan spores tilbake til en bestemt maskin og dennes bruker.[35]

Lovligheten av Google Analytics og liknende verktøy ble vurdert av Datatilsynet i 2012. De gjorde tilsyn hos Lånekassen og Skatteetaten, og undersøkte hvilke data som ble samlet inn og hvordan disse ble behandlet.[36] Etter å ha innhentet dokumentasjon fra Google som beskrev hvordan IP-adresser ble behandlet og lagret, ble bruken av Google Analytics godkjent, så lenge deler av IP-adressen ble maskert før informasjonen lagres på Googles servere.[37]

De aller fleste nettstedene Teknologirådet har undersøkt presiserer i sine personvernerklæringer at de følger Datatilsynets retningslinjer og maskerer IP-adresser. Det er likevel noen som ikke omtaler dette, for eksempel Tromsø og Bergen kommune, Direktoratet for samfunnssikkerhet og beredskap, Husbanken og Folkehelseinstituttet. Det er derfor umulig å vite om de gjør dette eller ikke.

BRUK AV INFORMASJONSKAPSLER OG SAMTYKKE

Bruk av informasjonskapsler reguleres av ekomloven, som forvaltes av Nasjonal kommunikasjonsmyndighet (Nkom).[38] Loven slår fast at brukeren må få informasjon om og gi et aktivt samtykke til bruken.[39] Dette betyr at det skal være klart og tydelig hvilke informasjonskapsler som brukes, hvilke opplysninger som behandles, hva informasjonen skal brukes til og hvem som behandler informasjonen.

Datatilsynene i både Storbritannia[40] og Belgia[41] behandler nå saker relatert til den digitale annonseindustrien og sporing på nett, og samtykke er et av elementene som vurderes. I Belgia er det ventet en uttalelse i begynnelsen av 2021. Også i Norge er myndighetene på banen. I januar 2021 varslet Datatilsynet

[35] Datatilsynet (2018)
[36] Jørgenrud, Marius (2012)
[37] Jørgenrud, Marius (2013
[38] Nasjonal kommunikasjonsmyndighet (2020)
[39] Nasjonal kommunikasjonsmyndighet (2020)
[40] McDougall, Simon (2020)
[41] Lomas, Natasha (2020)

dating-appen Grindr om en bot på 100 millioner kroner.[42] Tilsynet viser til at Grindr har delt brukernes personopplysninger med tredjeparter, uten gyldig samtykke.

OVERFØRING AV DATA

Sommeren 2020 ble Privacy Shield – avtalen som regulerer overføring av data mellom EU og USA – kjent ugyldig.[43] Fordi amerikansk etterretningslovgivning gjør det mulig å få tilgang til data hos private selskaper, mener den europeiske domstolen at data fra europeiske brukere ikke har god nok beskyttelse i USA.[44]

I annonseindustrien er mange av de dominerende aktørene amerikanske, og data som samles inn sendes derfor i all hovedsak til lagring på amerikanske servere.[45] Denne overføringen er nå ulovlig, og rammer dermed mange norske virksomheter som benytter seg av for eksempel Google Analytics. Bruk av Google Analytics og Facebook Connect har nå blitt satt i søkelyset av personvernaktivisten Max Schrems og hans organisasjon NYOB.[46] Over 100 selskaper som bruker disse verktøyene, inkludert tre norske, er meldt inn til europeiske datatilsyn, fordi de fortsatt overfører data til USA uten en gyldig avtale.

HVORFOR ER DETTE PROBLEMATISK?

DEMOKRATISK UTFORDRING

Innbyggernes interaksjon med myndighetene omfatter noen av de mest private hendelsene i våre liv. Hvilke offentlige nettsider vi besøker, hvilke tjenester vi bruker og hvilke etater vi kommuniserer med, kan si mye om livene våre som vi ikke ønsker at andre skal få innsyn i. Økt digitalisering og digitalt førstevalg gjør nå at innbyggerne i stor grad må samhandle med offentlige etater og tjenester over nett.

Offentlig sektor er avhengig av innbyggernes tillit for at digitaliseringsprosjekter skal kunne gjennomføres og bli tatt i bruk. Et viktig element for å få og beholde tillit fra innbyggerne er at man kan være sikre på at informasjon om

[42] Datatilsynet (2021)
[43] Court of Justice of the European Union (2020)
[44] Datatilsynet (2020)
[45] Drange, Jan Morgen og Vebjørn Søndersrød (2020)
[46] NOYB (2020)

bruken av offentlige tjenester ikke deles med uvedkommende. For at tillitsforholdet mellom staten og innbyggerne skal opprettholdes, bør det være en selvfølge at offentlige nettsteder er en sone helt fri for kommersiell sporing.

Når det i tillegg er slik at enkelte livshendelser gjør brukerne mer ettertraktet hos annonsører, er det enda større grunn til å unngå at data deles fra bruk av offentlige tjenester. Informasjon om at en innbygger søker om foreldrepermisjon eller barnehageplass kan fort bli brukt for å selge annonser for barnevogn eller nye vintersko.

VANSKELIG Å FORSTÅ HVA SOM SKJER

Mange nettsteder skaper et inntrykk av at brukerne har kontroll over hvordan data samles inn og brukes. De mange pop-up vinduene hvor man må godkjenne bruk av informasjonskapsler er eksempler på dette. Hos mange er dette imidlertid kun en overfladisk prosess, da alternativet til å godkjenne informasjonskapsler er å ikke bruke siden i det hele tatt. Forbrukerrådet har tidligere pekt på hvordan spekulativt design på nettsider manipulerer brukerne til å godta mer overvåking enn det man ellers ville gjort, for eksempel å si ja til at informasjon om nettbruk samles inn og analyseres.[47]

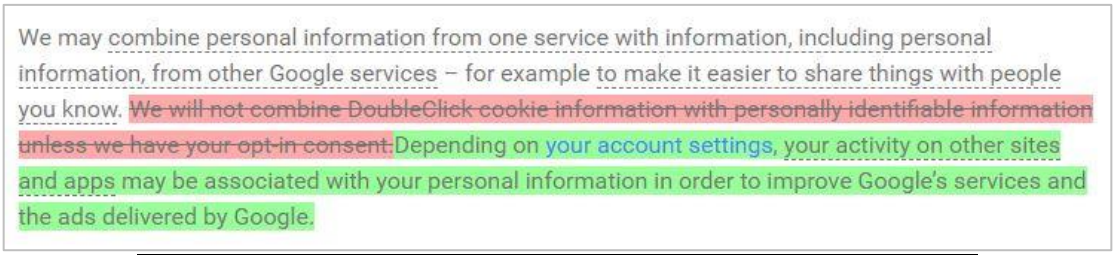
I tillegg er personvernerklæringer ofte vanskelige å sette seg inn i. Ordvalg, formuleringer og mengden informasjon gjør det omtrent umulig for brukeren å forstå hva man takker ja til. Dette gjelder både innsamlingen av informasjon på den konkrete siden, men også hvordan data deles og selges videre i det enorme økosystemet knyttet til digitale annonser.[48] Regjeringen har tidligere pekt på disse utfordringene, og at det fører til at brukerne enten ikke leser ferdig personvernerklæringene, eller at de samtykker til avtaler de ikke har forstått.[49]

Personvernerklæringer inneholder ofte et punkt om at vilkårene når som helst kan oppdateres, og at det er brukeren selv som må holde seg orientert om slike endringer. Dette kan føre til at mange ikke får med seg fundamentale endringer i hvordan data samles inn og brukes.

I 2016 endret Google en liten setning i sin personvernerklæring. Denne endringen førte imidlertid til store endringer i hvordan Google kobler sammen data fra ulike tjenester. Tidligere hadde informasjon fra annonsebørsen Doubleclick ikke blitt koblet mot identifiserbar informasjon fra Google-kontoer. Endringen

[47] Forbrukerrådet (2018)
[48] Kemp, Katharine (2019)
[49] Meld. St. 27 (2015–2016)

i 2016 førte nå til at informasjon fra brukernes kontoer kunne kobles mot informasjon hentet inn fra informasjonskapsler.



Bildet viser endringene i Googles personvernerklæring fra juni 2016.[50]

Flere av de offentlige nettsidene Teknologirådet har undersøkt skriver i sine personvernerklæringer at de benytter seg av de mulighetene som finnes for anonymisering av data (for eksempel maskering av IP-adresser) og deler minimalt med data videre. Det er likevel vanskelig å finne ut helt konkret hvordan data brukes og deles med andre, og hva formålet er. Personvernerklæringer er vanskelige å lese, og med mindre man har kjennskap til og forstår sporingsteknologien som brukes, er det vanskelig å forstå hva som egentlig skjer. Mange av personvernerklæringene er i tillegg mangelfulle, eller mangler helt beskrivelser av hvordan sporing på nettsiden foregår.

Det finnes flere verktøy man kan ta i bruk for å blokkere at informasjonskapsler installeres og brukes når man besøker en nettside. Flere av nettsidene advarer imidlertid mot dette, da det kan føre til at nettsiden ikke fungerer som den skal. Dette gjør det dermed enda vanskeligere for brukeren å ta egne grep for å hindre innsamling av informasjon.

STYRKER ALLEREDE DOMINERENDE AKTØRER

I tillegg til å bruke informasjonen til å påvirke adferden vår med reklame, fører den utstrakte bruken av slike verktøy til å bygge opp særlig Google og Facebooks markedsdominans.

Den store tilgangen de har på data er en vesentlig årsak til denne dominansen. De to selskapene samler inn store mengder data gjennom sine egne tjenester, i tillegg til det som samles inn gjennom tredjeparter. Og jo flere som bruker dem, jo mer data får de, og jo mer attraktive blir de for nye annonsekunder.

[50] Hentet fra https://www.google.com/policies/privacy/archive/20160325-20160628/

Den dominerende posisjonen til selskapene medfører at disse selskapene tjener langt mer enn hva som ville vært tilfelle dersom det var større konkurranse, noe som blant annet beskrives i en grundig rapport fra britiske konkurransemyndigheter.[51]

Når noen få selskaper får slike monopollignende posisjoner, kan det også bidra til å hindre innovasjon mer generelt. Dette er kanskje særlig relevant i den digitale økonomien, hvor data har blitt selve råvaren til mange typer tjenester, ikke bare markedsføring. Når data i stor grad tilfaller de som allerede har sterke markedsposisjoner, er det vanskelig for nykommere å etablere seg – også med helt andre tjenester – fordi de ikke får tilgang til dataene som er nødvendige for å utvikle nye tjenester og konsepter.[52]

Denne markedssituasjonen er grunnen til at konkurransemyndighetene blant annet i Storbritannia, USA og EU jobber aktivt med å begrense dominansen til de store aktørene. I desember 2020 ble det klart at de amerikanske konkurransemyndighetene saksøker Facebook,[53] og myndighetene i Texas, sammen med ni andre stater, går til sak mot Google.[54] Begge sakene tar for seg selskapenes misbruk av sin markedsmakt.

Også for norske myndigheter er det et uttalt mål å begrense markedsdominansen til teknologikjempene. I tildelingsbrevet fra Næringsdepartementet til Konkurransetilsynet for 2020 bes tilsynet om å prioritere etterforskningen av globale plattform-aktører som eventuelt bryter med konkurranseloven.[55] Tidligere finansminister Siv Jensen har også uttalt at det kan bli aktuelt å innføre en særnorsk digitalskatt, dersom arbeidet med et internasjonalt rammeverk for skattlegging av IT-gigantene i regi av OECD ikke gir resultater i løpet av 2020.[56]

[51] The Competition and Markets Authority (2020)
[52]The European Consumer Organisation (2019)
[53] Federal Trade Commission (2020)
[54] Paul, Kari (2020)
[55] Nærings- og fiskeridepartementet (2020)
[56] Vollan, Mari Brenna (2020)

SPORING PÅ OFFENTLIGE NETTSTEDER

Teknologirådet har undersøkt en rekke offentlige nettsteder med verktøyet Blacklight[57] for å se hvordan brukerne spores. Ved å taste inn en nettadresse i verktøyet, undersøker Blacklight det aktuelle nettstedet og ser etter prosesser som kan identifiseres som sporing av nettbruken, samt hvilke selskaper som mottar informasjon om bruken.

Teknologirådet har sett etter hvorvidt nettstedene:

- bruker Google Analytics
- om funksjonen for *remarketing audiences* er aktivert
- om det deles data med annonsebørsen Doubleclick
- om nettstedet bruker Facebook Pixel
- om det deles data med selskaper som utfører tastelogging eller opptak av nettsidebesøk.

I tillegg til den tekniske undersøkelsen med Blacklight, har vi har lest nettsidenes personvernerklæringer for å se hvordan virksomhetene selv beskriver sporingen, og hvorvidt de har tatt grep for å minimere innsamling og deling av data.

[57] https://themarkup.org/blacklight

Teknologirådet har undersøkt 41 offentlig nettsteder, inkludert regjeringen, direktorater, offentlige etater og et utvalg kommuner. Undersøkelsene ble gjort høsten 2020, med en oppdatering i januar 2021.

Av alle nettstedene var det kun Datatilsynet, Lånekassen og Konkurransetilsynet som ikke delte data videre med noen andre. De aller fleste delte data med Alphabet (Googles moderselskap), enten gjennom Google Analytics, Google Tag Manager eller annonsebørsen DoubleClick. Facebook Pixel er mindre vanlig, og brukes bare av fire av nettstedene.

Ingen av nettstedene brukte spesifikke verktøy for tastelogging. Fjorten av nettstedene brukte imidlertid Hotjar, et populært verktøy for opptak av nettsidebesøk. Dette kan i mange tilfeller også innebære at tekst som skrives inn på nettstedet registreres.[58]

NETTSTED	SPORINGSTEKNOLOGI				
	Google			**Facebook Pixel**	**Opptak av nettsidebesøk**
	Google Analytics	*Remarketing Audiences*	*DoubleClick*		
Arbeidstilsynet	X				
Barne-, ungdoms- og familiedirektoratet	X	X	X		X
Bergen kommune	X				
Datatilsynet					

[58] Wakefield, Jane (2017)

Digitaliserings-direktoratet	X				
Direktoratet for e-helse	X	X	X		
Direktoratet for samfunnssikkerhet og beredskap	X				
Folkehelseinstituttet	X				
Forbrukerrådet	X				
Forbrukertilsynet	X	X	X		X
Forskningsrådet	X	X	X	X	X
Helsedirektoratet	X				X
Helsenorge.no*					
Helsetilsynet	X				
Husbanken	X				
Innovasjon Norge	X	X	X	X	X
Integrerings- og mangfoldsdirektoratet	X				
Kompetanse Norge				X	
Konkurransetilsynet					
Likestillings- og diskriminerings-ombudet	X	X	X		

Lånekassen					
Medietilsynet	X	X	X	X	
Nasjonal sikkerhetsmyndighet	X	X	X		
NAV	X				X
Norge.no	X				
Norsk pasientskadeerstatning	X				X
Oslo universitets-sykehus	X				
Oslo kommune	X		X		X
Politiet.no	X				
Regjeringen.no	X				
Sivilombudsmannen	X	X	X		
Skatteetaten	X				
Statens vegvesen	X	X	X		X
Stavanger kommune	X	X	X		X
Stortinget	X	X	X		X
Tromsø kommune	X				
Trondheim kommune	X	X	X		
Utdanning.no	X	X	X		X

Utlendingsdirektoratet	X	X	X		X
Utlendingsnemnda	X				
Valgdirektoratet	X	X	X		

*Helsenorge.no bruker ikke de vanligste sporingsteknologiene fra Google og Facebook. Istedenfor bruker de liknende verktøy fra Adobe.

DE ALLER FLESTE SPORER BRUKERNE

Internasjonalt er Google den dominerende aktøren innenfor analyse av nett-trafikk. Dette er også tilfelle i norsk offentlig sektor. Av de 41 nettsidene vi undersøkte, brukte 36 én eller flere tjenester fra Google.

Alle disse 36 brukte Google Analytics, og 17 av nettstedene sendte i tillegg informasjon til DoubleClick (Googles annonsebørs). Ingen av disse 17 sidene gir informasjon om hvorfor dette skjer eller hva slags informasjon som deles i sine personvernerklæringer.

Både mengden data Google sitter på, og lagringstiden, er problematisk. For eksempel vil et besøk på Husbankens nettsider føre til at det sendes data til blant annet Doubleclick og Google-eide Youtube, som skal brukes til målrettet markedsføring. Hvis man selv ikke sletter informasjonskapslene i nettleseren, forbeholder Google seg retten til å la dem være aktive i hele 17 år.

Markedsføring (6)

Markedsførings-informasjonskapsler brukes til å spore besøkende på tvers av hjemmesider. Hensikten er å vise annonser som er relevante og engasjerende for den enkelte brukeren, og dermed mer verdifulle for utgivere og tredjeparts-annonsører.

Navn	Leverandør	Formål	Utløpsdato
YSC	.youtube.com	Samler informasjon om brukerne og deres aktivitet på nettstedet gjennom innebygde videospillere med det formål å levere målrettet annonsering.	Session
IDE	.doubleclick.net	Brukes til nettbasert markedsføring ved å samle inn informasjon om brukerne og deres aktivitet på nettstedet. Informasjonen brukes til å målrette annonsering til brukeren på forskjellige kanaler og enheter.	ett år
GPS	.youtube.com	Samler informasjon om brukerne og deres aktivitet på nettstedet gjennom innebygde videospillere med det formål å levere målrettet annonsering.	30 minutter
VISITOR_INFO1_LIVE	.youtube.com	Samler informasjon om brukerne og deres aktivitet på nettstedet gjennom innebygde videospillere med det formål å levere målrettet annonsering.	6 måneder
NID	.google.com	Lagrer dine seneste søk, dine foregående interaksjoner med annonsørenes annonser eller søkeresultater, samt dine besøk på en annonsørs nettsted for å kunne målrette annonser til deg på Google.	6 måneder
CONSENT	.google.com	Lagrer dine seneste søk, dine foregående interaksjoner med annonsørenes annonser eller søkeresultater, samt dine besøk på en annonsørs nettsted for å kunne målrette annonser til deg på Google.	17 år

Skjermbilde fra Husbankens personvernerklæring. Hentet 20. november 2020.

Det er problematisk at Google er til stede på en så stor del av offentlige nettsider. Når flere av nettstedene i tillegg er tydelig koblet mot de kommersielle annonsetjenestene blir utfordringene enda større. Det er vanskelig å se for seg hvilken begrunnelse de ulike virksomhetene kan ha for å gjør dette, som er viktigere enn brukernes personvern.

Funksjonen *remarketing audiences* er utviklet for å kunne målrette annonser mot kunder som tidligere har besøkt en nettside. Et eksempel på dette er når du ser reklamer på ulike nettsider for et produkt du tidligere har sett på i en nettbutikk. 16 av de undersøkte nettstedene bruker denne funksjonen, blant andre Trondheim kommune, Utlendingsdirektoratet, Statens vegvesen og Stortinget.no.

Barne-, ungdoms- og familiedirektoratet er den eneste av virksomhetene som adresserer dette i sin personvernerklæring, og forsøker å gi en forklaring på hvorfor de bruker det:

> *«Et av samfunnsoppdragene til Bufdir, er å rekruttere fosterhjem til barn og unge som trenger det. Da er vi avhengige av å komme i kontakt med så mange potensielle fosterforeldre som mulig. Derfor bruker vi cookies på den delen av bufdir.no som handler om fosterhjem. Dette gjør det mulig for oss å vise relevant innhold med mer informasjon om fosterhjemsoppgaven på andre nettsteder til de som har vist interesse, innenfor en begrenset tidsperiode. Denne typen cookies er også i bruk på sidene for foreldrehverdag og familievernkontorene.»*[59]

Selv om etaten ønsker å løse en reell utfordring med rekruttering av fosterforeldre, er det likevel uheldig at besøk på visse deler av Bufdirs nettsted blir videreformidlet og brukt videre i den digitale annonseindustrien.

Ved å bruke spore brukerne og bruke gratisverktøy fra de store teknologiselskapene er det også flere offentlige virksomheter som direkte motarbeider sine egne samfunnsoppdrag. For eksempel bruker Sivilombudsmannen Google Anaytics, remarketing audiences og de deler data med annonsebørsen Doubleclick. Dette samsvarer dårlig med deres oppgave om å ta vare på den enkeltes rettigheter i møte med forvaltningen.[60]

INFORMASJON OM SPORINGEN ER MANGELFULL ELLER FRAVÆRENDE

Det er en kjent problemstilling at brukervilkår og -avtaler er så lange og kompliserte at de aller fleste ikke leser dem. Forbrukerrådet har tidligere vist hvordan vilkårene til et utvalg av de mest vanlige appene på en telefon ville tatt 24 timer å lese høyt.[61]

Mengden tekst og høy kompleksitet gjør det derfor tilnærmet umulig å vite hva man godtar. I offentlig sektor er det i tillegg sjelden det finnes alternative tjenestetilbydere, så man er nødt til å godta vilkårene for å kunne få tilgang til tjenestene. Alle sidene Teknologirådet har undersøkt har egne

[59] Hentet fra personvernerklæringen på bufdir.no
https://bufdir.no/Personvern/personvern_og_cookies_pa_bufdir.no/
[60] https://www.sivilombudsmannen.no/om/
[61] Forbrukerrådet (2016b)

personvernerklæringer, men i mange tilfeller henviser de også videre til leverandørenes egne retningslinjer:

> *«Vi bruker analyseverktøy fra Google Analytics og Hotjar på vår hovedside www.forskningsradet.no. Ved å lukke meldingsboken som kommer opp når du besøker nettsiden samtykker du i bruken vår av informasjonskapsler ("cookies"), og du samtykker i at Google Analytics sine retningslinjer for personvern også gjelder for denne behandlingen.»*[62]

Det er dermed svært utfordrende for brukeren å få innsikt i de faktiske konsekvensene av datainnsamlingen og -behandlingen fordi man må besøke nettstedets leverandører for å kunne sette seg inn i dette.

Også Forbrukertilsynet, som blant annet arbeider nettopp med å forebygge urimelige vilkår i kontrakter[63], bruker sporingsverktøy fra Google. I sin personvernerklæring henviser Forbrukertilsynet videre til Googles personvernvilkår og skriver at brukere på deres nettsider også må godta Googles vilkår.

På noen nettsteder inneholder personvernerklæringen ingen informasjon om informasjonskapsler i det hele tatt, som for eksempel Direktoratet for samfunnssikkerhet og beredskap og Valgdirektoratet, selv om verktøyet Blacklight viser at nettsidene inneholder flere informasjonskapsler.

Et annet gjennomgående eksempel er at sidene lister opp informasjonskapslene som brukes, men ikke nevner at man også bruker Facebook Pixel, som hos Kompetanse Norge og Medietilsynet. Gitt Facebooks frynsete rykte når det gjelder behandling av persondata, er det uheldig at Medietilsynet, som blant annet har i oppdrag å veilede barn og unge i bruk av digitale medier[64], deler sporingsdata med Facebook.

Andre nettsteder har mye informasjon i sin personvernerklæring, men med en så komplisert fremstilling at det er nærmest uforståelig. Innovasjon Norge presenterer for eksempel en lang tabell på engelsk som lister opp informasjonskapsler som brukes, og deres formål, uten nærmere forklaring på hva dette innebærer.[65]

---

[62] Hentet fra personvererklæringen på forskningsradet.no
https://www.forskningsradet.no/bunntekst/personvernerklaring/
[63] https://www.forbrukertilsynet.no/om-forbrukertilsynet
[64] https://www.medietilsynet.no/om/vare-oppgaver/
[65] Se oversikten her https://www.innovasjonnorge.no/no/privacydeclaration/cookies/

Selv der personvernerklæringene er enkelt forklart er det vanskelig for brukeren å vite hva sporing på nett egentlig innebærer. Et enkeltbesøk på en nettside kan virke som en liten og ubetydelig bit av informasjon å gi fra seg. Det totale bildet av all nettaktivitet blir imidlertid svært detaljert, særlig når det er en dominerende aktør som får tilgang på all informasjonen.

OFFENTLIG SEKTOR BIDRAR TIL UHELDIG MARKEDSDOMINANS

Overvåkingsøkonomien domineres av en håndfull internasjonale selskaper, hvor Google og Facebook er to av de største. Både i Norge og internasjonalt jobbes det med konkurransepolitikk for å begrense dominansen fra de store internettselskapene.

Som beskrevet over skaper denne dominansen en monopollignende markedssituasjon som kan hindre andre selskaper i å etablere seg, og hindre innovasjon. De samme tendensene ser man når det kommer til tjenester for nettstatistikk. Google Analytics er så dominerende at det er vanskelig for andre, kanskje mer personvernvennlige aktører, å etablere seg på feltet. I tillegg er det vanskelig å konkurrere mot noen som tilbyr tjenestene sine gratis.

Innovasjon Norge skal bidra til nyskaping i arbeidslivet og vekst for norske selskaper. Likevel bruker de gratisverktøy fra både Google og Facebook på sine nettsider, noe som motvirker innovasjon i den digitale økonomien. Også Digitaliseringsdirektoratet, som blant annet skal bidra til hensiktsmessig digitalisering av samfunnet og være en premissgiver for innovasjon i offentlig sektor, bruker tjenester fra Google.

Sett i lys av det politiske ønsket om å jobbe mot de store selskapenes digitale dominans, burde ikke offentlige aktører støtte opp om de internasjonale selskapene og forretningsmodellene i overvåkingsøkonomien.

HVA KAN GJØRES?

Offentlig sektor bør gå foran og ta aktive grep for å minimere innsamling og sporing av brukere på nett.

Overvåkingsøkonomien har allerede gått for langt. Forretningsmodellen der data om brukerne kjøpes og selges mange ganger om dagen innebærer inngrep i personvernet som er dypt problematiske. Det er behov for regulering og håndheving som beskytter persondata og gjør slutt på at dette er valutaen i en global industri.

Offentlig sektor bør gå foran og ta et særskilt ansvar for å gi innbyggerne gode, digitale tjenester – uten at kommersielle aktører ser oss over skulderen.

MINIMER DATAINNSAMLING OG GI GOD INFORMASJON

Flere av nettstedene argumenterer med at de er avhengige av å samle inn data for å kunne tilby brukervennlige nettsteder. Brukervennlighet er et viktig aspekt av digitaliseringen av offentlige tjenester, og analyse av brukerdata er forståelig nok et viktig element for å kunne tilby dette.

Likevel er det problematisk at mange nettsteder ser ut til å veie dette tyngre enn beskyttelsen av brukernes personvern. Når de fleste av nettstedene i tillegg bruker gratistjenester fra de største aktørene i overvåkingsøkonomien, svekkes dette argumentet ytterligere.

Samtidig er det svært vanskelig, tidkrevende og dyrt å lage en nettside, nyhetsbrev eller andre digitale tjenester helt uten sporing av brukerne. The Markup, som har utviklet verktøyet Teknologirådet har brukt i arbeidet med denne rapporten, har brukt mer enn 500 000 kroner på å utvikle egne, sporingsfrie verktøy, fordi de ikke finner slike løsninger på markedet.[66] Eksisterende verktøy for å bygge nettsider og nyhetsbrev, spille av video og samle inn donasjoner, sporer som regel brukeren, uten mulighet til å skru dette helt av.

Her kan offentlig sektor, som en aktør med stor innkjøpsmakt, gå foran og aktivt velge og oppmuntre til utvikling av løsninger og verktøy som følger personvernprinsippene. Slik kan det samles inn minimalt med data, og kun til helt spesifikke formål. Personvernvennlige løsninger bør bli et konkurransefortrinn, heller enn en mangel på markedet.

Hvis en først skal samle inn data, må man kunne forklare formålet med sporingen på en enkel og tydelig måte. Dette er langt fra tilfelle i dag. Offentlig sektor bør derfor jobbe for å etterleve kravet i ekomloven om at det skal informeres klart og tydelig om innsamling og bruk av data gjennom informasjonskapsler. De fleste av nettsidene vi har undersøkt har personvernerklæringer med kun generelle beskrivelser av hvordan de bruker informasjonskapsler og sporingsverktøy.

STATEN BØR BETALE MED PENGER, IKKE INNBYGGERNES DATA

Når Google tilbyr sine analysetjenester gratis, er det ikke fordi de ønsker å være snille, men fordi de ser en verdi i dataene som samles inn gjennom verktøyet.

Selv om Google Analytics er den mest utbredte løsningen for analyse av nettbesøk, finnes det alternativer.[67] At disse koster penger bør ikke være god nok grunn til å fortsette å fôre Google og Facebook med data om oss.

Offentlig sektor må ta et aktivt valg om å ikke delta i overvåkingsøkonomien, og betale for verktøyene de bruker med penger – ikke med innbyggernes data. Dette kan også føre til en stimulering av markedet, ved at etterspørselen etter personvernvennlige løsninger etterspørres i større grad.

[66] Angwin, Julia (2020)
[67] Schwab, Katharine (2019)

VURDER ET FORBUD MOT MIKROMÅLRETTING

En av grunnene til at det samles inn data, er fordi det brukes til målrettet markedsføring. Det finnes allerede mange eksempler på hvordan slike teknikker for persontilpassing og mikromålretting er med på å påvirke demokratier og samfunnsstrukturer i hele verden.[68] Valgpåvirkning, desinformasjonskampanjer og skjult diskriminering er bare noen eksempler.

EU-parlamentet kaller slik detaljert målrettet markedsføring for en av de mest ødeleggende praksisene på nett i dag. De har bedt kommisjonen presentere forslag til hvordan dette kan reguleres på en mer effektiv måte, og blant annet foreslå hvordan man kan gjennomføre en utfasing og etter hvert et forbud mot mikromålretting.[69] I Norge har Venstre tatt til orde for et slikt forbud i sitt forslag til partiprogram.[70]

Det finnes allerede alternative metoder for digital annonsering som kan erstatte bruken av persondata til målrettet markedsføring. Såkalt kontekstuell annonsering innebærer at annonser plasseres basert på innholdet på en nettside, ikke hvem brukeren er.[71] For eksempel kan en reklame for norske gulrøtter plasseres ved en oppskrift for gulrotkake, eller reklame for strømming av lydbøker plasseres i et intervju med en forfatter.[72]

Et forbud mot å bruke persondata i annonser kan også bidra til å bedre konkurransesituasjonen. Ved å frata selskaper som Google og Facebook deres største fordel (persondata), kan andre selskaper i annonsemarkedet konkurrere på likere vilkår.

[68] Bayer, Judit (2019)
[69] European Parliament (2020)
[70] Veberg, Anders (2020)
[71] Iwańska, Karolina (2020)
[72] Eksemplene er hentet fra Kobler, et norsk selskap innen kontekstuell annonsering

REFERANSER

Angwin, Julia (2020) *Paying the Privacy Price*. Newsletter from The Markup, 12. desember 2020.
Hentet fra: https://www.getrevue.co/profile/themarkup/issues/paying-the-privacy-tax-298830

Baisotti, Valentina (2019) *Måten du taster på kan avsløre mye om hvem du er*. NRK.no, 23. januar 2019.
Hentet fra: https://www.nrk.no/vestland/maten-du-taster-pa-kan-avslore-mye-om-hvem-du-er-1.14392572

Barne-, ungdoms- og familiedirektoratet (udatert) *Personvern og cookies på Bufdir.no*. Lest oktober 2020.
Hentet fra: https://bufdir.no/Personvern/personvern_og_cookies_pa_bufdir.no/

Bayer, Judit (2019) *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*. EUs Policy Department for Citizens' Rights and Constitutional Affairs, februar 2019.
Hentet fra: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf

Brin, Sergey og Lawrence Page (1998) *The Anatomy of a Large-Scale Hypertextual Web Search Engine*
Hentet fra: http://infolab.stanford.edu/~backrub/google.html

Briz, Nock (2018) *This is Your Digital Fingerprint*. Mozilla.org, 26. juli 2018
Hentet fra: https://blog.mozilla.org/internetcitizen/2018/07/26/this-is-your-digital-fingerprint/

Chen, Brian X. (2019) *«Fingerprinting» to Track Us Online Is on the Rise. Here's What to Do*. New York Times, 3. juli 2019.
Hentet fra: https://www.nytimes.com/2019/07/03/technology/personal-tech/fingerprinting-track-devices-what-to-do.html

Christl, Wolfie (2017) *How Companies Use Personal Data Against People*. Cracked Lab, oktober 2017.
Hentet fra: https://crackedlabs.org/en/data-against-people

Consumer Reports (2020) *Platform Perceptions. Consumer Attitudes On Competition and Fairness in Online Platforms.*
Hentet fra: https://advocacy.consumerreports.org/wp-content/uploads/2020/09/FINAL-CR-survey-report.platform-perceptions-consumer-attitudes-.september-2020.pdf

Court of Justice of the European Union (2020) *Judgment in Case C-311/18. Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*
Hentet fra: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

Datatilsynet (2021) *Varsel om overtredelsesgebyr til Grindr*.
Hentet fra: https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/varsel-om-overtredelsesgebyr/

Datatilsynet (2020) *Privacy Shield-avtalen mellom USA og EU/EØS er opphevet*.
Hentet fra: https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/privacy-shield-avtalen-mellom-usa-og-eueos-er-opphevet/

Datatilsynet (2018) *Verktøy for statistikk og analyse av nettsider*.
Hentet fra: https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/webanalyse/

Digitaliseringsdirektoratet (udatert) *Digitalt førstevalg*. Lest oktober 2020.
Hentet fra: https://www.difi.no/fagomrader-og-tjenester/digitalt-forstevalg

Drange, Jan Morgen og Vebjørn Søndersrød (2020) *Digital markedsføring i Norge i skvis mellom EU og USA*. Dagens Næringsliv, 23. september 2020. Hentet fra: https://www.dn.no/innlegg/markedsforing/annonsering/anfo-annonsorforeningen/innlegg-digital-markedsforing-i-norge-i-skvis-mellom-eu-og-usa/2-1-879751

Ekeberg, Ingrid (2019) *Amedia og Aller Media tar opp annonsekampen mot Google og Facebook: Oppretter eget selskap*. Dagens Næringsliv, 21. juni 2019.
Hentet fra: https://www.dn.no/reklame/aller-media/amedia/dag-sors-dahl/amedia-og-aller-media-tar-opp-annonsekampen-mot-google-og-facebook-oppretter-eget-selskap/2-1-625425

eMarketer (2020) *Digital Ad Spending Worldwide, by company, 2019-2020*.
Hentet fra: https://www.emarketer.com/chart/234937/digital-ad-spending-worldwide-by-company-2019-2022-billions

European Parliament (2020) *REPORT with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL))*.
Hentet fra: https://www.europarl.europa.eu/doceo/document/A-9-2020-0177_EN.pdf

Facebook (udatert) *Find out What's Popular on Your Website with the Facebook Pixel*. Lest oktober 2020.
Hentet fra: https://www.facebook.com/business/learn/lessons/overview-of-how-facebook-pixels-work?course_id=314938442554416&curriculum_id=726377631115881

Federal Trade Commission (2020) *FTC sues Facebook for Illegal Monpolization*. Federal Trade Commision, 9. Desember 2020.
Hentet fra: https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization

Fedorovicius, Julius (2020) *Google Tag Manager vs Google Analytics: What's the difference?* AnalyticsMania, 16. juli 2020.
Hentet fra: https://www.analyticsmania.com/post/google-tag-manager-vs-google-analytics/

Forbrukerrådet (2020) *Out of control. How consumers are exploited by the online advertising industry*.

Hentet fra: https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf

Forbrukerrådet (2018) *Facebook og Google manipulerer oss til å dele personinformasjon.*
Hentet fra: https://www.forbrukerradet.no/siste-nytt/facebook-og-google-manipulerer-oss-til-a-dele-personinformasjon/

Forbrukerrådet (2016a) *Norske kommuner svikter innbyggernes personvern.*
Hentet fra: https://www.forbrukerradet.no/vi-mener/2015/fpa-digital-2015/norske-kommuner-svikter-innbyggernes-personvern/

Forbrukerrådet (2016b) *Du må lese over en kvart million ord med appvilkår.*
Hentet fra: https://www.forbrukerradet.no/vi-mener/2015/fpa-digital-2015/du-ma-lese-over-en-kvart-million-ord-med-appvilkar/

Foroohar, Rana (2019) *Don't be evil. How Big Tech betrayed its founding principles – and all of us.* New York, Penguin Random House

Google (udatert) *Data sharing settings.* Hentet oktober 2020
Hentet fra: https://support.google.com/analytics/answer/1011397/

Jørgenrud, Marius (2013) *Datatilsynet godtar Google Analytics.* Digi.no, 6. februar 2020.
Hentet fra: https://www.digi.no/artikler/datatilsynet-godtar-google-analytics/198644

Iwańska, Karolina (2020) *TO TRACK OR NOT TO TRACK? Towards privacy-friendly and sustainable online advertising*. Panoptykon Foundation, november 2020
Hentet fra: https://en.panoptykon.org/privacy-friendly-advertising

Jørgenrud, Marius (2012) *Ulovlig å bruke Google Analytics.* Digi.no, 20. august 2012.
Hentet fra: https://www.digi.no/artikler/ulovlig-a-bruke-google-analytics/204856

Kassner, Michael (2017) *Session-replay scripts disrupt online privacy in a big way*. Tech Republic, 26. desember 2017.
Hentet fra: https://www.techrepublic.com/article/session-replay-scripts-are-disrupting-online-privacy-in-a-big-way/

Kaspersky (udatert) *What is Keystroke Logging and Keyloggers?* Lest oktober 2020.
Hentet fra: https://www.kaspersky.com/resource-center/definitions/keylogger

Kemp, Katharine (2019) *Concealed Data Practices and Competition Law: Why Privacy Matters*. UNSW Law Research Paper No. 19-53 (2019)
Hentet fra: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3432769#

Konkurransetilsynet (2019) *Cookie Policy*.
Hentet fra: https://konkurransetilsynet.no/cookie-policy/

Konkurransetilsynet (2017) *Strategiplan for Konkurransetilsynet 2017-2021*.
Hentet fra: https://konkurransetilsynet.no/wp-content/uploads/2019/07/Strategiplan-2017-2021.pdf

Lomas, Natasha (2020) *IAB Europe's ad tracking consent framework found to fail GDPR standard*. TechCrunch, 16. oktober 2020.
Hentet fra: https://techcrunch.com/2020/10/16/iab-europes-ad-tracking-consent-framework-found-to-fail-gdpr-standard/

McDougall, Simon (2020) *Blog: Adtech - the reform of real time bidding has started and will continue*. Information Commissioner's Office, 17. januar 2020.
Hentet fra: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/blog-adtech-the-reform-of-real-time-bidding-has-started/

Meld. St. 27 (2015–2016) *Digital agenda for Norge — IKT for en enklere hverdag og økt produktivitet*. Melding til Stortinget 15. april 2016.
Hentet fra: https://www.regjeringen.no/no/dokumenter/meld.-st.-27-20152016/id2483795/

Nasjonal kommunikasjonsmyndighet (2020) *Informasjonskapsler/cookies*.
Hentet fra: https://www.nkom.no/internett/informasjonskapsler-cookies

NOYB (2020) *101 Complaints on EU-US tranfers filed*.
Hentet fra: https://noyb.eu/en/101-complaints-eu-us-transfers-filed

Nærings- og fiskeridepartementet (2020) *Konkurransetilsynet (KT) – tildelingsbrev 2020*.

Hentet fra: https://konkurransetilsynet.no/wp-content/uploads/2020/01/Tildelingsbrev-2020-Konkurransetilsynet.pdf

Paul, Kari (2020) *Texas and other states sue Google for abusing "monopolistic power"*. The Guardian, 16. desember 2020
Hentet fra: https://www.theguardian.com/technology/2020/dec/16/google-lawsuit-texas-monopolistic-power

Schwab, Katharine (2019) *It's time to ditch Google Analytics*. Fast Company, 1. februar 2019.
Hentet fra: https://www.fastcompany.com/90300072/its-time-to-ditch-google-analytics

Shead, Sam (2019) *Facebook owns the four most downloaded apps of the decade*. BBC, 18. desember 2019.
Hentet fra: https://www.bbc.com/news/technology-50838013

Solsman, Joan E. (2018*) YouTube's AI is the puppet master over most of what you watch*. Cnet, 10. Januar 2018.
Hentet fra: https://www.cnet.com/news/youtube-ces-2018-neal-mohan/

Statista (2020) *The 100 largest companies in the world by market capitalization in 2020*.
Hentet fra: https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/

Steel, Emely (2013) *Financial worth of data comes in at under a penny a piece*. Financial Times, 12. juni 2013.
Hentet fra: https://www.ft.com/content/3cb056c6-d343-11e2-b3ff-00144feab7de

Subcommittee on antitrust, commercial and administrative law of the committee on the judiciary (2020) *Investigation of competition in digital markets*.
Hentet fra: https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf

Teknologirådet (2016) *Personvern. Tilstand og trender*.
Hentet fra: https://teknologiradet.no/publication/personvern-trender-2016/

The Competition and Markets Authority (2020) *Online platforms and digital advertising. Market study final report.*
Hentet fra: https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf

The European Consumer Organisation (2019) *Access to consumers' data in the digital economy.*
Hentet fra: https://www.beuc.eu/publications/beuc-x-2019-068_european_data_policy.pdf

The Verge (2019) *What is a tracking pixel and can strangers really spy on me through email? Everything you need to know about the invisible e-mail tool that tracks you.* The Verge, 3. juli 2019
Hentet fra: https://www.theverge.com/2019/7/3/20681508/tracking-pixel-email-spying-superhuman-web-beacon-open-tracking-read-receipts-location

Veberg, Anders (2020) *Venstre vil forby målrettet reklame mot barn og unge.* Aftenposten, 23. November 2020.
Hentet fra: https://www.aftenposten.no/kultur/i/nA9Xzo/venstre-vil-forby-maalrettet-reklame-mot-barn-og-unge

Véliz, Carissa (2020) *Privacy is Power. Why and how you should take back control of your data.* London, Penguin

Vollan, Mari Brenna (2020) *Åpner for norsk it-skatt.* Klassekampen 13. januar 2020.
Hentet fra: https://arkiv.klassekampen.no/article/20200113/ARTICLE/200119987

W³Techs (2020) *Usage statistics and market share of Google Analytics for websites.*
Hentet fra: https://w3techs.com/technologies/details/ta-googleanalytics

Wakefield, Jane (2017) *More than 480 web firms record "every keystroke".* BBC, 21. November 2017.
Hentet fra: https://www.bbc.com/news/technology-42065650

Whatagraph (2019) *What is a tracking pixel and how does it work?*
Hentet fra: https://whatagraph.com/blog/articles/tracking-pixel

Which? (2018) *Control, Alt or Delete? The future of consumer data*. Hentet fra: https://www.which.co.uk/policy/digital/2659/control-alt-or-delete-the-future-of-consumer-data-main-report

Wired (udatert) *The Cambridge Analytica Story, Explained*. Lest oktober 2020. Hentet fra: https://www.wired.com/amp-stories/cambridge-analytica-explainer/

Zuckerman, Ethan (2014) *The Internet's Original Sin. It's not too late to ditch the ad-based business model and build a better web*. The Atlantic 14. august 2014. Hentet fra: https://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041/