

Forside

Bacheloroppgave

Studieprogram: BSSBAC - Sosiologi

Opptaksår: 2018/2019

Er oppgaven konfidensiell? (skriv X) NEI: X JA: _____

Kan oppgaven benyttes til undervisningsformål (anonymt)? JA: X NEI: _____

Forfatter(e)

| Studentnr (6 siffer) | Kandidatnr (4 siffer) | Navn: |
|----------------------|-----------------------|------------------------|
| 250811 | 4179 | Daniel Laupstad |
| 248990 | 4149 | Asger Sejrup Mikkelsen |

Oppgavens tittel:

Overvåkningskapitalismens gryende problemer i kjølvannet av Cambridge Analytica-skandalen:

- Et innblikk i atferdsdata og dens maktdannelse

Surveillance Capitalisms rising problems in light of the Cambridge Analytica-scandal:

- An insight into behavioral data and its creation of power

Veileder: Terje Hillesund

Sammendrag

Denne oppgaven har hovedfokus på hvordan overvåkningskapitalismen skaper atferdsdata som er med på å danne et maktforhold mellom teknologiselskaper og bruker. Det begynner med Shoshana Zuboffs bok om overvåkningskapitalismen, som handler om innsamling av atferdsdata. Her kommer det frem hvilke operasjonsmønstre som ligger til grunn for innsamlingen og hvilken tanke overvåkningskapitalismen er bygd på. Videre skal vi drøfte risikoer og konsekvenser knyttet til innhøsting, lagring og bruk av brukernes atferdsdata på sosiale medier og plattformer i lys av Cambridge Analytica-skandalen. Vi vektlegger Facebook, siden Cambridge Analytica-skandalen oppsto på dette sosiale mediet og utgjør en stadig større rolle i samfunnet som et informerende og nyhetsdekkende sosialt nettverk. Ved hjelp av Ulrich Becks teori om risikosamfunn ser vi på hvilken betydning Cambridge Analytica-skandalen kan ha på politiske valg, brukeres autonomi og demokratiets integritet. Vi skal også se litt på brukeren selv, og hvilke sosiale, psykiske og helsemessige konsekvenser som kan forekomme av et økende digitalisert samfunn. Til slutt går vi inn på Michel Foucaults forståelse av makt- og kunnskap gjennom hans teorier om panoptikonet, normalisering og maktforhold. Personvern er et sentralt tema og vi er kort innom meninger rundt personverndebatten, og drøfter enkelte løsninger som kan være nødvendige. Denne oppgaven har som hovedmål å belyse, drøfte og diskutere den digitaliseringen som teknologiselskapene utvikler, og bruke dette til å stille spørsmål rundt overvåkningskapitalismen og hvilke konsekvenser dette kan ha på samfunnet både på individnivå og i sin helhet.

Innholdsfortegnelse

| | |
|--|----|
| Forside | 1 |
| Sammendrag | 2 |
| Innholdsfortegnelse | 3 |
| Innledning..... | 4 |
| Overvåkningskapitalismens operasjonsmønster..... | 6 |
| Logikken..... | 8 |
| Produksjonsmidlene | 8 |
| Produktene | 9 |
| Markedsplassen..... | 9 |
| Risikosamfunn | 11 |
| Individuell risiko | 12 |
| Disiplinering og normalisering..... | 15 |
| Panoptikonet og Facebook..... | 15 |
| Cambridge Analytica..... | 18 |
| Opprinnelse | 18 |
| Cambridge Analytica sin metodikk | 19 |
| Innflytelse og betydning..... | 19 |
| Brukeren på nettet | 21 |
| Brukeren som råvare..... | 21 |
| To grupperinger..... | 22 |
| Maktforholdet | 23 |
| Instrumentarisme..... | 24 |
| Konsekvenser og regulering | 25 |
| Politiske konsekvenser | 27 |
| Psykiske konsekvenser | 28 |
| Regulering..... | 29 |
| Konklusjon | 33 |
| Referanser | 35 |

Innledning

Vi tenker ikke på privatliv hver dag, ei heller tenker vi på hvordan våre handlinger påvirker vårt privatliv. Mange vil nok makulere kontoutskriftene før de kaster dem, eller skjule pinkoden når vi handler på butikken. Det er ikke tvil om at mange vil hevde privatliv er en grunnleggende menneskerett. Selv om man føler seg trygg i eget hjem, og føler det er ganske privat, er det ikke nødvendigvis slik. Spesielt om du er tilknyttet internett, som de fleste er i år 2021. På internett ser man en aggressiv inntrengning av privatlivet. Dette handler ikke om å holde ting skjult, ikke handler det om hemmeligheter heller, det handler om valg. Internett opererer med en klar forretningsmodell, reklamering. Der brukere ikke betaler for tjenester eller innhold, ligger reklamering bak. Bak reklameringen ligger data og informasjon.

Informasjon som hvor og hvordan brukerne beveger seg på nettet blir omgjort til data. Store teknologiselskaper samler inn data om brukerne sine og deres atferd, og kaller det atferdsdata. Atferdsdataen blir så omgjort til forutsigelsesprodukter. Disse forutsigelsesproduktene kan fortelle bedriftene hvem som kan være interessert i deres produkter. Mer og mer informasjon om brukeres handlinger og går ut på å predikere ønskene deres. Dermed kan man enkelt reklamere for dette. Internett ser ut som det er gratis, men det er det ikke. For at Google skal tilby sin søkemotor og at Facebook skal gi oss mulighet til å holde kontakten med våre venner er vi nødt til å ofre våre personlige opplysninger, vår atferd og data blir lagret. Informasjon om hva, når, hvor og hvordan vi gjør ting på Google eller Facebooks tjenester. Shoshana Zuboff kaller denne prosessen for overvåkningskapitalisme.

Overvåkningskapitalismen tar for seg en ny råvare, og denne gang er det brukeren selv som er objektene denne råvaren blir utvinnet fra (Zuboff, 2019, s. 21). Overvåkningskapitalismen i lys av Cambridge Analytica skandalen viser at denne utviklingen kun startet som en måte å akkumulere profitt, men at den i dag har utviklet seg til flere felt i samfunnet, slik som politikken. Teknologiselskaper slik som Facebook og Google har såpass store mengder data om brukere, informasjon som er med på å identifisere oss geografisk, sosialt og politisk. Folk flest er nok ikke klar over hvor stor påvirkningskraft disse dataene kan ha på personer.

Cambridge Analytica-skandalen har satt personverndebatten mer på dagsordenen, men det viser seg at mange brukere fortsatt ikke ser på det som problematisk at det finnes så mye informasjon om seg selv på nettet. Informasjon som viser at gigantene vet mer om deg enn dine nærmeste venner og familie gjør. Vi vil gjennom oppgaven se litt på hvilken påvirkningskraft

teknologiselskaper slik som Facebook og Google kan ha på enkeltindivider gjennom atferdsdata. I lys av Cambridge Analytica skandalen vil vi se på hvilke politiske og samfunnsmessige konsekvenser dette kan ha gjennom Ulrich Becks risikosamfunnsperspektiv. Gjennom målrettede reklamer kan store teknologiselskaper med store mengder data være med på å svekke integriteten til den demokratiske prosessen. Samtidig tar vi for oss noen psykologiske perspektiver, særlig gjennom Michel Foucaults teori om disiplinering og normalisering samt panoptikonet, som utdyper hans forståelse av maktforholdet. Gjennom denne analysen vil vi belyse Facebooks maktforhold til brukeren, og hvordan sosiale medier generelt kan påvirke mennesker.

Overvåkningskapitalismens operasjonsmønstre

Google satte seg tidlig på 2000-tallet i førersetet for informasjonskapitalismens standardmodell, som over tid utviklet seg til overvåkningskapitalismen. Informasjonskapitalismen og overvåkningskapitalismen er begreper som kan brukes om hverandre, men vi går ut fra at overvåkningskapitalismen brukes som et begrep for standardmodellen av informasjonskapitalismen. Standardmodellen stammer fra Googles tidlige start innen annonsesalg. I 2003 leverte de et patent som stod for at Google skulle «Generere brukerinformasjon for målrettede annonser» og at denne innovasjonen skulle «etablere informasjon om brukerprofil og bruke denne for annonselevering» (Zuboff, 2019, s.95). Produktet ble kalt AdWords. En oppfinnelse som stadig avdekker nye muligheter for å utlede enkeltindividers og gruppers tanker, følelser, intensjoner og interesser gjennom en enveiskanal (Zuboff, 2019). Med enveiskanal mener hun at de enkeltindividene det gjaldt, ikke var klar over det eller samtykket. Google ønsket ikke kun å se etter muligheter for å forbedre sine egne tjenester, men så også etter muligheter for å finne hvilke reklamer som passet til brukernes interesser.

Overvåkningskapitalismen er begrepet brukt om selve standardmodellen for informasjonskapitalismen. Overvåkningskapitalisme omtaler prosessen med å omgjøre råmateriale til data, også kalt atferdsdata (Zuboff, 2019, s. 18). Atferdsdata refererer til informasjonen som blir produsert og prosessert når man beveger seg på internett. Enhver enhet som kan koble seg til internett, slik som PC-er eller smarttelefoner kan produsere data på vegne av deg. I tillegg til dette vil også tastetrykkene man foretar seg inne på nettsidene kunne bli lagret og omgjort til et datasett. Videre er det slik at atferdsdata ser på ting som hvilke nettsider man besøker eller hvilke apper man laster ned. Her vil man kunne finne hvor, når og hva man trykket på inne på nettsiden. Altså vil atferdsdata være informasjon om enkeltpersoners atferdsmønstre på internett.

Se for eksempel på Anders, som ønsker å kjøpe seg ny bil. Han plotter derfor inn "BMW" i Googles søkefelt. Han trykker inn på en av lenkene til en bilforhandler, og dermed vet Google at Anders ser hos bilforhandlere etter biler av typen BMW. Allerede har Google samlet inn en del data om Anders sin atferd på nettet. Først og fremst vil disse dataene brukes til å forbedre Google sine tjenester, men å utvikle sine egne tjenester bruker bare en bit av all dataen som blir samlet inn. De voksende lagrene av data skulle gjenbrukes til å forbedre inntjeningsmulighetene for både Google og annonsørene (Zuboff, 2019, s.93).

Atferdsdataen som kunne brukes til noe mer enn en simpel forbedring av tjenester, representerte et overskudd, og det var dette Zuboff kalte et atferdsoverskudd. Det er et overskudd fordi det er mer enn Google selv trenger for å utvikle sine tjenester. Atferdsoverskuddet blir eid av bedriften og brukes videre til avanserte produksjonsprosesser, kalt maskinintelligens:

«Et begrep som omfatter maskinelle læreprosesser, "klassisk" algoritmeproduksjon og mange andre dataoperasjoner som ofte omtales med andre begreper slik som "prediktiv analyse" eller kunstig intelligens. Blant disse operasjonene henviser Google til sitt arbeid med oversettelse av språk, telagjenkjenning, billedbearbeiding, rangordning, statistiske modeller og forutsigelser» (Zuboff, 2019, s.83).

Det er nettopp disse maskinelle operasjonene som omsetter råmateriale i form av informasjon til et produkt av algoritmer som skal forutsi brukernes atferd (Zuboff, 2019, s. 83). Maskinintelligens handler enkelt og greit om produksjonsprosessen. I maskinintelligensen blir overskuddet bearbeidet til produkter som skal forutsi de neste stegene, altså hva vi vil gjøre nå, etterpå eller senere (Zuboff, 2019, s.18). Overskuddet brukes til å utvikle forutsigelsesprodukter som kan fortelle bedriftene hvem som kan være interessert i deres produkter.

Helt til slutt blir disse forutsigelsesproduktene solgt videre til det Zuboff (2019, s.18) kaller for atferdsmarkedet. Atferdsmarkedet består av bedrifter som ønsker å vite hva deres kunder kommer til å gjøre og dermed være forberedt på å tilby nødvendige produkter eller tjenester. Dette skaper en konkurranse inne på atferdsmarkedet som fører til at selskapene som tilbyr dette atferdsoverskuddet stadig utvikler seg og finner nye måter å anskaffe seg mer atferdsoverskudd. I tilfellet med Anders ønsker han seg bil, de kan derfor bestemme seg for å selge reklamerings-tjenester basert på atferdsdata videre, til for eksempel en annonsør eller en bilforhandler, slik at de kan tilby bilreklamer til Anders, og øke sjansene enda mer for at han kjøper en ny bil. Samtidig er det et poeng at gjennom innsamlingen av atferdsdata vil ikke selskapene bare kjenne vår atferd, de vil også forme den (Zuboff, 2019, s.19). Denne nye markedsformen bygde på at det ble mindre viktig og lukrativt å lage gode tjenester, fremfor å selge informasjon om framtidig atferd. Zuboff (2019, s.113-116) tar for seg fire punkter som skal skape et overordnet mønster for overvåkningskapitalismens operasjonsmåte:

Logikken

Vi er et middel til andres mål. Operasjonsmønsteret starter med en type underordning og hierarki, der den tidligere formen for gjensidighet mellom firma og brukere, nå ble til innsamling av atferdsoverskudd som skulle brukes til andre formål (Zuboff, 2019, s.114). Mennesker er ikke subjektene for verdirealisering, ei heller er vi produktet som Google forsøker å selge (Zuboff, 2019, s.114). I stedet blir vi brukt som de objektene man innhenter informasjon fra, der informasjon er råmateriale. Produktene til Google består av det de vet om vår atferd, og som selges videre til bestemte kunder. Google oppdaget at de kunne bruke atferdsoverskuddet på det samme markedet som de selv deltok i. Dermed bruker de atferdsdata til å skape produkter som både tar i bruk atferden for å utvikle seg, og samtidig ble rettet mot markedstransaksjoner med ekte kunder, altså annonsører (Zuboff, 2019, s.113). Det begynte som en bieffekt av at brukere foretok søk på Googles søkemotor, før Google utviklet en aggressiv jakt på informasjonen, da særlig gjennom overvåkning.

Det er dette atferdsoverskuddet hun betrakter som overvåkningsressurser (Zuboff, 2019, s.113). Det vil si, ressurser som er avgjørende i kampen for overvåkningsinntekter og som videre omgjøres til kapital. Logikken i denne kapitaldannelsen er det som mer konkret omtales som overvåkningskapitalismen, og brukes som rammeverket for et økonomisk system basert på overvåkning - en overvåkningsøkonomi. På samme måte som industrikapitalismen omgjorde naturlige råvarer til handelsvarer, ser overvåkningskapitalismen etter råstoffer i menneskenes natur for å finne opp en ny type handelsvare (Zuboff, 2019, s.114). Selve kjernen er å gjøre våre liv om til atferdsdata for å forbedre andres kontroll over oss. Uvitenhet er et sentralt aspekt: andre vil bestemme over oss før vi i det hele tatt er klar over at vi har noe de kan bestemme (Zuboff, 2019, s.114). De ønsker å styre vår atferd i en bestemt retning som er gunstig for dem, og ikke for brukerne, som bare blir brukt til utvinning av råvaren.

Produksjonsmidlene

Mulighetene i Googles maskinintelligens er basert på atferdsoverskudd, og jo mer overskudd som mates inn i dem, desto mer presise atferdsprodukter resulterer det i. "Maskinintelligens" er et begrep Zuboff bruker om den konkrete teknologien som Google bruker for å innhøste informasjon, og påpeker at det er et begrep som stadig utvikler seg (Zuboff, 2019, s.114). Det kan bety en ting i dag, og noe helt annet om ett par år. Videre sier Zuboff (2019, s. 115) også at

dagens begrep er uklart - det er veldig bredt og dekker litt for mye. Hun drar frem som et eksempel at det kan være alt fra programmer som spiller bondesjakk, til systemer som skal kunne styre hele flåter med selvdrevne biler (Zuboff, 2019, s.115). Etter hvert som flere og flere bedrifter tar i bruk Google-lignende overvåkningsmetoder og teknologi, arbeider en betydelig del av verdens eksperter innen informatikk og beslektede områder med de produktene som kan og vil øke klikktallene på målrettede annonser. Det finnes tusenvis av små og store modeller, som hver har en ny bruksmulighet for de teknologinettverkene man opererer med når det er snakk om forskning på datainnsamlingsmetoder (Zuboff, 2019, s.115). Det er disse forskjellige modellene som utgjør de kostbare og komplekse produksjonsmidlene i det 21. århundret. Hver modell som blir introdusert forsøker å komme med noe banebrytende og nyskapende. Gjennom disse modellene skal de forsøke å ikke bare forbedre klikktallene på annonser, men også styre våre handlinger og vår atferd. (Zuboff, 2019, s.115).

Produktene

Selve produktene er det kun Google som har kontroll på. Produktene er altså maskinintelligensen som bearbeider atferdsoverskuddet og gjør det om til atferdsprodukter som spår våre følelser, tanker og handlinger (Zuboff, 2019, s.116). Teknologiselskapene selger ikke råmaterialet, eller det atferdsoverskuddet som samles inn. Snarere selger de disse spådommene de kan produsere ut fra det gigantiske lageret med atferdsoverskudd de sitter på (Zuboff, 2019, s.116). Det skaper en redusert risiko for kunder som ønsker å investere i framtidig atferd. Jo mer presist dette atferdsoverskuddet er, jo mer vil kjøpere kunne tjene, og dermed vil salgsvolumet stige. Både kvaliteten i spådommen og hvor konkurransedyktig det er, kommer an på presisjonen (Zuboff, 2019, s.116). Derfor trenger de mye data. Mer data vil også hjelpe stormakter som Google og Facebook å utvikle forutsigelsesproduktene. Produkter som ønsker å kunne predikere og styre våre handlinger og atferd.

Markedsplassen

Produktene blir videre solgt på markedsplassen. En ny type marked som utelukkende handler med framtidig atferd - et atferdsmarked, som Zuboff kaller det (Zuboff, 2019, s.116). Det er her overvåkningskapitalismens profitt kommer fra. Atferdsmarkedet handler med de opplysninger

om vår atferd som kan være med å påvirke framtidig atferd. Et marked der dataene for din atferd omgjøres til spådommer for hvordan vi vil oppføre oss fremover i tid. Annonsørene spiller hovedrollen, men ideen er å ikke begrense markedet til kun disse aktørene. De første forutsigelsessystemene handler bare tilfeldigvis om annonser, på samme måte som Henry Fords masseproduksjonssystem tilfeldigvis handlet om biler (Zuboff, 2019, s.116). Systemene vil i begge tilfeller kunne brukes på mange andre områder også, skriver Zuboff videre, og allerede nå kan man se et mønster der enhver aktør med interesse for framtidig atferd kan skaffe seg tilgang til dette atferdsmarkedet (Zuboff, 2019, s.116). Atferdsmarkedet er heller ikke begrenset til din internettatferd. Andre typer atferd slik som politisk velgeratferd er også del av atferdsmarkedet.

Risikosamfunn

Risikosamfunnet kom ut i 1986, nærmest samtidig som Tsjernobylhendelsen samme året (Andersen & Kaspersen, 2013, s. 491). Tsjernobyl viste for verden at vår utvikling, våre oppfinnelser og de risikoene som er knyttet til dem stadig blir mer omfattende og farligere. Katastrofers omfang og intensitet utgjør større skader. Siden 80-tallet har verden blitt mer sammensveiset og begreper som globalisering og kosmopolitisering eksemplifiserer hvordan verden ikke lenger er inndelt til hvert sitt hjørne med ubetydelig effekt på hverandre, tvert imot (Beck, 2009, s.36). Handlinger skaper ringvirkninger og reaksjoner rundt planeten, og våre risikoer er nå blitt globale. Dette tilsier at omfanget for en mulig katastrofe har konsekvenser for alle (Andersen & Kaspersen, 2013, s. 506).

Beck argumenterer for at de triumfene vi i modernitetet hyller, den teknologiske utviklingen og alle oppfinnelsene den medbringer, har en mørk underside. Dette kommer i form av risiko, altså sannsynligheten for en katastrofe. Han mener at verden har fått en drastisk økning av risiko etter den industrielle revolusjonen og den modernitetet vi nå lever i. Han sier at jordkloden beveger seg vekk fra den første modernitet, også kalt den simplifiserte modernitet. Denne modernitetet er det han anser som det tradisjonelle og tidlig industrielle samfunnet. Beck mener at vi nå befinner oss i den andre modernitetet, som er den refleksive modernitet (Beck, 2009, s. 3). Skillepunktet mellom de to verdensordrene er at den første omhandler distribusjon og produksjon av materielle goder gjennom det industrielle samfunnet, mens den andre består av utviklingen av mulige katastrofer gjennom risikosamfunnet. Det refleksive samfunnet vil alltid være tett knyttet med risiko, utviklingen av teknologi vil skape ukjente risikoer (Beck, 2009, s. 19).

Risikoer som global oppvarming, naturkatastrofer og terrorisme er det Beck kaller vidtrekkende risikoer. De kan ikke bekjempes gjennom tradisjonell krisehåndtering, eller av en enkelt nasjon. De er oftest irreversible, og skadeomfanget er globalisert og rammer alle (Beck, 2009, s. 22). Disse katastrofene tar ikke hensyn til sosioøkonomiske posisjoner. De skaper konsekvenser for alle, riktig nok i varierende grad, men når katastrofer stadig blir mer intense vil ingen kunne unngå å bli påvirket av dem (Beck, 2009, s. 37).

Individuell risiko

Beck mener at mennesker blir stadig mer individualisert. Moderniteten har avskaffet de tradisjonelle samfunnsfunksjonene i form av yrkes-, familie- og samfunnsroller og den sikkerheten og garantiene som det tradisjonelle klassesamfunnet skapte. Han mener at steget vekk fra det simple, før-industrielle samfunnet og innføringen av moderniteten og dens refleksivitet har gjort at mennesker i større grad er autonome, og at de ikke lengre går i samme fotspor som deres forfedre (Beck, 2009, s. 92). Denne individualiseringen skaper aktørfrihet, men samtidig må aktørene forholde seg til den refleksive moderniteten. Han påstår at utdanning og mulighet for å enkelt skifte yrke og posisjon skaper en individualisering. Konkurransestyling, på den andre siden, leder til en «hver mann for seg selv»-mentalitet. Det at man ikke kan regne med hjelp utenfra, framskyver individualiseringen (Beck, 2009, s. 91-94). Man er i større grad ansvarlig for seg selv. Noe som vil si at vi ofte står mer alene i våre risikoer i dag, og har en større tendens til å klandre oss selv for dem. Med tanke på sosiale medier vil vi bli isolerte, og utfallene av en individualisert, skreddersydd reklame vil kunne ramme enda hardere når vi står alene om det. Individualisering medfører et eget ansvar, ivaretagelsen av selvet, både i fysisk og psykisk forstand blir plassert på individet.

En slik individualisering gjør oss mer påvirkelig av teknologiselskaper slik som Facebook. Psyken vår er lett mottakelig og formes ofte i underbevisstheden. Hjernen til mennesker består av belønningssystemer som driver frem dopamin. Denne kjemiske reaksjonen skaper blant annet lykkefølelse og psykisk velbehag. Denne euforien kan være avhengighetsskapende, og dermed kan fysisk og psykisk stimulans være avhengighetsskapende på lik linje. Facebook har derfor laget sosiale valuter slik som likes og kommentarer for å fremme avhengighet og eufori (Drag, 2015). Brukere på Facebook blir stadig mer sammensveiset til det sosiale mediet og Facebook har blitt en del av flere milliarder personers rutiner og hverdag. Innen denne sammensveisingen har disse valutaene blitt internalisert og normalisert. Dette har skapt ett nytt begrep: «Facebook Addiction Disorder». En tysk studie som så på Facebook Addiction Disorder i forhold til brukere viste at Facebook var avhengighetsdannende, spesielt for brukere som allerede hadde narsissisme, eller andre underliggende psykiske sykdommer. Funnene viste til økt angst, stress og et popularitetskompleks (Brailovskaia & Margraf, 2020, s. 9). Designerne av teknologiselskapene prøver bevisst å gjøre brukeren avhengig av disse sosiale valutaene i form av likes, kommentarer og visninger (Zuboff, 2019, s. 86-87). Denne akkumulasjon skal reflektere

brukerens popularitet. Brukeren begynner å knytte deres identitet med deres popularitet på sosiale medier. Denne forvrengningen av selvtiliten skaper en avhengighet der man alltid må få godkjennelse fra det man legger ut eller kommenterer for å føle seg akseptert. Dette forer egoet, og skaper narsissisme, som igjen skaper en ideal av hvem vi burde være, basert på andres innlegg, bilder og poster. Et annet begrep som kan brukes om avhengighet knyttet til Facebook er «Fear of Missing Out. Frykten for å ikke henge med, altså at brukeren alltid må holde seg oppdatert for å forstå hvordan sine nærmeste og bekjente har det og hva de finner på. Begrepene Facebook Addiction Disorder og Fear of Missing Out, tydeliggjør et problem som er spesielt knyttet til yngre brukere av sosiale medier. Når unge blir eksponert for normaliseringen av spesifikke idealer, altså hvordan man skal oppføre seg på internett, skaper dette et enormt press for å passe inn i idealene. Denne avhengigheten av digital teknologi kan øke psykiske risikoer for brukere (Croteau & Hoynes, 2019, s. 339). Risikoene blir mer vidtrekkende når vi ser på hvordan maskinintelligensen til teknologiselskapene fungerer.

Beck mener refleksiviteten som oppstår i den andre modernitet etter den industrielle revolusjonen, får en egen autonomi. Samfunnsendringene blir så omfattende, og oppfinnelsene så versatile, at de blir automatiserte vesener. De får aktørfrihet, de kan drives uten menneskelig innvirkning, og blir refleksive (Beck, 2009, s. 218). Med tanke på maskinintelligens, kan det eksemplifiseres som et Frankenstein-kompleks. Der kunstig intelligens kommer til et punkt der den selv regulerer og styrer mål og mening. Algoritmer er sosialt konstruert i den forstand at mennesker skaper dem. Det er risikoer knyttet til algoritmer. Videre innovering av en slik maskinintelligens kan gi dem egen dømmekraft og handlingsrom som ikke er planlagt eller programmert.

Maskinintelligensen til Facebook samler data om deg, de skaper en atferdsprofil som består av dine interesser og preferanser. Hvis du har søkt etter babyklær, eller lignende produkter vil du kunne bli stemplet som gravid. Facebook vil dermed begynne å vise deg reklamer som reflekterer dette. En tidligere nyhetssak viste at en Washington Post-journalist forventet barn, men på tragisk vis var barnet dødfødt. Reporteren fortsatte etter dette å motta skreddersydde reklamer basert på hennes atferdsdata som var knyttet til graviditet, noe som selvfølgelig førte til unødvendig lidelse og smerte (Cabañas et al., 2021, s. 6). Dette viser at algoritmen er designet til å plukke opp på hva du søker, skriver og ser på nå, for å så vise deg lignende produkter i framtiden.

Når våre interesser lagres og blir gjort om til en atferdsprofil, vil sensitive opplysninger slik som legning lagres og kunne brukes imot oss. De fleste myndigheter aksepterer andre legninger enn heterofili, men i land som Saudi Arabia og Nigeria er homofili ulovlig, og kan i ytterste konsekvens føre til dødsstraff. Algoritmen er så presis at i disse landene har det blitt produsert data som avdekker at to prosent av brukergruppen har homoseksualitet som interessefelt (Cabañas et al, 2021, s. 7). Sjansen for at denne typen sensitive opplysninger kommer på avveie blir stadig høyere, og risikoen knyttet til en informasjonslekkasje kan være katastrofal for homofile i land der slik seksuell orientering er straffeforfulgt.

Risikoer som teknologiselskaper skaper, med deres innhøsting og samling av store mengder data kan være problematiske, både for enkelte og større grupperinger. Beck snakker om Boomerang-effekten (Beck, 2009, s. 37). Dette betyr at konsekvenser av en større katastrofe vil merkes universalt. Om du eier, eller jobber hos teknologiselskaper, er du heller ikke skjermet for utfallet av en eventuell katastrofe. Din data blir fortsatt samlet. Det hjelper ikke at du har forståelse for logikken og virkemåten til maskinintelligens, da konsekvensene er så vidtrekkende at alle brukere vil bli påvirket av en slik katastrofe.

Denne utviklingen kan skape ringvirkninger for det Jürgen Habermas kaller den borgerlige offentlighet og sivilsamfunnet (Andersen & Kaspersen, 2013, s. 389). Når algoritmer blir brukt på samfunnsnivå, for politiske formål eller som et budbringende verktøy på et individualisert nivå kutter vi ut den offentlige debatten. Dette svekker autonomien til borgerne. Habermas mener at den borgerlige offentlighet og sivilsamfunnet fungerte som en vakthund. Slik kunne borgere ansvarliggjøre og kritisere myndigheters beslutninger. Hvis kommunikasjon og meningsdeling blir digitalisert og individualisert i form av skreddersydde budskap og ekkokammer vil denne vakthund-funksjonen svekkes, og ødelegge integriteten av demokratiet. Samfunnsvitere og aktivister trodde at internettet ville avskaffe sensur, tyranni og innbringe en ny tidsepoke som skulle kvitte seg med monotone enveiskanaler, og bryte med det tradisjonelle (Croteau & Hoynes, 2019, s. 32).

Disiplinering og normalisering

Michel Foucault sin teori om disiplin og straff ble utgitt i 1975. Teorien kan ved første glans se ut som en oppsummering av hvordan kriminelle blir straffeforfulgt gjennom historien, beskrivelser av straffemetoder som i dag anses som barbariske. Staten som hadde makt, utøvde den for å disiplinere og korrigere borgerne i det før-industrielle samfunnet og mot den industrielle revolusjon (Foucault, 2020, s. 3-32). Foucault så mye på institusjoner og maktutøvelsen som de påførte sine undersåtter, i form av fengsler, sykehus og psykiatriavdelinger. En av hans hovedobservasjoner var at maktforholdet mellom mennesker og utøvelsen av den ikke er svart og hvit. Det er ikke lenger slik at vi har en konge og en slave, den mektige og den svake, men snarere at alle mennesker har ulike former for makt og mulighet til å utøve den. Foucaults makt- og kunnskapsbegrep er tredelt. Den baseres på hierarkisering, normalisering og eksaminering. Hierarkiet lokaliserer makten der den rettmessig skal være i forhold til statens perspektiv. Normalisering standardiserer maktforholdene gjennom internalisering slik at subjektene vil forholde seg til den. Eksamineringen skal overvåke, disiplinere og opprettholde maktforholdet gjennom korrigerende og sanksjoner ved avvik (Foucault, 2020, s. 170-184). Foucault mener at moderniteten er blitt et normaliseringssamfunn, siden hele samfunnet, alt fra fengsler til skoler, har en gitt rekke av normer, regler og atferdsmønstre ethvert subjekt må forholde seg til for å unngå straff. Alle skal være disiplinert til å vite sin plass og oppføre seg der etter (Andersen & Kaspersen, 2013, s. 348). Modellen som viser hvordan subjektet forholder seg til maktbalansen som Foucault snakker om er panoptikonet. (Foucault, 2020, s. 195). Foucaults teori omhandler forbryter og rettsvesen på overflaten, men når man ser nærmere på teorien gjenspeiler den forholdet mellom stat og individ.

Panoptikonet og Facebook

Panoptikonet var en arkitekttegning som ble introdusert av Jeremy Bentham og som Foucault brukte til å forklare disiplin og normalisering. Tegningen består av et høyt vaktårn plassert i midten av et fengsel, med celler som omringer vaktårnet slik at vekten får innsyn. Vekten eller vokteren overvåker alle cellene, men de innsatte har ikke mulighet til å vite når vekten ser på dem (Foucault, 2020, s. 168). På samme måte vil brukere av Facebook alltid få deres atferd overvåket på nettet, man vet noen kan se på, men ikke når. Når innsatte er usikre på om de blir

overvåket, vil de alltid oppføre seg som om de skulle vært observert. Under vaktårnet finnes det et møterom, der innsatte kan sosialisere med hverandre. De er stadig observert, men her er overvåkning forventet siden innsatte befinner seg i offentligheten sammen med andre innsatte, samt vakter og andre arbeidere i fengselet.

Hvis vi skal forstå Facebook i lys av Foucaults fengsel, må vi ta tegningen av panoptikonet og forene det med tjenestene Facebook tilbyr. Cellene innen panoptikon kan anses som de personlige tjenestene Facebook tilbyr. Privat kommunikasjon og interaksjon brukeren har med sine relasjoner. Atferdsoverskuddet som lagres av søk og klikk, utgjør atferdsprofilen til brukeren. Dataoverskuddet brukes for å styre atferd. Overvåkningen vil gjøre brukeren paranoid, som skaper selvregulering (Foucault, 2020, s. 203). Det offentlige rommet i panoptikonet, kan gjennom Facebook bli ansett som din offentlige profil. Altså nyhetsveggen som konstant oppdateres og inviterer til kommunikasjon og meningsdanning. Brukeren har mulighet til å publisere innlegg, starte diskusjon og samtaler med andre på et offentlig rom. Brukere vet at det offentlige rommet blir overvåket, som vil fremme en naturlig selvdisiplinering. Tanken er at man vet det er noen som befinner seg i tårnet, men man vet ikke når det er noen der, derfor må man til enhver tid oppføre seg.

Et eksempel fra den fysiske verden ville være forskjellen mellom hvordan vi oppfører oss foran våre nærmeste relasjoner i enerom, og bekjente i offentligheten. Det er her vi ser normaliseringssamfunnet i praksis. Foucault sier at vi kjenner sanksjonene av normalisering når vi bryter med samfunnets eksplisitte og implisitte regler. Sanksjonen kan metaforisk beskrives som et barn som går over streken i nærvær av voksne. Når unger skjønner at de har gjort noe dumt, vil de føle skam. Foucault mente at borgere på samme vis utfører selvdisiplin når de bryter med samfunnsnormene (Foucault, 2020, s. 178).

Panoptikonet er for Foucault det verktøyet som myndigheter bruker til å disiplinere mennesker til perfekte borgere, ett ideal som fremmer spesifikke atferdsmønstre. Facebook har på samme måte en form for normalisering og disiplinering. De prøver å skape den perfekte forbrukeren, gjennom atferdsdataen de besitter om brukeren. Makt for Foucault er sammensveiset med kunnskap, og kunnskap i dag består i større grad av data. Det Zuboff kaller atferdsoverskudd, som tidligere bare var dataen som medfølgte et søk eller klikk, har i dag blitt kjernen til kunnskapen som store teknologiselskaper har om oss. Makthierarkiet mellom bruker og Facebook plasserer Facebook på toppen. Denne praksisen har i tråd med Foucaults definisjon av makt blitt normalisert og blitt et implisitt paradigme.

Facebook sitt design åpner opp for en felles konsensus, som danner en idealisert bruker. Det finnes avvik fra idealene som korrigeres, men majoriteten er tilbøyelig. Poenget er at de verdiene vi har, det vi oppfatter som rett og galt, er bestemt av verdisystemene. De dannes i vår oppvekst, men blir formet etter våre omgivelser i livets løp. Vårt verdenssyn blir gjenforsterket av samfunnet, gjennom staten, media og sist, men ikke minst, Facebook (Croteau & Hoynes, 2019, s. 195). De får en definisjonsmakt som de kan eksponere for mangfoldige milliarder brukere. Dette medfører at Facebook som regulerende organ, har laget en arena som kan normalisere sine brukere slik Foucault mente staten gjorde. Facebooks korrigerende av brukere som viker fra deres idealer og retningslinjer har paralleller med Foucaults eksamineringsbegrep. Facebooks normalisering blir som i panoptikonets eksaminering basert på overvåkingen som skal passe på at brukerne opptrer slik Facebook ønsker. Dette skjer via selvdisiplineringen som drives av paranoide brukere, som frykter at de kontinuerlig blir observert. Verktøyene Facebook bruker for å skape deres eksaminering er maskinintelligensen som samler inn atferdsdata, samt retningslinjene for plattformen. Det skaper en normalisering som fremmer overvåkningskapitalisme gjennom salg av brukernes data. De korrigerer avvikene som forekommer gjennom sensuring av en bruker, eller promotering av en annen, samt utkastning av brukere som ikke samsvarer med retningslinjene.

Cambridge Analytica

Cambridge Analytica-skandalen tilbake i 2018 kan si mye om hvor vi står i dag, Cambridge Analytica-skandalen kan forstås annerledes, basert på politisk og ideologisk ståsted. Betydningen og omfanget er svært omdiskutert, forskjellige kilder hevder at Cambridge Analytica hadde stor og liten innflytelse på det amerikanske presidentvalget i 2016. Det vi vet med en viss sikkerhet er at denne bedriften tok for seg en stor oppgave i det amerikanske valget i 2016 (Croteau & Hoynes, 2019, s. 323), og det har vært spekulasjoner om at de også var delaktig i Brexit-kampanjen i 2016, uten at man vet det med sikkerhet.

Opprinnelse

Skandalen oppsto på bakgrunn av at en dataanalytisk bedrift med navn Cambridge Analytica sto bak en rekke politiske reklamer rettet på amerikanske velgere som sto på vippen mellom å stemme på republikanerne eller demokratene under det amerikanske valget i 2016. Disse politiske reklamene ble skreddersydd ved hjelp av velgeres atferdsdata. Data som ble samlet inn uten at de var klar over det eller hadde tillatt bruk av deres personlige opplysninger. Hensikten var å overbevise velgere om å stemme på republikanerens kandidat Donald Trump (Hinds, Joinson, Williams, 2020, s. 1). Trump-kampanjen ansatte Cambridge Analytica med den hensikt å bruke dataen de satt på for å rette reklamer og meldinger mot spesifikke personer (Croteau & Hoynes, 2019, s. 323).

Dataen som ble brukt kom opprinnelig fra en quiz som het «This is Your digital Life». Denne spørreundersøkelsen var en personlighetsquiz, som samlet inn personlig data om deltakerne. Når en bruker samtykket til å dele sine opplysninger, førte dette indirekte til at hele deres nettverk av venner og bekjente på Facebook også fikk deres personlige data stjålet, helt ufrivillig og ubevisst (Hinds, et al, 2020, s. 2.). Disse dataene ble samlet inn fra 200.000 villige deltakere, men tallet ble mye større når man tar inn betraktning deres sosiale krets. Omtrent 87 millioner brukere ble profilert og loggført av denne enkelte undersøkelsen (Heawood, 2018, s.1).

Cambridge Analytica sin metodikk

Effektiviteten av verktøyene Cambridge Analytica tok i bruk under presidentvalget i 2016 er omdiskutert. Gjennom deres «OCEAN» profileringsprogram, kunne de sende spesiallagde reklamer som skulle treffe spesifikke velgere under valgkampanjen. Via dette profileringsverktøyet kunne de sikte seg inn på individuelle brukere med særegne interesser, meninger og atferdsmønstre, noe som blir kalt for «micro-targeting». Slik kunne de manipulere og styre velgere som var på vippen, til å stemme på deres kandidat (Heawood, 2018, s. 1). Gjennom deres profilering kunne de også identifisere stemmere som høyst sannsynlig ikke ville stemme på Trump, men heller stemme på Hillary Clinton. Disse brukerne fikk reklamer som satte Clinton i dårlig lys, for å unngå at velgere som ikke likte Trump skulle stemme på motstanderen Hillary Clinton (Croteau & Hoynes, 2019, s. 323).

Innflytelse og betydning

Samfunnsvitere og internettaktivister argumenterer for at disse skreddersydde reklamene har liten til ingen innflytelse på brukere (Bartlett, 2019), andre mener at metodikken virket imot sin hensikt. Algoritmene som prediker hva vi er interessert i er ikke alltid riktige. Funksjonen og effektiviteten av maskinintelligensen avhenger av at atferdsoverskuddet stemmer med brukeren. I Cambridge Analytica sin «OCEAN» laget de atferdsprofiler av brukere basert på atferdsoverskudd som ble samlet inn i 2013, for å påvirke velgere i 2016. Personligheter forandres og det vi mente for tre år siden er ikke alltid det vi mener og føler i dag (Hinds, et al, 2020, 2). Jamie Bartlett, en journalist og aktivist som har dekket flere aktuelle emner rundt sosiale medier og internett, argumenterer at vi har blitt oppslukt i den ulovlige datainnhøstingen Cambridge Analytica utførte. Bartlett erkjenner ikke effektiviteten av de atferdsprofilene som ble skapt av «This is Your digital Life» spørreundersøkelsen. Han påstår at teknologien ikke er avansert nok til å brukes effektivt, men om 10-15 år vil et slikt verktøy være mulig å skape (Bartlett, 2019). Bartlett fokuserer isteden på de lovlige midlene Cambridge Analytica brukte.

Cambridge Analytica hentet informasjon fra datameglere, blad- og avis abonnenter, tv-kanaler samt all offentlig informasjon knyttet til brukeres tidligere stemmer i politiske valg. Informasjon som ble lovlig innhentet fra tredje-parter bidro også til at Cambridge Analytica kunne identifisere velgere som fortsatt var på vippen under presidentvalget i de amerikanske vippestatene. De samme velgerne som muligvis utgjorde utfallet av presidentvalget i 2016

(Bartlett, 2019). Bartlett mener derfor at vi burde se nærmere på de lovlige datainnhøstningsverktøyene disse politiske reklamebyråene besitter. Innhenting av data har utviklet seg så raskt at brukere ikke er klar over mengden sensitive opplysninger reklamebyråer som Cambridge Analytica har. Hastigheten av den digitale utviklingen har medført at rettsorganer ikke klarer å holde tritt med teknologiselskapene. Lovverket er utdatert og reguleringen foregår som om vi stadig var i det tradisjonelle før-digitaliserte mediebildet vi så for noen tiår siden (Bartlett, 2019).

Alexander Nix, tidligere CEO av Cambridge Analytica, mener at deres innflytelse under det amerikanske valget har blitt overdrevet på grunn av utfallet av USA-valget i 2016. Han hevder at Cambridge Analytica sin bruk av atferdsdata er forenlig med resten av den digitale reklamebransjen. Cambridge Analytica utførte samme standardprosedyrer innen fagfeltet som lignende bedrifter. Nix mistenkte at grunnen for at de ble målet for kritikk og kriminell etterforskning var resultatene av det Amerikanske valget og Storbritannias referendum i 2016 (Nix, 2019). Nix hevder at Cambridge Analytica utgjør en dråpe i havet med tanke på alle de andre reklamebyråene, som henter og bruker data på de samme premissene (Alexander Nix, 2019). Nix sin vitneforklaring under høringen i det britiske parlamentet frikjenner ikke Cambridge Analytica. Hans forklaring kan tyde på at Cambridge Analytica ene og alene ikke kan klandres for personvernsmisbruk, men at denne skandalen kan bidra til avdukingen av flere uetiske praksiser innen reklamebyråer og sosiale medier generelt.

Brukeren på nettet

I et stadig mer digitalisert samfunn er personvern og databeskyttelse på agendaen i de fleste kretser. Cambridge Analytica-skandalen startet debatten, og innføringen av EUs General Data Protection Regulation viser tydelig behovet for regulering, i hvert fall fra myndighetenes side. Nyhetsmediene belyser datalekkasjer, og stiller spørsmål til Facebook, Google eller andre teknologiselskaper som igjen og igjen trækker inn i lovens gråsoner. Brukeren blir pepret med nyheter om hvor utsatt de er, samt hvor håpløst det er å beskytte seg fra disse risikoene. Begrepet «privacy fatigue», beskriver følelsen av å være utmattet som følge av mangelen på kontroll over sitt eget personvern. Dette kan skape et personvernspadoks, som går ut på at vi blir mer oppmerksomme på risikoen med å dele vår data på internettet (Gerber, Gerber & Volkamer, 2018). Samtidig fortsetter vi å dele den fordi det er nyttig for oss. Personvernspadokset er vektleggingen mellom individers ønske om å beskytte personvernet, og nytten brukere får ved å dele sitt privatliv. Når vi gir teknologiselskapene innsyn, blir vi sårbare, men vi tillater det fordi vi får bedre skreddersydde tjenester og reklamer. Brukeren er uvitende om omfanget og skadepotensialet av dataen teknologiselskaper slik som Facebook og Google besitter. Alternativt er brukeren overbevist om at de ikke kan bli manipulert gjennom dataen de tillater teknologiselskapene å bruke. Noen brukere er igjen så gjennomsyret av nyheter om datalekkasjer og uetiske praksiser at de blir handlingslammet. Den videre ansvarsfraskrivelsen og mangelen på reelle sanksjoner mot teknologiselskapene resulterer i at brukere blir for maktesløse til å ivareta deres personvern (Hinds, et al, 2020, s.3).

Brukeren som råvare

Digitalisering er i stadig vekst og forandring. Internettet i sin opprinnelse var mottatt med seiersrop og glede, oppfinnelsen som skulle trumfe myndigheters styreformer. Internettet skulle knytte oss sammen på en måte vi aldri kunne ha drømt om for drøye 30 år siden. Starten på den digitale revolusjonen, oppfinnelsen av Facebook. Det sosiale nettverket som skulle bli det største verktøyet til å føre mennesker sammen og opprettholde sosiale interaksjoner. Et sosialt medium som kombinerer alle tidligere kommunikasjonsredskaper til et utrustet kommunikasjonsorgan. Røttene til det Marshall McLuhan kalte «The Global Village». Et utopia med endeløse framgangsmuligheter innen rettferdighet, demokrati og solidaritet (Croteau & Hoynes, 2019, s. 32). Uheldigvis er dette optimistiske synet ikke helt forenlig med realiteten. Facebooks mørkere trekk begynner å bli gjennomskuet. Slik som Beck spådde, er

modernitetens triumfer etterfulgt av risikoer (Beck, 2009, ss. 46-47). Facebook sitter på store mengder data om våre atferdsmønstre på nett. Bruken av personlige opplysninger kan føles som en nødvendighet for å få bedre tjenester i et innovativt, serviceorientert internettsamfunn. Spørsmålet er burde vi være så naive, og godtroende å tenke at bedrifter som Facebook bare har våre beste interesser på hjertet?

Drivkraften i teknologiselskapene er oss, aktiviteten og dataen vår er råvaren som driver Facebook og Google. Denne råvaren har de stor respekt for. Teknologiselskapene er avhengige av oss, så til gjengjeld gjør de oss avhengige av dem. Vi føler at vi må lese siste nytt, oppdatere statusen og vente på den neste kommentaren. Hvis man ikke henger med, vil man bli glemt, og vil ikke kunne kommunisere med andre som er informerte. Foucault introduserte et begrep som het «Docile Bodies», han gjengir eksempelet om hvordan en soldat blir disiplinert til å marsjere, vise tapperhet og alltid være beredt til å motta og gjennomføre ordre med kald presisjon og ufølsomhet. Soldaten blir en maskin, som adlyder dens øverst kommanderende (Foucault, 2020, s. 135). Det skapes vanedannende praksiser for å lage en eksemplarisk soldat. På samme måte kan en bruker innen Facebook bli opplært til å danne vaner som skal fremme en god forbruker og bli et automatisert vesen designet til å klikke, observere og motta informasjon slik Facebook ønsker. Brukeren er ikke en kunde, men heller kilden til råvaren som innhøstes for å lage produktet.

To grupperinger

Denne formen for individualisert, micro-målrettelse av reklamer har skapt to grupperinger. Den første grupperingen vil typisk si «jeg har ikke noe å skjule», eller «jeg liker skreddersydde reklamer, siden jeg får tilbud som passer min smak og preferanse». En studie som så på disse sidene av personverndebatten (Hinds, et al., 2020), så at brukere som ikke hadde noe imot Facebook sin metodikk var i liten grad informert, eller rett og slett uvitende om Cambridge Analytica-skandalen. Den andre grupperingen, de som var mer skeptisk og kritisk til Facebook og deres praksiser, var i kontrast paranoide for overvåkning. Kunnskapen om Facebook og Cambridge Analytica skandalen gjorde at de paranoide brukerne følte seg mere skjermet fra markedsinnflytelse og politisk manipulering (Hinds, et al, 2020, s. 6). Oppmerksomheten rundt personvern har, i større grad, gjort brukere klar over verktøyene teknologiselskapene besitter, og til en viss grad hvordan de blir rettet mot brukerne. Informasjonen vi har rundt

markedsstrategien til Facebook er overfladisk, men noen brukere blir overbevist om at de ikke er tilbøyelige til denne strategien. De har en illusjon om at de har oversikten på hvordan Facebook virker. I realiteten er dette taktikken Facebook har laget for å skape en falsk forståelse, slik at den virkelige sannheten ikke blir avduket for andre enn de som styrer den selv (Zuboff, 2019).

Maktforholdet

Nå som vi har sett på Facebooks bruk og innhenting av atferdsdata skal vi utforske makten som ligger i kunnskapen Facebook har om sine brukere. Vi skal se på paralleller mellom det Foucault observerte mellom borger og stat, og veie det opp mot maktforholdet brukeren og Facebook har. Foucault mente at makt kunne ikke utøves uten et kunnskapsgrunnlag, samtidig kunne ikke kunnskap eksistere uten at den hadde maktbetydning (Foucault, 2020, s. 27). Forholdet mellom makt og kunnskap er gjensidig, videre poengter Foucault at kunnskap ikke er begrenset til vitenskap, men kommer også i form av informasjon. Foucault prøver å forklare at makt tradisjonelt sett blir sett gjennom et fysisk og voldelig perspektiv. Fysisk makt preget det før-moderniserte samfunnet, straffen var brutal, offentlig og eksplisitt. Innføringen av fengsler som baseres på panoptikonet erstatter den fysiske og direkte maktutøvelsen med en psykisk, systematisk og individualisert maktutøvelse i form av overvåking og korrigerende. Slik skapes en usynlig og altomfattende disiplinering, som kan normalisere hele befolkningen, fra sykehuset til fengselet og alt imellom (Foucault, 2020, s. 218). Dette tillater staten innsyn i borgeres liv, samtidig får de påvirkningskraft til å skape idealer og normer.

Facebook har gjennom datainnsamling klart å skape et kunnskapsverktøy som stater og myndigheter tidligere bare kunne drømme om. De har makt over brukeren gjennom strukturen av plattformen og har muligheten til å normalisere og korrigere brukere. Slik som staten utfører disiplinering gjennom institusjoner, kan teknologiselskaper utøve disiplinering gjennom deres tjenester. Brukeren har i sitt eget perspektiv en form for autonomi. Brukeren kan la være å bruke tjenestene de blir tilbudt og redusere hvor mye data som blir innsamlet om dem. Men dette er en illusjon av makt, brukeren har i helhetlig perspektiv veldig liten kontroll over sin egen data og hvordan den blir brukt. Zuboff (2019) viser til at teknologiselskaper tjener på at brukerne føler at de har kontrollen, men bedrifter slik som Facebook og Google vet at makten er i deres hender.

Instrumentarisme

Denne implisitte kontrolleringen av brukerne kaller Zuboff instrumentarisme. Instrumentarisme fungerer via maskinintelligensen til teknologiselskapene. Frykten er at bedrifter slik som Facebook eller Google eventuelt vil klare å omstrukturere menneskets natur. Zuboff mener at instrumentarisme er en ny form for totalitarisme (Zuboff, 2019, s. 397). Instrumentarisme er påvirkning gjennom ytre omgivelser, det vi opplever, ser og hører internaliseres i vår ubevissthet og danner vår forståelse av samfunnet. Instrumentarisme kan bare fungere gjennom akkumulering av data, og tanken om at brukere på internettet forblir ubevisste om hva atferdsdataen blir brukt til. På samme måte forklarer Foucault hvordan staten gikk fra å utøve disiplin og makt gjennom vold, til å disiplinere gjennom overvåkning. Staten samlet informasjon om borgere gjennom deres institusjoner. Fengsler, skoler og sykehus ble en arena for atferdsstyring som skapte et overvåkningssamfunn der informasjon om borgeren ga staten større kontroll. Statens overvåkning av borgerne sett i lys av Zuboff sin instrumentarisme, kan tyde på at brukeren vil bli styrt på samme måte og at enhver handling fra brukeren vil kartlegges og kategoriseres slik at Facebook gjennom sin data om brukere vil skape det Foucault kalte «Docile Bodies» (Foucault, 2020, s. 141).

Konsekvenser og regulering

Hovedpoenget med reklamene er å få personer til å kjøpe produkter. Dersom atferdsdata kan brukes til å forutsi hvem som ser etter visse produkter vil man kunne innsnevre hver eneste reklame til å kun tilby de produktene hvert enkeltindivid ser etter. I eksempelet med Anders så han etter BMW, og hans reklamer vil reflektere dette. Håkon på den andre siden ser kanskje ikke etter bil, men er på jakt etter en ny støvsuger. Dette blir også vist gjennom hans atferd på internett og han vil heller få reklamer på støvsugere. Annonser blir ikke lengre rettet mot spesifikke søk, som eksempelvis en bil eller støvsuger, men blir skreddersydd basert på atferdsdataen til enkeltindividets preferanser og profil. Anders og Håkon får to vidt forskjellige reklamer som følge av deres atferdsdata, selv om de ikke er klar over det.

Enveiskanaler er et begrep Zuboff nevner i sammenheng med at brukere ikke direkte forstår at dataen deres innsamles, eller at de ikke nødvendigvis har sagt seg enig i det (Zuboff, 2019). Teknologiselskaper samler inn små og store data gjennom deres tjenester. Ting som Google Maps eller Facebooks Messenger er eksempler på tjenester, og viser at de ikke kun samler inn data gjennom å ferdes på deres nettsider, men også ved å bruke deres apper. Man legger igjen spor, som de kan utnytte til å senere forutsi hva du vil foreta deg. Det er viktig å påpeke at det ikke er selve personene man samler inn data fra som selger, de er ikke produktet i overvåkningskapitalismen, men det er dataen de produserer som er produktet. Det vil si at det er dataen og dataoverskuddet som blir brukt til tjenester av Facebook eller Google, som er den råvaren som skaper profitten, og hvis enveiskanalen slutter å være monoton, vil råvaren bli svekket (Zuboff, 2019).

Cambridge Analytica-skandalen er svært relevant i konteksten til overvåkningskapitalisme. Skandalen opererer med alle kjennetegn på overvåkningskapitalisme, den eneste forskjellen er måten de forsøker å styre atferden på. Cambridge Analytica-skandalen er mest kjent for påvirkning av politisk velgeratferd, i motsetning til Facebook sin standard – atferdspåvirkning til fordel for profitt gjennom reklamering. Brukere tenker ikke over at de holder på å bli manipulert til å stemme på spesifikke partier. Man kan stå på vippekanten mellom to partier, helt til man får en reklame rettet mot det ene partiet, som svaier stemmen over. En reklame som kun vil treffe deg, basert på hva du har søkt på tidligere på internettet, eller hvilke Facebook-grupper du er medlem av, for eksempel.

533 millioner Facebook brukere har nylig fått deres personlige opplysninger på avveie (Holmes, 2021). Risikoer blir stadig mer omfattende og katastrofale, vi kan ikke forutse eller unngå digitale katastrofer og skandaler, som Beck henviser til. Dette kan medføre konsekvenser blant forbrukere, politikk og samfunnet i sin helhet. Overvåkningskapitalismen som føres av teknologiselskapene vil stadig utvikle seg, de vil akkumulere mer kunnskap om brukeren som vil bli omformet til makt. Makten består av atferdsoverskuddet som er samlet om brukerne og danner maktgrunnlaget mellom Facebook og bruker. Facebook vil kunne gjennom maskinintelligensen, forutse våre handlinger og hva vi vil ha.

Dette kan bli problematisk hvis algoritmene som forer oss til slutt vil ha kunnskapen, teknologien og viljen til å forme oss, altså styre brukere i en retning som er gunstig for Facebook (Croteau & Hoynes, 2019, s. 330). Slik vil de kunne disiplinere, eller skape selv-disiplin blant forbrukere. Disse risikoene må håndteres snarest, ettersom utviklingen av teknologien, over tid, vil gjøre det vanskeligere å reversere utviklingen eller å skille mellom menneske og maskin. Vi vil stadig bli mer sammensveiset til teknologigigantene og ikke lenger kunne styre våre egne valg i like stor grad. Man kan være nødt til å introdusere en form for regulering (Zuboff, 2019, s. 33), gjennom upartiske organer, myndigheter eller FN. Dersom dette ikke er en mulighet må brukerne selv innføre personlige tiltak for å forebygge og forhindre deling av personlige data, noe som høyst sannsynlig ikke er nok.

Cybersikkerhetsekspert Bruce Schneier, stipendiat og foreleser ved Harvard University, viser i sin bok fra 2015 - *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* - til noen enkle tips enhver person med minimal teknologiforståelse kan foreta seg, hvis man ønsker å minske utslippene av sin atferdsdata. Det er viktig å tenke på at internettet utvikler seg raskt, og siden boken ble skrevet i 2015 kan enkelte av tipsene være litt utdaterte. Likevel vil det være en grei start når det kommer til å redusere ditt utslipp av atferdsdata. Til å begynne med vil det enkelt nok være å ikke legge ut identifiserende bilder eller innlegg på nettet. Altså å ikke tagge disse innleggene med hvor du er eller hvem som er med. I sammenheng med dette vil det å slå av stedstjenester hjelpe på, når de ikke trengs. Med dette kan ikke mobilen eller datamaskinen vite hvor du er til enhver tid, med mindre det er nødvendig. I tillegg kan man enkelt begynne å bruke andre søkemotorer, som tar vare på personvern, slik som søkemotoren DuckDuckGo. Han nevner også å ikke bruke skylagringstjenester, selv om dette gir deg muligheten for å ha alt tilgjengelig, hvor enn du er. Det er fordi disse tjenesteleverandørene, slik som Google også bruker dataen fra

skylagringstjenesten for å finne informasjon om deg. Alt kobles til din profil av atferdsdata. Til slutt kan man endre innstillingene på nettleseren, slik at du sletter informasjonskapsler, også kalt cookies, når du er ferdig på en nettside. En informasjonskapsel er en liten fil med tekst som lagres på brukerens datamaskin når man åpner en nettside. Denne kapselen brukes for eksempel til å lagre ting som innloggingsdetaljer, hva man har i handlekurven i nettbutikker eller registrere hvor man beveger seg på nettsider (Datatilsynet, 2018). Rett og slett alt som kan henvise til den atferdsdataen som samles inn. Dette betyr ikke at du blir kvitt alle problemene, men teknologiselskapene får samlet inn mindre som de senere kan bruke. For å stoppe muligheten for lekkasje av personlige data, burde likevel sterkere reguleringer innføres, slik at Facebook ikke kan bruke personlige opplysninger til å forårsake psykiske og sosiale risikoer for brukeren. Regulering vil også redusere tilfeller der større grupper med brukere blir manipulert til å stemme i form av valgkampanjer som med Cambridge Analytica og det amerikanske valget. Hvis vi skal unngå risikoer slik som Beck definerer dem, kreves det gjensidighet mellom bruker og teknologiselskaper, og et samarbeid på tvers av bedrifter, brukere og nasjonale rettsorganer.

Politiske konsekvenser

Politiske partier prøver oftest å appellere til så mange som mulig for å skape størst mulig oppslutning. De vil gi løfter for å garantere at folk stemmer på dem. Dette, sett i lys av Cambridge Analytica-skandalen, viser at dersom man forener politiske kampanjer og deres løfter i kombinasjon med utviklingen av sosiale mediers skreddersydde tilnærming av brukeren kan man skape et individualisert løfte. Hvis et politisk parti bruker Facebook til å appellere til flere brukere med forskjellige meninger kan en bruker få enkelte politiske løfter, mens en annen bruker får helt andre løfter. Dette er ikke noe revolusjonerende i seg selv, men tidligere ville alle disse reklamene ha et mål om å treffe interesse-grupper og appellere til et gitt antall mennesker. Om Cambridge Analytica sin «OCEAN» modell var så effektiv som Alexander Nix mente, eller blir det i nærmeste framtid, vil enhver bruker på Facebook kunne få egne individualiserte appeller om å stemme på partiene. Løftene som blir gitt vil baseres ene og alene på den spesifikke brukerens profil av atferdsdata, og bare være synlig for den det angår. Hvis flere brukere får hundrevis av forskjellige løfter og de stemmer basert på det, vil det nesten bli umulig å ansvarliggjøre partiet (Bartlett, 2019). Dette fordi et gitt parti muligens har gitt en bruker ett løfte, og den neste ett annet.

Videre vil denne skreddersyningen av politiske budskaper i kombinasjon med sosiale mediers algoritmer skape det som blir kalt ekkokammer (Croteau & Hoynes, 2019, s. 332). Facebook sin maskinintelligens prøver å gi brukere det de vil se, høre og lese. Hvis brukere tydeliggjør sitt politiske ståsted for Facebook vil den da gi dem kommunikasjonskanaler som tilbyr samme politiske ideologi. Dette medfører en gjenforsterking av brukerens egne oppfatninger og livssyn. I USA ser vi at disse ekkokamrene bidrar til polarisering og radikaliserings, siden man bare hører den ene siden (Croteau & Hoynes, 2019, s. 332). Brukere får ikke et kritisk innblikk eller høre andre meninger, som medfører en rivalisering. Det blir en slags «oss mot dem»-mentalitet som er startfasen på rasisme, diskriminering og undertrykking. Denne utviklingen er så dynamisk og rask at innflytelsen den har på politikk og demokrati nå og i fremtiden forblir ubevisst. Bartlett (2019) er redd for at innflytelsen av sosiale media på politikken er i ferd med å ødelegge integriteten av demokratiet. Dette er en risiko som er så stor at dersom trusselen er autentisk vil konsekvensene av et slikt utfall være både irreversible og store for legitimiteten av politiske valg og tilliten til myndigheter og regjeringer.

Psykiske konsekvenser

Vår avhengighet til en stadig mer digitalisert utvikling vil skape ringvirkninger for menneskers oppfatning og forståelse av omverdenen. En slik framtid vil bli preget av mye problematikk hos psyken til mennesker (Croteau & Hoynes, 2019, s. 339). Vi har allerede diskutert korrelasjonen mellom Facebook og psykiske problemer i form av avhengighet og påvirkning sosiale medier kan ha på psykiske lidelser. Jo mer vi forener oss med den digitale sammensveising av tjenester desto vanskeligere blir det å koble seg av, og unngå og bruke tjenestene store teknologiselskaper tilbyr.

Når vi tar inn i betraktning hvilken definisjonsmakt plattformer som Facebook, Instagram og YouTube har, og den forrang de har til å skape idealer - sånn som hvem som promoteres og hvem som dukker opp først i søk – vises det at de har makten til å kunne skape og fremme et ideelt samfunn gjennom deres funksjoner og tjenester. Vi blir altså disiplinert til å akseptere hva som er normen, og unngå å bryte med hva som er normalt. Hvis en skulle bryte med hva som er sosialt akseptert vil sanksjoner forekomme. Brukere må leve i tråd med hva som er normalisert av Facebook og gjenforsterket av andre brukere på plattformen. Facebook kombinert med overvåkningskapitalismen har skapt en dominans over brukeren. Slik

maktforholdet står nå, er det et tydelig skille mellom Facebook og brukeren. Brukeren er som tidligere nevnt en «råvare» for teknologiselskapene. Når en bruker, som er et menneske med rettigheter, blir ansett som en råvare, mister personen autonomien og aktørfriheten til å forhandle.

«Privacy fatigue» viser til en psykisk utmattelse hos brukeren. Mange mennesker som bruker tjenestene til Facebook er helt uvitende om hvordan de blir utnyttet, og hvis de forstår deler av hvordan tjenestene fungerer er dette som regel så lite at de ikke får gjort noe med det. De føler på en maktløshet siden de har ikke kontroll på deres egen atferdsdata. Gjennom personvernsparadokset tillater vi disse tjenestene å samle informasjon om oss, så lenge vi får bedre tjenester på bakgrunn av at vi gir fra oss mer personlig data.

De psykiske konsekvensene vi ser på brukere i dag, vil i framtiden bare bli mer vidtrekkende slik Beck definerer dem. I en framtid der all vår informasjon blir innsamlet og kategorisert vil vår psyke i verste fall kunne bli formet og dannet etter ønskene til de som besitter all informasjonen om oss. Slik som Foucault så på staten og borgeren vil sjansene øke for at selvdisciplin vil skje automatisk gjennom digitaliseringen vi ser i dag.

Regulering

Den digitale utviklingen går stadig raskere. Hvis vi ser tilbake på hastigheten på utviklingen av teknologi som for noen tiår siden ikke eksisterte er det grunn til å tro at den videre innoveringen av tjenestene som teknologiselskaper bruker bare kommer til å gå raskere enn tidligere. Dette er problematisk når reguleringen ikke holder tritt. Lovverket er utdatert, og konsekvensene for brudd på reglene er en dråpe i havet for teknologiselskaper som Facebook og Google (Zuboff, 2019, s. 33). De tjener så mye på utvikling og utnyttning av maskinintelligensen, at bøtene er en pris de er veldig villig til å betale. Myndigheter, land og befolkningen på global basis er i stor grad uvitende om hvor mye makt som blir tilegnet teknologiselskapene gjennom individenes personlige opplysninger. Det kan også være at enkeltindivider er fullstendig klar over hvor mye makt som ligger i det, men at ikke ønsker, eller kan gjøre noe med det.

Eksemplene som ble nevnt tidligere med Washington Post journalisten og landene Saudi Arabia og Nigeria, poengterer tydeligere at data medfører større risikoer jo mere avanserte de blir. Atferdsoverskudd har gått fra å bli sett på som lite anvendelig og overflødig til den viktigste brikken i teknologiselskapenes algoritmer. Disse selskapene pryder seg på å være innovative

og nytenkende. De skaper nye verktøy og oppfinnelser hvert år for å skape enda større datasett som igjen skaper mer informerende profiler om sine brukere. Cambridge Analytica hadde profiler på drøyt over 80 millioner brukere. Nylig fikk 533 millioner brukere dataen sin lekket, som viser at teknologiselskapene allerede sitter på enda større mengder atferdsdata. Hvis vi skal anta at de som besitter denne atferdsdataen bare har gode intensjoner vil sjansen for at dataen ender opp hos noen med mindre ærlige intensjoner være mer sannsynlig, selv om teknologiselskapene ikke er de ærligste når det kommer til overvåkning.

Det er stor mulighet for at det kommer et punkt, om vi ikke allerede er der, hvor atferdsoverskudd og overvåkningskapitalisme vil bli den nye oljen. Det er her pengene ligger. Teknologigiganter vil allerede ligge langt foran i prosessen ettersom det er her man finner atferdsoverskuddet. Facebook og Google er de største innsamlerne og dermed vil deres data styre mesteparten av atferdsmarkedet (Zuboff, 2019, s. 35). For å forhindre dette er man kanskje nødt til å gjøre reguleringer eller gjøre atferdsdata mer tilgjengelig for alle, og ikke bare de som samler det inn. Det er Google og Facebook som lager spillereglene samtidig som de spiller det. Andre bedrifter og selskaper henger etter og vil ikke ha mulighet for å ta igjen stormaktene. Det er reguleringer som teknologiselskaper er mest redd for. Helt siden dette startet har de kunnet bygge og utvikle seg uten begrensninger. Det finnes ingen lover eller regler som forhindrer dem i å utvikle seg på sin egen måte (Zuboff, 2019, s. 31). Ingen regler utenom de som teknologigigantene lager selv, vel og merke. De kan strekke grensene så langt de vil, og det er ingen som kan hindre dem. Facebook og Google er skaperne av et nytt spill hvor brikkene er atferdsdata, og de kan derfor gjøre akkurat som de selv ønsker. Reglene er ikke skapt enda, Facebook og Google har fritt spillerom for å lage sine egne regler. Og alt dette skjer mens de selv samler inn data, bearbeider den, og selger tjenester for egen profitt.

Regulering gjennom myndigheter er et alternativ, enten gjennom offentlige organer, eller innføring av «Antitrust»-regler, et regelverk som skal avverge høy markedskonsentrasjon og verne forbrukere (Croteau & Hoynes, 2019, s. 41). Hvis maskinintelligensen blir distribuert til flere aktører kan det muligens bidra til en likestilling av datainnhenting og gjensidighet mellom bruker og utgiver. Hvorvidt de er villig til å regulere må man også vurdere om regulering kun gjennom myndigheter egentlig kan være gunstig for befolkningen. Det er en kort vei fra regulering til sensur, og vi ser allerede eksempler fra land som Kina der de har gått fra regulering til komplett sensur av Facebook (Croteau & Hoynes, 2019, s. 353). Denne utviklingen virker skremmende, og viser at regulering kan være et tveegget sverd. Hvis

regulering ikke forekommer på statsnivå, kan det tenkes at brukere må ty til andre midler for å beskytte sitt personvern.

Det hele er blitt så forførende at vi har forsømt å beskytte mye av det som gjør oss unike eller spesielle: våre ansikter, ønsker og sårbarheter. Det er et paradoks der også - vi gir regjeringer og teknologiselskaper flere av våre hemmeligheter enn noen gang før, men i bytte lager vi flere forbindelser enn vi noen gang har hatt. Det hele er så nytt at vi fremdeles ikke vet om kompromisset er verdt det. Derfor har sikkerhetseksperten Bruce Schneier, en klar beskjed til personer som ønsker å gjøre noe med dette: "Den beste anbefalingen jeg har for folk er å bli involvert i den politiske prosessen. Det beste vi kan gjøre som forbrukere og borgere er å gjøre dette til et politisk spørsmål. Tving lovgiverne våre til å endre reglene" (Schneier, 2017). Han ønsker at vi som individer ikke ønsker å overgi personopplysningene våre frivillig til hendene på teknologibedrifter og myndigheter, som kun ønsker å gjøre vår atferd og våre preferanser om til profitt.

I det digitale samfunn synes forbrukere i stadig større grad å gi opp grunnleggende aspekter av deres privatliv for å gjøre det lettere å bruke telefonene og datamaskinene sine, og har motvillig akseptert at det å overvåkes av selskaper, og til og med myndigheter, bare er et faktum i det moderne liv. Det er her personvernsparadokset kommer inn. Vi sier alle at vi verdsetter personvern, men så ser det ut til at alt vi gjør på nettet er i strid med det. Det blir litt som å ha en skjult figur som følger deg rundt overalt og tar notater om hver eneste ting du gjør: hva du spiser, hvor du spiser, hvem som er med, når dere spiste, osv., det ville jo vært ganske tvilsomt, sant? Likevel går vi på nettet og deler all denne infoen selv, og dermed tenker man ikke at det er en rar ting å gjøre i det hele tatt. Du blir nesten utenfor om du ikke går rundt og deler hva du holder på med på sosiale media-plattformer som Facebook eller Instagram.

Fordi det digitale samfunn beveger seg inn og ut av landegrensener må regulering også sees i et globalt perspektiv. Et transnasjonalt samarbeid mellom statsmakter vil kunne øke sjansene for ansvarliggjøring og håndheve regulering. Det er naturlig å trekke inn FN som organ når ideen om multilateralt samarbeid oppstår. FNs hovedformål er blant annet å være et samlingspunkt for medlemsstater og sammen lage felles strategier og planer for ivaretagelse av enkeltmenneskets rettigheter og sikkerhet (Knudsen & Ravndal, 2021). FN har en anerkjent posisjon når det kommer til det globale samarbeidet mot en bedre verden og organisasjonen påvirker andre medlemsstater og forhandler med enkeltstående myndigheter. Delegasjoner bestående av offisielle beslutningstakere inviteres sammen med representanter fra

sivilsamfunnet for å forhandle og samarbeide rundt en rettferdig, fredelig, likestilt og bærekraftig verden.

Historisk sett kan vi se at sivilsamfunnet har hatt en nødvendig posisjon i kampen for endring og rettferdighet. Eksempelvis har kvinnebevegelsen og de feministiske bølgene som strekker seg fra slutten av 1700-tallet frem til dagens dato (Holst, 2009, s. 46). De har gjennom opplysning og presslegging på myndigheter skapt forandringer, lovendringer og muligheter for kvinner verden over. Dette viser at individuelle handlinger kan utgjøre en forskjell når de blir organisert (Beck, 2009, s. 198). Hvis brukere går sammen og skaper en interesseorganisasjon som beskytter personvern på sosiale medier, kan de appellere til regulering, forlange at brukeres stemmer blir hørt, og deres interesser ivaretatt.

Når vi ser på likestillingskampen kan vi anta at uten politisk påvirkning fra sivilsamfunnet og kvinnene selv ville ikke beslutningstakere ha håndhevet deres rettigheter i like stor grad. Forandring skjer ikke gjennom politiske beslutninger i et vakuum, det er først når borgere identifiserer et behov for forandringen og utvikling. Derfor kan man si at beslutningstakere og sivilsamfunnet er i en avhengighet av hverandre for reell endring. Derfor er opplysning og kunnskap ytterst viktig for å skape engasjement rundt personverndebatten, slik at det skapes politisk motivasjon for regulering til fordel for brukeren (Beck, 2009, s. 199). For å avsløre overvåkningskapitalismen må menneskers rettigheter til privatliv styrkes.

Schneier (2017) påpeker at vi lever i en verden der dataen vår er utenfor vår kontroll. Det er ikke enkeltindividene som har kontroll på hva som befinner seg på nett av deres atferd og deres preferanser. I stedet er det de store teknologiselskapene og bedriftene som Facebook og Google som har kontroll på atferdsdataen.. Det er lagret i deres skyer, altså deres systemer. Selv om det finnes strategier som du kan foreta deg for å minske din atferdsdata, er det et mye større tiltak enn det behøver å være, og strategiene tar heller ikke for seg kjernen av problemet med overvåkningskapitalismen. De strategiene det er snakk om her, er de tipsene som Schneier skrev i sin bok, og som ble vist til tidligere. Man skal ikke trenge å måtte ty til disse tekniske strategiene for å måtte beskytte seg selv fra å bli brukt som et middel til andres mål. Man er nødt til å ta grep i roten av problemet. Altså ansvarliggjøring av bedrifter som Google og Facebook slik at de ikke kan fortsette å praktisere usynlig datainnsamling i så stor grad.

Konklusjon

Vi har sett at sosiale media og teknologiselskapene har mye større innflytelse på oss og funksjonene i samfunnet enn mange tror og tenker på i det daglige liv. De siste årene har bedrifter som Facebook og Google startet en ny form for valuta der det er informasjonen om vår atferd og våre aktiviteter som handles for. Atferdsdata kalles den. Atferdsdataen har frem til nå vært samlet inn på nettsider man er inne på, men det er ingenting som stopper teknologiselskapene fra å samle inn data fra ditt daglige, virkelige liv. Når internettjenester slik som Facebook og Google blir en større del av brukeres hverdag, og deres funksjoner mer altomfattende vil opplysningene som blir innhentet fra dem avsløre mer av vårt personlige liv. Det vil videre gjøre oss mer mottakelig for både cyberangrep og datalekkasjer, men også manipulering i form av skreddersydde beskjeder og reklamer som skal styre deg i en spesifikk retning. Når brukere går fra å være villige, informerte deltakere av sosiale medier, til å bli kjernen og drivkraften bak Facebook og Google, skaper det et tydelig maktforhold som setter teknologiselskapene på toppen av pyramiden. Teknologiselskaper som sitter på store mengder atferdsdata har muligheten og makten til å kunne styre brukere, slik som Cambridge Analytica-skandalen viste under det amerikanske valget i 2016.

Utviklingen i dag har skremmende paralleller til Foucaults beskrivelse om det skjeve maktforholdet mellom stat og borgere. Dersom en slik allegori stemmer med dagens eller fremtidens forhold mellom Facebook og brukere, vil konsekvensene av en enda mer digitalisert verden kunne bli store. Når teknologien som blir brukt stadig tar på seg flere ansvarsområder og nærmest blir et integrert og automatisert vesen vil risikoene knyttet til atferdsdata kunne øke over tid. Brukerne har ikke kontroll på hva som er lagret om dem på nett, det er teknologiselskapene Facebook og Google som kontrollerer atferdsdataen. I et historisk perspektiv ser vi at det er enkeltindividene som har måtte utfordre og stå opp mot makter for å oppnå rettferdighet og rettigheter. Kvinnesaken har sine røtter i en grasrotbevegelse. Det betyr at de selv har vært initiativtakere for å få lovfestet sine rettigheter på lik linje med menn og har gjennom politisk påvirkning oppnådd dette. Det må en ny politisk vilje til fra befolkningen for å motivere beslutningstakere til å regulere innhenting og oppbevaring av vår atferdsdata (Beck, 2009, s. 195). Samtidig må vi som brukere identifisere behovet for regulering. Selv om det finnes tips og triks som du kan foreta deg for å minske din atferdsdata, er det et mye større tiltak enn det behøver å være, og disse tipsene tar heller ikke for seg kjernen av problemet med overvåkningskapitalismen. Man skal ikke trenge å måtte gå

ut av sin vei for å måtte beskytte seg selv fra å bli brukt som et middel til andres mål. Man er derfor nødt til å ta grep i roten av problemet. Opplysningen av folket og politisk mobilisering er ytterst viktig for å skape nok bluss rundt personverndebatten. Slik vil overvåkningskapitalismen kunne avdukes, og i det tilfellet også svekkes.

Referanser

- Andersen, H., & Kaspersen, L. B. (2013). *Klassisk og Moderne Samfundsteori*. Copenhagen: Hans Reitzels Forlag.
- Beck, U. (2009). *Risk Society Towards a New Modernity*. London: SAGE Publications Ltd.
- Bartlett, J. (2019). *The Cambridge Analytica Scandal & Our Future* – Jamie Bartlett. Tilgjengelig fra: <https://www.youtube.com/watch?v=H6WLqr2Ld3o&t=6s> (Hentet 04. mai 2021)
- Brailovskaia, J., & Margraf, J. (2017, desember 14). Facebook Addiction Disorder (FAD) among German students - A longitudinal approach. *PLOS ONE*, ss. 1-15.
- Brailovskaia, J., Rohmann, E., Bierhoff, H.-W., & Margraf, J. (2020, november 2). The anxious addictive narcissist: The relationship between grandiose and vulnerable narcissism, anxiety symptoms and Facebook Addiction. *PLOS ONE*, ss. 1-17.
- Croteau, D., & Hoynes, W. (2019). *Media/Society Technology, Industries, Content and Users*. Los Angeles: SAGE.
- Datatilsynet. (2019, oktober 10). *Cookies og informasjonskapsler*. Hentet fra Datatilsynet: <https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/cookies/>
- Drag, S. (2015). Sug etter facebook. *ROP*. Hentet fra <https://rop.no/aktuelt/sug-etter-facebook>
- Foucault, M. (2020). *Discipline and Punish The Birth of the Prison*. London: Penguin Classics.
- Foucault, M. (2020). *Power Essential Works 1954-84: Volume Three*. London: Penguin Random House UK.
- Gerber, N., Gerber, P., & Volkamer, M. (2018) *Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior*, Computers & Security, Volume 77, Pages 226-261. <https://doi.org/10.1016/j.cose.2018.04.002>.
- González, J. C., Cuevas, Á., Arrate, A., & R. C. (2021, januar). Facebook labels 67% of its users with potential sensitive interests, sometimes at great risk to user. *COMMUNICATIONS OF THE ACM VOL. 64, NO. 1*, ss. 62-69.
- Heawood, J. (2018). Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal. *IOS PRESS*, ss. 429-434.
- Hinds, J., Joinson, A. N., & Williams, E. J. (2020, juni 13). "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies*, ss. 1-14.
- Holmes, A. (2021, April 3). *533 million Facebook users' phone numbers and personal data have been leaked online*. Hentet fra Business Insider: <https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4?r=US&IR=T>
- Holst, C. (2009). *Hva er FEMINISME*. Oslo: Universitetsforlaget.
- Knudsen, F, K., Ravndal, E, J. (2021) *FN (Forente nasjoner)*. Hentet fra https://snl.no/FN_-_Forente_nasjoner
- Mineo, L. (2017, august 24). *On internet privacy, be very afraid*. Hentet fra The Harvard Gazette: <https://news.harvard.edu/gazette/story/2017/08/when-it-comes-to-internet-privacy-be-very-afraid-analyst-suggests/> (Hentet: 04 april 2021)

Nix, A. (2016) *Cambridge Analytica – The Power of Big Data and Psychographics*. Tilgjengelig fra:

<https://www.youtube.com/watch?v=n8Dd5aVXLcC&t=1s> (Hentet: 04. mai 2021)

Nix, A. (2018) *Former Cambridge Analytica CEO Alexander Nix faces MPs (full version)*. Tilgjengelig

fra: <https://www.youtube.com/watch?v=weQ9E6e3aJo> (Hentet: 04. mai 2021)

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York City: W. W. Norton & Company.

Zuboff, S. (2019). *Overvåkningskapitalismens tidsalder. Kampen for en menneskelig framtid ved maktens nye frontlinje*. Oslo: Spartacus Forlag AS.

Zuboff, S. (2019, januar). *Velkommen til overvåkningskapitalismens tidsalder*. Hentet fra Le Monde Diplomatique: <https://www.lmd.no/2019/01/velkommen-til-overvakingskapitalismens-tidsalder/>