OSLOMET

FORBRUKSFORSKNINGSINSTITUTTET SIFO

Årvåken og overvåket?

Norske forbrukeres forhold til digitale data, sporing, personalisering og målretting i overvåkningsøkonomien

Dag Slettemeås, Helene Fiane Teigen og Henry Mainsah

OSLO METROPOLITAN UNIVERSITY
STORBYUNIVERSITETET

OsloMet – storbyuniversitetet
SIFO-Rapport 10 - 2022

Forsidefoto: pexels-pixabay-270373

Forbruksforskningsinstituttet SIFO
OsloMet – storbyuniversitetet
Stensberggt. 26 – 7. etg.
Postboks 4 St. Olavs plass
0130 Oslo
www.oslomet.no/om/sifo

Forbruksforskningsinstituttet SIFO utgir:

- Rapporter – som er kvalitetssikret og godkjennes av SIFO ved direktør/forskningsledere
- Notater – som godkjennes av prosjektleder.

STORBYUNIVERSITETET
FORBRUKSFORSKNINGSINSTITUTTET SIFO

Tittel	Antall sider	Dato
Årvåken og overvåket? Norske forbrukeres forhold til digitale data, sporing, personalisering og målretting i overvåkningsøkonomien	82	15.02.2023

Title	ISBN
Alert and monitored? Norwegian consumers' relations to digital data, tracking, personalization and targeting in the surveillance economy	978-82-7063-548-1

Forfatter(e)	Prosjektnummer	Faglig ansvarlig sign.
Dag Slettemeås, Helene Fiane Teigen og Henry Mainsah	202689	

Oppdragsgiver

Barne- og familiedepartementet

Sammendrag

Bakgrunnen for dette prosjektet er den omfattende sporingen, innsamlingen og kommersielle bruken av forbrukerdata i dagens digitale samfunn, et fenomen omtalt som overvåkningsøkonomien. I rapporten har vi tatt utgangspunkt i norske forbrukeres egne erfaringer, holdninger, kompetanse og praksiser knyttet til overvåkningsbaserte tjenester og markedsføring. Til dette formålet har vi benyttet to fokusgrupper, gjennomført i juni 2022 og en landsrepresentativ spørreundersøkelse, gjennomført i oktober 2022. Ettersom temaet er omfattende og sammensatt, følges tematikken gjennom en «overvåkningskjede» bestående av tilkobling, data, sporing, personretting og til slutt overvåkning mer generelt. Rapporten konkluderer med at forbrukere i dag utfordres av informasjonsoverflod, oppmerksomhetsjag, samtykketrøtthet, data-fatigue, algoritmeforvirring, personvernapati og digital resignasjon – men også av normalisering, aksept, rasjonalisering og tilfredshet med dagens overvåkningsbaserte systemer. Dette skaper en kompleks aura av ambivalens og usikkerhet, som gjør det svært krevende for forbrukere å navigere trygt i dagens overvåkningsøkonomi.

Summary

The background for this project is the extensive tracking, collection and commercial use of consumer data in today's digital society, a phenomenon referred to as the surveillance economy. In the report, we have taken Norwegian consumers' own experiences, attitudes, skills and practices related to surveillance-based services and marketing as a starting point. For this purpose, we have used two focus groups, conducted in June 2022, and a nationally representative survey, conducted in October 2022. As the topic is extensive and complex, the topic is followed through a "surveillance chain" consisting of connection, data, tracking, targeting and finally surveillance more generally. The report concludes that consumers today are challenged by an abundance of information, a fight for attention, consent exhaustion, data fatigue, algorithm confusion, privacy apathy and digital resignation - but also by normalization, acceptance, rationalization and satisfaction with today's surveillance-based systems. This creates a complex aura of ambivalence and uncertainty, which makes it challenging for consumers to navigate safely in today's surveillance economy.

Stikkord

Overvåkningsøkonomien, forbrukerdata, sporing, personalisering, målretting

Keywords

Surveillance economy, consumer data, tracking, personalization, targeting

Forord

Denne rapporten har tatt utgangspunkt i fenomenet «overvåkningsøkonomien», der forbrukere i stadig større grad spores og overvåkes av digitalbaserte kommersielle aktører. Overvåkning skjer ikke kun i tradisjonelle markedskontekster, men stort sett i alle hverdagskontekster. Prosjektet har tatt utgangspunkt i en norsk virkelighet. Vi har gjennomført en bakgrunnsstudie for å sikre en kunnskapsbasert operasjonalisering av spørsmål til to fokusgrupper og en landsrepresentativ spørreundersøkelse. Målet har vært å få innsikt i hvordan norske forbrukere forholder seg til dette fenomenet i egen hverdag.

Rapporten er finansiert av Barne- og familiedepartementet (BFD) og er basert på prosjektet *«Årvåken og overvåket? Norske forbrukeres holdninger og erfaringer med digital forbrukerovervåkning»*. Funnene fra undersøkelsen vil være nyttige for forbrukermyndigheter og politiske beslutningstakere, men også for forskere og interessegrupper. Kunnskapen kan bidra til å støtte forbrukerpolitiske tiltak og utformingen av virkemidler for å trygge forbrukernes digitale hverdag.

Vi ønsker å takke Barne- og familiedepartementet for oppdraget og for interessen rundt dette temaet. Prosjektet er gjennomført av Dag Slettemeås (prosjektleder), Helene Marie Fiane Teigen og Henry Mainsah. Rapporten er kvalitetssikret av forskningsleder Torvald Tangeland. Alle er tilknyttet SIFO ved OsloMet.

Oslo, februar 2023

Forbruksforskningsinstituttet SIFO

OsloMet – Storbyuniversitetet

Innhold

Sammendrag

Bakgrunnen for dette prosjektet er den omfattende sporingen, innsamlingen og kommersielle bruken av forbrukerdata i dagens digitale samfunn – et fenomen omtalt som overvåknings-økonomien. I rapporten har vi tatt utgangspunkt i norske forbrukeres egne erfaringer, holdninger, kompetanse og praksiser knyttet til overvåkningsbaserte tjenester og markedsføring. Til dette formålet har vi benyttet to fokusgrupper, gjennomført i juni 2022, og en landsrepresentativ spørreundersøkelse, gjennomført i oktober 2022. Ettersom temaet er omfattende og sammensatt, har vi forsøkt å forenkle analysen ved å følge tematikken gjennom en «overvåkningskjede» bestående av tilkobling, data, sporing, personretting og til slutt overvåkning mer generelt.

Utviklingen av tingenes internett og smarte produkter innebærer stadig mer tilkopling. Flere tilkoplede produkter gir flere digitale inngangsporter – og dermed økt sårbarhet – for negative overvåkningseffekter. Forbrukerne i materialet artikulerer både nytte og skepsis til slik tilkopling, en ambivalens som gjør kost(risiko)-nyttevurderinger krevende. Det at forbrukerne er usikre på antallet nettilkoplede enheter og apper de har, viser begrenset oversikt og kontroll. Cyberhygiene og appmoderasjon kan bidra til å styrke forbrukerkontrollen og redusere overvåkningsrelatert sårbarhet.

Flere tilkoplede produkter gir mer omfattende innsamling av forbrukerdata. «Data» fremstår samtidig som noe abstrakt, immaterielt og uhåndgripelig for forbrukerne i materialet. Slik diffus dataforståelse gjør det krevende å knytte følelser og bygge sterke relasjoner til egne data, og samtidig foreta fornuftige risikovurderinger. Få har dessuten negative erfaringer med datautnyttelse og misbruk, mens de fleste har erfart positive og umiddelbare nytteeffekter. Andre utfordringer er følelsen forbrukere i materialet har av å ha mistet kontroll over egne data, i tillegg til at de fremviser stor usikkerhet til hva data er, hvor de er, hva de brukes til, og konsekvenser av databruk. De mener også at mye av deres personinformasjon allerede er offentlig tilgjengelig, mens databytte mot tjenester oppleves som rettferdig. Forbrukerne ønsker bedre kontrollmuligheter for egne data, men ser samtidig at dette vil resultere i ytterligere «kontrollarbeid». Regulering bør derfor avlaste forbrukerne, mens visualisering og konkretisering av data kan bidra til å styrke forbrukernes relasjon til egne data og synliggjøre at de i sum utgjør deres «digitale representant».

Datainnsamling krever sporing, og forbrukerne i materialet aksepterer i stor grad sporing som «normalen» i en datadrevet verden. Enkelte forsøker å begrense sporingen, men utmattes og gir ofte opp grunnet dårlige brukeropplevelser, uendelig med samtykkeforespørsler, og manipulerende design. Samtidig «åpner» flere selv for sporing fordi de oppfatter målrettet reklame som en effektiv måte å skaffe seg relevant informasjon på. Sett i et forbruker-perspektiv bør ikke «avsporings»-strategier straffes med dårligere brukeropplevelser, mens alternative, sporingsfrie alternativer bør tilby tilsvarende relevans og kvalitet for forbrukere som dagens systemer. Kunnskap om sporingsmekanismer ser ikke ut til å forhindre at forbrukere bevisst lar seg spore i bytte mot tilbud og tjenester; altså en tilsynelatende paradoksal og uheldig forbrukeratferd. Dette gapet mellom kunnskap og atferd kan bunne i en normalisert sporingsmodell, manipulerende design, få negative erfaringer, delvis «rasjonelle» forbrukeravgjørelser der nytten vurderes høyere enn kostnaden, eller en form for digital resignasjon.

Tilkopling, sporing og datainnsamling muliggjør personretting (personalisering, skreddersøm og målretting) av budskap og tjenester. Disse mekanismene er i stor grad kjent for forbrukerne i materialet. Mange er positive til relevante forslag, tilpasset innhold og tidsbesparingen slik personretting kan tilby. Ubehag kan derimot oppleves hvis teknologien husker for mye, hvis for personlige/intime data benyttes, hvis budskap/reklame blir for nærgående, hvis algoritmene plasserer forbrukere i feil bås, eller hvis budskap blir for ensrettede. Samtidig oppfattes påvirkningsmekanismer, som manipulering og diskriminering, som vanlige og mindre «farlige» i kommersiell sammenheng. Flere synes likevel det er krevende å forstå den fulle rekkevidden av data- og algoritmebruk, og mener slik kunnskap ikke bør ligge hos forbrukerne.

Målrettet markedsføring oppfattes både positivt og negativt av forbrukerne i materialet. Positive faktorer er at den kan virke mindre irriterende, bedre tilpasset interesser og behov og få «tiden til å gå raskere». Enkelte interagerer også strategisk med algoritmer for å signalisere reklameønsker. Målrettet markedsføring oppleves heller ikke som særlig risikofylt av forbrukerne i materialet. Negative faktorer som fremkommer i materialet knyttes til at man kan få mer styrte og ensrettede budskap, at man havner i feil bås, og at reklamen kan bli klein og ubehagelig dersom det benyttes for personlige data. Utfordringen ligger i å synliggjøre for forbrukere at de spores for å få målrettet reklame. Samtidig bør alternative markedsføringsmodeller fortsette å tilby relevans, forenkling og tilpasning for forbrukerne. Regulering bør på sin side sikre forbrukere mot uheldig algoritmebruk, ensretting, manipulering og diskriminering.

Tilkopling, databruk, sporing og personretting gir ikke forbrukerne i materialet sterke assosiasjoner til «overvåkning». Overvåkningsbegrepet forbindes primært med menneskelig overvåkning og bruk av video/lyd. Flere mener dessuten at de «forsvinner i mengden» og at de «ikke har noe å skjule». Den digitale overvåkningen (dataveillance) oppleves dermed ikke nær eller truende nok til å motivere til beskyttelse mot negative overvåkningseffekter. Likevel er flere villige til å la seg spore, og bruke personlige data, for å løse store samfunns-utfordringer. Dette sammenfaller med høy tillit til myndigheters håndtering av forbrukerdata i offentlige tjenester. Tilliten er dessuten relativt høy til kommersielle selskaper, som ikke primært anses som overvåkningsagenter, men som profittorienterte selskaper. Her anses en viss grad av manipulasjon (reklame) og diskriminering (segmentering) som normalt. Likevel er forbrukerne i materialet bekymret for digitale selskapers dataakkumulasjon over tid, og at økt makt og kontroll som kommer med slik datakunnskap kan utnyttes til større grad av manipulering og diskriminering. Det å ikke kunne unnslippe digital observasjon gir dessuten forbrukerne en følelse av å miste frihet. Studien preges i stor grad av *følelser* rundt de ulike overvåkningsrelaterte problemstillingene, heller enn av konkrete risikovurderinger.

Personvernet står sentralt i diskusjonen om forbrukerovervåkning. I studien oppfatter enkelte at personvernet er noe vi absolutt må kjempe for, mens andre mener personvernet allerede er «dødt». Bekymringer rundt digital overvåkning oppleves uansett ikke å være store nok i materialet til å aktivere betydelige personvernstrategier. Dette forsterkes av aksepten for bruk av persondata som råvare i den datadrevne økonomien. Personvernet oppfattes dessuten som mindre viktig i forbruker-/markedskontekster enn i andre borger-/samfunnskontekster. På den annen side skaper diskurser rundt usikre tider (krig, pandemi og statlig overvåkning) økt refleksjon om temaer som digital avhengighet og sårbarhet i materialet, og viktigheten av personvern re-aktualiseres. Dette samsvarer med at forbrukerne mener deres «avslappede» holdning til sporing, data og overvåkning bunner i en grunnleggende tillit til norske myndigheter og en stabil demokratisk orden. En mer ustabil

verden tilbyr samtidig et mulighetsrom for å belyse digitale sårbarheter og forsterke forbrukernes refleksjon og kompetanse om personvern. Personvern bør dessuten være et viktig konkurranseparameter i utviklingen av offentlige og kommersielle digitale tjenester.

Forbrukerovervåkning i den digitale økonomien er et svært sammensatt problemfelt. Sentralt står forbrukernes følelse av kontroll. Studien viser at forbrukerne ønsker mer kontroll, eksempelvis gjennom «styringsverktøy» for data og algoritmer, men mange erkjenner at full kontroll er nytteløst og at det uansett vil kreve en enorm arbeidsinnsats. Derfor er det en viss aksept for å ikke ha full kontroll, noe som kan utfordre forbrukernes autonomi, integritet, personvern – og frihet. Rasjonaliseringer for slik aksept er blant annet at sporing og datadeling er en «naturlig» del av den digitale hverdagen og «prisen man betaler» for å delta i det teknologiske samfunnet. Det uttrykkes dessuten tilfredshet og trivsel med dagens system, og et «forbrukeropprør» mot dagens forbrukerovervåkning er dermed ikke nært forestående. Det at datadeling og eksponering er blitt normalisert og rutinisert, tilsier at fungerende digitale praksiser vil være krevende å endre. Velfungerende etablerte rutiner som forbrukerne er fornøyde med må avlæres og gradvis erstattes av nye modeller og rutiner. Dette kan være krevende. Nye systemer bør dessuten tilby tilsvarende bekvemmelighet, forenkling, nytte og relevans som det dagens overvåkningsbaserte systemer tilbyr.

Selv om tilliten til norske myndigheter er høy, er tilliten lavere til myndigheters evne til å beskytte forbrukere i overvåkningsøkonomien gjennom regulering. Det forventes eller «håpes» likevel at myndigheter vil sikre viktige forbrukerinteresser. Gjennom GDPR og DSA skal forbrukere få styrkede rettigheter, men fremdeles hviler et stort ansvar på forbrukernes digitale kompetanse og evne til kritisk refleksjon. Samtidig er forbrukere allerede overlesset med «arbeid» og har liten innsikt i lover og reguleringer som beskytter dem. Skillet mellom forbrukere som økonomiske aktører og borgere som samfunnsaktører eroderes dessuten gradvis i digitaløkonomien, noe som kan komplisere forbrukernes rolle- og ansvars-forståelser. Samtidig kan digital forbrukererfaring være nyttig og overførbar til andre samfunnsarenaer. Uansett vil sektoroverskridende samordning av regulering, ansvar og kompetansebygging være nødvendig.

Forbrukere utfordres i dag av informasjonsoverflod, oppmerksomhetsjag, samtykketrøtthet, data-fatigue, algoritmeforvirring, personvernapati og digital resignasjon – men også av normalisering, aksept, rasjonalisering og tilfredshet med dagens overvåkningsbaserte systemer. Dette skaper en kompleks aura av ambivalens og usikkerhet. De kan oppfatte at de har tilgang til nøytral og ufiltrert informasjon eller at de tar frie og upåvirkede beslutninger, mens de i realiteten kan utsettes for filtrering, manipulering og diskriminering. En relatert utfordring er at mange *ikke anser seg selv* for å være sårbare for ulike typer påvirkning, selv om de anerkjenner mekanismene og problemstillingene. Konstant overvåkning kan redusere forbrukernes frihetsfølelse, oversikt og kontroll, og svekke evnen til refleksjon og egenbeskyttelse. I tillegg kan uoverskuelige langtidseffekter og økt relativ makt til markedsaktører resultere i svekket forbrukeragens og sterkere teknologisk strukturering og styring av forbrukernes informasjon, valgmuligheter og beslutninger. Dette kan være uheldig for forbrukernes personvern, autonomi, integritet, verdighet og velferd. Vi kan stå overfor en type «overvåkningsrealisme» der forbrukere og myndigheter opplever en uro over datainnsamling samtidig som det foregår en aktiv normalisering av overvåkning. Dette begrenser mulighetene til å tenke nytt om digitalt medborgerskap og fornuftige alternativer til overvåkningsøkonomien. Teknologisk akselerasjon og utvikling av kunstig intelligens kan ytterligere intensivere forbrukerovervåkningen og samtidig gjøre forbrukere enda mer avhengige av autonom teknologi.

Summary

The background for this project is the extensive tracking, collection and commercial use of consumer data in today's digital society – a phenomenon referred to as the surveillance economy. In the report, we have taken Norwegian consumers' own experiences, attitudes, skills and practices related to surveillance-based services and marketing as a starting point. We have used two focus groups (conducted in June 2022) and a nationally representative survey (conducted in October 2022) for this purpose. As the topic is extensive and complex, we have tried to simplify the analysis by following the topic through a "surveillance chain" consisting of connection, data, tracking, personalization/ targeting and finally the concept of surveillance more generally. The development of the Internet of Things and smart products means more connectivity, which imply more digital gateways – and thus increased vulnerability – to negative surveillance/dataveillance effects. Consumers in the material articulate both benefits and skepticism about such a connectivity, an ambivalence that makes cost(risk)-benefit assessments demanding. The fact that consumers are uncertain about the number of internet-connected devices and apps they have, indicates their lack of overview and control. Cyber hygiene and app moderation can help strengthen consumer control and reduce surveillance-related vulnerability.

More connected products provide more comprehensive collection of consumer data. Consumers in the study, however, associate “data” with something immaterial and intangible. Such a diffuse understanding of data makes it difficult for them to build strong relationships with their own data and make proper risk assessments. Few have negative experiences with data exploitation, while most have experienced immediate benefits. Other challenges relate to how consumers in the material have lost control over their own data. In addition, they present great uncertainty about what data is, where it is, what it is used for, and the consequences of data use. They also believe that much of their personal information is already publicly available, while exchanging data for services is perceived as fair. Consumers want better control options for their own data, but at the same time they see that this will result in further "control work". Regulation should therefore relieve consumers, while visualization and concretization of data can help strengthen consumers' relationship with their own data and make visible to them that their data, in sum, constitute their "digital representative".

Data collection requires tracking, and consumers in the study largely accept tracking as "normal" in a data-driven world. Some try to limit tracking but get exhausted and often give up due to bad user experiences, endless consent requests, and manipulative design. At the same time, some tend to "open up” to tracking because they perceive targeted advertising as an effective way of obtaining relevant information. Seen from a consumer perspective, strategies to avoid tracking should not be punished with poorer user experiences, while alternative, tracking-free options should offer similar relevance and quality for consumers as current systems. Knowledge of tracking mechanisms does not seem to prevent consumers from knowingly allowing themselves to be tracked in exchange for offers and services; in other words, an apparently paradoxical and unfortunate consumer behavior. The gap between knowledge and behavior can be explained by the “normalization” of the tracking model, manipulative design, few negative experiences, or "rational" consumer decisions where benefits are considered higher than costs.

Connection, tracking and data collection enable personalization, tailoring and targeting of messages and services. These mechanisms are also largely known to the consumers in the study. Many are positive when it comes to relevant suggestions, tailored content and the time

savings that personalization offers. On the other hand, discomfort can be experienced if the technology remembers too much, if too personal data is used, if the messages/ advertisement become too intimate, if the algorithms place consumers in the wrong segment, or if messages become too one-sided. At the same time, influence-mechanisms, such as manipulation and discrimination, are perceived as common and less "dangerous" in the commercial context. Many still find it difficult to understand the extent and consequences of algorithm use and believe that such knowledge should not lie with consumers.

Targeted marketing is perceived both positively and negatively by consumers in the material. Positive factors are that it is less annoying, better adapted to interests and needs and makes "time go faster". Some also interact strategically with algorithms to signal their advertising wishes. Targeted marketing is not perceived as particularly risky by the consumers. Negative factors are linked to more steered/controlled and one-sided messages, erroneous segmentation, and advertising can be considered creepy and unpleasant if it uses too personal data. The challenge – to increase consumer awareness – lies in making visible to consumers that they are being tracked in order to receive targeted advertising, while alternative marketing models should continue to offer relevance, simplification and customization to consumers. Regulation should protect consumers against inappropriate use of algorithms, one-sided information, manipulation and discrimination.

Connection, data use, tracking and personalization/targeting do not give consumers in the study a strong association with "surveillance". The term surveillance is primarily associated with human surveillance and the use of video/audio. Many also believe that they "disappear in the crowd" and that they "have nothing to hide". In that sense, digital surveillance (dataveillance) does not appear to be intimate or threatening enough to motivate protection against negative surveillance effects. Also, many of the consumers are willing to let themselves be tracked, and use personal data, to solve major societal challenges. This coincides with a high level of trust in the authorities' handling of consumer data in public services. Trust is also relatively high in commercial companies, which are not primarily regarded as surveillance agents, but as profit-oriented companies. Here, a certain degree of manipulation (advertising) and discrimination (segmentation) is considered to be normal. Nevertheless, the consumers in the material are concerned about how digital companies accumulate consumer data over time, and that increased power and control that comes with data knowledge can be exploited in more extensive manipulation and discrimination efforts. Not being able to escape digital observation also gives consumers a sense of losing their freedom. The study is characterized to a large extent by feelings around various surveillance-related issues, rather than by concrete risk assessments.

Privacy is central to the discussion on consumer surveillance. In the study, some people perceive that privacy is something we have to fight for, while others think privacy is already "dead". In any case, concerns about digital surveillance are not felt to be big enough to activate considerable privacy strategies. This is reinforced by the acceptance of using personal data as raw material in the data-driven economy. Privacy is also perceived as less important in consumer/market contexts than in other citizen/societal contexts. On the other hand, discourses on uncertain times (war, pandemic and state surveillance) create increased reflection in the study on dependence and vulnerability issues, and the importance of privacy is re-actualized. This corresponds with consumers’ beliefs that their "relaxed" attitude towards tracking, data and surveillance is rooted in a fundamental trust in Norwegian authorities and a stable democratic order. At the same time, a more unstable world offers an opportunity to shed light on digital vulnerabilities and strengthen consumers' reflection and competence about privacy. Privacy should also be an important competitive parameter in the development of public and commercial digital services.

Consumer surveillance in the digital economy is a highly complex problem area. A key issue is the consumer's sense of control. The study shows that consumers want more control, for example through "management tools" for data and algorithms, but many recognize that full control is unattainable and will require a huge amount of work. Thus, there is a certain acceptance of not having full control, which, however, can challenge consumers' autonomy, integrity, privacy - and freedom. Rationalizations for such acceptance include that tracking and data sharing is a "natural" part of digital everyday life and the "price you pay" for participating in the technological society. Satisfaction and well-being with the current system is also expressed, and a "consumer revolt" against current consumer surveillance is therefore not imminent. The fact that data-sharing and exposure have become normalized and routinized indicates that already functioning digital practices can be hard to change. Established routines that consumers are satisfied with must be unlearned and gradually replaced by new models and routines. This can be demanding. New systems should also offer similar convenience, simplification, utility and relevance as the current surveillance-based systems offer.

Although Norwegian authorities are high trusted, trust is lower in the authorities' ability to protect consumers in the surveillance economy through regulation. Consumers in the study still expect or "hope" that authorities will safeguard consumer interests. Through GDPR and DSA, consumers will be given strengthened rights, but a large part of the responsibility still rests on consumers, and their digital competence and abilities for critical reflection. But consumers are already overburdened with "work" and have little insight into the laws and regulations that protect them. Furthermore, the distinction between consumers as economic actors and citizens as social actors in the digital economy is gradually being eroded, which can complicate consumers' understanding of roles and responsibilities. At the same time, digital consumer experience can be useful and transferable to other societal arenas. In any case, cross-sector coordination of regulation, responsibility and competence building will be necessary.

Consumers today are challenged by an abundance of information, a fight for attention, consent exhaustion, data fatigue, algorithm confusion, privacy apathy and digital resignation – but also by normalization, acceptance, rationalization and satisfaction with today's surveillance-based systems. This creates a complex aura of ambivalence and uncertainty. They may perceive that they have access to neutral and unfiltered information or that they make free and uninfluenced decisions, while in reality they may be exposed to filtering, manipulation and discrimination. A related challenge is that many do not consider themselves to be vulnerable to various types of influence, even if they recognize the mechanisms more generally. Constant monitoring can reduce consumers' sense of freedom, overview and control, and weaken their ability to reflect and protect themselves. In addition, unforeseeable long-term effects and increased relative power of market players can result in weakened consumer agency and stronger technological structuring and management of consumers' information, choices and decisions. In the long term, this is unfortunate for consumers' privacy, autonomy, integrity, dignity and welfare. We may be facing a type of "surveillance realism" where consumers and authorities experience an uneasiness about data collection at the same time as an active normalization of surveillance takes place. This limits the possibilities for rethinking digital citizenship and sensible alternatives to the surveillance economy. Technological acceleration and the development of artificial intelligence can further intensify consumer surveillance and at the same time make consumers even more dependent on autonomous technology.

1. Innledning

Denne studien tar utgangspunkt i det norske forbrukerapparatets interesse for fenomenet *overvåkningsøkonomien*, både Barne- og familiedepartementets (BFD) fokus på kommersiell bruk av persondata og forbrukernes personvern (BFD 2019) og nyere studier om tematikken utført av Forbrukerrådet (2021). Sentralt står digitale forbrukertjenester og en eskalerende innsamling, analyse, salg og bruk av forbrukerdata i markedsføring og tjenesteutvikling. Forbrukere spores og overvåkes tilnærmet kontinuerlig i digitalbaserte kommersielle systemer. Overvåkning skjer ikke kun i tradisjonelle markedskontekster, men stort sett i alle typer hverdagskontekster (Zuboff 2019).

I denne rapporten ser vi på overvåkningsøkonomien i en norsk kontekst. Vi tar utgangspunkt i foreliggende studier, eksisterende regulering, og forbrukerpolitiske tiltak. Dette danner utgangspunkt for en kunnskapsbasert operasjonalisering og utvikling av spørsmål til en kvalitativ studie, der to fokusgrupper er benyttet. Funn fra fokusgruppene har deretter blitt testet i en landsdekkende representativ spørreundersøkelse for å avdekke om funnene kunne generaliseres til hele befolkingen. Målet har vært å få innsikt i hvordan norske forbrukere selv oppfatter, vurderer og handler i relasjon til dette fenomenet i egen hverdag. På denne måten kan vi se deres forståelser og erfaringer opp mot kommersielle aktørers «overvåkningsmetoder», og opp mot politiske/juridiske forståelser relatert til overvåknings-økonomien. Slik kunnskap vil gjøre det enklere å iverksette forbrukerpolitiske tiltak og utforme virkemidler som kan bidra til å trygge forbrukere i møte med en raskt eskalerende overvåkningsøkonomi.

1.1. Bakgrunn

Frykten for overvåkningssamfunnet har eksistert lenge. Orwells dystopi *1984* har i mange tiår bidratt til å diskurser om overvåkningstrekk i samfunnet. Samtidig har frykten for sporing og overvåkning av forbrukere eksistert helt siden introduksjonen av strekkoden i varehandelen på 1970-tallet[1] (Slettemeås 2009). Mens begrepet *Big brother* (Orwell 1949) fremdeles benyttes hyppig i norsk og internasjonal diskurs om en sentral overvåkende aktør, gjerne en stat, har Zuboff (2019) vektlagt kommersielle digitale plattformers inntreden som *Big other.* Disse står sentralt i konstruksjonen av et nytt paradigme – «overvåkningskapitalismen», skal vi tro Zuboff.

Ser vi noen tiår tilbake, til det kommersielle internettets første fase, var det stor optimisme knyttet til muligheter for kunnskapsdeling og en åpen, transparent, gratis og brukerstyrt markedsarena, der forbrukere kunne samarbeide om å tilgjengeliggjøre og dele informasjon og tjenester seg imellom (Slettemeås og Storm-Mathisen 2021). Utstrakt anonymitet sikret personvernet, og ideen om en opplyst, aktiv og styrket forbruker etablerte seg (Slettemeås 2018). Personvern- og markedsføringslovgivningen i EU og Norge ble samtidig liberalisert i den tidlige formative fasen rundt årtusenskiftet, blant annet for å sikre vekst i digitale markeder gjennom å tillate økt bruk av persondata i tjenesteutvikling og markedsføring.

[1] Jf. også kronikk i Aftenposten, 14.02.2018, Dag Slettemeås: «Amazon gir oss et glimt av fremtidens handel». Ref: https://www.aftenposten.no/meninger/kronikk/i/215qBx/Amazon-gir-oss-et-glimt-av-fremtidens-handel---Dag-Slettemeas

Ifølge Clarke (2019) var det på denne tiden likevel få tegn til «overvåkningselementer» i digitaløkonomien.

I de senere år, med forbedret teknologi og tiltakende plattformisering, har kommersialisering av brukerdata bredt om seg (Throne-Holst og Kjørstad 2016). Anonymiteten er borte, og forbrukere på nett har blitt stadig mer transparente. Istedenfor fri deling av kunnskap, blir data og kunnskap om forbrukere nå sett på som en handelsvare som et fåtall aktører profiterer på (Slettemeås og Storm-Mathisen 2021, Dulrud og Alfnes 2017). Zuboff hevder at det er utviklet en utbyttende overvåkningskapitalisme som bidrar til å strukturere markedet som helhet. De digitale plattformenes makt anses å være illegitim fordi de kun ekstraherer bruker- og hverdagsdata til egen profitt. Selv om store globale teknologiselskaper som Google og Facebook leder an, antas effekten å være smittende på nær sagt alle forretningsmodeller (Zuboff 2019).

Fundamentet i overvåkningsøkonomien er høsting og konsolidering av enorme mengder personlige data, der menneskelig atferd anses å være råmateriale som konverteres til atferdsdata, som så utnyttes til å forutsi forbrukerhandlinger, som videre utnyttes til skreddersydd markedsføring målrettet mot den enkelte, og som igjen kan resultere i ytterligere manipulering av forbrukeratferd (Zuboff 2015, Zuboff 2019, Christl 2017). Det antas dessuten at slik atferdsmodifisering fungerer best jo lavere brukerbevisstheten er, noe som strider imot prinsippet om informert samtykke. Med bakgrunn i en slik beskrivelse er det behov for mer empirisk forskning som kan bidra til å vurdere i hvilken grad digitale forretningsmodeller kan sies å være overvåkende, hvorvidt forbrukere selv føler de blir overvåket, diskriminert, manipulert eller gjort sårbare på andre måter, og hvordan forbrukerbevisstheten på dette feltet er.

I likhet med Zuboff (2019) mener Clarke (2019) at den digitale overvåkningsøkonomien innebærer store trusler for individers og samfunnets interesser. Selv om innsamling av brukerdata kan gagne brukere ved at det utvikles nyttige og relevante tjenester, bidrar slik datainnsamling til å forsterke kunnskapsasymmetrien i favør kommersielle aktører, mens forbrukere får stadig mindre oversikt, innsikt og kontroll over både egne data og selskapers virkemåter (Cinnamon 2017). Dermed blir det vanskelig å overskue langsiktige negative konsekvenser for forbrukeren og slike effekters opphav. Store plattformaktører lagrer data i proprietære siloer, noe som setter barrierer for deling, transparens og overføring (portabilitet) av data. Slik blir forbrukere forhindret fra å få innsikt i egne data, benytte disse til ulike formål, og dermed selv vurdere dataenes bytteverdi i markedet.

Det hevdes at selv om forbrukere historisk sett ikke har vært under kapitalens kontroll, så påvirkes og «administreres» de i dag gjennom utstrakt kommersiell overvåkning (Sandoval 2013, Ogura 2006). Forbrukerrådet (2021) anser dessuten kommersiell overvåkning og utnyttelse av forbrukerdata som den nye «normalen» på internett, og støtter derfor en systemisk reform, spesielt av den overvåkningsbaserte markedsføringsindustrien. Samtidig trengs det mer kunnskap om forbrukernes ståsted; i hvilken grad forbrukerne faktisk mangler oversikt og kontroll på dette området, hvordan de forholder seg til egne data, sporing, analyse og personaliserte budskap, hvorvidt de oppfatter dette som «overvåkning», om denne type datainnsamling og målretting har gått for langt eller om forbrukerne selv godtar dette som den nye normalen, og i hvilken grad det er behov for ytterligere regulering på feltet.

I tillegg til at store plattformselskaper høster data fra forbrukere, bidrar også andre teknologiske endringer til den massive «dataformeringen». Utviklingen av tingenes internett (IoT) gjør at markedet oversvømmes av rimelige, smarte, datainnsamlende og delvis autonome forbrukerprodukter (Slettemeås 2019). Disse «tingene», som ofte er nært knyttet til forbrukerne selv (som *wearables* og smarthjemteknologi), anses å utgjøre den desidert største produsenten av såkalte «ting-data» i tiden fremover. Dessuten er de fleste digitale enheter tilkoplet skybaserte tjenester som binder forbrukere i langvarige relasjoner (og kontraktsforhold) til tjenestetilbydere, der konstant datautveksling mellom brukere og plattformer er blitt en grunnleggende forutsetning for tjenesten. Både nye «datatyper» og permanente «data-tappende» relasjoner mellom forbrukere og selskaper, gjennom skybaserte forbruksprodukter, forsterker utfordringen med forbrukerovervåkning i hverdagen (Christl 2017, Forbrukerrådet 2021, Slettemeås og Storm-Mathisen 2021).

For å møte denne utviklingen har forbruker- og personvernreguleringen blitt styrket, gjennom GDPR[2] og den kommende Digital Services Act (DSA)[3] på europeisk nivå, gjennom økt bruk av personvernprinsipper i designfasen av produkter (Pbd[4]), og gjennom personvern-fremmende teknologier (PETs[5]). Likevel mangler det fremdeles gode og fleksible nok juridiske, tekniske og økonomiske rammer og normer som gir forbrukere tilstrekkelig eierskap, transparens og kontroll i omgangen med egne data (Nesta 2017). GDPR er et forsøk på å håndtere liberaliseringen fra 20 år tilbake – ikke ved å redusere bruken av data, men ved å forsøke å gi borgere/forbrukere bedre kontroll og makt over egne data gjennom styrkede rettigheter, samtykke, bevisstgjøring, og mer effektiv sanksjonering. Likevel påligger det fremdeles et stort ansvar på forbrukerne i å kritisk reflektere, bli informert, aktivt samtykke, og bygge tilstrekkelig digital forbrukerkompetanse til å navigere og håndtere overvåkningsutfordringen.

Forbrukerrådet (2021) identifiserer en rekke mulige negative effekter i forbindelse med kommersiell overvåkning, slik som manglende transparens, personvernbrudd, manglende databeskyttelse, manipulering, diskriminering, desinformasjon, redusert konkurranse, svindel, sikkerhetsrisiko, redusert tillit, ineffektiv teknologi, og disproporsjonalt bytteforhold mellom brukerdata og personrettet reklame. Clarke (2019) identifiserer også en rekke trusler i den digitale overvåkningsøkonomien, blant annet tvangskjøp, høyere priser, diskriminerende beslutninger, beslutninger tatt på feilaktige data, beslutninger basert på uklare motiver fra tilbydere, redusert forbrukerautonomi, «psychic numbing» og passivitet blant brukere. Puntoni et al. (2021) fremhever at forbrukere kan oppleve redusert livskvalitet ved at de føler seg fremmedgjort og utnyttet i overvåkningssituasjoner. Su (2020) hevder videre at tre typer kapital knyttes til det digitale; sosial kapital, informasjonskapital og økonomisk kapital, og at dagens internettplattformer (og deres privatisering av brukerdata) effektivt blokkerer flyten av kapital mellom økosystemer. Dette hindrer forbrukere i å få økt kontroll og å kunne utnytte data til egen vinning. Forbrukere oversvømmes dessuten av samtykkeforespørsler, som kan resultere i samtykketrøtthet, også omtalt som «personvern-fatigue» eller «digital resignasjon», som hindrer dem i å kritisk vurdere hver forespørsel de

[2] General Data Protection Regulation

[3] Ref: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

[4] Privacy by design

[5] Privacy-enhancing technologies

står overfor (Choi og Jung 2018, Draper og Turow 2019). Blant annet viser SIFO-forskning at forbrukere sliter med å sette seg inn i omfanget av databruk, at holdninger og handlinger ikke alltid samsvarer, og at samtykkepresset blir overveldende og belastende (Haga 2017, Berg og Dulsrud 2018).

Digital forbrukerrobusthet, gitt dagens situasjon med stort forbrukeransvar, er og blir en viktig forutsetning for å klare å håndtere og unngå trusler og negative konsekvenser for forbrukere, og samtidig utnytte de fordeler som foreligger i den digitale hverdagen. Spørsmålet er hvor informerte, bevisste, reflekterte, kompetente og motiverte forbrukerne faktisk er i møte med dette mulighetsrommet og disse utfordringene. Det kan være at de digitale utfordringene øker i omfang og intensitet, at underliggende mekanismer i digitale økosystemer fravrister forbrukere oversikt og kontroll, og at styrket forbrukerrobusthet gjennom økt refleksjon og kompetanse ikke klarer å holde tritt med utviklingen i markedet. Derfor kan det stilles spørsmål ved om forbrukere i større grad bør «avlastes» gjennom sterkere grad av regulering, der mer ansvar legges på datainnsamlende plattformer i å redusere belastninger på forbrukere som følge av dagens forbrukerovervåkning.

1.2. Forbrukerpolitisk og vitenskapelig nytteverdi

EU vektlegger en omfattende strategi for «det digitale tiåret»[6] frem mot 2030, med hovedfokus på å skape tillit til kunstig intelligens, online markeder og digitale tjenester. I den kommende *Digital Services Act (DSA)*[7] fremheves behovet for et trygt og ansvarlig digitalt marked, med bedre beskyttelse av rettigheter, økt cybersikkerhet og robusthet for å sikre data og verdier, mer demokratisk kontroll over store plattformer, og redusert systemisk risiko knyttet til manipulasjon og feilinformasjon. Med en slik storstilt satsing er det helt avgjørende å ha forbrukere med på laget og samtidig forstå deres holdninger og atferd, slik at virkemidler og tiltak kan utformes og målrettes på en god måte. I dette bildet er overvåkningsøkonomien svært problematisk fordi den trekker i motsatt retning av transparens, tillit, forbrukermakt og brukerkontroll, som de ulike digitale strategiene på EU-nivå etterstreber.

Forbrukerpolitikken i Norge er dessuten i økende grad blitt opptatt av problemstillinger knyttet til digitaliseringen av markeder (jf. BFD 2019), fordi det digitale ikke bare gjennomsyrer markeds- og forbrukskontekster, men også hverdagslivet som helhet. Dermed viskes skillene ut mellom det rent forbrukerpolitisk relevante og det som faller inn under andre politiske ansvarsområder. Studier og innsikt som kan bedre forståelsen av denne utviklingen er derfor avgjørende, slik at samarbeid og koordinering kan forenkles og forbedres på tvers av politikkområder. Videre vil kunnskap om hvordan forbrukere forholder seg til disse problemstillingene være nyttig for tilsynsmyndigheter når de skal håndheve eksisterende regelverk. Studien vil dessuten bidra med ny empirisk innsikt som det kan bygges videre på i vitenskapelig produksjon.

[6] Ref: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

[7] Ref: https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/feb/forordning-om-digitale-tjenester-digital-services-act-dsa/id2860429/

1.3. Problemstillinger

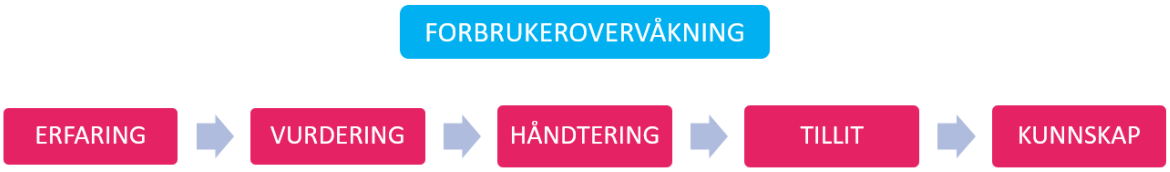
Nedenfor tar vi for oss hovedproblemstillingen i denne rapporten, som understøttes av en rekke underproblemstillinger.

Hovedproblemstilling

- Hvordan opplever norske forbrukere selv «overvåkningsøkonomien» i egen hverdag? (FORBRUKEROVERVÅKNING)

Underproblemstillinger

- Hvilke konkrete erfaringer, holdninger, kompetanse og praksiser har forbrukere knyttet til overvåkningsbaserte tjenester og markedsføring? (ERFARING)
- Foretar forbrukere avveininger av dilemmaer knyttet til kostnad/risiko-nytte ved å inngå i slike tjenester og i relasjon til markedsføring? (VURDERING)
- Har forbrukere utviklet strategier for å håndtere utfordringer/risiko som kan oppstå i forbindelse med overvåkningsbaserte tjenester og markedsføring? (HÅNDTERING)
- I hvilken grad har forbrukere tillit til selskaper i det digitale markedet, og til at myndigheter og regulering gjør den digitale hverdagen trygg? (TILLIT)
- Har forbrukere kunnskap om lovverk og rettigheter tilknyttet nettbasert forbrukeratferd? (KUNNSKAP)



Figur 1: Oversiktsfigur som visualiserer problemstillingene i studien

2. Metode og utvalg

Denne rapporten tar utgangspunkt i antakelsen om en sterkt tiltakende forbrukerovervåkning i det digitale markedet og i hverdagslivet generelt, der begrepet «overvåkningsøkonomi» benyttes som sentralt navigasjonspunkt. I studien har vi først foretatt en avgrenset strategisk kartlegging av relevante artikler og rapporter knyttet til temaet overvåkningsøkonomi. Deretter har det blitt gjennomført en dybdestudie av forbrukererfaringer gjennom to separate fokusgrupper, og til slutt en landsrepresentativ befolkningsundersøkelse for å få et oversiktsbilde over de funn og utfordringer som ble analysert frem i dybdestudien. Hver metodisk del danner grunnlaget for neste del.

Figur 2: Oversiktsfigur som viser metodisk gjennomgang i studien

2.1. Bakgrunnsstudie

I første del av prosjektet ble det gjennomført en bakgrunnsstudie av relevante artikler og dokumenter knyttet til temaet overvåkningsøkonomi. Dette var ikke en systematisk gjennomgang av litteraturen på feltet, men en *overview* (Grant & Booth 2009) med hovedformål å skaffe oversikt og avgrense temaet for å kunne fokusere studien. Samtidig ble litteraturen benyttet til å identifisere relevante spørsmål til den videre kvalitative og kvantitative delen av prosjektet.

I gjennomgangen av litteratur ble det i hovedsak benyttet rapporter og dokumenter som var kjent for forskerne, fra Forbrukerrådet, Datatilsynet, BEUC og en rekke SIFO-bidrag. I tillegg ble det gjort databasesøk i OsloMet sitt søkesystem. Her ble søketermene «surveillance economy», «consumer surveillance» og «surveillance-based marketing» benyttet. Litteraturen ble gjennomgått og sortert under temaene overvåkningsøkonomi, overvåknings-markedsføring, forbrukersårbarhet og kontroll, tingenes internett og kunstig intelligens, og til slutt autonomi og personvern.

Etter at litteraturen var gjennomgått, ble det i første fase utledet en rekke relevante spørsmål fra hvert litteraturbidrag som passet til prosjektets problemstillinger. Det ble deretter gjennomført en sortering av begreper og tematikker som det virket fornuftig å kategorisere spørsmålene etter. Dette resulterte i en omfattende kategorisering av potensielle spørsmål; overvåkning som begrep, teknologier, tjenestetyper, data, markedsføring, sporing, overvåkningsutfordringer og risikoer, sårbarhet, barn, forbrukernytte, personalisering, autonomi/agens/kontroll, samtykke, forbrukerkompetanse og forbrukerbeskyttelse.

For å forenkle og spisse kategoriseringen av spørsmål ble det gjennomført en ny analyse og sortering. Denne resulterte i en kortere og mer sammenhengende fremstilling av spørsmål under hovedtemaene; tilkopling, forbrukerdata, sporing av forbrukere, personalisering og målretting, overvåkningsbasert markedsføring, overvåkningsøkonomien, autonomi og

kontroll, og til slutt forbruker- og samfunnsutfordringer i tiden fremover. Intervjuguiden til fokusgruppene ble deretter utviklet basert på denne kategoriseringen.

2.2. Fokusgrupper

For å få innsikt i norske forbrukeres erfaringer, holdninger, kompetanse og praksiser relatert til digital overvåkningsproblematikk, ble det gjennomført to fokusgrupper. I forkant av fokusgruppene ble deltagerne bedt om å notere ned det de oppfattet som internettilkoblede enheter i hjemmet, og hvilke av disse som var personlige og hvilke som var delt med andre husstandsmedlemmer. Deltakerne fikk utdelt en hjemmeoppgave der de skulle lage en liste over internettilkoplede enheter hjemme, antall apper på telefonen, og apper de var usikre på med tanke på personvern. De skulle også velge ut apper de var spesielt usikre på, og tenke gjennom hvorfor de lastet ned disse.

Spørsmålene til fokusgruppene fulgte et narrativ som startet med forbrukernes egne tilkoblede enheter hjemme og apper på mobilen, til innsamlede data og hva de brukes til, hvordan data samles inn gjennom sporing, videre til personalisering og målretting basert på analyse av sporede data, og til slutt en mer overordnet diskusjon om overvåknings-økonomien som begrep og fenomen, og fremtidige utfordringer. Intervjuguiden fokuserte på deltagernes erfaringer, holdninger, kompetanse og praksiser relatert til disse temaene.

Deltagerne ble rekruttert av analysebyrået Norstat, mens SIFO har stått for gjennomføring og etterarbeid i form av transkribering, koding, og analyse. Norstat tok seg av samtykke-skjemaer og incentiver for deltakelse (gavekort). Til fokusgruppene ønsket vi voksne personer i alle aldre, og utvalget ble screenet etter alder, kjønn og bosted. Av praktiske årsaker ønsket vi deltakere fra Oslo og nærliggende områder ettersom fokusgruppene ble gjennomført på ukedager, rett etter arbeidstid. Fokusgruppene ble gjennomført i juni 2022 i SIFOs lokaler.

Fokusgruppene bestod av til sammen 13 deltagere i alderen 18-57 år, hvorav sju var kvinner og seks var menn. To deltagere hadde barn, og alle var bosatt i området Oslo og Viken. Deltagerne hadde ulike tilnærminger til, og kunnskap om, overvåkningsøkonomien og relaterte temaer. I analysen er deltakerne gitt nye navn, mens riktig alder vises i parentes etter pseudonymet. Fokusgruppe én bestod av 7 deltakere i alderen 18-57 år, mens fokusgruppe to bestod av 6 deltakere i alderen 24-43 år.

Tabell 1: Oversikt over deltakere i fokusgruppe 1, gjennomført 07.06.2023. Deltakerne er blitt tildelt fiktive navn

Fokusgruppe 1				
Navn	*Alder*	*Kjønn*	*Bosted*	*Sivil status*
Eva	29	Kvinne	Oslo	Enslig/Singel med hjemmeboende barn
Even	18	Mann	Oslo	Gift/Samboer uten barn
Elisabeth	31	Kvinne	Oslo	Enslig/Singel uten barn
Harald	57	Mann	Viken	Enslig/Singel uten barn
Petter	26	Mann	Oslo	Enslig/Singel uten barn
Celine	43	Kvinne	Oslo	Enslig/Singel med hjemmeboende barn
Susanne	42	Kvinne	Oslo	Gift/Samboer uten barn

Tabell 2: Oversikt over deltakere i fokusgruppe 2, gjennomført 21.06.2023. Deltakerne er blitt tildelt fiktive navn

Fokusgruppe 2				
Navn	*Alder*	*Kjønn*	*Bosted*	*Sivil status*
Oda	32	Kvinne	Oslo	Gift/Samboer uten barn
Awan	29	Mann	Oslo	Gift/Samboer uten barn
Tim	31	Mann	Oslo	Enslig/Singel uten barn
Henriette	24	Kvinne	Oslo	Enslig/Singel uten barn
Jorunn	43	Kvinne	Oslo	Enslig/Singel uten barn
Jonas	27	Mann	Oslo	Enslig/Singel uten barn

2.3. Landsrepresentativ spørreundersøkelse

Basert på funn fra bakgrunnsstudien og fokusgruppene utviklet vi et spørsmålsbatteri til en standard webbasert spørreundersøkelse. Her er Norstat sitt sannsynlighetspanel benyttet, og respondentene ble trukket tilfeldig fra panelet med kvoter for å sikre landsrepresentativitet. Ettersom dette er en webbasert undersøkelse forutsettes tilgang til internett, men respondentene rekrutteres i hovedsak via telefon til selve panelet.

Spørreundersøkelsen ble gjennomført i september/oktober 2022 med voksne i alderen 18-80 år (N=1000). Kjønn, alder og bosted/landsdel er benyttet som bakgrunnsvariabler, og dataene er vektet på disse tre variablene for å kompensere for skjevheter og for å sikre representativitet. Analysene er gjennomført i statistikkprogrammet SPSS og presentert i Excel, og kommenteres kun som prosentfordelinger i rapporten. Alle forskjeller mellom gruppene er signifikante på minst 5%-nivå.

Denne spørreundersøkelsen er i rapporten brukt til å underbygge og kontrastere resultatene fra fokusgruppene. Den gir et mer representativt bilde av hvordan norske forbrukere forholder seg til overvåkningsøkonomien enn det fokusgruppene gir.

Tabell 3: Vektet fordeling, etter kjønn, alder og bosted. N=1000. Sig.lev.: 95%

Kjønn		**Alder**					**Bosted**					
Mann	*Kvinne*	*18-29 år*	*30-39 år*	*40-49 år*	*50-59 år*	*60-80 år*	*Nord-Norge*	*Midt-Norge*	*Vest-landet*	*Øst-landet*	*Sør-landet*	*Oslo*
51 %	49 %	20 %	18 %	17 %	18 %	27 %	9 %	14 %	20 %	30 %	14 %	13 %

3. Bakgrunnsstudie

3.1. Innledning

I dette kapittelet går vi gjennom litteratur som dekker de problemstillinger vi ønsker å belyse i prosjektet. Litteraturen er identifisert gjennom forskernes tidligere kjennskap til litteratur, samt litteratursøk i databaser ved hjelp av sentrale nøkkelord slik det står beskrevet i metodekapitlet. Det er ikke foretatt et systematisk søk, men søkt strategisk etter utvalgt litteratur som svarer på flere problemstillinger knyttet til forbrukerovervåkning, og som adresserer både prosessen rundt forbrukerovervåkning i markedet og sentrale utfordringer forbrukere blir stilt overfor.

3.2. Overvåkningsøkonomien

Det er en rekke bidrag som direkte eller indirekte omtaler overvåkningsøkonomien som tema. I en rapport fra Datatilsynet og Teknologirådet (2016) ble «overvåkingsøkonomien» fremhevet som en sentral tematikk for *Personverndagen 2016*. Her var målet å rette søkelyset mot hvordan internettøkonomiens sporing av brukere har utviklet seg til en ren overvåkningsøkonomi preget av sterke kommersielle interesser. I 2013 bidro Snowden-avsløringene til en bred offentlig debatt om statlig overvåkning, mens EU i 2015 strammet grepet for å sikre bedre personvern for europeiske borgere ved at *Safe Harbor*-avtalen, som regulerer dataflyten mellom EU og USA, ble kjent ugyldig. Senere samme år ble arbeidet med GDPR igangsatt. Rapporten peker på fire sentrale teknologiske utviklingstrekk som bidrar til å bygge opp overvåkningsøkonomien; a) *tingenes internett*, b) *data og metadata*, c) *billig datalagring og regnekraft*, og d) *Big data-analyse og ny mønstergjenkjenning*. I tillegg fremheves to trender som påvirker forbrukere direkte; 1) *ekstern lagring/skytjenester*; det at data ikke lenger lagres på brukernes maskiner og kan kontrolleres av dem, men styres av store selskaper med kontroll over innhold og metadata, og 2) *produsentkontrollerte enheter*; der produsenter og leverandører i stor grad kontrollerer hva vi kan gjøre med enhetene våre. I tillegg står teknologien som muliggjør datainnsamling i overvåkningsøkonomien gjerne sentralt i å levere tjenestene forbrukerne får tilgang til. Det trekkes frem at dersom vi bruker Google Maps så forventer brukerne at den vet hvor vi er, mens Apples Siri fungerer bedre dersom den kjenner igjen stemmene våre.

Det finnes en rekke sporingsmetoder som kan sikre data fra forbrukere på nett. Her er *cookies/informasjonskapsler* mest utbredt, der en liten kode plasseres på brukerens maskin for å kjenne igjen nettsider og for å hente informasjon om brukeratferd. Samtidig hevdes det i rapporten til Datatilsynet/Teknologirådet (2016) at slike informasjonskapsler blir mindre relevante jo mer mobile plattformer og apper tas i bruk. Videre benyttes brukernes *IP-adresser* til å identifisere enheter i et nettverk. Ofte er brukeren et enkeltindivid, og dermed kan denne personen i praksis følges over tid. Det refereres også til *digitale fingeravtrykk*, som en sammensetning av informasjon om IP-adresse, programvare brukt, innstillinger, elektronikken i enheten, etc., noe som til sammen kan gi detaljert informasjon om brukeren. Når det gjelder *innloggede løsninger* benyttes dette internt i selskap og kan gi svært presis informasjon om brukere, spesielt hvis disse er kontinuerlig innlogget og beveger seg mellom tjenester i økosystemet og mellom brukerenheter.

Videre er *mobil sporing* blitt mer utbredt, gjennom mobiltelefoner, kroppsnær teknologi, aktivitetsbånd og smarte produkter hjemme og i bilen. Apple og Google gir dessuten smarttelefonbrukere en unik *annonse-ID* til annonseringsformål, som kan benyttes av operativsystem-eiere, app-utviklere og andre (Datatilsynet og Teknologirådet 2016). ID-en kan skrus av, men er aktivert som standard. Gjennom disse sporingsmetodene samles det inn person- og atferdsdata, og i mange tilfeller benyttes slike data i annonsemarkedet. Automatisert annonsehandel har økt kraftig i omfang og er nærmest umulig for forbrukere å få innsikt i. Annonsører, publisister, annonsebørser og datameglere samler, analyserer og selger data om forbrukere, som det lages brukerprofiler og segmenter av. Forbrukere derimot har liten innsikt i disse tredjepartene, hva slags data som omsettes, og til hvilke formål. Dette er svært vanlig for nettjenester der forbrukere bytter egne data mot gratis bruk av tjenester (jf. Throne-Holst og Kjørstad 2016).

Rapporten fra Datatilsynet og Teknologirådet (2016) fremhever at det finnes ulike strategier som kan benyttes for å «stå imot» sporing og datainnsamling, som å bruke adblocking, installere sporingsverktøy som undersøker sporing, slette cookies, bruke nettleserutvidelser som blokkerer sporing fra datasamlende tredjeparter, skru av annonse-ID, opprette annonsereservasjon hos f.eks Facebook og Google, benytte sporingsfrie søkealternativer som DuckDuckGo, og droppe fordelsprogrammer. Utfordringen er gjerne at forbrukere i liten grad er kjent med disse alternativene, eller benytter dem i liten grad selv om de har kunnskap om hvordan de fungerer (Hargittai og Marwick 2016, Hoffmann et al. 2016).

Datatilsynet og Teknologirådet (2016) identifiserer en rekke utfordringer i overvåknings-økonomien; 1) *nærgående kartlegging* og bygging av innholdsrike brukerprofiler på tvers av hverdagskontekster, 2) brukere som mister *oversikt og kontroll* fordi personvernet bestemmes av andre, mens brukerdata lekker ut til selskaper og ut av landet, 3) manglende åpenhet og *skjult innsamling* av personopplysninger til kommersielle formål utfordrer muligheten til å praktisere eget personvern, skaper ubalanse i maktforholdet mellom selskaper og forbrukere, og gjør diskriminering vanskelig å oppdage, og 4) *økende samtykkeapati* (Hargittai & Marwick 2016) kan oppstå ved for mange forespørsler, mens for mye/villedende/manglende informasjon og manipulerende design/*dark patterns* (European Commission 2022), forhindrer informerte beslutninger. Fra Datatilsynet og Teknologirådets side fremmes ideen om en type «dashboard» for data som kontrolleres av brukeren, med oversikt over samtykkeerklæringer og innsamling og bruk av data. Dette kan gi brukeren mulighet til å utøve større grad av kontroll over egne data.

I en rapport fra Christl (2017) pekes det på at stadig flere daglige interaksjoner på nettet er gjenstand for ubegrenset digital overvåkning (monitorering), analyse og vurderinger. Det fremheves at den nyvunne datamakten misbrukes i stor grad av selskaper til egen vinning, der forbrukere kan manipuleres på sårbare tidspunkter og «nudges» til overforbruk. Her er det en rekke delvis sammenkoplede databaser og selskaper fra ulike sektorer som står bak, og som samler, analyserer, deler, handler og utnytter data fra milliarder av mennesker. Utfordringene ligger i at; 1) markedet blir svært uoversiktlig, sammenflettet og ugjennomsiktig, 2) data-drevne beslutninger om folk kan være unøyaktige, tilfeldige eller partiske, og 3) folks muligheter og valg kan begrenses og lede til diskriminering og sosial eksklusjon, der spesielt algoritmiske beslutninger basert på digitale profiler kan forsterke eksisterende skjevheter og sosial ulikhet.

I tillegg til at mye av datainnsamlingen er skjult, uten kunnskap eller samtykke fra brukeren, kan følelsen folk sitter med av å bli overvåket gi en «nedkjølingseffekt» (chilling effect) der folk selv begrenser egne handlinger eller utsagn. Det er samtidig vanskelig å ikke delta i disse systemene, ettersom de fleste tjenester i dag er digitale. Man kan velge bort overvåkningskapitalisme, hevder Christl (2017), men i praksis betyr det å velge borte mye av det moderne liv.

Christl peker videre på at dagens online markedsføringsøkosystemer, som vi ser nærmere på i neste avsnitt, er en sentral driver for den omfattende digitale sporingen og profileringen vi er vitne til. Samtidig er det mange – også forbrukere – som anser dette som et lite problem, fordi de ikke klarer å se rekkevidden av potensielle sosiale, økonomiske og etiske konsekvenser. Men risikoen er reell ettersom den gjennomgripende sanntidsovervåkingen som er utviklet for online markedsføring raskt brer om seg til andre områder, fra prising og kredittvurdering, til risikostyring og politisk kommunikasjon. Dermed mener Christl at mange har feil forståelse av «markedsføring», og at dette i dag går langt utover det å vise annonser. Datadrevet prediktiv analyse, personalisering, måling og testing er derimot utviklet i den hensikt å kunne påvirke atferd i stor skala. Forbrukere blir konstant evaluert, sortert, kategorisert og rangert – og gjøres dermed mer transparente og forutsigbare – mens selskaper og forretningspraksiser blir mer ugjennomsiktige. Dette skaper en maktasymmetri i favør selskapene. Spesielt innen helse, forsikring og finans ses det som problematisk at feilaktige, skjeve, og diskriminerende automatiserte beslutninger basert på digitale forbrukerprofiler kan forekomme, og at store selskaper kontrollerer interaksjonen med forbrukere (Christl 2017). Og trekker man utfordringen enda lenger, stiller Christl spørsmålet ved hvordan kommersiell digital profilering og datadrevne algoritmiske beslutninger vil kunne påvirke likhet, frihet, autonomi, demokrati og verdighet – på individ- og samfunnsnivå – over tid.

En sentral utfordring her er hva slags personopplysninger og brukerdata kommersielle selskaper får tak i (Christl 2017). For å gjenkjenne folk på tvers av plattformer, tjenester og hverdagskontekster samles, aggregeres og sammenkoples personlige identifikatorer (som epost, tlf.nr, IP-adresser, etc). I tillegg brukes i større grad biometri til å identifisere og verifisere identitet – som fingeravtrykk, iris- og ansiktsgjenkjenning – men også ganglag, stemme og tastemønster. Disse digitale representasjonene blir mer og mer sentrale, ettersom navn i seg selv ikke er nyttige i den digitale verden. Med en slik personlig kopling kan «personalisering» eller målretting av budskap gjennomføres. Personalisering er blitt et viktig verktøy for å påvirke atferd, men også for å eksperimentere på folk. Man kan kontinuerlig teste og måle hvordan folk reagerer på innhold og på variasjoner i testingen. Samtidig er veien kort til å utnytte data og sporing til andre formål, en type «formålsglidning» (*mission creep*) som forbrukere ikke har samtykket til. Datakategoriene som benyttes til personalisering kan være mange, slik som *frivillige data* delt av personene selv, *observerte data*, data som inneholder *faktainformasjon* om individer, eller *utledete data* om antatt atferd.

I og med utviklingen og adopsjonen av smarttelefoner og tingenes internett (IoT) i forbrukermarkedet (jf. Kjørstad et al. 2017, Slettemeås 2019), er det dette som nå i stor grad bidrar til dagens omfattende sporings- og profileringsøkosystem. Dessuten må alle brukere av smarttelefoner være tilknyttet de store tech-selskapene (Google, Apple eller Microsoft) med en konto for å få telefonene til å fungere, mens de fleste apper overfører data til tredjeparter (Christl 2017). Med IoT kommer dessuten stadig mer utstyr med sensorer og

nettverks-funksjonalitet, som kan gi enorm innsikt i forbrukeratferd på tvers av hverdags-kontekster. I dag består hverdagen vår dermed av et gjennomtrengende nettverk av digital sporing og profilering, der en rekke sektorer slår seg sammen i en ny omfattende dataindustri som utnytter aggregerte og anonymiserte Big data, metadata om nettsider, apper, innhold og lokasjon, nettleser- eller enhetsspesifikke data, og individ- og husholdsdata (Christl 2017). Den store utfordringen i dette landskapet, hevder Christl, er at forbrukere har for liten forståelse og innsikt i de teknologiske prosessene og i kortsiktige og langsiktige konsekvenser, grunnet stor grad av kompleksitet og abstraksjon, manglende transparens, manglende informasjon, forvirrende spørsmål i forespørsler, og lange brukeravtaler som systematisk lurer forbruker inn i datakontrakter.

Mens mye av litteraturen rundt overvåkning og forbrukere er knyttet til spesifikke mekanismer eller modeller som opererer i markedet, løfter Zuboff (2019) blikket og ser på mer omfattende konsekvenser for hverdagslivet. Hun spør, mer eksistensielt, om den digitale fremtiden er levelig og om den vil bli et «hjem» for oss. Hun mener vi ser konturene av at den digitale sfæren tar over og redefinerer alt vi kjenner til (jf. Slettemeås og Storm-Mathisen 2021), og at dette skjer så raskt at det er krevende å reflektere godt om endringene og hva de betyr for oss, på godt og vondt, både nå og i tiden fremover[8].

Zuboff retter blikket bakover i tid for å kontekstualisere utfordringen. I år 2000 initierte Georgia Tech prosjektet *Aware Home*, et laboratorium for allestedsnærværende teknologi, der menneske-hjem symbiosen skulle testes ut med en plattform som høstet personlig informasjon både fra *wearables* og fra omgivelser via kontekstfølsomme sensorer. Her så man for seg en helt ny kunnskapsproduksjon fra de nye datasystemene, og at rettighetene til den nye kunnskapen, og makten til å bruke den til å forbedre egne liv, ville beholdes innenfor husholdet. Dette skulle styrke hjemmet som et selvstendig og privat fristed, basert på tillit, enkelhet og individets suverenitet, ettersom *Aware Home*'s informasjonssystem ble sett på som et sluttet system. Fordi huset kom til å overvåke beboernes handlinger og bevegelser kontinuerlig, ble det sett på som nødvendig at beboerne selv beholdt kunnskap og kontroll over denne informasjonen.

I dag, derimot, er smarthjem-markedet enormt, men i liten grad styrt av lukkede systemer under forbrukernes kontroll[9]. Hvert enkelt smartprodukt må koples trådløst til et hjemmenettverk og disse har alle egne brukeravtaler[10]. De fleste løsningene er dessuten sky- og nettverkbaserte, der data styres ut av hjemmene og inn i store servere. Både eierskap, dataflyt, oppdateringer og funksjonalitet styres utenfra av kommersielle selskaper, og forbrukere er bundet til en rekke avtaler. Forbrukere må følge alle oppdateringer for å sikre at systemene ikke hackes, kompromitteres ellers svekkes fordi de ikke er oppdaterte (jf. problemstillinger som adresseres i det SIFO-ledete prosjektet *Relink*[11]).

[8] Jf. debattinnlegget i Aftenposten «Teknologi må temmes», Dag Slettemeås SIFO/OsloMet, oktober 2017: https://www.aftenposten.no/meninger/debatt/i/gXk29/kort-sagt-tirsdag-24-oktober

[9] Jf. kronikken i Morgenbladet «Trojanske hester under juletreet», Dag Slettemeås SIFO/OsloMet, desember 2019: https://www.morgenbladet.no/ideer/kronikk/2019/12/12/trojanske-hester-under-juletreet/

[10] Privacy policies (PP), Terms and conditions (T&C) og/eller End-user license agreements (EULAs)

[11] Relink: https://uni.oslomet.no/relink/

Zuboff (2019) ser på «overvåkningskapitalisme» som et system der menneskelig erfaring utvinnes som «gratis råmateriale», og som igjen omgjøres eller oversettes til atferdsdata. Atferdsdata kan brukes til produktutvikling og tjenesteforbedring, men det meste vurderes som «atferdsmessig overskudd» (behvioural surplus) som fores til tekniske systemer (machine intelligence) for å lage «prediksjonsprodukter» (prediction products), som det til slutt handles med på markedsplasser (behavioural futures markets). Målet til kommersielle selskaper er å komme nærmest mulig en forståelse av forbrukeres fremtidige atferd, for så å kunne intervenere ved bruk av påvirknings- og manipuleringsteknikker som benyttes for å personalisere og målrette budskap. Dermed bidrar ikke slike maskinautomatiserte prosesser kun til å avdekke mulig atferd, men til å *forme og endre* menneskelig atferd mot *andres* (les: kommersielle) *formål og ikke forbrukernes egne*. Kontinuerlig tilkopling og en allestedsnærværende dataarkitektur gjør det det dessuten vanskelig for forbrukere å unnslippe og finne alternativer. Zuboff sikter til at markedet endres til et prosjekt som søker total visshet, der troen på tall og prediksjon av fremtiden over tid vil erstatte politikk og demokratiske beslutninger.

Overvåkningskapitalismens produkter og tjenester er heller ikke gjenstand for et naturlig bytteforhold mellom produsent og forbrukere. Istedenfor blir forbrukere lurt gjennom gratis tjenester og kompliserte avtaler til å utlevere personlige opplevelser og erfaringer. Ettersom vi er blitt avhengige av internett for sosial deltakelse, og internett nå er gjennomsyret av kommersialisme, blir nettopp forbrukernes avhengighet kjernen i det kommersielle overvåkningsprosjektet, mener Zuboff (2019). Dermed er motstand vanskelig og en «psychic numbing»[12] oppstår der vi vennes til å bli sporet, analysert, utvunnet og modifisert. Måten forbrukere reagerer på dette kan variere, fra å hengi seg til fatalisme og hjelpeløshet (Draper og Turow 2019), til å rasjonalisere at man «ikke har noe å skjule»[13], eller at det ikke finnes gode alternativer.

I en artikkel av Clarke (2019) fremheves det at digitaliseringen av data om mennesker over tid har vært tilknyttet diverse samfunnsforestillinger, slik som informasjonssamfunnet, overvåkningssamfunnet, overvåkningsstaten og overvåkningskapitalismen – mens Clarke omtaler fenomenet som den «digitale overvåkningsøkonomien»[14]. Clarke ser historisk på internettutviklingen, der den tidlige fasen bar med seg anonymitet. Etter dotcom-boblen sprakk i år 2000 og frem til 2010 var det optimisme knyttet til at forbrukermarkedsføring ville fremstå som mer samhandlende enn manipulerende (Slettemeås og Storm-Mathisen 2021). Men web 2.0-arkitekturen la tvert imot grunnlaget for den digitale overvåkningsøkonomien – langt unna den tette, tosidige dialogen man så for seg mellom forbrukere og bedrifter. Mens det ikke var antydning til overvåkningselementer i midten av 1990-tallets skildringer av den digitale økonomien, så man utover på 2000-tallet tendensene til en universell overvåkningsøkonomi, ifølge Clarke (2019).

[12] Zuboff skriver at for et par tiår siden så man på teknikker for å modifisere atferd i stor skala som uakseptabelt for individets autonomi og den demokratiske orden, mens dette i dag har blitt rutine.

[13] Jf. kronikken i Vårt Land, «Selvsagt har vi noe å skjule; vårt eget privatliv», Dag Slettemeås SIFO/OsloMet, oktober 2016: https://www.vl.no/nyheter/2016/10/12/selvsagt-har-vi-noe-a-skjule-vart-eget-privatliv/

[14] Selve begrepet «digital overvåkningsøkonomi» ble fremsatt av Andrejevic (2014), sammen med den populariserte ideen om at «hvis du ikke betaler, så er du produktet».

Sentralt i ideen om overvåkningsøkonomien står en ny form for forretningsmodell som er basert på oppkjøp og konsolidering av svært store mengder personopplysninger, og utnyttelse av disse for å målrette annonser og manipulere forbrukeratferd (slik tidligere bidrag har pekt på), i tillegg til å prise varer og tjenester på det høyeste nivået hver enkelt forbruker er villig til å betale. Forbrukere overtales til å gjøre egne data tilgjengelige for markedsførere slik at denne type personalisering kan gjennomføres. Men Clarke (2019) mener den digitale overvåkningsøkonomien ikke kun representerer alvorlige trusler mot interessene til enkeltpersoner, samfunn og politikk, men også mot bedrifter. I følge Clarke kan institusjons-tilpasning eller folkelig opprør bidra til å overvinne de verste negative konsekvensene, men dette er ikke nødvendigvis tilstrekkelig.

Clarke identifiserer videre enkelte nytteverdier for forbrukere i den digitale overvåkningsøkonomien, som bekvemmelighet og tidsbesparelse, fordi attraktive muligheter byr seg frem hele tiden, mens underholdningsverdi bygges inn som en naturlig del av kundeopplevelsen. Han fremhever *hedonistiske fordeler* (underholdning, nytelse, moro), *funksjonelle fordeler* (informasjon, effektivitet, bekvemmelighet), *sosiale ytelser* (kommunikasjon, relasjon, involvering, tillit) og *psykologiske fordeler* (tilhørighet, identifikasjon).

Samtidig er det en rekke trusler mot individet som følger med, som *stimulering til økt impulskjøp* eller tvangsmessige kjøp basert på målrettet markedsføring som trykker på forbrukernes «kjøpsknapper», *diskrimineringsteknikke*r som forhindrer tilgang til tjenester (eller svartelisting), eller *dårlige data* som kan være utdaterte, feil, irrelevante, sensitive, eller av lav kvalitet. Dessuten kan data fremstå som datakompositter bestående delvis av individdata og delvis at data fra andre individer i samme hushold. Videre kan digitaliseringen gå utover ren kvantifisering til *automatisert beslutningstaking*, umoderert av mennesker. Dermed kan uheldige eller feilaktige beslutninger tas, som heller ikke lar seg avdekke eller korrigere grunnet algoritmers manglende transparens. Clarke (2019) trekker også frem, som Christl (2017), faren for *nedkjølingseffekter,* der utstrakt overvåkning kjøler ned atferd – og *psychic numbing*, som Zuboff (2019), som beskriver resignasjonen folk kan oppleve i møte med det å bli sporet, analysert og påvirket.

Cecez-Kecmanovic (2019) viser til Zuboffs (2019) utsagn om at vi for få år siden så på utfordringer knyttet til informasjonssamfunnet, mens vi med digital overvåkning står overfor helt andre trusler mot individuelle interesser og demokratiske verdier. Forfatteren peker også på Clarkes (2019) forskingsagenda, og da spesielt på den *manglende motstanden* mot den digitale overvåkningsøkonomien. Det henvises også her til historien, og at det ved årtusenskiftet var mye entusiasme rundt internett og ideen om å kommunisere og dele ideer og kunnskap. Men tjenestetilbydere slet med gode forretningsmodeller for å sikre gratis bruk av tjenester, og betalingsmodeller ble sett på som uaktuelt fordi det manglet sikre betalingsløsninger. Dermed dominerte reklamebasert finansiering, en forretningsmodell som krevde mer og mer data og invasiv kunnskap, samtidig som forbrukere ble mer og mer vant til gratis innhold og tjenester. Denne gradvise «normaliseringen» av en overordnet forretningsmodell kan ha bidratt til å forhindre omfattende og aktiv motstand, og utvikling av nye ikke-persondata-baserte forretningsmodeller. Spørsmålet er hvem som skulle stått i bresjen for slik aktiv motstand – forbrukere selv, forbrukersammenslutninger, regulerende myndighet eller andre?

I artikkelen til March (2019), som ser overvåkningsøkonomien som en krysning mellom IT og samfunn, vektlegges det at teknologien kan ha intenderte (for designere) og uintenderte (for forbrukere og samfunn) konsekvenser, og at forståelse for dette er avgjørende. March mener begrepet «overvåkningsøkonomien» i utgangspunktet er negativt ladet og må klargjøres. Det er ikke tydelig nok at eksempelvis målrettet markedsføring er «dårlig» uavhengig av kontekst, og heller ikke i hvor stor grad forbrukeratferd faktisk manipuleres eller prisdiskriminering forekommer – og hvor skadelige markedføringen eventuelt er for forbrukere (gitt at mekanismene eksisterer). March mener at bedrifters mål til alle tider har vært å *forutsi* (gjennom markedsundersøkelser) og *modifisere* (gjennom markedsføring) atferd. Derfor må det heller rettes studier mot faktiske opplevelser og konsekvenser av den nye datadrevne økonomien.

I artikkelen vektlegges forbrukernes agens og evne til å ta til seg og handle på bakgrunn av informasjon (March 2019). Det eksemplifiseres at brukere av Alexa[15], som ønsker å benytte assistentens informasjonstjenester, må forstå økosystemet der disse tjenestene tilbys, at dette er «prisen av gratis», og at det å bytte data for tjenester kan være en rimelig transaksjon. Utfordringen ligger i at folk ikke tilskriver egne data nok verdi eller at forbrukere kanskje ikke forstår at deres data brukes til å kategorisere dem i markedssegmenter. Her peker han på forbrukeropplæring som en strategi, eller bruk av nettjenester der forbrukere kan selge sine egne data[16], hvis de er bekymret for å ikke få tilstrekkelig kompensasjon for dataene sine. Dersom problemet er bruken av persondata for å målrette annonser, kan forbrukere gjøre defensive tiltak, som for eksempel å bruke adblocking, mener March.

I motsetning til Clarke (2019), som hevder at forbrukeren konverteres fra kunde til et produkt, mener March at forbrukeren ikke er et produkt per se, men ressursen som genererer produktet – og at forbrukerens interesse er sentral i prosessen. Forbrukeren må være interessert i produktet som annonseres, og March stiller spørsmål ved hvorvidt forbrukeren faktisk kan foreta kjøp som er imot deres velferd. Her anerkjenner for så vidt ikke March mulighetene for manipulasjon i forbindelse med målrettet markedsføring, eller dataøkonomiens grunnleggende overvåkende og påvirkende strukturer.

Uansett posisjon, så er March (2019) opptatt av det å stille viktige forskningsspørsmål knyttet til relasjonen mellom forbrukere, kommersielle aktører og overvåkningsøkonomien; hvilke forbrukerholdninger er knyttet til bytte av data for tjenester? Er det forbrukerbevissthet omkring dette byttet? Er det spørsmål om hvor rettferdig byttet er? Eller hva forbrukere bør gjøre hvis de oppfatter byttet å være for invaderende? Handler det om den etiske naturen til markedsføringsnettverkene? Er det maktrelasjonen mellom datainnsamlingsselskaper og forbrukere som står sentralt? Er det spørsmål om effekten annonsering har på forbrukeratferd? Dette er sentrale spørsmål som er relevant for videre undersøkelser.

Aho og Duffield (2020) tar en annen posisjon enn March (2019), og som ligger nærmere Zuboff (2019). Forfatterne viser til at ettersom stadig mer av menneskelig aktivitet beveger seg over på nett blir individer omgjort til «datasubjekter» hvor handlinger, beslutninger og holdninger kan tolkes og manipuleres for profitt. I Zuboffs logikk «kommodifiseres» og «monetiseres» hverdagslivet og gjenskapes som «atferd» – og mennesker reduseres til

[15] Alexa er en virtuell assistent utviklet av Amazon

[16] Her nevner March tjenesten https://datacoup.com/

kvantifiserbare subjekter, som gjennom Big data analyse blir mer leselige og manipulerbare. I artikkelen til Aho og Duffield (2020) vektlegges det at teknologien ikke har gjort individer til tankeløse roboter der fri vilje er totalt overtatt av algoritmer, men at ettersom mer av livet går fra å være analogt til å bli digitalt, må en huske på at digitale grensesnitt stort sett utformes av profittorienterte bedrifter. I hovedsak fremstår det som overvåkningskapitalismen har i seg en slags sosial kontrakt der folk stilltiende aksepterer dataovervåkning så lenge de får gratis og relevante tjenester. I overvåkningsstudier fremheves det hvordan asymmetrisk dataakkumulering fratar subjekter kontroll over egen informasjon og dermed agens, og legger fundamentet for tilsynelatende «rettferdige» datapraksiser, inkludert sosial sortering og diskriminering (Cinnamon 2017).

Responsen globalt på denne utviklingen har vært ulik. Derfor bør fenomenet ikke nødvendigvis diskuteres som at problemstillingene er universelle, hevder Aho og Duffield (2020). Mens EU ser på muligheter for å begrense overvåkningskapitalismens makt, omfavner Kina den. EU har de siste årene reagert reaktivt gjennom GDPR, og fremhevet viktigheten av innbyggernes personvern og begrensinger på kommersiell innsamling og bruk av persondata, både for bedrifter og stater. Kinas sosial-kreditt system (SCS[17]) ses derimot som proaktivt ved å benytte en kombinasjon av overvåkningsarkitektur og kunstig intelligens til å fremme statlige formål. For Kina ses dette som del av en omfattende sosial reform som vil sikre Kinas utvikling i informasjonsalderen. Mer inngående hevdes det at Kinas mål er å overføre dataovervåkningsmakt fra privat til offentlig sektor, og dermed fremme statens (eller partiets) politiske agenda (Aho og Duffield 2020). Europa, derimot, har et normativt mål om å beskytte individuell frihet og personvern, som er ensbetydende med å begrense atferdskontrollen bedrifter har over forbrukere.

Heilmann (2016) omtaler SCS-prosjektet som den «mest ambisiøse orwelliske planen i menneskets historie», nettopp ved å søke å etablere en all-seende stat. Grunnlaget er tildeling av dynamisk kredittskåre til alle økonomiske aktører som opererer innenfor det nasjonale markedet, fra gigantiske konglomerater og statseide virksomheter, ned til små bedrifter og enkeltpersoner. Poengsummene tildeles av en rekke algoritmer som operativt administreres av en sentral myndighet. Her overvåkes atferd av et system med skreddersydde belønninger og straffer. SCS muliggjør overvåkning og justering i sanntid og gir staten mulighet til å rulle ut nye retningslinjer og programmer svært raskt, og observere, eksperimentere og justere umiddelbart. Aho og Duffield (2020) oppsummerer at EUs og Kinas fremgangsmåter fremstår som radikalt forskjellige i hvordan data konseptualiseres og formål formuleres, men begge har kommet i kjølvannet av den globale digitale akkumuleringslogikken som Zuboff (2019) skisserer.

3.3. Overvåkningsbasert markedsføring

Et sentralt aspekt ved overvåkingsøkonomien er fenomenet «overvåkingsbasert markedsføring» (OBM). Forbrukerrådet (2021) hevder at det er overvåkningsbasert annonsering som har bidratt til å drive frem selve overvåkningsøkonomien. I utgangspunktet er all reklame delvis målrettet, og delvis designet med en viss grad av manipulasjon for å få oss til å kjøpe produktet. Kontekst, plassering og design av reklame betyr at den er rettet mot

[17] Social credit system

visse målgrupper, noe som også gjelder tradisjonell reklame. Det som skiller overvåknings-basert markedsføring fra andre varianter er at den preges av en sterk grad av segmentering, gjennom sporing og profilering basert på persondata og brukeratferd. Tradisjonell reklame kan være plassert på bakgrunn av kontekst, mens OBM målretter mot et individ eller gruppe, og den følger forbrukeren på tvers av kontekster. Forbrukerrådet (2021) nevner variasjoner av OBM som *atferdsmarkedsføring* (behavioural advertising), *mikromålretting* (micro targeting), eller *programmatisk markedsføring* (programmatic advertising).

I hovedsak er ideen med OBM å vise forbrukere ulike reklamer basert på slutninger om deres interesser, demografi, eller andre karakteristikker innhentet gjennom sporing av deres aktiviteter i tid og rom (ConsFed 2021). Sporing går oftest gjennom identifisering av en nettilkoplet enhet (PC/mobil) som brukeren benytter til å søke informasjon, kjøpe, være på sosiale medier, se videoer på, etc. Disse dataene kan settes sammen og gi et detaljert bilde av individer – eller hele hushold – til og med uten personidentifiserbar informasjon. Det er adtech[18]-industrien som er sentral i overvåkningsbasert markedsføring. De sporer, lager forbrukerprofiler, matcher forbrukere med reklame basert på profiler, og plasserer reklamen i relevante kontekster. Adtech kan holde til på publisistenes nettsider eller på apper og sporer hva brukere gjør. Når en forbruker besøker en slik plattform formidler adtech-selskapet brukerprofilen til annonsører, og en automatisert auksjon starter og avsluttes i løpet av millisekunder, der rettigheten til å reklamere til den aktuelle personen selges. Publisistene (nettsteder) får penger når forbrukeren trykker på reklamen. Google og Facebook har sine egne adtech-økosystemer og sporer brukere både på egne plattformer og andres nettsteder og apper.

ConsFed (2021) mener, som Forbrukerrådet, at det er en rekke utfordringer knyttet til nettopp denne type overvåkningsbasert markedsføring. Spesielt nevnes mulighetene for *diskriminering*, for eksempel i boligmarked, arbeidsmarkedet og på kredittfeltet. *Manipulasjon* nevnes også her, altså potensialet for bruk av usynlige og invaderende teknikker for å manipulere forbrukere, noe som kan frarøve dem valgmuligheter eller få dem til å tro at de selv velger fritt og upåvirket. Videre bidrar personalisert prising til å *skjule prisen* fra andre forbrukere. Dette gjør det vanskelig å vite om prisen man oppgis er forskjellig fra andres, noe som dessuten gjør kollektiv motstand mot prisregimer krevende for forbrukere. Algoritmer kan også fores med *feilaktige data* og lede til slutninger som er uheldige eller problematiske for forbrukeren.

Risiko for eksponering av forbrukere oppstår på grunn av at enorme mengder personlige data lagres og benyttes, blant annet i overvåkningsbasert markedsføring. Dette kan lede til id-tyveri, ondsinnet sporing, innsyn i data fra myndigheter uten lovlig hjemmel, etc. Dessuten refereres det til studier som viser at overvåkningsbasert reklame ikke er så effektiv til målretting som tidligere antatt. Uansett fremheves det i rapporten til ConsFed (2021) at risikoen langt overgår fordelene ved denne type markedsføring. Et alternativ som nevnes i rapporten er *kontekstuell reklame*, som plasserer relevant reklame på nettsiden som forbrukeren benytter til enhver tid, basert på tema og karakteristikk ved innhold, og uten å spore brukeren. Det vises til at denne formen også er mer kostnadseffektiv enn målrettet

[18] Advertising technology

reklame, og kan gi større inntekter til publisister, fordi kostnadene som skal dekke tredjeparter i adtech-industrien forsvinner.

Forbrukerrådet (2021) trekker frem at det å overvåke brukeratferd, kommersialisere personopplysninger og utnytte forbrukere er blitt normen på internett, der de konstant overvåkes og loves relevant reklame som motytelse. Forbrukerrådet mener dette er i strid med grunnleggende *personvernrettigheter* og skadelig for *forbrukerbeskyttelsen,* og kan føre til manipulasjon og diskriminering i stor skala, slik vi ser at andre har påpekt. I tillegg til personvernutfordringer mener Forbrukerrådet at høsting og lagring av personopplysninger og ugjennomsiktige forretningsmodeller bidrar til betydelige *sikkerhetsproblemer*, og øker faren for desinformasjon, radikalisert innhold, og svindel, i tillegg til mulige negative effekter for folkehelsen og for journalistikken. Individualiseringen, personaliseringen og mikromålrettingen av reklame gjør det vanskelig å avdekke ulovlig aktivitet og øker dermed forbrukersårbarheten.

Derfor mener Forbrukerrådet (2021) at den høye risikoen for forbrukere – i tillegg til begrensede muligheter for håndheving fordi dette er ressurs- og tidkrevende og ofte skjer etter skaden har inntruffet – gjør at et forbud mot denne type markedsføring anses som det beste alternativet. Det vises til at både EU-parlamentet og European Data Protection Supervisor mener overvåkningsbasert annonsering gradvis bør fases ut og med tiden forbys. Og som ConsFed (2021) over, mener Forbrukerrådet at systemet med omfattende overvåkning fremstår som disproporsjonalt for forbrukere, der nytten ikke oppveier risikoen.

En grunnleggende utfordring Forbrukerrådet peker på er at alle forbrukere er sårbare i utgangspunktet når de står overfor systemer som samler inn data i det skjulte, lager profiler og målretter budskap (jf. også BEUC nedenfor). Alle nettaktiviteter blir kommersialisert, og omfanget og innvevingen av teknologi i forbrukerhverdagen betyr at forbrukere selv har få muligheter til å beskytte seg. Med bruk av kunstig intelligens og maskinlæring kan disse utfordringene bli større med tiden. Forbrukerrådet (2021) peker på flere problematiske og til dels skadelige effekter av OBM. Et aspekt som ofte trekkes frem er at *følelsen* forbrukere opplever ved å bli sporet, profilert, eller overvåket, er at det er «ekkelt» eller «ubehagelig» (creepy). Et annet aspekt er at mange av prosessene rundt OBM er *usynlige* for forbrukeren; de vet ikke hvilke data om dem som oppbevares, hvordan de prosesseres, overføres, eller utnyttes – eller av hvem. De vet ikke hvem som får samme type reklame, og kan dermed heller ikke vite om de diskrimineres mot eller manipuleres, og at de dermed er sårbare. Her vektlegger Forbrukerrådet et viktig aspekt; manglende transparens i systemet er et overbyggende problem som forsterker de skadelige effektene relatert til personvernbrudd, manipulering og diskriminering. Dette mener de ikke kan løses med mer transparens eller bedre forbrukerinformasjon, men at forbud kan bedre situasjonen. I sum lister Forbrukerrådet følgende utfordringer: manglende transparens, fare for personvern- og datasikkerhetsbrudd, manipulering, diskriminering, desinformasjon, konkurransehindring, svindel og tillitsutfordringer.

Dagens marked forutsetter at forbrukere har urealistisk stor makt og teknologisk og juridisk kompetanse til å ta informerte valg, bruke tid på å lese juridisk dokumentasjon, og kjempe mot manipulerende design som søker å påvirke deres autonomi, beslutninger og valg. Forbrukerrådet (2021) mener at enkelte av utfordringene som skisseres knyttet til OBM allerede er regulert gjennom GDPR og ePrivacy-direktivet, men at svak håndheving har ført

til at problemene vedvarer. Et viktig aspekt som fremheves er at utfordringene med overvåkningsbasert reklame går langt utover kun databeskyttelse og personvern. I det kommende DSA vil det likevel gis større mulighet til å ta tak i denne type utfordringer.

En landsrepresentativ spørreundersøkelse som ble gjennomført i 2015 av Opinion (jf. Datatilsynet og Teknologirådet 2016), viste at 76% hadde fått opp annonser på skjermen med direkte forbindelse til hva de hadde foretatt seg på nett i forkant. 70% mente de hadde dårlig oversikt over hvilke opplysninger ulike nettaktører samlet inn om dem, og en like stor andel mente de hadde dårlig oversikt over hvordan nettaktørene brukte opplysningene om dem. Videre mente 79% at det var ubehagelig at nettaktører samlet og analyserte personopplysningene deres og delte disse med andre selskap for å vise tilpasset reklame. Folks holdninger til bruk av personopplysninger til ulike formål ble også undersøkt. Det viste seg at 56% var enige i at i situasjoner der kjøpsmønstre registreres (fordi man er medlem) var det greit at medlemskundene fikk lavere pris[19] enn andre, ettersom butikken kunne analysere deres kjøpsvaner og belønne lojalitet.

For nettaviser var responsen mer laber, kun 19% mente det var greit at nettaviser logget leservaner for å kunne tilpasse reklame til enkeltindivider. Respondentene ble informert om at gratis nettjenester (nettaviser og sosiale medier) gjerne reklamefinansierer denne virksomheten og at brukernes personopplysninger i stor grad analyseres for å kunne tilby individuelt tilpasset reklame. Hvis folk kunne velge, viste undersøkelsen at hele 73% ønsket tilfeldig reklame, mens 27% ville ha tilpasset reklame[20]. Det påfølgende spørsmålet var hvorvidt folk ville betalt for nettjenester med penger for å unngå at tjenesten analyserte personopplysninger for å gi tilpasset reklame. Her svarte 52% at de ikke ville betalt, mens 20% hadde takket ja til et betalingsalternativ. Samtidig fremkom det et tilsynelatende paradoks i Opinion-undersøkelsen: Det var et tydelig misforhold mellom ubehag og bekymring hos brukere, og praksis. De som bekreftet ubehag ved innsamling/analyse av persondata, oppga samtidig å bruke flere gratistjenester. I den forbindelse mente 45% at det var vanskelig å finne personvernvennlige alternativer, mens 21% ikke hadde tenkt noe særlig over egen praksis, mens 15% oppga å ikke være klar over hvordan opplysningene blir brukt.

3.4. Forbrukersårbarhet og kontroll

Den europeiske forbrukerorganisasjonen, BEUC, fremhever i en rapport at forbruker-sårbarhet i den digitale hverdagen gjerne er knyttet til *atferdsmanipulasjon*, *utnyttelse av sårbarheter* og *påvirkning av valgfrihet* (BEUC 2021). Det presiseres at sårbarhet ikke er en stabil egenskap ved en person; kilder til sårbarhet varierer, de er ofte situasjonelt betinget, og det kan være ulike grader eller stadier av sårbarhet. BEUC peker på forskning som viser at kompetente forbrukere forventes å ha makt til å ta informerte valg og til å kunne gi eller trekke tilbake samtykke til datainnsamling og prosessering. Men det å ha kontroll over deling av privat informasjon kan også bidra til å redusere personvernbekymringer og øke villigheten til å publisere sensitiv informasjon, det såkalte «kontrollparadokset». Slik falsk

[19] Men her var det en større andel svært uenige (22%) enn svært enige (16%)

[20] En Telenor-undersøkelse fra 2015 viste også svært lav villighet til å dele personopplysninger for å få tilpasset reklame, mens delingsviljen var høyere for andre formål som personaliserte apper, nettjenester eller service. Ref: http://www.telenor.no/om/teknologi-norge/personvern-internettets-tidsalder.jsp

sikkerhetsfølelse (som også kan knyttes til ulike former for personvernmerking) kan komme av for sterk tiltro til samtykke som grunnleggende prinsipp for dataprosessering, og BEUC etterspør alternative post-samtykke løsninger. Dessuten fremheves strukturelle makt-relasjoner som introduseres i slik valgarkitektur og det at plattformer kan kjøre konstante eksperimenter mot forbrukere for å indentifisere sårbarheter og målrette budskap tilpasset disse.

BEUC-rapporten (2021) viser til at ideen eller idealet om en «gjennomsnittlig forbruker» gjennomsyrer store deler av europeisk forbrukerlovgivning, og har vært sentral i å bygge fortellingen om forbrukermakt, der forbrukere beskytter seg selv gjennom aktive og velinformerte valg i markedet. Dette står i kontrast til den «sårbare forbrukeren», som anses å være mer utsatt for urettferdig handelspraksis enn andre, og som i mindre grad evner å beskytte seg selv. BEUC hevder at i digitale markeder er stort sett alle forbrukere potensielt sårbare. Digital sårbarhet innebærer en universell tilstand av forsvarsløshet og mottakelighet for (utnyttelse av) maktasymmetri, som resultat av økende automatisering av handel, databaserte forbruker-selger-relasjoner, og selve arkitekturen til digitale markedsplasser.

Digitalisering av forbrukermarkeder skaper økt avhengighet av algoritmisk profilering, automatisert beslutningstaking og prediktiv analyse. Data benyttes til å foreslå tjenester, minne forbrukere på ting de kan ønske seg, og gi dem personlige tilbud. Fordelene med denne type system er at det kan forbedre forbrukeropplevelsen, hjelpe forbrukere å finne varer og tjenester, og gjøre relasjonen mellom kjøper og selger mer personlig og intensiv. Ulempene derimot, er faren for en ny maktubalanse mellom kjøper og selger, og nye urettferdige kommersielle praksiser (jf. European Commission 2022). Innen målrettet markedsføring etableres personaliserte overtalelsesprofiler (*persuasion profiles*) i kombinasjon med adaptive målrettingsstrategier (som leverer rett budskap, til rett tid og sted, til rett forbruker) og *dark patterns*[21].

I konseptualiseringen av forbrukersårbarhet under UCPD[22], GDPR og menneskerettighets-lovgivning, benyttes en «offertilnærming» til sårbarhet, der visse grupper forbrukere identifiseres som mer utsatt for skade, skjev behandling eller urettferdighet, for eksempel barn og eldre (Berg 2016). Her pekes det på iboende svakheter til grupper, og redusert kapasitet for å forstå markedsføring. Men kritikken mot denne tilnærmingen viser at det er stigmatiserende å anse spesielle grupper som (iboende) sårbare. En mer universell tilnærming er, som nevnt, å vurdere alle forbrukere som potensielt sårbare, og at forbrukersårbarheten er situasjonell. Men denne tilnærmingen er igjen kritisert for å ta for lite hensyn til individuelle og strukturelle forskjeller, for eksempel identitet og status. Universalisme gjør det umulig å erkjenne forskjeller mellom spesielt sårbare forbrukere, ifølge BEUC.

[21] Luguri & Strahilevitz (2021) fremhever at deres studie er den første med bevis på makten til dark patterns. Eksperimenter viste at det var mer enn dobbelt så sannsynlig at gruppen utsatt for milde dark patterns takket ja til en tvilsom tjeneste enn kontrollgruppen, og at dette økte til fire ganger så sannsynlig ved mer aggressive dark patterns. Samtidig ga aggressive dark patterns kraftig tilbakeslag hos forbrukere når disse ble avslørt, mens dette ikke skjedde ved milde dark patterns. «Skjult informasjon», «lurespørsmål» og «obstruksjonsstrategier» tenderte til å manipulere forbrukere, mens for eksempel «handle nå!» og «anbefalte valg»-beskjeder ikke gjorde det mer sannsynlig at forbrukere kjøpte dyre tjenester.

[22] Unfair commercial practices directive

Kommersielle budskap er nå del av en større systematisk tilnærming for å påvirke forbrukeratferd, som ikke kan skilles fra den tekniske infrastrukturen (et adaptivt overtalelsessystem) som genererer det (BEUC 2021). Dermed kan en ikke kun evaluere budskapet, men hele systemet må vurderes, for å avgjøre rettferdigheten i kommersielle praksiser. I sum ser BEUC på digital sårbarhet som; 1) *arkitektonisk* (digitale valgarkitekturer er datadrevne, dynamisk justerbare og personaliserbare, og tillater konstant eksperimentering med forbrukere), 2) *relasjonelt* (pågående kommersielle relasjoner gjør forbrukere mer sårbare over tid og skaper ytterligere maktubalanse), 3) og knyttet til *mangel på personvern* (innsamling og analyse av brukerdata styrker selgers maktposisjon, mens det å styrke personvernet kan forstås som en autonomi-forsterkende verdi).

Spørsmål som BEUC (2021) stiller i rapporten er hvordan forbrukere kan bli meningsfylt informert om teknisk komplekse forhold som nettbasert datainnsamling? Og hvor realistisk er informert samtykke gitt informasjonsoverbelastning og oppmerksomhetspress? Og hvordan kan lovgivning hjelpe forbrukere til å håndtere egne data i en post-samtykkefase? Den store utfordringen, også for forbrukerrelatert lovgivning, er at i det digitale samfunnet så eroderes skillet mellom forbrukeren som økonomisk aktør og innbyggeren som sosial aktør. Data om forbrukere kan benyttes til beslutninger som påvirker oss på andre områder i livet, som politikk, helse og arbeid. Dermed er de digitale forbrukerutfordringene blitt del av en altomfattende livsutfordring.

I en studie av vanOoijen og Vrabec (2018) vektlegges *kontroll* som en hovedutfordring i kommersielle praksiser. Teknologisk kompleksitet og omfattende datautnytting gjør det krevende for forbrukere å ha kontroll over personlige data. Atferdsforskere peker på utfordringer med individuell kontroll, som «dataoverbelastning» (information overload) og «datausynlighet» (data invisibility) (Kamleitner & Mitchell 2018). Her ses individuell kontroll som en refleksjon av grunnleggende verdier som autonomi, personvern og verdighet. Blant annet vurderes kontroll som friheten til å bestemme, noe som lett kan kompromitteres i en data-dreven økonomi der en rekke digitale aktører sitter på omfattende digital informasjon, som ikke oppveies med kontroll fra andre aktører. Selv om målet med GDPR er å styrke individuell kontroll over persondata, tenker gjerne ikke forbrukere (datasubjektene) på de fulle konsekvensene av det å gi et samtykke, ifølge vanOoijen og Vrabec (2018).

Her er det flere trusler mot individuell kontroll, ifølge forfatterne. En utfordring er *informasjonsoverbelastning*. Individuell kontroll betinger at man blir informert, men det er krevende å kognitivt prosessere massive mengder informasjon om datainnsamling fra en rekke utstyr, medier og tjenester. Paradokset ligger i at jo mer informasjon som gis, desto mindre informasjon evner brukere å filtrere. Dette gjelder informasjon både fra kommersielle aktører og fra regulatoriske myndigheter. En annen utfordring som fremheves er *informasjonskompleksitet*. Både kognitive evner og ferdigheter spiller inn på evnen til å ta til seg personvernrelatert informasjon. Personvern policy'er er omfattende og krevende å forstå, mens hvordan algoritmer opererer, og utfall fra disse, er uforutsigbare. Forslag til forenklinger kan være ikoner – standardiserte bilder som gir info om dataprosessering. Disse kan øke individuell kontroll ved å redusere informasjonsoverflod og informasjonskompleksitet. Men ikoner gir ikke omfattende kunnskap om datainnsamlingspraksiser, kun generalisert og forenklet informasjon. Dermed kan forbrukere bli mindre oppmerksomme på at de kun mottar delinformasjon, noe som igjen kan øke utfordringen med datausynlighet og immaterialitet.

Persondata brukes ikke kun en gang, men gjenbrukes, og på en slik måte at bruken blir enda mindre gjennomsiktig og gir mindre kontroll for brukeren (vanOoijen og Vrabec 2018). I tillegg til liknende utfordringer som er fremhevet av andre, peker forfatterne på utfordringer som ligger i karakteristika ved data i seg selv – *datausynlighet* – at data kan oppleves som immaterielt, usynlig, omfangsrikt og flytende – noe som også reduserer individuell kontroll i gjenbruksfasen. Det kan være vanskeligere å føle kontroll over noe som er usynlig og lite håndgripelig, mens det viser seg at folk tilskriver en høyere verdi til objekter som er fysiske heller enn digitale, samt at de identifiserer seg mer med fysiske ting når det gjelder psykologisk eierskap. Immaterialiteten til persondata gir også større muligheter for duplisering og deling av data, og gjør det mer krevende å stadfeste verdien og lokasjonen til data. Det foreslås derfor tiltak for å gjøre personlige data mer «synlige», både for å gi forbrukere en bedre forståelse av data og en bedre følelse av kontroll. Dermed kan kontrollrettigheter definert i GDPR, som dataportabilitet, tilgang og sletting, utøves på en bedre måte.

Kotras (2020) vektlegger *personalisering* i sin studie, eller rettere sagt *masse-personalisering*. Kotras antyder at det er en gammel drøm om en-til-en markedsføring i enorm skala som nå utspiller seg. Et paradoks her er at massepersonalisering benytter algoritmiske prosesser der finjustering av prediksjon til unike individer innebærer beregning av enorme datasett, men at også lokal forhåndskunnskap og såkalte avpersonaliserings-mekanismer er viktige i denne prosessen. Med fornyingen av markedsføringen på 1990-tallet, med internett og datafisering, ble individuell atferd mer målbar og man kunne eksperimentere for å «kalkulere» forbrukere. Denne type datafisering og «life-mining» har gradvis blitt normalisert som et nytt paradigme, både i vitenskapen og i samfunnet, og hviler ifølge van Dijck (2014) på en «dataisme»-ideologi; troen på objektiv kvantifisering for å forstå fremtidig sosial atferd, noe som nødvendiggjør sporing av tidligere menneskelig atferd.

Nå kan algoritmer basert på kunstig intelligens gjøre statistiske prediksjoner fra store, heterogene og ofte helt ustrukturerte data – og den prediktive markedsføringen lover langt mer individualisert og finkornet kunnskap om kunder enn det som produseres fra tradisjonelle markedsundersøkelser. Gjennom systematisk modellering av veldig store mengder variable kan algoritmene forutse individuell atferd. Her mener samtidig Silver (2012) at slike prediksjoner er helt avhengige av kvaliteten på data som benyttes, og at det er viktig å skille «signalet» (relevante data) fra «støyen» (unyttige data) for at datadrevne prediksjoner ikke skal slå fatalt feil (jf. Slettemeås 2018b). boyd og Crawford (2012) retter også kritikk mot den påståtte objektive karakteren til data. De dekonstruerer den utbredte myten om at store datasett (Big data) tilbyr en «høyere form for intelligens og kunnskap», som gir innsikt det tidligere var umulig å oppnå, støttet av en aura av sannhet, objektivitet og nøyaktighet

I en annen kritisk studie av Big data, hevder Kotras (2020) at det gjerne er et fokus på «overvåkning» og «kontroll» i algoritmisk prediktiv markedsføring. Selv peker han på et paradoks innen massepersonalisering; at dette ikke bare er personlig, og aldri handler om en enkelt person, men at det involverer *generalisering*. Personalisering i denne sammenheng avhenger av algoritmiske beslutninger knyttet til ting vi kjøper, nyheter vi leser, musikk vi hører på, og som antas å være skreddersydd etter våre interesser. Dette knyttes det diverse utfordringer til, som overvåkning, *nudging*, personvernbrudd, kommersiell målretting, filterbobler, o.l. Markedsføringsprosesser forbindes med konstant overvåkning av individers

handlinger, kolonisering av stadig flere aspekter ved hverdagslivet, og bedrifters økende kontroll av forbrukere. Men her fremmer Kotras at personalisering også betyr en *frigjøring fra store statistiske kategorier*, og at prediktive algoritmer oppløser referansen til den mest sentrale figuren i liberale økonomier – det *individuelle subjektet*. Algoritmene trenger bare å kjenne til enkle datapunkter, abstrahert fra deres sosiale meningskontekst, og fra subjektet som produserer dem. Dermed er ikke subjektet – eller forbrukeren – interessant i seg selv.

Når personaliseringen blir massiv, må det kalkuleres «likhet» mellom store utvalg av individer. Effektive prediksjoner krever at algoritmer «blindes» når de trener seg på data. Først får de fragmenterte data til en individualisert profil, så blindes algoritmene for de enkeltpersoner som er representert. Algoritmer er konstruert for å diskriminere mellom kunder (matematisk) men begrenses av regler for autorisert diskriminering (f.eks inntekt) og uautorisert diskriminering (f.eks kjønn og rase). Algoritmen må dessuten ikke vite for mye om individet i treningsmiljøet; en *for* personalisert kalkulering vil hindre effektiv prediksjon av atferd fra nye personer. Et sånt perspektiv vil kunne berolige forbrukere som knytter overvåkning til noe veldig personlig og til følelsen av «ubehag» ved at noen følger med på den digitale atferden, skal vi tro Kotras (2020).

3.5. Tingens internett og kunstig intelligens

I forlengelsen av diskusjonen rundt forbrukersårbarhet, anses barn som spesielt utsatt. Holloway (2019) ser mer spesifikt på *barn som forbrukere*, og spesielt hvordan tingenes internett – nettilkoplede leker, wearables, smarte hjemmeassistenter, samt enheter og apper som ikke opprinnelig utviklet for barn – likevel gir store muligheter for å samle inn data om barn for kommersiell vinning i overvåkningsøkonomien. Utfordringen Holloway peker på, er at barn ofte er for unge til å samtykke og til å forstå implikasjoner av egne handlinger. En annen stor utfordring er alle data som akkumuleres over barnas levetid, og de mulige langsiktige negative konsekvensene dette kan føre til. Her ses barn både som objekter i økonomisk aktivitet (datakilder) og som subjekter i markedsrelasjoner (digitale forbrukere).

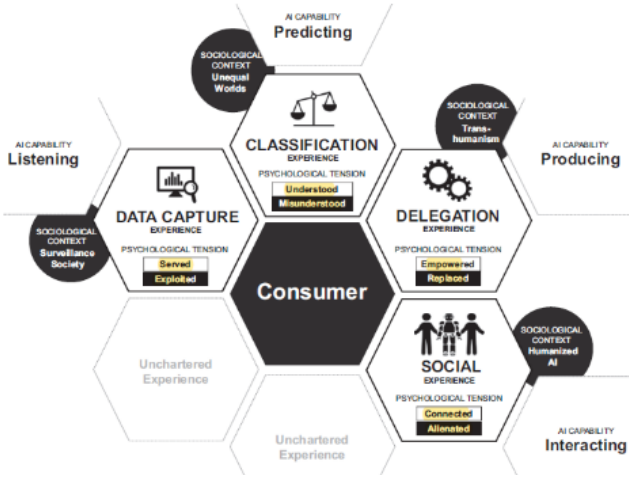
Selv om digitale enheter kjøpes, så bindes brukere gjennom langvarige kontrakter i og med programvaren som finnes i enhetene, og brukeravtalene muliggjør dataoverføring mellom barnet (som del av husholdet) og plattformen, men også mellom barn og foreldre, og barnet og andre datadelingsmottakere. Sensorer i tilkoplede enheter kan dessuten i noen tilfeller kapre stemmer, bevegelser, lokasjoner, bilder, pustemønstre og hjerterytme. En hovedutfordring med det utvidete sensor-baserte samfunnet, er intensiveringen av digital tilkopling og overvåkning i stadig flere aktiviteter, inkludert selvsporing, smarthjem, helseanalyse, etc. Med en slik utglidning av tilkopling og dataflyt blir også barn – tilsiktet eller utilsiktet – del av overvåkningsøkonomien.

Studier viser at barns data blant annet deles og videreselges fra apper, og at når barnet er 3-4 år har 5 millioner datapunkter blitt samlet inn av adtech som leverer annonser til barn og familier, og dette har økt til 72 millioner datapunkter før de fyller 13 år, ifølge Holloway. Datainnsamlingsteknologien som benyttes av adtech er bygd for «voksnes data», men samler likevel inn informasjon om barns lokasjon, apper brukt, nettsider besøkt, enhets-ID'er, og mer personaliserte data. Barns bevegelser, kropper, lekbaserte aktiviteter, kommunikasjon og sosiale og kognitive utvikling er nå blitt «digitaliserbar» og «kommodifiserbar». Og med tingens internett og smarte, tilkoplede produkter vil man gradvis

kunne normalisere en kultur der overvåkning gjøres til noe vanlig og umerkelig. Men her er langtidskonsekvensene – spesielt for dagens unge – usikre. Likevel er det påfallende lite bruk av føre-var-prinsipper. En bekymring er personvern, men Holloway (2019) trekker også frem, som flere av de tidligere bidragene, det å miste kontroll over personlige data, diskriminering, profilering, formålsglidning, teknologisk avhengighet – og skjermløse plattformer (sensorer, tingenes internett) som vil gjøre forbrukere mindre oppmerksomme på datainnsamling og forbrukerovervåkning.

Mens Holloway tar for seg tingenes internett og spesielt utfordringer for barn, ser Puntoni et al. (2021) mer spesifikt på *kunstig intelligens* (KI). KI gir bedrifter mulighet til å tilby fordeler for forbrukere, som helseovervåking ved bruk av wearables, råd i forslagssystemer, og bekvemmelighet med smarthjemprodukter og stemmeaktiverte virtuelle assistenter. KI kan av enkelte anses som et nøytralt verktøy som måles på effektivitet og korrekthet, men da tas det ikke hensyn til rekken av sosiale og individuelle utfordringer som oppstår når KI introduseres. Puntoni et al. introduserer et rammeverk som konseptualiserer KI som et økosystem med fire kapabiliteter, der fokus ligger på forbrukererfaring, og der både mikro-nivå (psykologisk) og makro-nivå (sosiologisk) aktualiseres.

Datafangst er erfaring med å høste og gi data til KI; *klassifisering* er erfaring med å motta personlige prediksjoner fra KI; *delegering* er erfaring med prosesser der forbruker delegerer oppgaver til KI; og det *sosiale* er erfaring med interaksjon med en KI-partner. Disse elementene assosieres med kapabiliteter som henholdsvis å lytte, forutsi, produsere og kommunisere. Datainnsamlingsutstyr *lytter* (sensorer som skanner omgivelser, wearables som lagrer fysisk aktivitet), algoritmer bruker data til å *forutsi* (forslags-systemer i Spotify), output-systemer *produserer* et svar, eller *kommuniserer* med forbrukere (veibeskrivelse i Google Maps). Forbrukererfaringer knyttet til dette kan være følelsesmessige, kognitive, atferdsmessige, sensoriske eller sosiale. Det er dessuten psykologiske spenninger knyttet til disse erfaringene; datafangsterfaring kan *tjene/utnytte* forbrukere, klassifiseringserfaring kan *forstå/misforstå* forbrukere, delegeringserfaring kan *styrke/erstatte* forbrukere, og sosial erfaring kan *sammenkoble/fremmedgjøre* forbrukere.



Figur 3: Rammeverk for kunstig intelligens. Puntoni et al. (2021)

Datafangst; data kan deles av forbrukere, med høy eller lav usikkerhet om videre bruk, eller kan fanges av KI gjennom spor forbrukere etterlater seg (ansiktsgjenkjenning i butikk, eller kart som Roomba robotstøvsugere lager hjemme). Datafangsterfaring gir forbruker verdi fordi de føler seg tjent av KI, og det å avgi data gir tilgang til skreddersydde tjenester, informasjon og underholdning, ofte gratis. Her kan man unngå trøttende beslutninger og oppnå selvforbedring, men samtidig føle seg utnyttet gjennom datafangst. Og det kan true forbrukeres eierskap og kontroll med personlige data. Sett fra et sosiologisk perspektiv

aktiveres narrativet om overvåkningssamfunnet, der manglende eierskap til persondata og manglende personlig kontroll gir teknologien potensiale til å overvåke menneskelig atferd. Fra et psykologisk perspektiv aktiveres ideen om den utnyttede forbruker. Forbrukere vet at datafangst tillater KI å tjene dem gjennom skreddersøm, men KI's iboende mangel på transparens gjør at forbrukere også kan føle seg utnyttet, og kan dermed lede til tap av motivasjon og hjelpeløshet.

Klassifisiering; selskaper utnytter prediktiv kapasitet til å skape skreddersydde tilbud og til å maksimere engasjement, relevans og tilfredshet hos forbrukere. Forbrukere, som ikke vet hvordan algoritmer virker, kan tro at forslag er basert på at de klassifiseres som en viss type forbruker. Denne erfaringen kan være positiv; forbrukere føler seg forstått eller som del av gruppe de liker å assosieres med – eller de kan føle seg misforstått, ved å bli feilaktig plassert i en bås eller gruppe de ikke kjenner seg igjen i. Fra et sosiologisk perspektiv kan det trekkes på ulikhetsnarrativet, der klassifiseringserfaringer formes av populære myter om rasjonalisering, kvantifisering og automatisert ulikhet, og fremveksten av undertrykkings-algoritmer grunnet KI's potensial for sosial klassifisering. I et slikt ideologisk system kan KI-systemer sies å forhindre menneskelig skjønn (bias), og redusere komplekse erfaringer til enkle kategorier, men de kan også utsette marginaliserte søkere for etnisk profilering, feilrepresentasjon, eller f.eks begrense lån til folk fra fattige områder (diskriminering). Fra et psykologisk perspektiv er det en underliggende spenning mellom det å føle seg forstått og misforstått.

Delegering; delegeringserfaring knyttes til forbrukeres bruk av en KI-løsning i produksjons-prosessen for å utføre oppgaver/ta beslutninger de selv skulle tatt. Forbrukere kan føle makt ved å slippe å engasjere seg i oppgaven KI utfører og samtidig frigjøre tid til noe annet meningsfylt, eller der forbrukere er dårligere kvalifisert. Det kan øke mestringsevnen, men for mange delegeringsmuligheter kan det også lede til motvillighet og en følelse av å bli erstattet. I et sosiologisk perspektiv kan det trekkes på et transhumanistisk narrativ, som fremhever faren ved å speile menneskelige egenskaper teknologisk, og det å følge idealet om teknologisk perfeksjon. Dette kan lede til at mennesker blir erstattet, der resultatet blir massearbeidsløshet og maskiner oppnår 'udødelighet'. Negative erfaringer kan også knyttes til systemisk «dehumanisering». Fra et psykologisk perspektiv kan delegering gi en følelse av makt, men også av å bli erstattet. Det kan oppstå en psykologisk trussel ettersom mennesker gjerne ønsker at utfall skal knyttes til deres egne ferdigheter og innsats.

Sosialt; KI's kapasitet til å inngå i gjensidig kommunikasjon bidrar til å produsere en sosial erfaring, enten når forbrukeren vet at hen interagerer med en KI (f.eks stemmeassistent), eller når hen ikke vet det (f.eks tjeneste fra en automatisert chatbot). Sosiale erfaringer kan være positive når KI brukes som middel for informasjonsdeling, eller ved «sosial robotikk» som kan skape følelsesmessig behagelige og meningsfylte KI-baserte interaksjoner. Men sosiale erfaringer kan også fremmedgjøre forbrukere, gjennom simulerte interaksjoner, og ved å trigge en følelse av ubalanserte relasjoner eller diskriminering. I et sosiologisk perspektiv kan dette knyttes til et narrativ om menneskeliggjort KI, med utgangspunkt i en kulturell fascinasjon for menneskeliknende maskiner, men det kan bidra til sosial fremmedgjøring av visse grupper i samfunnet (f.eks kvinner og etniske minoriteter). I et psykologisk perspektiv kan den fremmedgjorte forbruker trekkes frem; mens KI-baserte sosiale erfaringer kan fremme forbruker-bedrift relasjoner, kan de også bidra til å fremmedgjøre forbrukere, eksempelvis gjennom ubehag skapt av feilaktige automatiserte

tjenestesvar, eller når KI feiler i å interagere godt med visse grupper forbrukere (f.eks i sosiale støtteordninger der man ses på som et nummer og ikke som et menneske).

3.6. Autonomi og personvern

Til slutt i bakgrunnsstudien ser vi på *autonomi og personvern* i relasjon til overvåknings-tematikken. I et bidrag fra Lanzing (2019) rettes fokus mot selvsporingsteknologi, autonomi og skillet mellom informasjons- og beslutningspersonvern. I det følger en kritikk av den personaliserte valgarkitekturen som benyttes i mye av dagens selvsporingsteknologi. Selvsporingsteknologi promoteres gjerne som et middel til selvforbedring, med personalisert feedback som *nudger* brukeren til atferdsendring. Her er normative intervensjoner blitt svært vanlige, spesielt innen helse og det å ta sunne/grønne valg. Utfordringen ligger i at sanntidspersonalisering krever kontinuerlig overvåkning og kraftig teknologi til *hypernudging*, noe som reiser bekymring rundt spesielt manipulering og personvern. Hypernudging kan i utgangspunktet kompromittere forbrukernes autonomi fordi det både krenker informasjons- og beslutningspersonvernet. Derfor, for å vurdere om teknologi som bruker hypernudging gir brukermakt, må *begge personvernforståelser* benyttes som konseptuelle begrep, ifølge Lanzing (2019).

Informasjonspersonvern er det vanlige begrepet som benyttes i vurderingen av bruk av digitale data, spesielt evnen til å kontrollere hvem som har tilgang til personlig informasjon og i hvilken grad. Begrepet informasjonspersonvern kan være nyttig for å forklare skadelige aspekter ved datainnsamling fra tredjeparter som ikke forventes å skulle ha tilgang til slik informasjon. Likevel, en mer generell typologi av personvern bør bestå av flere dimensjoner knyttet til kropp, atferd, tanker, lokalitet, og valg/beslutninger, ifølge Lanzing. **Beslutningspersonvern**, på den annen side, ses på som retten til å hindre uønsket innblanding i beslutninger, valg og handlinger. Altså, forhindre at andre har tilgang til å kommentere, tolke eller styre beslutninger og endre ens atferd. Det skal altså beskytte mot påvirkning fra andre. I relasjon til digital hypernudging så kan informasjonspersonvern dermed sies å hindre feil i innsamling og formidling av informasjon, mens beslutnings-personvern kan forhindre bruk av informasjon for å påvirke en persons beslutningsprosess.

Beslutningspersonvern er nært knyttet til *autonomi*. Det skal beskytte friheten til å ta frie, autonome, og personlige valg. Dette er ikke del av den europeiske lovtradisjonen, men den europeiske menneskerettighetskonvensjonen erkjenner personvernets funksjon som en rett til personlig utvikling og autonomi, altså selvbestemmelse, og det å kunne ta egne valg (Lanzing 2019). Alle dimensjoner ved personvern beskytter aspekter ved autonomi, som autonom beslutningstaking, selvutvikling, og selvpresentasjon. Innblanding i beslutningstakingsprosessen gjennom overvåkning krenker dermed både informasjons- og beslutningspersonvernet. Uten disse vernene kan ikke folk være sikre på om de handler basert det de selv velger og identifiserer seg med, eller det manipulatoren ønsker.

Sentrale utfordringer er, ifølge Lanzing, *nedkjølingseffekter,* som kan komme av flere overvåkningsgrunner, både at noen har tilgang til informasjon, at valg kan påvirkes gjennom manipulasjon, eller at informasjonen kan lekke slik at andre uautoriserte kan få tak i det. Slike effekter kan oppstå dersom en ikke handler konformt med oppfattede sosiale normer og frykter sosiale sanksjoner. Videre er det *filterutfordringer*, der hypernudges fôrer tidligere beslutningsdata fra forbrukeren inn i valgarkitekturen og kan skape en feedback-loop som

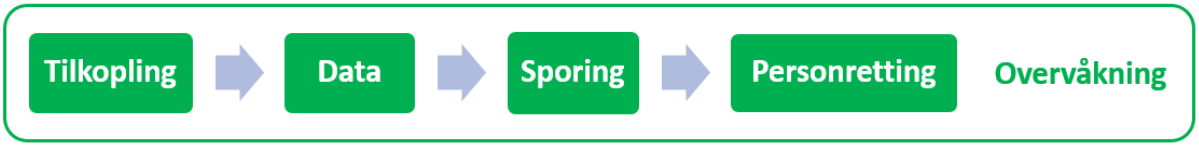
resulterer i selvoppfyllende profetier og ensretting av budskap. En tredje utfordring er *profilering*, som benyttes for å gjøre beslutningsprosesser mer effektive, men som produserer nye former for sårbarhet. De skjuler eller fjerner sosial kontekst og relasjoner ved å redusere kropper og atferd til data, som igjen lett kan kontrolleres og manipuleres under dekke av teknologisk objektivitet og nøytralitet.

Rosen (2020) på den annen side, utfordrer ideen om hvorvidt personvern er et umistelig gode. Han innleder med spørsmålet om det finnes alternativer til at Facebook, Google og Amazon sporer hvert steg og overvåker hvert øyeblikk i folks liv, og utnytter disse dataene til profitt. Med andre ord, finnes det en mulighet for å utvikle et nytt, demokratisk og desentralisert internett der brukere har suveren kontroll over egne data? Samtidig mener Rosen at det ikke er enkelt å skru av informasjonsstrømmen, ettersom vi over tid har akseptert at vi på internett får tilgang til et univers av digitale goder i bytte mot personlige data. Her mener Rosen at Zuboff tar feil, og at de store selskapene faktisk har påført samfunnet store gevinster der forbrukere (amerikanere i dette tilfellet) i stor grad har akseptert *trade-off*'en hvor personlige data byttes mot gratis tjenester.

Rosen mener, igjen i motsetning til Zuboff, at det ikke er noe genuint nytt i kapitalismen (jf. Morozov 2019), og at for Google ses ikke brukerne på som direkte kunder, men de deltar likevel i et bytte de har nytte av eller profiterer på. Vi som forbrukere blir objektifisert, men dette er noe alle profittorienterte selskaper gjør, mener Rosen. De ekstraherer inntekt og vi ser på selskapene som verktøy for vår egen nytte. Rosen mener i stor grad at forbrukere er aktive og informerte, og at de frivillig inngår i avtaler der data byttes mot tjenester eller fordeler – og at digitale selskaper har vært åpne om den *trade-off*'en, der personvern er prisen man betaler for en rekke fordeler knyttet til informasjon, tilkopling og andre digitale varer. Han forfekter også at data ikke blir «tatt» fordi forbrukeren ikke «mister» sine data, og at dette ikke er snakk om et nullsumspill. Videre legger Rosen vekt på at fokuset på personvern er mer populært i Europa enn i USA, og at amerikanere ikke ser på personvern som et umistelig gode, men noe som kan balanseres eller byttes mot andre individuelle og samfunnsmessige goder. Med bakgrunn i denne argumentasjonen mener Rosen at «overvåkning» ikke er beskrivende for dagens digitale, økonomiske praksis.

4. Analyse av fokusgrupper og survey

Analysen som er gjennomført i denne rapporten er basert på resultatene fra fokusgruppene og den påfølgende spørreundersøkelsen. Funnene fra fokusgruppene ble benyttet til å utvikle et spørsmålsskjema for den landsrepresentative spørreundersøkelsen. Dette skjemaet går ikke i dybden på samme måte som spørsmålene i fokusgruppene gjør. Derfor har vi i analysen valgt å presentere relevante funn fra spørreundersøkelsen til slutt under hvert delkapittel der de faller naturlig inn, mens vi i diskusjonskapitlet ser de kvalitative og kvantitative funnene mer i sammenheng. Dette kapitlet er relativt omfattende og innehar mange sitater fra fokusgruppene, mens diskusjonskapitlet er noe kortere og sammenfatter funnene i større grad.



Figur 4: Figuren viser sortering av hovedtemaer i analysen; tilkopling, data, sporing, personalisering/målretting, og begrepet «overvåkningsøkonomien».

Første del av analysen følger i hovedsak de overordnete temaene som ble tatt opp i fokusgruppene; deltagernes *tilkopling* gjennom nettverkstilkoblede enheter i hjemmet og telefonapper; holdninger og erfaringer med bruk av personlige *data*; kunnskap om hvordan slike data blir identifisert og høstet gjennom *sporing*; bearbeiding og tilpasning av data gjennom prosesser for *personalisering* av innhold og *målretting* av budskap; og til slutt overordnete refleksjoner rundt *overvåkning* som begrep, samt utfordringer knyttet til temaer som personvern, tillit, kontroll og regulering.

4.1. Tilkoblede enheter og mobilapper

Nettilkoplede produkter

Fremdeles er det mobiltelefoner, datamaskiner og nettbrett som i hovedsak står for forbrukernes nettilkopling i hverdagen. I analysen valgte vi, når vi skulle diskutere tilkopling, å fokusere på to konkrete aspekter; 1) tilkopling til smarte produkter, og 2) tilkopling gjennom mobilapper. Grunnen til dette valget var for å unngå at deltakerne måtte forholde seg til alle mulige tilkoplinger samtidig, noe som kan bli overveldende og resultere i generelle beskrivelser.

Deltagerne i de to fokusgruppene hadde et bredt spekter av tilkoblede enheter i hjemmet, hvor noen var personlige, og kun brukt av dem selv, mens andre var delt med husstands-medlemmer. Alle deltagerne hadde mobiltelefon og en stasjonær eller bærbar datamaskin koblet til internett, og de fleste hadde også en internettilkoblet TV. Videre hadde omtrent halvparten nettbrett og spillkonsoller, og to deltagere hadde lesebrett. Smarthjem-teknologier, i form av andre nettilkoblede husholdsprodukter, var ikke like utbredt blant deltagerne i fokusgruppene. Det var kun en til to deltagere som hadde følgende nettilkoplet

utstyr; Google mini (stemmestyrt smartassistent), Sonos høyttaler, panelovner, støvsuger, vifte, lys, stekeovn og strømplugg. En deltager hadde enkelte enheter som kunne kobles til internett, men som av ulike grunner ikke var det for øyeblikket; en TV, en spillkonsoll og en panelovn.

Halvparten av deltagerne uttrykte overraskelse over antallet internettilkoblede enheter de hadde tilgang til hjemme. To fortalte at det var mer enn de antok, mens fire var overrasket over at de ikke hadde flere. Awan (29) sier for eksempel: *«Jeg trodde jeg skulle ha mange flere, eller jeg trodde liksom at alt var koblet til nettet»*. Dette viser at antall internettilkoblede enheter i hjemmet ikke nødvendigvis er noe forbrukere forholder seg til særlig bevisst. Tre av deltakerne uttrykte også at de gjerne skulle hatt flere ting koblet til internett, som Petter (26): *«Jeg skulle ønske at alt kunne kobles til, så jeg kunne fjernstyre absolutt alt i hele huset»*. Tidsbesparing, lavere pris, bekvemmelighet, trygghet og kontroll nevnes som grunner til hvorfor deltagerne ønsker større grad av nettilkobling i hjemmet. Automatiserte tjenester i hjemmet vil for eksempel spare tid til kaffelaging om morgenen, smart styring av elektriske produkter gir mulighet for å spare penger på strøm, i tillegg til at fjernstyring vil gi en ekstra trygghet om man glemmer å skru av elektronikk før man drar hjemmefra. Andre var mer skeptiske til for mye tilkobling. For eksempel sier Susanne (42):

> *«Jeg har veldig behov for at ikke noen har full styring på meg, så det hadde aldri vært aktuelt. Jeg tenker at det faktum at jeg har ting kobla opp gjør jo at noen andre har fordeler av at jeg gir informasjon til dem. Det er jo selvfølgelig sånn vårt samfunn funker på en måte. Alle plasser du er kunde er du også en tilbyder av en vare, så jeg har liksom valgt ting som gjør livet mitt enklere, og så setter jeg liksom en stopp hvis jeg ser at det her, det er ikke så viktig».*

Hun fremstår som bevisst på at kommersielle aktører vil nyte fordeler av hennes tilkobling, og at de får større grad av styring på henne jo flere produkter som er tilkoblet nettet. Derfor setter hun en grense ved produkter som bidrar til å gjøre ting «enklere» for henne, resten forblir frakoblet. Flere mener dessuten at det er enklere når ikke alt er tilkoblet, som Even (18): *«Jeg liker når ting er litt enklere»* og viser til at han ikke ønsker å ha alt mulig i livet sitt koblet til nett, og Harald (57) istemmer med at *«hvis du skal ha styring på alt, så må du ha en utdannelse innen feilsøking og elektro. Det er jo helt håpløst det her».* Han er opptatt av komplikasjoner som oppstår ved feilmeldinger og elektronikk som går i stykker. Her ser vi at fokusgruppedeltagerne har ulike oppfatninger av hva som oppfattes som *enkelt*. De som kunne tenke seg at mer var tilkoblet forbinder enkelt med teknologi som ordner opp, mens de andre heller anser teknologien som noe som kompliserer ting hjemme og skaper merarbeid.

Survey-data

Den landsrepresentative surveyen, som ble gjennomført i etterkant av fokusgruppene, viser at 9 av 10 norske forbrukere (89%) i stor grad føler at hverdagen nå er digitalisert og tilkoplet. Det er hele 59% som i svært stor grad sier seg enig i dette, mens 30% i stor grad er enige. De yngre føler i større grad enn eldre at hverdagen er digitalisert; hele 67% i alderen 18-29 år er i svært stor grad enige, mot 47% i alderen 60-80 år.

Det er imidlertid relativt få som har tilgang til mange nettilkoblede eller smarte enheter utover mobiltelefon, datamaskin og nettbrett. Her svarer kun 1 av 10 (9%) at de har tilgang på mange slike tilkoblede enheter, mens litt over halvparten (56%) svarer at de har tilgang på noen få enheter. Rundt 1 av 3 (31%) sier at de ikke har noen tilkoblede enheter utover mobiltelefon, datamaskin og nettbrett. Det er interessant å merke en kjønnsforskjell her; det er 12% blant menn som har tilgang på mange slike enheter, mot 6% blant kvinner. Det er

også 25% blant menn mot hele 38% blant kvinner som melder at de ikke har tilgang til noen tilkoblede enheter utenom mobiltelefon, datamaskin og nettbrett. Vi ser dessuten en aldersforskjell her blant dem som ikke har tilgang til ekstra tilkoblede enheter; i alderen 18 til 49 år ligger andelen på rundt 2 av 10 mens for de over 60 år er det halvparten som ikke har noen ekstra tilkoplete enheter.

Blant dem som har tilgang på tilkoblede enheter utover «standardpakken», er det rundt 7 av 10 (68%) som svarer at de ikke har opplevd ubehag eller negative konsekvenser relatert til personvern eller sikkerhet ved å bruke de tilkoplete enhetene. Det er likevel nesten 2 av 10 (18%) som har opplevd problemer eller ubehag, og en gruppe skiller seg ut; de i alderen 18-29 år. Her har 3 av 10 (31%) hatt negative erfaringer knyttet til personvern eller sikkerhet.

Utviklingen av tingenes internett, der stadig flere produkter blir koblet til internett, stiller de aller fleste, rundt 4 av 10, seg nøytrale til. Det er 36% som er positive og 20% som er negative til denne «smartutviklingen». Vi ser noen forskjeller både på kjønns- og aldersvariabelen; mens 17% er svært positive i alderen 30-39 år, er kun 4% svært positive i alderen 60-80 år. På samme måte er det 17% blant menn som er svært positive, mot bare 5% blant kvinner.

Apper på mobiltelefoner

Blant de 13 fokusgruppedeltakerne i denne studien var det et stort spenn i hvor mange apper de hadde på sine telefoner. Den med færrest antall hadde 77 apper og den med mest hadde 201. De aller fleste deltagerne hadde godt over 100 apper, med en median på 126 og et gjennomsnitt på 132.

Mange av deltagerne hadde flere apper enn det de trodde før opptellingen. Bare Even (18) var positivt overrasket over sitt antall, og da med det laveste antallet apper i materialet. Oda (32) var overrasket over hvor mange apper hun hadde, men kom på at disse var sortert i ulike mapper på telefonen, og dermed så det ut som det var færre ved første øyekast. Eva (29) ble overrasket fordi telefonen var relativt ny og hun trodde ikke hun hadde rukket å laste ned så mange apper på så kort tid. Petter (26) og Celine (43) var dessuten overrasket over app-antallet fordi de regelmessig sletter apper de ikke bruker. Det var dessuten flere som nevnte at telefonen selv sletter apper som ikke er i bruk.

Mange av appene følger med operativsystemet til telefonen, påpekte noen av deltakerne, og en rekke av disse blir liggende ubrukt fordi de ikke er relevante for dem. Samtidig viser mange av appene seg å være viktige i hverdagen; en deltaker forteller at appene blir brukt på alle områder i livet, og en annen viser til at en håndfull apper benyttes i forbindelse med jobb. En tredje hevder også at noen apper bare lastes ned for gøy og prøves en gang, for så å bli glemt. Flere istemmer at mange av telefonappene kun benyttes sporadisk.

Gjennom deltakelsen i fokusgruppene, og det forberedende app-tellingsarbeidet, forteller flere at de har oppdaget apper de ikke bruker og som de har lyst til å slette i etterkant av fokusgruppeintervjuet. Dette tyder på at det å gå igjennom og telle apper bidrar til økt bevissthet. Det at et lavt antall apper forbindes med noe positivt, og mange apper med noe negativt, er interessant. Dette kan muligens knyttes til ideen om at app-selskaper i stor grad samler data om brukere, og at det henger en personvern/sikkerhets-risiko ved apper, slik Forbrukerrådets #appfail-kampanje[23] vektlegger. Det kan også knyttes til en normativ moderasjonstankegang, der nøysomhet og det å kun ha «nødvendige» apper vektlegges, i

[23] Ref: www.forbrukerradet.no/appfail

motsetning til et hedonistisk, ureflektert «overforbruk» av apper. En tredje forklaring, som følger de to andre, er i tråd med tankegangen rundt digital sikkerhet og begrepet «cyberhygiene»[24]. På samme måte som individet engasjerer seg i visse personlige hygienepraksiser i den virkelige verden, for å opprettholde god helse og velvære, bør en følge cyberhygiene-praksis for å holde egne data trygge og godt beskyttet.

Usikre apper og personvern

Når telefonapper diskuteres dreier samtalene raskt over mot personvern og hvor mye og hva slags informasjon appene har tilgang til. En grunn til dette er at deltakerne før de to gruppesesjonene fikk beskjed om å tenke gjennom apper de var usikre på, med tanke på sikkerhet og personvern, men som de likevel hadde på sine telefoner. Jorunn (43) forteller at når bare så vidt er innom flere av appene, er man lite bevisst på hva man samtykker til når de tas i bruk: *«For du skal bruke det kanskje to ganger, eller en gang akkurat der og da. Og så tenker man jo ikke så mye over det etterpå. Det bare ligger der».* Jonas (27) sier også at *«man har skrevet inn mye personlig informasjon der»,* og at dersom det skjer et sikkerhets-brudd, noe han selv har opplevd, *«så har de plutselig passordet til mailen min og sånne ting».* Flere deltagere mener de uansett har mistet kontrollen over informasjonen de har lagt inn i appene. Awan (29) forteller:

> *«Jeg føler jeg liksom har mistet kontrollen uansett. Jeg vet på en måte ikke hvor jeg har lagt igjen sånn – ikke farlig informasjon – men sånn informasjon som kan utnyttes da. Så jeg tenker litt over det, at har jeg virkelig 102 apper som har all informasjon om meg. Det var litt sånn ja... fikk lyst til å slette alt, og så på en måte ha litt kontroll over det. Men ja, jeg føler det kanskje er der ute uansett, at det ikke går an å gjøre noe med det.»*

Det er tydelig fra disse samtalene at deltagerne i større grad knytter appene på telefonen til personvernutfordringer, og dette ga flere en følelse av ubehag og tap av kontroll. Her var det i stor grad antallet apper som gjorde kontrollmulighetene mer krevende, i tillegg til en noe skjødesløs nedlasting av apper man strengt tatt ikke trenger, fra selskaper man ofte ikke kjenner bakgrunnen til. I dette tilfellet knyttes tap av kontroll til både informasjonen man deler med appene, men også sikkerhetsrisikoen som ligger i å potensielt miste kontroll dersom apper eller informasjon hackes. Tiltak som deltakerne trekker frem, er i tråd med den nevnte cyberhygiene-tankegangen; å slette unødvendige apper og å reflektere mer over nye apper som installeres.

Deltagerne ble også spurt om å velge ut konkrete apper de var mer usikre på enn andre. Her fremkom det ulike kriterier for skepsis, men som alle var personvern-relaterte. Flere trakk frem sosiale medier-apper som de appene de er mest skeptiske til. Awan (29) er for eksempel mest usikker på TikTok og begrunner det med at han har lest artikler om kinesisk overvåkning og ansiktsgjenkjenning. Ansiktsgjenkjenning kan gjelde flere apper, men han sier TikTok føles mest usikker av en eller annen grunn. Petter (26) erkjenner at han heller ikke er konsekvent i sin usikkerhet. Han er for eksempel skeptisk til apper som sporer hvor han beveger seg og unngår treningsapper med denne funksjonen, men han bruker samtidig Google Maps. For andre deltagere går bekymringen i større grad ut på hva informasjonen kan brukes til. Jorunn (43) er for eksempel usikker på Strava, en treningsapp som bruker

[24] Ref: https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more

GPS-data for å vise brukernes bevegelser. Hun betrakter ikke lokasjonsdata som personlig informasjon, men erkjenner likevel at informasjonen kan bli utnyttet. Hun forteller at hun synes det er ubehagelig at andre kan se hvor hun er: *«Det er vel det at folk kan følge med...'stalke' deg nesten, altså uten at du selv er nesten bevisst på hva slags data som ligger der ute»*. Det er litt usikkert om hun her sikter til selskapet bak appen eller andre brukere. Det at lokasjon ikke oppfattes som personlig kan være at dette er informasjon som ikke er direkte eller permanent tilknyttet en person, men noe mer situasjonelt som likefullt forteller noe inngående om en persons bevegelser og atferd.

Andre er mer bekymret for at informasjonen som legges igjen i appene kan komme på avveie. Jonas (27) sier at han la inn «ganske mye» informasjon i den appen han var usikker på, inkludert betalingsinformasjon, men at han vil slette appen i etterkant av fokusgruppen. Lignende forteller Susanne (42) at hun er mest bekymret for Google Drive, hvor hun har personlige dokumenter som CV og jobbsøknader og ikke vet hvem som har tilgang til disse. Celine (43) legger til at hun stoler mer på offentlige tjenester enn på private.

For de fleste av deltagere er bekymringene rundt apper fokusert rundt potensielt misbruk av informasjonen deres, enten fra andre brukere, selskapene bak appene, eller aktører med onde hensikter. Elementer av dette er usikkerhet rundt hva slags personlig informasjon appene har tilgang til og hva den kan brukes til. Deltagerne beskriver dermed en generell usikkerhet og mangel på kontroll over personlige data.

Dette peker på et paradoks der deltagerne beskriver bekymringer rundt personvern, men likevel har beholdt appene på mobilen og aktivt bruker dem. For noen deltagere er bekymringene til stede, men de er ikke så store. Flere beskriver at nytten av appene veier opp for eventuelle usikkerheter. Elisabeth (31) sier at hun er klar over all informasjonen Google samler og lagrer om henne, men at *«hvis jeg skal bruke det på den måten jeg ønsker å bruke det på, så tenker jeg jo at 'it is what it is'»*. Lignende sier Eva (29) at *«man må gi for å få. De har syke mengder informasjon, men det er det som er en av årsakene til at jeg også velger å bruke alle disse Google-tjenestene»*, og viser til at man må gi fra seg noe for å kunne bruke tjenestene. Videre har de ikke opplevd noen sikkerhetsbrudd med tilbydere som gjør at de vegrer seg for å stole på dem. Andre deltagere har en annen tilnærming. Celine (43) forteller for eksempel at hun tenker over hva slags informasjon Google har om henne, men at de allerede vet så mye at hun godtar det. Andre, som Susanne (42), benytter konkrete strategier for å håndtere usikkerheten. Hun velge bort Facebook som app og bruker tjenesten kun gjennom nettleseren:

> *«Jeg har bevisst valgt å ikke ha Facebook-appen, den har jeg aldri hatt. Jeg går alltid i den via browser. Bare for at jeg tenker at... den store stygge ulven...om jeg kan liksom hindre noe som helst slags overvåkning derfra. Jeg klarer ikke det på alle de andre 197 [appene], men hvis jeg klarer det derfra så kanskje det er verdt det».*

Hun demonstrerer her en annen tilnærming til tap av kontroll, der det å gjøre noe er bedre enn ingenting. Dette står i kontrast til noen av de andre deltagerne som oppfatter det som nytteløst ettersom de ikke kan oppnå full kontroll uansett.

Her er det flere momenter det kan reflekteres over. Det ene kan knyttes til det såkalte «personvernparadokset» (Barth og de Jong 2017) der forbrukere oppgir å være opptatt av personvern, men ikke nødvendigvis handler i tråd med egne holdninger. Et annet viktig poeng er hvordan forbrukerne selv graderer bekymringer og risiko. Det kan dermed synes

rasjonelt i en del tilfeller, sett fra forbrukerens ståsted, at en antatt stor eller umiddelbar nytte veier opp for risikoen i en kost-nytte-vurdering. Det fremkommer også et snev av fatalisme, at de store selskapene vet så mye om den enkelte at det ikke er noe å gjøre med. Dette, sammen med mangel på erfaringer med faktiske tillitsbrudd, ser ut til å styrke praksisene omkring deling av informasjon i digitale apper.

Survey-data

I den landsrepresentative surveyen er det 23% som svarer at de kjenner til de fleste selskapene som står bak appene de har lastet ned på sine mobiltelefoner. Det er 32% som kjenner til noen, 36% som kun kjenner til enkelte og 9% som hevder de stort sett ikke kjenner til disse selskapene i det hele tatt. Med andre ord er det 77% som hevder de kun kjenner til noen få eller ingen av app-selskapene som står bak telefonappene de har. Dette samsvarer med funnene i fokusgruppene, at man med et stort antall apper mister oversikt over både disse og hvem som står bak. Ser vi på kjønn hevder 39% blant menn at de kun kjenner noen få eller ingen app-selskaper på mobilen, mot hele 52% blant kvinner. På aldersvariabelen er det derimot ingen store forskjeller.

På spørsmål om det er apper de er usikre på eller mangler tillit til, men som de fremdeles har på telefonen, er det 30% som svarer noen eller mange, mens 70% svarer få eller ingen. Her er det ingen tydelige kjønnsforskjeller, men det er hele 44% blant 18-29 åringer som mener de har noen eller mange apper de ikke har tillit til, mens dette kun gjelder 23% blant 60-80 åringer. Dette kan delvis forklares med at eldre er mer risikoaverse enn yngre, men også at yngre antakeligvis har langt flere apper på sine mobiltelefoner.

Når det gjelder appenes brukeravtaler, og hvorvidt forbrukere stort sett setter seg inn hvordan apper samler inn og bruker personlig informasjon, er det 11% som svarer at de ofte eller alltid gjør dette, mens 25% gjør det av og til, og 64% gjør det sjeldent eller stort sett aldri. Her er det heller ingen tydelige kjønnsforskjeller, mens 71% blant de yngste (18-29 år) gjør dette sjeldent eller aldri, mot 56% blant 60-80-åringer.

Samtidig er det interessant å vite, ettersom mange ikke kjenner til appselskaper eller leser brukeravtaler, om de faktisk har opplevd ubehag eller problemer med noen av appene sine, spesielt knyttet til sikkerhet og personvern. Det er 12% som hevder å ha hatt slike negative opplevelser (14% blant menn og 9% blant kvinner), mot 68% som ikke har opplevd problemer, mens 20% ikke vet. Ser vi på alder har 18% av de yngste (18-29 år) opplevd app-ubehag, mot kun 7% blant de eldste (60-80 år).

4.2. Forbrukernes data

Diffuse og uhåndgripelige persondata

Et viktig moment for å forstå forbrukernes holdninger og praksiser i «overvåkingsøkonomien» er å finne ut hvilket forhold de har til sine egne data. Dette vil påvirke i hvor stor grad de beskytter disse dataene og hvilken verdi de tillegger dem både i personvern-øyemed og som et byttemiddel i markedstransaksjoner. I de to fokusgruppene varierer deltagernes oppfatninger av hva data er, fra å anse det som noe komplisert, ukjent og uhåndgripelig, til å

se det som en verdi som kan byttes mot tjenester og apper. De fleste deltagerne har kjennskap til personlige data, og nevner blant annet navn, epostadresse, fysisk adresse, og telefonnummer. De kjenner også til lokasjonsdata og data om bruksmønster, og en deltager påpeker spesifikt at bruksmønster gjerne er data man ikke selv har tastet inn, men som plukkes opp gjennom bruk av apper og tjenester.

Det var derimot uenighet rundt hva som er sensitive data. For noen er lokasjonsdata og informasjon om hvor de befinner seg, og hvilke vaner de har i hverdagen sensitivt, mens dette er noe andre synes er helt greit å dele. En deltaker påpeker at sensitive data kan være informasjon som gir andre anledning til å opprette kredittkort i ditt navn, eller noe uspesifikt som det vil være ukomfortabelt at «det store flertallet» får vite om. Dette kan signalisere en form for «sosial risiko», der kompromitterende informasjon – som det er flaut, ubehagelig eller avslørende at andre får vite om – kan lekke ut til grupper av mennesker man ikke vet hvem er. Likevel viser de aller fleste deltagerne en avslappet holdning til hvilke og hvor mye data som samles inn om dem. Denne holdningen ser ut til å bygge på tre hovedfaktorer som alle henger sammen; 1) en risikovurdering der de har kommet fram til at det ikke er så farlig å dele dataene sine, 2) en kost-nytte-vurdering der fordelene veier opp for ulempene, og 3) en mangel på kunnskap om mengden data som samles inn, hva de kan brukes til og hvordan de eventuelt kan misbrukes.

Data og risikovurdering

Når det gjelder risikovurdering mener de aller fleste deltagerne at det ikke er farlig å dele data. Petter (26) sier for eksempel: *«Hva er det verste som kan skje?»* og sammenligner det med at han ofte har innbrudd i boden, og at det er mennesker han ikke vil at skal vite hvor han bor. Den fysiske risikoen knyttet til at andre mennesker tar seg inn på hans eiendom vurderes som farligere eller mer brysomt enn at selskaper har informasjon om ham og hans vaner. Flere av deltagerne gir også uttrykk for at data knyttet til person, lokasjon og søkeatferd er noe de synes er greit å dele. Elisabeth (31) hevder at det meste av informasjon om oss er tilgjengelig på nett uansett gjennom telefonkataloger, ansattsider, sosiale medier og så videre. Og hun legger til at *«jeg lever godt med at de vet at jeg foretrekker sushi fremfor pizza liksom, det gjør meg ingenting»*. Jonas (27) sier også at *«jeg tror ikke vi skal være så redde for [at de sporer lokasjon], det er bare en tracker»*. Dette gir en indikasjon om at det eksisterer en form for mental avstand mellom forbrukerne og deres data, der de ikke klarer å relatere nært nok til disse, slik som de gjør med materielle gjenstander og fysiske situasjoner i hverdagen. Dette forsterkes av ideen om at personlig informasjon allerede er offentlig tilgjengelig på nett. Dermed ser det også ut til at dette er med på å senke terskelen for hva som oppleves som privat og sensitivt, som igjen kan svekke forsvaret av egne data og dermed personvernet. Samtidig ser vi en annen dimensjon, der sosial risiko (som kan resultere i skam) i mange tilfeller kan anses som vel så «risikabelt» for forbrukere som materiell risiko (som kan resultere i tap av penger/verdier).

Data som byttemiddel

Flere av deltagerne beskriver hvordan de synes det er greit å dele data i bytte mot tjenester. For eksempel forteller Eva (29) at omfattende datainnsamling også kan gagne forbrukere ved at man får utviklet nye apper og tjenester man ellers ikke ville hatt. Dette forutsetter anonymitet, der aggregerte data ikke kan spores tilbake til henne. Men det er også deltagere som mener det er greit å dele data selv om anonymitet ikke kan garanteres. Det ble for eksempel nevnt at det kan være nyttig å bli gjenkjent for eksempel når Google Maps tilpasser tjenesten til personlige behov, for å få presentert relevant heller en tilfeldig reklame, eller at algoritmene foreslår nytt innhold basert på deres historikk. Awan (29) sier blant annet: «*Jeg synes det er helt greit at, for eksempel på Spotify da, at de gir meg alternativer til ny*

musikk basert på hva jeg liker, så slipper jeg å liksom lete etter det selv da, så jeg synes det greit». Google Maps trekkes frem i begge grupper, og en deltager påpeker hvordan Google samler inn informasjon og bruker den til å blant annet justere tidsanslagene i appen for å tilpasses hennes personlige gangtempo. Ikke alle deltagerne er enige i denne type løsninger, og kvinnene i materialet ser ut til å være mest skeptiske. Celine (43) sier for eksempel: *«Det er utrolig mye data vi gir fra oss på godt og vondt»*, og forteller at hun har opplevd *'stalking'*, noe som gjør at hun synes det er ubehagelig at andre kan finne ut hvor hun er til enhver tid og få en oversikt over rutinene hennes. Oda (32) sier også at hun synes det er ubehagelig at noen sitter på informasjon om hennes vaner i hverdagen. Jorunn (43) nyanserer synet på hva som er greit å dele med at det kan være forskjell på hva man gir fra seg bevisst og ubevisst:

> *«Men da skjønner en kanskje litt mer selv også, eller at det er mer bevisst, jeg tenker sånn kanskje andre bruksmønster, altså hvordan man, som du snakket om, hvor du beveger deg, det er litt mer ubevisst. At vi ikke er så bevisste på at det er ting som fanges opp da, knyttet til oss. Men type Spotify, der kjenner...der er det kanskje noe som man verdsetter mer».*

Det kan være en kjønnsdimensjon her, knyttet til sårbarhet, som gjør at kvinner opplever informasjon om spesielt deres lokasjon og hverdagsrutiner som mer sensitivt enn det menn gjør, og som kan forsterkes av tidligere erfaringer. Her er Celine (43) et godt eksempel, som vi så hadde opplevd 'stalking'. Lignende forteller deltagerne som har en mer avslappet holdning at de har positive opplevelser med hvordan algoritmene bidrar til mer relevant innhold, noe vi kommer tilbake til i delkapittelet om personalisering og målretting. Dette er et aspekt som kan bidra til å forstå forbrukernes ofte defensive relasjon til egne data, det at positive og nyttige erfaringer forsterker ideen om data som akseptabelt byttemiddel, spesielt når det mangler selvopplevde negative konsekvenser av datamisbruk.

Kunnskapsmangel om databruk

Mangel på kunnskap kan også bidra til at deltagerne ikke er så opptatt av innsamling av deres personlige data. Flere av deltagerne påpeker at de ikke helt vet hva selskapene har av informasjon om dem og hva den brukes til, og noen åpner for at de kanskje hadde endret sin avslappede holdning til data dersom de visste mer. For eksempel sier Petter (26*): «Det kan hende at hvis jeg ser på den informasjonen de faktisk har, at jeg da blir overrasket over noe av de tingene som er lagret om meg da, at jeg da kanskje endrer mening».* Og flere deltagere i begge fokusgrupper sier de har en viss oppfatning av hva som samles inn, men ikke hva informasjonen kan brukes til. Som Jonas (27) formulerer det: *«Jeg vet ikke hva jeg ikke er redd for på en måte. [Jeg] ser kanskje bare de gode sidene, og at de kjipe sidene kanskje er litt skjult for meg, jeg vet ikke»*.

Dette fremstår som et viktig poeng. Det er mye usikkerhet knyttet til hvilke data som samles inn (selv om flere hevder de har en viss oversikt), hva de kan brukes til nå og i fremtiden, og hvilke konsekvenser dette kan få for den enkelte. Manglende kunnskap kan dessuten knyttes til både selskapers intensjon med bruk av data (om de har gode eller «onde» hensikter), og deres kapasitet til å håndtere dataene på en forsvarlig måte (om de er slepphendte med utlevering av data til tredjeparter eller sikrer dataen godt nok mot sikkerhetsbrudd). Data kan også være krevende å håndtere for selskapene selv, og formidle godt om til forbrukerne, både fordi de kan være uhåndgripelige og vanskelige å «oversette» til noe relaterbart. Samtidig kan resultater og konsekvenser av algoritmers prediksjoner også være uforutsigbare for selskapene, ikke kun for forbrukerne. Uansett, sett fra et forbruker-perspektiv kan nytten eller «de gode sidene» ofte være erfarte og håndgripelige, mens risiko eller de negative sidene forblir uerfarte og abstrakte for forbrukerne. Denne kunnskaps-

asymmetrien gjør at erfart nytte ved databruk ser ut til å vinne frem i mer eller mindre reflekterte kost-nytte-vurderinger.

I fokusgruppene kom det videre frem at flere har fått med seg kritiske dokumentarer på TV, blant annet en NRK-reportasje hvor det ble demonstrert hvordan man kunne spore en enkelt person og hans personlige data, samt lokasjon, ut fra et aggregert datasett produksjonen kjøpte tilgang til. En deltager synes dette er ubehagelig og påpeker at hun passer bedre på hva hun legger igjen av informasjon på nett, mens en annen ikke oppfatter det som så ille. Selv om slike innslag vurderes ulikt, kan det indikere at de har en effekt som kan kompensere for manglende erfart risiko og negative konsekvenser. Det å visualisere konkret for forbrukere, både kjeden fra datahøsting til bruk, og videre til konsekvenser, kan ha større effekt enn tekstbaserte påminnelser og henvisninger til økt kompetanse og bevissthet omkring rettigheter og regulering.

Dataenes verdi

I diskusjonen om deltakernes syn på egne data, fremkom det uenighet og usikkerhet rundt hvor mye dataene deres er verdt, og om det er en rettferdig byttehandel å gi bort data i bytte mot tjenester. Noen deltagere mener at persondata er verdt en del for selskapene som samler dem inn, men flere mener at deres data kun har verdi som del av en større mengde data, og ikke bare deres individuelle data. Det er også noen som mener at dataene ikke er spesielt verdifulle, nettopp fordi de ikke gir verdi alene. Her er en av deltagerne tydelig uenig: Celine (43) argumenter for at vi som forbrukere må se oss selv som del av et større bilde, og anse oss selv som produkter som selskapene tjener penger på (jf. Andrejevic 2014). Andre poengterer at det kan være vanskelig å vite hvor mye dataene er verdt fordi man ikke vet hva de brukes til av selskapene, og hva slags verdi det genererer for dem. For eksempel sier Jorunn (43): *«Jeg vet jo hva jeg får, men jeg vet ikke hva de gjør med den videre»*. Awan (29) og Jonas (27) prøver seg på en utregning:

> *Awan (29): For hvis en app koster 22... nei hvordan blir det da? Hvis en app koster 22 kroner, er min informasjon vært 22 kroner da? Det er jo ikke det, det er jo mye mer enn det, tenker jeg da.*
>
> *Jonas (27): For andre da. Fordi det at du er tjuefire år er jo verdiløst vil jeg si.*
>
> *Awan (29): Ja, hvis noen velger å kjøpe den informasjonen...*
>
> *Jonas (27): ...så får den en ver…*
>
> *Awan (29): ...så får den en verdi, og da er den kanskje verdt mer enn 22 kroner. Så da vet jeg ikke om det er en bra byttehandel. Men jeg tenkte jo mer på det nå da, jeg har ikke tenkt på det før, egentlig.*

Det blir også bragt opp at dataene er betaling for å kunne bruke apper og tjenester «gratis». Hvorvidt dette oppleves som en rettferdig eller en jevn byttehandel er det også uenighet om. Noen mener ja, andre nei, og noen synes det er vanskelig å vurdere. Oda (32) sier for eksempel at om hun laster ned en app, oppgir personlig data og lar den samle inn brukerdata om seg, så vil selskapet fortsatt ha disse dataene selv om hun bestemmer seg for å slutte å bruke og slette appen igjen: *«Bare fordi jeg ikke har den appen på telefonen lenger, så er ikke de dataene, den informasjon borte»*. Hun begrunner det også med at hun synes det er ubehagelig at noen har persondata om henne, og at hun ikke vet hvor mange som har denne informasjonen.

Hvilke alternativer som eksisterer til denne byttehandelen ble også diskutert. Noen deltagere nevner at det åpenbare alternativet er å betale med penger, enten gjennom abonnements-løsninger eller en engangssum. Et par av deltagerne er tydelige på at de ville foretrukket dette framfor en gratis app som samler inn data. En annen påpeker at det burde være enklere for forbrukere å selv velge hva som skal samles inn og ikke. Som Eva (29) sier, de som utvikler apper og tjenester burde *«gjøre det trygt og lett for oss forbrukere å ha eierskap til den dataen, så har jeg ikke problemer å gi det»*. Flere er enige i at det burde gjøres enklere for forbrukere å få mer kontroll over egne data.

Oppsummert ser vi at flere opplever det å bytte data mot tjenester som en rimelig og rettferdig byttehandel. De ser ikke helt den konkrete (penge)-verdien i sine egne individuelle data, men erkjenner at forbrukerdata kollektivt sett har stor verdi for selskapene. Persondataene er også et råstoff som skal videreforedles. Men det at deltakerne selv ikke vet hva det resulterende produktet faktisk blir, gjør det vanskelig å sette en pris på egne data som innsatsfaktor til «ukjente» sluttprodukter. Og til slutt mangler det gode alternativer til databytte, ettersom de færreste tjenester tilbyr både en gratis tjeneste i bytte mot data, og en alternativ betalingstjeneste uten datahøsting.

Survey-data

I den landsrepresentative surveyen kommer det frem at 8 av 10 (82%) ofte eller av og til reflekterer over at det samles inn mye data om det de gjør digitalt i hverdagen, som å søke, netthandle, se på serier, være på sosiale medier og bruke smarte produkter hjemme. Her er det ingen tydelige kjønnsforskjeller, men yngre og eldre reflekterer noe ulikt. Blant de yngste (18-29 år og 30-39 år) er det henholdsvis 28% og 23% som sier de ofte tenker over datainnsamlingen som foregår på nett, mens blant de eldste (60-80 år) hevder 40% det samme.

I surveyen fremkommer det at omtrent 1 av 3 (30%) i stor grad mener de har oversikt over *hva som utgjør* deres personlige data, mens en omtrent like stor andel (31%) mener de i liten grad har en slik oversikt. Igjen er det marginale kjønnsforskjeller, mens det er noe forskjell på de yngste og de eldste. I alderen 18-29 år mener 36% de har liten oversikt, mens 26% i alderen 60-80 år mener det samme. Likeledes, 24% blant de yngste mener de har god oversikt mot 38% blant de eldste. I forlengelsen av dette spurte vi om *kontroll over egne data* og hvor disse brukes på nett. Her mente 19% i stor grad at de hadde kontroll, mens 48% i liten grad mente det samme. Blant 18-29-åringer mente 17% i stor grad å ha kontroll, og 58% i liten grad å ha kontroll. Blant 60-80-åringer mente derimot 21% i stor grad å ha kontroll, mens 42% i liten grad mente det samme.

Det er 47% som i liten grad synes det er greit at det samles inn data for å tilpasse tjenester, forbedre funksjonalitet, og skreddersy innhold til den enkeltes antatte behov, mens 17% i stor grad synes dette er greit. Her er det ingen tydelige kjønnsforskjeller. Igjen skiller alder seg ut; mens 36% blant 18-29-åringer i liten grad synes denne praksisen er grei, synes 63% blant 60-80-åringer det samme.

Noe overraskende finner vi omtrent samme andeler når vi spør om det er greit at data samles inn for å skreddersy og målrette markedsføring til den enkeltes antatte behov. Det er 50% som i liten grad synes dette er greit, mens 18% i stor grad synes det er greit. Grunnen kan være at spørsmålene stilles etter hverandre med tilsvarende ordlyd, og at respondentene ikke skiller godt nok mellom data som benyttes til *funksjonstilpasning og skreddersydde tjenester* – og til *målretting av markedsføring*. I det kvalitative materialet argumenterte deltakerne forskjellig i tilsvarende situasjon.

Vi ønsket også å avdekke faktiske erfaringer, og om forbrukere har opplevd negative konsekvenser ved at data har kommet på avveie eller blitt brukt uten deres samtykke. Det viste seg at 15% hadde opplevd negative konsekvenser i forbindelse med slike hendelser, mens 68% ikke hadde opplevd dette, og 17% var usikre. Usikkerhet her kan være et naturlig resultat ettersom det ikke alltid er enkelt å avklare årsakssammenhenger mellom datatap og negative hendelser i etterkant. Det ser ut til at en noe større andel blant menn (17%) enn kvinner (13%) har opplevd negative konsekvenser, mens en klart større andel yngre enn eldre har opplevd det samme. Det er 22% i alderen 18-29 år som har hatt negative erfaringer med datatap eller samtykkemisbruk, mot 14% i alderen 40-49 år, og 9% i alderen 60-80 år.

4.3. Sporing av forbrukere

Cookies til besvær

For å få tak i personlige data må forbrukerne identifiseres og spores digitalt, og det finnes flere måter dette kan gjøres på. I fokusgruppene nevnte deltakerne flere metoder, som bruk av cookies[25], IP-adresse, og geolokasjon. Cookies var det som ble nevnt flest ganger og av flest deltagere. Tim (31) kommenterer at apper kan spore uten at cookies er involvert, men at selskaper må spørre om lov til å spore på tvers av apper. Han påpeker at det kan være forskjell på nettleserversjonen av tjenester og app-versjonen når det gjelder hva de kan samle inn. Flere av deltakerne hevder at de ofte forsøker å klikke på 'nei' til cookies når disse dukker opp på en nettside, og Celine (43) som er opptatt av personvern, hevder at hun *«bruker den tida»*, men synes de gjør det vanskelig fordi *«jeg føler at jeg må gjøre det hele tida»*. Susanne (42) istemmer at hun hele tiden får opp cookie-spørsmål, selv på de nettsidene hun har vært inne på før. Hun resonnerer at det er GDPR som krever at du må spørres hver gang. Dermed fremstår det som at lovverket, som skal beskytte forbrukerne, samtidig kompliserer og kanskje forverrer situasjonen fordi forbrukere til slutt gir opp og klikker 'ja til alt', noe som gir selskapene større legitimitet i bruken av personlige data.

Dette bringer oss over på temaet om samtykke. Som nevnt i avsnittet om data så savnet flere av deltagerne enklere måter å få mer kontroll over egne data på. Ingen av deltagerne i fokusgruppene oppgir å regelmessig lese gjennom brukervilkårene eller personvern-erklæringene som følger med apper og tjenester. De nevner grunner som at det er mye tekst, gjerne på engelsk, med en komplisert og uvant ordlyd, at vilkårene kan være vanskelige å finne, og at det gjerne er veldig enkelt å trykke på «godkjenn» samtidig som det er ekstra komplisert å ikke godkjenne, noe som kan skyldes manipulerende design-teknikker (dark patterns). Det ble også påpekt at deltakerne gjerne ønsker å bruke appen eller tjenesten uansett, og dermed opplever at de ikke har et reelt valg. Som Tim (31) sier: *«Det er sjelden man får et alternativ 'nei, men jeg ønsker fortsatt å bruke appen', det skjer jo ikke».* Eva (29) mener også at det skulle vært enklere å velge hva man vil takke ja til og ikke, og Susanne (42) synes det tar for mye tid å forholde seg til valgene. Hun sier:

> *«Hvis jeg føler at jeg har tid, så går jeg inn og trykker nei nei nei nei på alt. Men som oftest så gidder jeg ikke, så bare trykker bare godkjenn og lagre. Men hvis det hadde vært 'godkjenn' og 'ikke godkjenn', så hadde det vært*

[25] Informasjonskapsler

> *mye enklere å trykke 'ikke godkjenn', men når du trykker 'ikke godkjenn' så må du skru av hver enkelt cookie. Og jeg gidder ikke å forholde meg til at det er så tungvint. Så da lar jeg meg heller bli en salgsvare».*

Her fremkommer det tydelig at 'tid' er en svært viktig faktor for forbrukere. Det å bruke dyrebar tid på gjentakende cookie-/samtykkeforespørsler anses som både irriterende og belastende fordi det gjentar seg hver eneste gang man er på en nettside. Dermed har tid en høy verdi, men som på samme måte som data kan oppleves som noe immaterielt og vanskelig å prissette. Tid bør likevel anerkjennes som en del av kost-nyttekalkuleringen forbrukere (bevisst eller ubevisst) utfører. Vi ser i utsagnet over at deltakeren aksepterer 'å bli en salgsvare' i en *trade-off*-situasjon som involverer tidsbruk.

Strategier for å forhindre sporing

Flere er enige i at det å forhindre sporing og påfølgende datainnsamling krever tid og innsats. Likevel nevnes det noen strategier som deltagerne bruker for å hindre eller redusere sporingen av dem. Flere huker av for minst mulig cookies når de får valget, noen bruker eller har brukt adblock, mens enkelte benytter sporingsvennlige nettlesere som DuckDuckGo eller inkognitomodus i nettleseren. Det som går igjen derimot, er at slike valg ofte går på bekostning av brukervennlighet og funksjoner. Flere har opplevd å måtte akseptere cookies og skru av adblock for å kunne bruke nettsidene eller tjenestene slik de ønsker, og søkemotoren DuckDuckGo gir andre (og ofte dårligere) resultater enn tilsvarende søk i Google.

Bruk av adblocking kan eksempelvis forringe brukeropplevelsen på nett; Susanne (42), som har brukt adblocking i mange år, opplevde at «*mange nettsider deaktiverte seg selv og sa at 'du kommer ikke inn her hvis du har adblock på så vår tjeneste er utilgjengelig'»*. Dermed måtte hun skru av denne funksjonen for å få bedre funksjonalitet og tilgang til nettsider. På samme måte benyttet Petter (26) en funksjon på nettleseren som forhindret cookies, men han måtte skru den av fordi funksjonaliteten på mange nettsider ble mye dårligere: *«Jeg skjønte at det var noe godt i det [cookies]».* Brukervennlighet er derfor en sentral faktor i forbrukernes vurderinger av situasjoner der de ser ut til å devaluere verdien av personvern.

Inkognitomodus blir bevisst brukt for å skjule spor og identitet. Enkelte av deltakerne benytter dette i forbindelse med netthandel, for å hindre at sporing fører til høyere priser, men også motsatt, at man går ut av inkognitomodus for å signalisere hva man ønsker reklame og tilbud om. Elisabeth (31) hevder å bruke inkognitomodus ganske bevisst når hun skal kjøpe ting. Spesielt hvis hun ønsker å sjekke pris på en vare/tjeneste i forkant av kjøp, ønsker hun at det ikke skal lagres at hun har vært inne og sett på akkurat den varen/tjenesten:

> *«For noen ganger hvis man ser på flybilletter eller lignende så tracker de deg. Og så vet de hvilken destinasjon du skal søke på. Og så er prisene litt høyere neste gang. Akkurat sånne typer ting bruker jeg incognito-mode ganske mye på».*

Eva (29) benytter flere strategier i forbindelse med kjøpsrelatert atferd på nett. Hun bruker både DuckDuckGo for å slippe cookies og for å forhindre at det påvirker hva slags resultater hun får, mens inkognitomodus benyttes, på samme måte som Elisabeth (31), for å forhindre at prisene skrus opp. Men også motsatt; hvis hun ønsker et spesielt produkt, så søker hun åpent for å få mest mulig målrettet reklame om dette produktet: *«Så jeg bruker det også motsatt av deg da [Elisabeth (31)], for å – ikke manipulere – men fortelle liksom 'Google, nå*

skal jeg kjøpe, kan dere sende meg litt reklame'». Selv om det siste tilfellet ikke nødvendigvis er en type mot-manipulasjon, viser den at noen forbrukere er bevisste på mekanismene i markedet, og kan bruke disse strategisk til sin fordel.

Survey-data

I den landsrepresentative spørreundersøkelsen tok vi også for oss sporing på nett. Respondentene ble spurt om de reflekterer over at de blir sporet på de fleste nettsteder når de er på internett. Her hevder 31% at de ofte reflekterer over dette, mens 53% gjør det av og til. Det er 17% som sjeldent eller aldri reflekterer over slik sporing når de er på nett. Det er ingen tydelige kjønnsforskjeller her, men alder slår ut igjen; blant de yngste (18-29 år) hevder 26% at de ofte reflekterer over sporing, mot 37% blant de eldste (60-80 år). I motsatt ende sier 22% av de yngste at de sjeldent eller aldri tenker over sporing, mens kun 13% av de eldste gjør det samme.

Respondentene ble også spurt om hva de vanligvis gjør en når cookie-forespørsel dukker opp på nettsider de går inn på. Her svarer 41% at de vanligvis godtar alle cookies, mens 56% hevder at de kun godtar nødvendige cookies eller prøver å avhuke alle de kan. Det er kun 3% som vanligvis benytter sporingsfrie alternativer, som inkognito-modus, krypterte nettlesere som DuckDuckGo, VPN eller annet. Det er en tendens til at menn (44%) i noe større grad enn kvinner (37%) godtar alle cookies. Ser vi på alder godtar 36% av 18-29 åringer (og 30-39-åringer) alle cookies, mens 47% av 50-59-åringer og 43% av 60-80-åringer gjør det samme.

Det er videre 74% totalt sett som synes det er vanskelig å finne (og velge) alternativer som i liten grad innebærer sporing av egen aktivitet på nett. 68% av de yngste (18-29 år) mener dette er vanskelig, mot 81% blant 60-80-åringer. På spørsmål om hva de synes om å bli sporet på denne måten, der hensikten er å samle inn data om dem og deres hverdagslige handlinger, ble respondentene presentert for en rekke alternativer der de kun kunne velge ett svar. Her svarte 9% at de mener dette er greit ettersom de ikke har noe spesielt å skjule, mens 8% mener det er greit fordi slik sporing er nødvendig for å gi nettstedene data til statistikk, tjenesteutvikling og personrettet informasjon. Med andre ord mener rundt 17% at denne sporingspraksisen er akseptabel. Det er en kjønnsforskjell her, der menn (22%) i større grad enn kvinner (12%) synes sporing er greit. Det er også en langt større andel blant de yngre som aksepterer slik sporing enn blant de eldre, hhv. 28% i alderen 18-29 år mot kun 9% i alderen 60-80 år.

Videre er det 39% som ikke synes sporing er helt greit, men som aksepterer at dette er normalen i en datadrevet verden der alternativene er få. Det er 34% blant menn og 44% blant kvinner som mener dette. På aldersvariabelen spriker svarene, og blant 30-39-åringer svarer nesten halvparten (48%) at de aksepterer dette som normalen i den datadrevne økonomien. Det er dessuten 29% som ikke synes slik sporing er greit, men som heller ikke gjør noe spesielt med det. Her er det ingen kjønnsforskjeller, men ser vi på alder er det 20% som svarer dette alternativet blant 18-29-åringer mot 41% blant 60-80-åringer. Til slutt er det 15% totalt sett som ikke synes sporing er greit og som aktivt prøver å unngå dette. Det store bildet er uansett at flesteparten, nesten 7 av 10, ikke er helt fornøyd med sporingen fra nettaktiviteter, men heller ikke gjør noe spesielt med det eller stilltiende aksepterer situasjonen.

4.4. Personalisering og målretting

Sporingen av personlige data på nett bidrar i stor grad til å generere personalisert eller skreddersydd innhold og budskap – en typer massepersonalisering (Kotras 2020) – som målrettes mot enkeltforbrukere. I fokusgruppene er deltagerne klar over denne mekanismen, og kanskje den delen av «overvåkningsøkonomien» som de kjenner best til fra egen erfaring. Dette avsnittet vil først ta for seg personrettet innhold mer generelt, for deretter å gå inn på markedsføring mer spesifikt.

Persontilpasning og ensretting

Personrettet innhold blir av mange deltagere i fokusgruppene oppfattet som noe positivt. Det gir, som vi var inne på tidligere, mer tilpassede tidsanslag i Google Maps, forslag til lignende innhold basert på tidligere aktivitet, og bidrar til at tjenestene husker brukere på tvers av enheter. Spesielt funksjonen med å få anbefalt nytt innhold basert på tidligere bruk blir sett på som nyttig. Dette passer med de tidligere argumentene til deltakerne, der tid, bekvemmelighet og det å forenkle ting (gjennom gode grensesnitt eller tilpasning) er viktige aspekter i den digitale hverdagen. Dessuten er det å bli 'sett' og 'husket' noe iboende menneskelig, som man kanskje forventer i tradisjonelle markedskontekster, og som også gjør seg delvis gjeldende i den digitale økonomien (jf. Ruckenstin og Granroth 2020). Dersom man går inn i en lokal butikk vil mange kunne ønske at betjeningen hilser ved navn eller husker varer man kjøper ofte, og kanskje kommer med tilsvarende kjøpsforslag. Men en slik type tilpasning blir ikke sett på som utelukkende positiv blant deltakerne i en digital kontekst. Enkelte har også opplevd at innhold blir for ensrettet. For eksempel forteller Petter (26):

> *«Jeg husker da jeg lastet ned TikTok så så jeg på en basketballvideo, da var det basketball hele veien ned, selv om jeg også kanskje kunne likt å se på tango for eksempel. Men det vil da aldri bli foreslått for meg. Og det syns jeg er problematisk fordi, TikTok er en ting – at det er underholdning – men litt sånn som vi snakket om i sted, det finnes mange andre måter det kan bli misbrukt på da, eller sklir skjevt ut».*

Som Petter beskriver over, oppfattes ikke ensrettet innhold å være så farlig når det gjelder underholdning på TikTok, men det er en fare for misbruk i andre henseender. Even (18) påpeker at det kan være problematisk hvis andre typer innhold personaliseres, sånn som nyheter: *«Jeg tror det er veldig viktig...at folk generelt opplyses av nyheter fra mer enn bare en kilde, eller en side av politikken, eller sånn, og at det... tenker at akkurat der er det veldig veldig viktig å liksom hindre sånne ting»*. Ensretting blir også sett på som et større problem i kontekst av politiske videoer på YouTube. Jonas (27) forteller at det ikke skal mange trykk på «oppdater»-knappen til før man blir eksponert for mer ekstremt innhold, noe som kan være skadelig, spesielt for unge brukere som er lettere å påvirke. Deltagerne er enige i at bruk av personalisert og filtrert innhold kan resultere i filterbobler og ekkokamre, noe som er problematisk dersom man kun får bekreftet egne meninger og ikke utfordres av andre syn og perspektiver (jf. konspirasjonsteorier).

Deltagerne mener at også vi i Norge er sårbare for målrettede politiske budskap, selv om dette er mer fremtredende i andre land. En deltager påpeker at de aller fleste politiske partier og organisasjoner er til stede på de samme plattformene som forbrukere, dermed er det kort

avstand og gode muligheter for direkte og personlig påvirkning. Samtalene i fokusgruppene kom også inn på temaer som manipulering og kildekritikk. En av deltagerne har en datter og en annen er lærer, og de jobber begge bevisst på hver sin måte med å gjøre ungdommene oppmerksomme på at de må være kritiske til innholdet de ser på internett. En deltager er litt bekymret for å bli manipulert, og ikke være klar over at hun styres, mens en annen føler hun har god kritisk sans og mener hun ikke er sårbar for sånt. Disse aspektene oppfattes derfor ulikt i gruppene, spesielt hvor sårbar man selv er i møte med digitale påvirkningskrefter.

Filterbobler kan også være problematisk fordi det kan føre til diskriminering, men her er deltagerne noe usikre. En mener for eksempel at prisdiskriminering ikke er noe nytt, men en naturlig del av hvordan konvensjonelle markeder fungerer. Men flere er enig i at det vil være uheldig hvis diskriminering bidrar til å begrense enkeltindividers muligheter. For eksempel sier Petter (26): *«Hvis det begrenser muligheter til ulike individer da, for eksempel hvis du skal inn på Finn og søke på jobb og de som er på utkikk etter en ny arbeidstager, ønsker de liksom...Jeg kan se for meg at algoritmene der kan fungere på en måte som kan ekskludere noen personlig og det er jeg skeptisk til».* En annen deltager forteller at hun ikke oppfatter det som en villet diskriminering, men en konsekvens av at selskapene vil tjene penger. Deltakerne er også opptatt av at myndighetene bør sørge for at slik diskriminering ikke er mulig, og slik sett sikrer at alle har like muligheter.

Her ser vi igjen en tendens til at kommersielle selskapers praksis aksepteres som normal; at det er naturlig å skille på forbrukere gjennom en viss form for diskriminering, og at dette primært gjøres for å tjene penger og ikke for å utnytte eller diskriminere forbrukerne som sådan. Samtidig mener de at myndighetene bør følge med på uheldige diskriminerings-praksiser, og at diskriminering dermed knyttes til noe strukturelt som forbrukerne selv ikke kan gjøre noe med. Det fremstår også i fokusgruppene som at diskriminering er en type sårbarhet som angår «andre» i større grad enn dem selv. Vi ser også at det igjen skilles på markedspraksiser og andre samfunnspraksiser, f.eks tilknyttet arbeidslivet, der diskriminering anses som langt mer alvorlig enn i markedet.

Algoritmer og båssetting

En deltager påpeker at det er vanskelig å få grep om hvordan algoritmene fungerer og hvilke konsekvenser det kan ha. Elisabeth (31) sier: *«Det er så mange ting med disse algoritmene som man ikke engang...selv om man er skeptisk, selv om man oppgående […] Hvordan skal vanlige folk klare å forholde seg til de tingene og forstå at det skjer?»*. I tillegg til ensretting kan også algoritmene ta feil, noe enkelte deltakere oppfatter som irriterende og som får dem til å tenke over hvilken informasjon innholdet er basert på. For eksempel forteller Awan (29):

> *«Jeg fikk opp en del sånn Jordan Peterson destroys feminism, liksom, fordi jeg er ung mann og er singel på Facebook. Jeg tror det er derfor, jeg håper det er derfor. For jeg følger jo ikke noe sånt. Men det er liksom én ting jeg tenker...det er ikke noe jeg trykker meg inn på eller har gjort tidligere, så det tenker jeg er feil da».*

Her reflekterer Awan (29) i sitatet over hvorvidt innholdet han ble presentert for er basert på demografiske data om ham (mann, singel) og knyttet opp mot Facebook-informasjonen hans (personlige data). Han mener i dette tilfellet at de må ha feiltolket ham, og at hans egen søkeatferd på nett ikke kan stemme med denne type kategorisering. Med andre ord erkjennes det at algoritmiske feiltolkninger kan skje (selv om man er usikker på hvilke data som benyttes som bakgrunn for tolkninger), og det kan oppleves som både irriterende og frustrerende å bli satt i «feil bås» (jf. Puntoni et al. 2021); altså å bli plassert i en kategori man ikke føler seg hjemme i, eller det å ikke bli sett som den personen man er.

Personrettet markedsføring

Markedsføring er et tema de fleste i fokusgruppene har et forhold til, og som de har utstrakt erfaring med, og vi kommer inn på dette temaet gjentatte ganger i diskusjonene. Her er også deltagerne noe uenige. Flere sier at de ikke har noe imot å få personrettet reklame, mens noen mener at det generelt sett er for mye reklame og gjerne reklame de opplever som irrelevant. Igjen så fremstår det som om de deltakere som ikke har negative oppfatninger om denne type markedspraksis heller ikke opplever den som særlig risikofylt.

På spørsmål om hva deltagerne synes om reklame på nett er meningene som nevnt delte. For Awan (29) bidrar reklamen til at han bruker mobilappene mindre, fordi han blir lei av all reklamen. Andre sier de er mindre bevisste på all markedsføringen som finnes på de digitale plattformene, og Jorunn (43) tror hun overser mye av den. Noen ser derimot fordeler med personrettet reklame: Ettersom man uansett ikke slipper unna reklamen kan den like godt treffe litt bedre i forhold til interesser og behov. Petter (26) sier videre:

> *«Når jeg ser på forskjellige strømmetjenester og videoer, og mest YouTube da egentlig, sånn før videoen hvor jeg faktisk må sitte og faktisk se på den videoen, og da hvis det er noe jeg overhodet ikke bryr meg om, så synes jeg det er irriterende. Men hvis det er noe jeg liksom kanskje bryr meg om, så hadde det vært...det hadde gjort de fire sekundene litt kortere.»*

Sitatet tyder på at det ikke nødvendigvis er reklamen (innholdet) i seg selv som er positiv, men at personrettet reklame som «sjanger» oppfattes som det minste av to onder. Den kan også gi følelsen av at tiden går raskere. Her er imidlertid ikke deltagerne enige. Noen mener det er bedre med generell, ikke personrettet reklame. Even (18) er blant annet opptatt av at mer generelle budskap kan gjøre ham oppmerksom på tjenester og produkter han ellers ikke ville tenkt på. Her er prinsippet det samme som ble nevnt tidligere, at personretting kan lede til ensretting og innsnevring, og dermed forhindre mangfold og tilgang til nye og overraskende produkt- eller tjenestebudskap.

Susanne (42) mener at mer generell reklame på nett er mindre «klein og ubehagelig» fordi den minner om å se reklame på TV. Personrettet reklame er derimot ubehagelig når den er «styrt» og baseres på demografiske og personlige data for å tilpasses hennes livssituasjon:

> *«En ting er på en måte at jeg ønsker meg et par nye sko. Og så søker jeg på sko og så får jeg opp reklame deretter de neste to ukene, og sånne ting. Men en annen ting er Facebook som vet hvor gammel jeg er, hvor jeg bor og hvilken livssituasjon jeg er i, som på en måte plutselig pumper ned med reklame de mener passer for min livssituasjon akkurat nå. Jeg vet ikke hvor mange sånne fillers og ansiktsløftning-reklamer som jeg overhodet ikke er interessert i, som faktisk ganske ofte dukker opp på Facebook».*

Her oppfatter deltakeren det som ubehagelig at reklamen koples til kjønn, alder, bosted og livssituasjon, slik hun ser det. Reklamene hun nevner (fillers/ansiktsløftning) kan i utgangspunktet knyttes til enkle demografiske variabler som kjønn og alder, men for henne fremstår det som om reklamene baseres på enda mer intime og nære data om hennes livssituasjon. Denne opplevelsen eller oppfatningen er i seg selv viktig å forstå, uavhengig av hva slags data annonsene faktisk baserer seg på.

En annen kvinnelig deltager peker på kjønnsdimensjonen i reklamene, der spesielt kvinner ser ut til å få flere reklamer som spiller på usikkerhet og dårlig selvbilde. En annen deltager, av samme kjønn, mener derimot at også menn kan utsettes for budskap som spiller på usikkerhet og tilhørighet, og at mye av reklamen sender kjøpssignaler knyttet til hvordan man

skal være som person. Deltagerne er enige om at personrettet reklame kan bidra til at man går glipp av muligheter, fordi man ikke hører til den tiltenkte målgruppa. Lignende opplever flere at det kan være frustrerende å føle at de blir satt i bås av annonsørene, for eksempel når det gjelder nettbasert politisk reklame. Tim (31) forteller:

> *«Men igjen så er det jo da frustrerende, man føler at man blir brukt for liksom den personen man er og de egenskapene man sitter på. Ikke nødvendigvis for det man selv tenker da […] selv om jeg er en person i den og den alderen, og med det kjønnet, så er det ikke nødvendigvis alltid at jeg trenger lettkledde damer for å bli interessert i et politisk budskap».*

Det oppleves altså som frustrerende når reklamen fremstår personrettet, men bommer ved å enten basere seg på feil informasjon eller på for lite nyansert informasjon. I nevnte sitat ligger frustrasjonen i at han er mann (riktig demografisk informasjon) men at hans verdigrunnlag gjør at lettkledde damer i politisk reklame resonnerer dårlig med hvordan han oppfatter seg selv (feil verdibasert informasjon). For noen kan dette oppleves som å få presset på seg samfunnets normer og stereotypier, som for eksempel at Tim (31) som ung mann skal la seg lokke av lettkledde damer, eller at Susanne (42) som voksen kvinne skal ønske å begynne med kosmetiske inngrep. Her vil enda mer finmasket segmentering kanskje kunne avdekke et riktigere verdigrunnlag og et bedre tilpasset budskap. Samtidig vil dette bety ytterligere innsamling av person- og atferdsdata, som nok både vil stride imot det forbrukerne selv ønsker, og det som er forbrukerpolitisk ønsket.

Strategier for å styre innhold

Deltagerne forteller om ulike strategier for å styre hva slags innhold de får, både markedsføring og annet. Noen forteller at de bare ignorerer eller blar seg forbi innhold de ikke vil ha. Dette er både en naturlig konsekvens av at de ikke er interesserte, men gir også en mulighet til å sende et signal til algoritmene ettersom disse logger hvor lenge man ser på ulike typer innhold. Lignende forteller deltagere at de aktivt navigerer seg bort fra sider eller innhold som kan føre til feil profilering, eller at de endrer informasjonen de selv legger inn i plattformer, for eksempel ved å bytte kjønn på Facebook. En deltaker forteller at han trykker seg inn på innlegg-funksjonen der man kan se hvorfor han får se akkurat det innholdet, og deretter velger å ikke se det samme eller liknende innhold igjen.

Dette er strategier som følger av at reklamen er personrettet, men bommer på deltagernes interesser eller selvoppfatning. I tillegg ønsker deltagerne mer kontroll og det å aktivt kunne påvirke algoritmene. For eksempel sier Eva (29):

> *«Jeg skulle ønske istedenfor å gjøre som jeg gjør da, å gå og 'google' ting og håpe at det dukker opp, så tenker jeg at hvis jeg kunne gått og trykket på en knapp at 'nå ønsker jeg meg'... og da få likeverdig informasjon, litt som du snakket om i stad, å vite at da får jeg det samme som de andre får, det hadde vært, for min del da i hvert fall, veldig interessant».*

Det deltakeren her indikerer er at svaret på feilkategorisering av forbrukere i markeds-føringen ikke er å benytte mer data og bedre algoritmer til å forbedre treffsannsynligheten. En slik utvikling vil kanskje redusere irritasjonen med å bli satt i feil bås, men samtidig øke ubehaget med å bli sett og overvåket av allvitende kommersielle systemer. Dermed fremstår det heller som et ønske om at forbrukere selv bør få bedre oversikt og kontroll med egen representasjon og samtidig kunne signalisere når og hva slags reklame som ønskes, f.eks gjennom en type «dashboard» (jf. Datatilsynet og Teknologirådet 2016).

Survey-data

I den landsrepresentative surveyen tok vi også for oss personalisering og målretting av budskap, samt personrettet (eller overvåkingsbasert) markedsføring mer spesifikt. Her ble respondentene informert om at mye av grunnen til at vi spores, og at persondata samles inn, er for at kommersielle aktører skal kunne skreddersy innhold og tjenester og målrette dette direkte til den enkelte forbruker. Respondentene ble så spurt om de foretrekker personlig tilpasset innhold og tjenester eller mer generelt innhold og tjenester. Her var 26% helt eller delvis enige i at personlig tilpasning var noe de ønsket, mens 39% var uenige eller helt uenige i dette. Det var ingen tydelige kjønns- eller aldersforskjeller.

Det samme spørsmålet om persontilpasning ble stilt på nytt, men «innhold og tjenester» ble byttet ut med «markedsføring», slik at valget stod mellom personlig tilpasset markedsføring eller generell markedsføring. Her var det en like stor andel (26%) som i forrige spørsmål, som var enige i at de foretrakk persontilpasset fremfor generell markedsføring, mens 42% var uenige i dette og foretrakk generell reklame. Altså svarte respondentene tilnærmet likt i begge tilfeller.

Videre ble de spurt om det er greit at deres personlige data benyttes slik at algoritmer kan foreslå liknende serier, musikk, nyheter og sosiale medier-innlegg som de har vist interesse for tidligere. Her var 30% enige i at dette var greit, mens 36% var uenige. Det var også en aldersforskjell her; mens 27% blant de yngste (18-29 år) mente at persondata *ikke* burde spores og benyttes til slike formål, mente 47% blant de eldste (60-80 år) det samme.

Respondentene ble også spurt om de synes det er problematisk at personlige data blir benyttet dersom algoritmene bidrar til å snevre inn forslag, noe som kan resultere i lite variasjon i hva en får av serie-, musikk-, nyhets- og sosiale medier-innlegg. Her var det en langt større andel som var enige i at dette var problematisk (63%), mens 12% var uenige. Eldre ser ut til å være noe mer enige i denne problemstillingen enn de yngre.

Videre ble det spurt om det fremstår som problematisk at persondata spores dersom det betyr at man kan plasseres i en bås man ikke føler seg hjemme i, og som det er vanskelig å komme ut av. Her var 55% enige at dette kunne være problematisk, men 15% var uenige. Blant de yngste (18-29 år) var kun 20% helt enige i dette mot 42% blant de eldste (60-80 år).

Respondentene ble også spurt om de oppfattet det som problematisk at deres personlige data benyttes dersom algoritmene trekker dem mot stadig mer ekstremt innhold, der en risikerer å havne i ekkokamre hvor konspirasjonsteorier florerer. Her var det, noe overraskende, en noe lavere andel enn i de to forrige spørsmålene som var enige i at dette var problematisk (46%), samtidig som 19% var uenige. Dette kan bety at mange *ikke anser seg selv* for å være sårbare for denne type ensretting og ekkokamre, selv om de kan vurdere at andre er sårbare, eller at mekanismen i seg selv er problematisk.

4.5. Overvåkning

Begreper og assosiasjoner

Ettersom begrepet «overvåkning» fører med seg en del konnotasjoner fra offentlige og populære diskurser, og dermed kan lede diskusjoner i en bestemt retning, ble dette og relaterte begrep som «overvåkningsbasert markedsføring» og «overvåkningsøkonomi» introdusert relativt sent i sesjonene. Det ble fremhevet at målrettet eller overvåkingsbasert markedsføring gjerne pekes på som den drivende faktoren i overvåkningsøkonomien (jf. Forbrukerrådet 2021). Den grunnleggende ideen er at økonomien i hovedsak baseres på kontinuerlig monitorering eller overvåkning av brukere og deres data, som så benyttes til å utvikle produkter og verdier i økonomien.

I de to fokusgruppene gir begrepet overvåkning i hovedsak deltagerne negative assosiasjoner. Jonas (27) forbinder begrepet i mindre grad med logging av brukernes «digitale» data og atferd, slik vi så langt har diskutert, men knytter det mer til lyd og bilde:

> *«Ikke bare generell info om en person eller deres bruksvaner, men litt mer personlig enn det, som video eller lyd».*

Tim (31) kobler også overvåkning til video og mer «personlig oppfølging», og det forbindes først og fremst med mennesker som sitter og følger med, og føles dermed ikke beskrivende for den maskinstyrte økonomien det her er ment å beskrive. De føler seg dermed ikke overvåket på nett. Tim påpeker at det ikke er et menneske som sitter og følger med, og at han som person forsvinner i mengden, og at det dermed ikke føles så ille fordi *«det er sannsynligvis ingen som sitter og klarer å holde orden på absolutt alt jeg personlig driver med*». Likevel sier han at det er frustrerende å *«føle at man ikke slipper unna […] selv om det ikke er noen direkte personlig overvåkning».*

Med andre ord er den umiddelbare assosiasjonen til «overvåkning» at mennesker lytter, ser og følger med på hva man foretar seg, og dette oppleves som verre for deltagerne enn «digital overvåkning». Dette forklares med at det ikke er mennesker som ser dem, at sporingen og registreringen er så omfattende at de selv forsvinner i mengden, og at deres individuelle data ikke kan være veldig interessante å følge med på. Samtidig knyttes det frustrasjon til det å ikke unnslippe denne type digital overvåkning; det å vite at uansett hva man foretar seg så blir det registrert og brukt i en eller annen form. Dette «ubehaget» beskrev vi tidligere i analysen som noe som ikke knyttes til konkret risiko eller skade, men til en følelse av ubehag, frustrasjon og manglende frihet, altså noe som rokker ved mer grunnleggende menneskelige behov.

Muligheter, utfordringer og personvern

Videre ble økonomien diskutert på et mer helhetlig plan i fokusgruppene. Her trakk deltakerne fram både muligheter og ulemper. Blant mulighetene nevnes potensialet til å løse store samfunnsproblemer innen helse og klima. En deltager viser til hvordan Big data har gjort det mulig for smartklokker å identifisere at man er i ferd med å få et hjerteinfarkt og kan varsle medisinsk personell. Smittesporing under covid-19 pandemien blir også trukket fram som et mulig gode, men enkelte deltagere er også skeptiske til myndighetenes intensjoner og kritiske til deres avveining mellom sporing og personvern, blant annet den eldste deltakeren Harald (57). I tillegg påpeker en deltaker at det er viktig å være tydelig på hvem som skal ha tilgang til hvilke data slik at helsedata ikke kan selges til forsikringsselskaper og bidra til diskriminering. En annen deltaker sier at de positive sidene har et forbehold; at man som individ har en viss kontroll over egne data og kan «gå inn og skru av ting». Respondentene er enige om at det er et viktig forbehold for tilliten deres at offentlige instanser ivaretar innbyggernes interesser.

Av ulemper knyttet til overvåkningsøkonomien nevnes blant annet elektronisk krigføring og sårbarhet for utnytting og misbruk. Denne sårbarheten knyttes til fiendtlige eksterne krefter, som ved en krig, men også til egne myndigheter. I tillegg oppfatter deltakerne at sårbarhet kan dreie seg om avhengighet til teknologi og infrastrukturer – både i kontekst av en krig – men også mer generelt, som for eksempel til elektroniske betalingssystemer og smarthjem.

Forskerne trakk frem at mange myndighetsorgan ser store utfordringer for personvernet i den datadominerte økonomien. Det er variasjon i hvor viktig deltagerne selv oppfatter personvernet å være. Noen er tydelige på at de ønsker et personvern, blant annet Celine (43), som bastant mener at privatlivet vårt må beskyttes:

> *«Jeg tenker jo at vi må kjempe for privatlivet vårt, fordi uten det så kan vi fort ende opp som i Kina der vi får poeng for å smile og være hyggelige og oppføre oss ordentlig, og plutselig miste privilegier eller vanlige normale rettigheter».*

Andre derimot stiller spørsmål ved om det egentlig er noe som er verdt å beskytte. For eksempel sier Petter (26) at han ikke er bekymret for personvern og er usikker på om vi noen gang har hatt et «privatliv» når det kommer til kommersielle tjenester og apper. Vi så også tidligere i analysen at flere deltakere oppfattet det slik at mye av deres personlige data allerede ligger tilgjengelig ute på nettet, noe som kan bidra til å forringe følelsen av hvilke persondata som kan eller bør beskyttes.

Likevel, spesielt når Kina nevnes, der personlige data i større grad utnyttes av myndighetene (jf. Aho og Duffield 2020), gjør flere det tydelig at det er viktig å ivareta personvernet for å ikke miste privilegier og rettigheter. Og de påpeker at deres avslappede forhold til personvern og bruk av persondata bunner i en grunnleggende tillit til landets myndigheter og den demokratiske orden de er del av. Det kan dermed se ut som om personvern «snakkes frem» som viktigere når kontekster som krig i Europa, pandemi, statlig overvåkning og andre trusler diskuteres. Men i kontekst av data samlet inn på apper og tjenester, og ved personalisert innhold og markedsføring, framstår personvern generelt som mindre viktig. I korte trekk ser det ut til at personvernet oppfattes som viktigere i borger- enn i forbruker-kontekster.

Survey-data

I den landrepresentative surveyen trakk vi, på samme måte som i fokusgruppene, inn begrepet «overvåking» underveis. Vi spurte blant annet om i hvilken grad respondentene følte at det å bli sporet gjennom nettbasert aktivitet ga dem en følelse av å bli «forfulgt» eller «overvåket». Det var 43% som i stor eller svært stor grad kjente på denne følelsen, mens 27% i liten grad gjorde det samme. Her var det ingen tydelige forskjeller på kjønns- eller aldersvariabelen.

Det ble videre informert om at personlig og målrettet markedsføring også har fått betegnelsen «overvåkingsbasert markedsføring». Her ble respondentene spurt om i hvilken grad de føler at dette stemmer med deres opplevelse. Det var 65% som i stor eller svært stor grad mente at dette stemte, mens 11% mente det i liten grad stemte. Det var ingen tydelige forskjeller på kjønns- eller aldersvariabelen.

Vi ønsket å vite om respondentene følte at personvernet var truet eller hadde forsvunnet i dataøkonomien. De ble spurt om de følte at personvernet deres i stor grad var «dødt» fordi det ligger så mye data og informasjon om dem ute på nettet, hos offentlige og private

selskaper, og i sosiale medier og på andre digitale plattformer. Her var hele 32% enige eller helt enige i påstanden, mens 18% var uenige eller helt uenige.

En tilsvarende påstand var at mindre personvern er noe vi må regne med, fordi alle typer data, inkludert våre personlige data, er råvaren i en global datadrevet økonomi. Her var det en noe lavere andel, 24% som var enige/helt enige i påstanden, mens en større andel var uenige/helt uenige (36%). Det var ingen tydelige kjønnsforskjeller. På aldersvariabelen var 11% i alderen 18-29 år helt enige, mens kun mellom 3-6% var helt enige i påstanden i de eldre gruppene.

Når vi ser på overvåkning og sporing av data for ikke-kommersielle formål, blant annet for å håndtere store samfunnsutfordringer, ba vi respondentene forholde seg til påstanden: «Jeg er villig til å akseptere en del sporing av mine data for å bidra til å håndtere store samfunns-utfordringer innen helse, energi og miljø/klima.» Her svarte 41% at de var villige til å bidra med egne data (enige/helt enige), mens 23% ikke ønsket dette (uenige/helt uenige).

I det kvalitative materialet kom det frem at deltakerne var blitt mer oppmerksomme på egen sårbarhet, både digitalt og ellers, i og med større samfunnskriser som pandemi og krig i Europa. Deres tillit til dataøkonomien var også i stor grad tuftet på at demokratiske institusjoner fungerer som de skal, og at markedsaktører i bunn og grunn har gode (og kommersielle) intensjoner. Vi ønsket å se hvorvidt graden av bekymringer i befolkningen mer generelt hadde økt i og med krigen i Europa, og stilte spørsmål om krigen hadde gjort dem mer bekymret for egne digitale data, personlig overvåkning, og digital sikkerhet. Her svarte 39% at de var enige i at krig hadde gjort dem mer bekymret, men 29% var uenige i dette. Her var det en aldersforskjell; mens kun 30% blant de yngste (18-29 år) var blitt mer bekymret, gjaldt dette 51% blant eldste (60-80 år).

4.6. Kontroll og regulering

Brukerkontroll og aktøransvar

De fleste deltagerne i fokusgruppene har tillit til både myndigheter og kommersielle aktører, men det er ulike forventninger til hva disse aktørene antas å gjøre med data de samler inn. For eksempel forventer deltagerne at myndighetene ikke selger data videre og kun bruker dem til oppgitte formål. I en av fokusgruppene ble det påpekt at staten bruker private underleverandører, og dette anses som noe mer usikkert ettersom data kan kompromitteres. Flere av deltagerne har opplevd sikkerhetsbrudd i apper og tjenester de bruker, der passord er kommet på avveie. For de det gjelder hadde ikke dette fått store konsekvenser og virket ikke å ha endret deres syn eller praksiser med tanke på håndtering av persondata eller personvernet mer generelt.

Som vi har vært inne på tidligere i analysen føler mange av deltakerne at de ikke helt har oversikt eller kontroll på hva slags data som ligger hvor, hvem som har tilgang, eller hva dataene brukes til. En gjenganger under diskusjonene er ønsket om mer kontroll over egne data og hvordan algoritmene utnytter dataene til å tilby tjenester og innhold. Oda (32) sier blant annet: *«Jeg mener at vi bør få mer valgmuligheter selv, og at det bør være mer opp til forbrukeren hvilken informasjon som selskapene kan hente inn.»* Hun bruker som eksempel en app som varsler om jordskjelv og at hun forstår at den vil ha tilgang til hennes lokasjon, men at den ikke nødvendigvis trenger annen informasjon.

Andre igjen har mer eller mindre akseptert at de ikke har kontroll over egne data, og at det er en del av det å ta del i det digitale samfunnet. For eksempel sier Tim (31):

> *«Det blir jo nesten en jobb i seg selv å holde orden på alt. Og da er det jo ganske lett noen ganger å bare late som man ikke orker å bry seg. Hvis man skal liksom sitte å ha full oversikt over alle appene man bruker og nettsidene man har vært inne på og hvilke cookies man har akseptert og sånn, så blir man jo...får jo nesten ikke tid til å bruke disse appene og tjenestene, eller leve et normalt liv i 2022 liksom. Det blir jo vanskelig å kunne henge med da, hvis du for eksempel blir så bevisst at du ikke ønsker å bruke Snapchat eller ikke er tilgjengelig på Instagram eller Facebook Messenger fordi du blir så bevisst på hvilke data som skal sendes og godtas og sånt»*

Han sier altså at det å ikke være på digitale plattformer ikke er et godt alternativ ettersom det er der mye av det sosiale og praktiske hverdagslivet foregår (jf. Christl 2017). Flere deltagere har samme holdning, at det å være til stede på digitale plattformer er blitt en sentral del av hverdagslivet. Elisabeth (31) ønsker å *«være en del av det teknologiske samfunnet»,* og hun er villig til å akseptere en del sporing av seg selv, helt til *«det punktet der jeg blir utnyttet enten av en stor bedrift eller av staten på noe overvåkning eller sånn type ting»*. Hun erkjenner at mye av både jobb- og sosialt liv går via telefonen i lommen, og hun trives med måten det fungerer på. Likevel nevnes det forbehold hos flere deltakere om at bedrifter ikke utnytter dataene, og at myndigheter ivaretar forbrukernes interesser.

Deltakerne opplever at selskapene bak tjenester og apper har mye makt og ofte mye penger, og at deres agenda er å tjene enda mer penger. Deltagerne er ikke spesielt opptatt av hva slags ansvar selskapene eventuelt har for personvern, men viser heller til ansvar de selv har som forbrukere og det overordnete ansvaret myndighetene har. Det eneste konkrete ansvaret som legges på bedriftene er å gjøre personvernerklæringene mer forståelige og lettleste, og å gi forbrukere mer kontroll. Eva (29) sier:

> *«Men jeg tenker at hvis alle kunne gjort den jobben da med...som lager apper eller som lager produkter som er koblet til nettet, med å gjøre det trygt og lett for oss forbrukere å ha eierskap til den dataen, så har ikke jeg noe problemer å gi det. Så lenge jeg får det igjen som jeg opplever at jeg får»*

Som forbrukere ønsker deltakerne å være informerte og samtidig kunne ta kontroll over data som deles med kommersielle tjenester. Men deretter mener flere det må være opp til hver enkelt hvor mye og hva de ønsker å dele i bytte mot tjenester. Samtidig, som Tim (31) påpeker over, så vil det å holde orden, oversikt og kontroll over alle data og bruksområder generere enormt mye arbeid for forbrukere.

Myndigheter og regulering

Når det gjelder regulering i det digitale markedet, dukker det flere ganger opp under gruppediskusjonene utsagn om at de håper myndighetene er til stede og sørger for like muligheter for alle forbrukere, at de hindrer diskriminering, og beskytter borgere mot potensielt misbruk av personlige data. Som Celine (43) utbryter i en diskusjon om diskriminering i markedet: «*Jeg håper for Guds skyld at myndighetene er på ballen og har lovverk på det*». Deltagerne refererer derimot ikke til spesifikke lovverk (selv om GDPR nevnes) og instanser, men heller til en ide om at de regner med at staten eller myndighetene ivaretar deres interesser. En deltaker nevner at hun er fornøyd med et «årvåkent Datatilsyn»,

for eksempel det at de tok tak i smittesporingsappen under pandemien da den ikke ble ansett for å være i tråd med gjeldende personvernregler.

En deltager foreslår dessuten at Datatilsynet kan hjelpe bedrifter med å skrive gode personvernerklæringer som er enklere for forbrukere å lese – helst i én setning. Det nevnes videre at det er viktig å skille bedrifter og staten, slik at ikke staten kan samle inn sensitive data og selge det til bedrifter. Men det stilles spørsmål ved hvor grensene kan settes for hvem som skal ha tilgang til å kjøpe data og ikke. Og det presiseres at staten ikke burde ha databaser med personlig informasjon som kan bli brukt inn i politiske agendaer. Én av deltagerne ser for seg at staten kunne lagt mer føringer i viktige saker som klima. Som Even (18) sier:

> *«Hvis jeg skal være helt ærlig, så på mange måter så kunne jeg tenkt at det hadde vært bra med noe...eller ikke bra sånn da men...det kunne hjulpet på det med klima, for eksempel, hvis det var noe sånn poengsystem... Det blir jo veldig ekstremt da men. Men noe som legges til som kan få litt futt på sakene».*

Staten kan og bør legge føringer for bedrifter og individer, men det er også viktig for deltakerne at forbrukere gis nok handlingsrom til å velge selv. Her ligger det en sentral utfordring mellom det å sikre nok valgfrihet og samtidig unngå at forbrukere i for stor grad «blir valgt for» gjennom systemer som ensretter, manipulerer eller diskriminerer (jf. Lanzing 2019 og ideen om beslutningspersonvern).

Survey-data

Til slutt ønsket vi å få innsikt i om norske forbrukere mer generelt anser seg selv som manipulerbare. Dermed ble respondentene i den landsrepresentative spørreundersøkelsen stilt spørsmålet om de er redde for at store digitale selskaper etter hvert vet så mye om dem at de kan bli manipulert eller diskriminert uten å vite det. Dette var 56% enige i at var en utfordring, mens 19% var uenige. Her erkjennes det, at selv om man er reflektert og kritisk innstilt, er manipulerings-mekanismer designet for å ikke være lette å avsløre. Dermed kan man selv bli påvirket uten å vite det.

Videre ble respondentene spurt om de har tillit til at store selskaper som Facebook, Google, Amazon, Apple, etc. håndterer deres data på en forsvarlig måte, og ikke utnytter eller misbruker informasjonen de sitter med. Her viser resultatene noe av den samme tendensen som spørsmålet over; kun 18% var enige i at de har tillit til de store tech-selskapenes håndtering av deres data.

Vi var også interessert i tilliten til offentlige tjenesteleverandører, og spurte om respondentene har tillit til at norske myndigheter, som tilbyr offentlige tjenester, håndterer deres data på en forsvarlig måte og ikke utnytter eller misbruker informasjonen de sitter med. Her var det en langt større andel enn for de kommersielle selskapene som var enige i påstanden; 52% sa seg enige/helt enige i at de har en slik tillit, mens 19% sa seg uenige/helt uenige.

En naturlig oppfølging er å avklare om befolkningen har tillit til at regulerende myndigheter og tilsyn i Norge beskytter dem i den datadrevne eller overvåkningsbaserte økonomien. Her viser andelene at selv om tilliten kan være høy til norske myndigheter generelt, så er den varierende når det gjelder deres evne til å beskytte borgerne/forbrukerne i overvåknings-økonomien; det er kun 36% som sier seg enige i at de har tillit.

Til slutt ønsket vi å avdekke om respondentene selv mente de hadde kunnskap nok om lover/regler til å beskytte seg selv. Vi ba dem si seg enige/uenige i påstanden: Jeg har oversikt over hvilke lover og regler som finnes for å beskytte meg mot omfattende kommersiell overvåking og misbruk i digitale markeder. Her var det få som hadde slik oversikt; kun 13% sa seg enige/helt enige i påstanden, mens 53% sa seg uenige/helt uenige.

5. Diskusjon

5.1. Tilkopling

Moderat og delvis «overraskende» tilgang til nettilkoplede produkter

I en gjennomdigitalisert hverdag der data flyter og internett trenger inn i hverdagslige tjenester og produkter, er *tilkoblingen til nettet* den første kritiske pilaren for å forstå fenomenet forbrukerovervåkning. Flere tilkoblinger betyr flere inngangsporter til potensiell overvåkning og dermed større grad av sårbarhet. Oversikt og bevissthet om antall tilkoblinger kan derfor si noe om forbrukernes refleksjonsnivå når det gjelder dataproduksjon, sporing, personretting og overvåkning som slik nettilkobling legger til rette for, og hvilke strategier forbrukere benytter for å beskytte egne data og personvern. I surveyen ble dette temaet dekket mer generelt, og funnene viste at mens 9 av 10 opplevde hverdagen som i stor grad digitalisert og tilkoblet, hadde kun 1 av 10 tilgang til mange nettilkoplede enheter utover mobiltelefon, datamaskin og nettbrett.

Utfordringen i dag er at forbrukere kan ha flere tilkoblingspunkter enn de selv er klar over, mye grunnet utviklingen av tingenes internett og smarte produkter. TV-er, støvsugere, panelovner, leker, klokker og alarmsystemer kobles til internett, mens forbrukernes bevissthet om slik tilkobling kan variere (jf. Slettemeås 2019), gjerne fordi tilkoplingen i større grad er skjult, og fordi manglende skjermer og tastatur gjør produktene mer like ikke-digitale produkter. Dette så vi i fokusgruppene, der det både var stor variasjon i antall nettilkoplede produkter, men også i bevisstheten rundt hvilke produkter som faktisk var tilkoplet. Interessant nok viste det seg at «overraskelsen» over antall nettilkoplede enheter gikk flere veier; noen trodde flere enheter var tilkoplet, andre færre, og noen ønsket seg flere tilkoplinger enn de allerede hadde.

Tilkopling gir nytteverdi, men uro over å kunne miste styring og kontroll

Selv om kritiske studier av tingenes internett og overvåkning fremhever en rekke problematiske sider, ser forbrukerne i materialet positive sider ved det produktene har å tilby, slik som *tidsbesparing, kostnadsreduksjoner, forenkling, bekvemmelighet, trygghet* og *kontroll*. Surveyen viste dessuten at 1 av 3 generelt var positive til utviklingen av tingenes internett. Disse faktorene er viktige å avdekke ettersom de påvirker forbrukernes mer eller mindre bevisste kost-nyttevurderinger når kjøps- og tilkoplingsbeslutninger tas.

Likevel, økningen i antall tilkoblinger bidrar til forbrukerskepsis. I fokusgruppene ble det artikulert en viss uro over at andre kunne ta *styring og kontroll* og få fordeler av deres informasjon. Flere deltakere nevnte faren for å fremstå som en «vare» eller et «produkt» i dataøkonomien. Surveyen viste dessuten at 2 av 10 med tilkoblet utstyr utover mobil, PC og nettbrett hadde opplevd *ubehag og negative konsekvenser* knyttet til personvern eller sikkerhet. I fokusgruppene så vi videre at opplevelsen av «forenkling» var ulik blant deltakerne; tilkoplet utstyr ble både assosiert med en forenklet hverdag gjennom teknologisk støtte, men også med tekniske komplikasjoner og feilmeldinger. Dermed ble også «frakobling» synonymt med forenkling for enkelte.

Appmoderasjon representerer nøysomhet og reduserer sårbarhet

Som for tilkoplet utstyr kan bevissthet om antall og typer mobilapper si noe om forbrukernes refleksjonsnivå og evne til å håndtere de utfordringer som appene representerer. I fokusgruppene varierte antall mobilapper mellom 77 og 201, og mange ble overrasket fordi de hadde flere apper enn de selv trodde. Et høyt antall apper ble implisitt vurdert som noe

negativt, selv om mange av appene ble oppfattet som nødvendige. Dette kan antakelig knyttes til pågående mediediskurser om at det hefter personvern- og sikkerhetsrisiko ved mange mobilapper. Et fåtall apper kan også representere moderasjon og nøysomhet, i tråd med tankegangen rundt *cyberhygiene*, og at man ikke ønsker å være representant for et skjødesløst og risikoøkende app-overforbruk. Ved å redusere antall apper reduseres antall koplinger til kommersielle selskaper og samtidig antall sårbarhetspunkter for hacking og utnytting. I surveyen kjente kun 2 av 10 til de fleste selskapene som stod bak mobilappene deres, og 3 av 10 manglet tillit til flere apper. Kun 1 av 10 satte seg ofte inn i appenes brukeravtaler. Omtrent like mange hadde opplevd ubehag eller problemer knyttet til sikkerhet og personvern i appene.

I fokusgruppene klandret deltakerne seg selv for omfattende nedlasting av mobilapper. De skyldte ikke på manipulasjon fra markedsaktører, men innrømte heller at de ofte lastet ned apper på tynt behovsgrunnlag, selv om de ikke stolte på selskapene bak appene eller leste brukeravtaler. Samtidig følte flere at mengden personlig informasjon de må avgi for å kunne ta i bruk apper var uproporsjonal, men ikke nok til at de lot være å laste ned apper «for gøy». Ifølge dem selv kan slike app(u)vaner gi negative konsekvenser, som *ubehag*, *data på avveie*, *misbruk av personinformasjon*, *tap av kontroll,* og *generelle personvernutfordringer*. Deltakerne knyttet størst skepsis til sosiale medier-apper, spesielt TikTok grunnet potensiell kinesisk overvåkning, men også andre apper som sporer lokasjon og bevegelser. Google Maps unngikk likevel i stor grad kritikk; her ble bruksnytten vurdert som svært høy.

5.2. Data

Diffuse og uhåndgripelige data skaper svake bånd mellom brukere og deres data

«Data» var noe deltakerne i fokusgruppene så på som *diffust, usynlig, uhåndgripelig* og *komplisert,* og som det var vanskelig å knytte følelser eller bygge relasjoner til (jf. vanOoijen og Vrabec 2018). Nettopp det immaterielle aspektet kan bidra til å forklare vekten brukerdata tillegges i kost-nyttevurderinger som involverer nettjenester, mobilapper og markedsføring. Nytten kan oppleves som *umiddelbar og erfart*, mens kostnadssiden (som inkluderer risiko) kan fremstå som *fjern og uerfart*, ettersom data oppleves som noe langt mer abstrakt enn penger eller andre verdivariable. Dette gjør det krevende å foreta gode og informerte kost-nyttevurderinger sett i et «rasjonelt» forbrukerperspektiv. I surveyen reflekterte 8 av 10 ofte over at det samles inn mye data om dem på nett. Samtidig var det et mindretall, 1 av 3, som mente de hadde god oversikt *hva som utgjør* deres personlige data, og enda færre, 2 av 10, mente å ha *god kontroll* over slike data. En stor andel, 7 av 10, hadde fremdeles ikke opplevd *negative konsekvenser* med samtykke- eller datamisbruk.

Men fokusgruppedeltakerne poengterte at data ikke bare var krevende å håndtere for dem, men også for selskapene. Det at data oppfattes som flyktige og uhåndgripelige, og at det ikke alltid er lett å skille personlige data fra andre typer data, gjør det antatt vanskelig for selskapene å formidle på en god måte, og «oversette» til forbrukere, hva data er og hva de kan resultere i. Konsekvenser av algoritmers prediksjoner basert på brukerdata kan eksempelvis være uforutsigbart selv for de kommersielle selskapene.

Svake datarelasjoner, i kombinasjon med manglende negative erfaringer med datamisbruk (i tillegg til markedsmekanismer som fremmer datahøsting), kan vi anta leder til svak forståelse blant forbrukere for hva som utgjør digital personvernrisiko. Dessuten kan de føle at andres bruk av deres data ikke gjør at de «mister» data; de beholdes selv om andre benytter dem. Dermed kan følelse av «tap» forsvinne. Dette kan få konsekvenser for hvordan data og personvern håndteres av forbrukerne, og bidra til å forklare det tilsynelatende «personvern-paradokset» som oppstår mellom idealer og praksis (Barth & de Jong 2017).

Åpent tilgjengelige persondata reduserer oppfatningen av behov for vern

I fokusgruppene ble det fremhevet at mye persondata (som navn, adresse, telefonnummer og annet) allerede ligger ubeskyttet på nett, og dermed anses å være utenfor deres kontroll. Det at slike data allerede er «offentlig tilgjengelig» kan bidra til følelsen av at det er mindre viktig å *beskytte og forvalte* denne type data. Inflasjonen i data som ligger på nett kan dessuten bidra til å senke terskelen for hva som oppleves som *privat og sensitivt*. I fokusgruppene var det ulike oppfatninger av hvor personlige data oppleves å være. Eksempelvis mente en deltaker at sensitive data kan være noe uspesifikt, men like fullt ukomfortabelt at andre får vite om; en type «sosial risiko» som kan resultere i skam. Likevel trenger ikke dette å være data som er definert som personlig eller sensitivt i juridisk forstand. I mange tilfeller kan sosial risiko oppleves som vel så «risikabelt» for forbrukere som materiell risiko (som tap av penger/verdier).

Blant deltakerne var det ulike oppfatninger av hva som var greit å dele av informasjon. Noen oppfattet data om hvor de befinner seg (lokasjon) og hvilke vaner de har i hverdagen (atferd) som personlige eller sensitive, mens andre syntes dette var helt greit å dele. I diskusjoner rundt apper som sporer bevegelser, var det blant annet flere som ikke betraktet lokasjonsdata som personlig informasjon, selv om slike data kan misbrukes, skape ubehag, og muliggjøre *stalking*. Dette tilsynelatende paradoksale funnet kan ha sin forklaring i at bevegelse og lokasjon ikke oppfattes som «personlig» fordi det ikke representerer permanente trekk ved en person, men noe mer situasjonelt. Slike lokasjonsspor kan likefullt si noe nært, avslørende eller varig om enkeltforbrukere, men slike assosiasjoner skapes ikke nødvendigvis av alle. Likevel ser det ut til å være en kjønnsdimensjon her knyttet til sårbarhet; kvinner opplevde informasjon om lokasjon og hverdagsrutiner som mer sensitivt og ubehagelig enn det menn gjorde.

Avslappet holdning til kommersiell deling av data – og data akseptabelt byttemiddel

Generelt viste deltakerne i fokusgruppene en avslappet holdning, med noen få unntak, til hvilke og hvor mye data som samles inn om dem, spesielt i kommersielle sammenhenger. Det var en relativt utbredt oppfatning at det å dele data om *person, lokasjon* og *søkeatferd* ikke var så farlig, og at «datarisiko» (eks. datainnbrudd) ikke ble oppfattet som like farlig som «fysisk risiko» (eks. innbrudd i en bod), delvis støttet av argumentet om at mye informasjon om oss ligger på nett uansett. I tillegg oppfattet flere deltakere at de hadde mistet kontrollen over personlig informasjon i apper. En deltaker omtalte appinformasjon som «ikke farlig informasjon», selv om den kunne utnyttes. Dette var likevel ikke nok til at tiltak, som å justere innstillinger eller slette apper, ble gjennomført. Igjen ser vi en svak relasjon, eller en form for mental avstand, mellom forbrukere og deres data. De ser ikke ut til å relatere til immaterielle data på samme måte som til materielle gjenstander eller verdier (jf. vanOoijen og Vrabec (2018).

Det var også en aksept for å bytte data mot tjenester blant flere deltakere (jf. Rosen 2020). Brukerdata kan bidra til at Google Maps tilpasser tid og vei, at Spotify foreslår ny musikk basert på lyttehistorikk, og at forbrukere kan nyte godt av nye innovative produkter. Igjen inntok flere deltakere en «hva er det verste som kan skje»-holdning til bruken av personlige data, og rekken av konkrete nytteerfaringer blant deltakerne forsterket ideen om data som akseptabelt byttemiddel, spesielt i mangel av selvopplevde negative erfaringer med datamisbruk.

Deltakerne var usikre på hva slags data selskapene hadde om dem, hva de ble brukt til, eller hvilke resultater eller konsekvenser databruk kunne gi. Slik kunnskapsmangel og usikkerhet kan slå begge veier; at man forbeholder seg til et *føre-var prinsipp* og er restriktiv fordi utfallet er usikkert (jf. Holloway 2019), eller at det bidrar til *resignasjon* (Turow et al., 2015; Draper &

Turow, 2019), *apati* (Hargittai & Marwick, 2016), eller en form for *kynisme* (Hoffmann et al., 2016; Lutz et al., 2020), der man er mer «slepphendt» med datainnsamling – eller der tjenestefordeler vektes relativt sett høyere enn risikoelementer i kost-nytte-vurderinger. I våre data er det sistnevnte mest fremtredende. Enkelte hevdet likevel at de ville endret sin avslappede holdning til data dersom de visste mer («Jeg vet ikke hva jeg ikke er redd for»).

Deltakernes svake relasjon til egne data ble også reflektert i uklarheten rundt dataenes *verdi* som byttemiddel. Generelt opplevde flere at bytte av data mot relevante tjenester var en *rettferdig byttehandel*, men de syntes det var vanskelig å sette en pengeverdi på egne data. Flere mente dessuten at denne verdien da ville bli lav hvis den måtte konkretiseres. Flere mente likevel at *kollektive forbrukerdata* kunne ha stor verdi for selskapene.

Forbrukerne ønsket seg i hovedsak *mer og enklere forbrukerkontroll* over egne data. Likevel var hovedtendensen at data fremsto som relativt «ufarlige» for dem og innsatsen for å verne dem var deretter. De hadde dessuten en del positive opplevelser med hvordan algoritmene kan bidra til mer relevant innhold for dem. Her ser tre hovedfaktorer ut til å henge sammen; 1) en risikovurdering der det vurderes som lite farlig å dele dataene sine, 2) en kost-nyttevurdering der fordelene veier opp for ulempene, og 3) mangel på kunnskap om mengden data som samles inn, hva de kan brukes til og hvordan de eventuelt kan misbrukes. Det kom også frem at flere kontrollmuligheter også sannsynligvis vil bety mer arbeid for forbrukere.

5.3. Sporing

Cookies utmatter brukerne, som gradvis gir opp

Data om forbrukere anskaffes gjerne gjennom identifisering og sporing av atferd på nettet. Surveyen viste at 7 av 10 aksepterte at sporing var «normalen» i en datadrevet verden, selv om de ikke syntes det var helt greit eller forholdt seg passivt til dette. 2 av 10 aksepterte sporing fordi de mente de ikke hadde noe å skjule eller så sporing som nødvendig for nettsteders tjenesteutvikling. Et lite mindretall prøvde aktivt å unngå sporing, fordi de ikke syntes denne praksisen var grei i det hele tatt og det. Dermed viste 9 av 10 på en eller annen måte «aksept» for sporing og motarbeidet ikke den eksisterende modellen (jf. Cecez-Kecmanovic 2019).

Enkelte av deltakere i fokusgruppene kjente til sporingsmetoder som bruk av IP-adresse og geolokasjon, mens de fleste kjente til cookies[26] som de regelmessig støtte på i sin nettaktivitet. Mange forsøkte å unngå cookies, men endte ofte opp med å takke ‘ja’ fordi det var enklest. De som var mest kritiske til sporing brukte mye tid på å huke av ‘nei’ eller ’minst mulig’, men ble oppgitt over å måtte gjøre det hele tiden. En deltaker nevnte at regulering (som GDPR) gjorde at selskapene måtte spørre brukerne hver gang. Slik regulering kunne dermed bidra til ytterligere forbrukerutmattelse, ettersom mange endte opp med å ukritisk samtykke. Dette gir samtidig selskapene større legitimitet til å spore og ta i bruk data. Surveyen viste at 4 av 10 vanligvis godtok alle cookies, mens flesteparten kun godtok nødvendige cookies. Kun 3% brukte aktivt alternativer som ikke sporer. Generelt mente 4 av 5 at det var vanskelig å finne sporingsfrie alternativer.

[26] Informasjonskapsler

«Dark patterns» og «dyrebar tid» kan bidra til ukritisk samtykke

Ingen av fokusgruppedeltakerne leste regelmessig brukervilkår eller personvernerklæringer som følger med apper og nettjenester. De viste til flere barrierer; at det er *mye tekst*, gjerne på *engelsk,* med en *komplisert og uvant ordlyd*, i tillegg til at vilkårene kan være *vanskelige å finne*. Det var dessuten veldig *enkelt å trykke på godkjenn* mens det var langt mer *komplisert å ikke godkjenne*, noe som kan skyldes manipulerende designteknikker (*dark patterns*). Derfor endte de ofte opp med å godta de fleste vilkår, men opplevde egentlig at de ikke hadde et reelt valg om de ville ha fullt utbytte av apper og tjenester. Deltakerne ønsket enklere forklaringer og valg som likevel ville gi dem god tilgang til tjenester.

Det å bruke dyrebar tid på gjentakende samtykkeforespørsler relatert til cookies og brukervilkår ble ansett som både irriterende og belastende. *Tid* – selv sekunder eller minutter – viste seg å ha høy verdi blant deltakerne, men på samme måte som *data* kan tid oppleves som diffust og vanskelig å prissette. Likevel, i et eksempel fra fokusgruppene, nevnte en deltaker eksplisitt at hun heller aksepterte «å bli en salgsvare» enn å bruke unødvendig med tid på tungvinte forespørsler. Derfor burde tidsbruk og tidsavveining i større grad vektlegges i forståelsen av tilsynelatende paradoksal forbrukeratferd.

Strategier for å hindre – og åpne opp for – sporing

Selv om det å forhindre sporing og datainnsamling krever tid og innsats, benyttet flere deltakere i fokusgruppene likevel strategier for å redusere sporingen, slik som å huke av for minst mulig cookies, og det å bruke adblock, sporingsvennlige nettlesere som DuckDuckGo, eller inkognitomodus i nettleseren. Men de opplevde gjerne at de ble «straffet» for slike strategier, ved at det gikk ut over *brukervennlighet* og *funksjonalitet*, eller at det kunne medføre *deaktivering av tjenester*, eller gi *mindre presise søk* (f.eks DuckDuckGo vs Google). Som med *tid*, fremstår *brukervennlighet* som sentralt i forbrukernes kost-nyttevurderinger, der forsøk på personvernvennlig atferd etter hvert trumfes av behovet mer brukervennlighet.

I analysen så vi at deltakerne kunne være strategiske på flere måter. På den ene siden benyttet enkelte inkognitomodus for å skjule spor og identitet, for å forhindre at produktsøk gir dem høyere priser. I andre tilfeller ble søkene gjort bevisst «åpne» for å gi et signal til Google og annonsører om at reklame var ønsket for spesifikke produkter. Dette kan tolkes som en form for mot-manipulasjon, eller kanskje heller taktisk bruk av et teknologisk målrettingssystem fra forbrukernes side. Det viser dessuten at flere er kjent med hvordan mekanismene i «overvåkningsinfrastrukturen» fungerer, og at de kan bruke den til sin fordel. Slike handlinger kan fremstå som forbrukerrasjonell praksis, som gir redusert søketid og relevant produktinformasjon, men som samtidig åpenr for ytterligere datainnsamling og profilering.

5.4. Personretting

Delvis positive til personalisering og målretting av innhold og budskap

I fokusgruppene var de fleste deltagerne klar over mekanismen der sporing av personlige data benyttes til å generere personalisert innhold som kan målrettes mot enkeltforbrukere. Slik skreddersøm eller personretting ble oppfattet som positivt av mange, fordi det kunne resulterte i *relevante forslag* basert på tidligere aktivitet, gi *tilpassede tjenester og innhold*, og

bidra til at en blir *husket på tvers av enheter og tjenester*. Disse faktorene ble koblet til nytteeffekter som tidsbesparing, forenkling og bekvemmelighet. I surveyen var forbrukerne noe mer avmålte til personlig tilpasset innhold og tjenester basert på sporing av egne data; kun 1 av 4 foretrakk dette fremfor mer generelt innhold og tjenester. Her kan det ligge en forskjell i at fokusgruppedeltakerne fikk mer rom til å vurdere og veie fordeler og ulemper ved slik tilpasning, og samtidig et bedre grunnlag for å skille databruk til *tjenestetilpasning* fra databruk til *markedsføringsformål*.

Ubehag ved nærgående teknologi og feilrepresentasjon

Selv om det generelt sett var positivitet knyttet til personalisert innhold og tjenester, ble en rekke negative aspekter tatt opp. Vi kan anta at det ligger noe iboende menneskelig i det å ønske å bli sett og husket, og bli oppfattet riktig (slik en ser seg selv) av andre, noe som kan koples til ideer om tilhørighet, identitet og integritet. Samtidig kan det gi en følelse av ubehag dersom teknologien *husker for mye*, blir for *personlig eller intim* i typer data som brukes, eller blir *for nærgående* i buskap og kommunikasjon. Dessuten kan relasjoner som er for teknologibaserte føles annerledes enn menneskerelasjoner, spesielt hvis de er ensidige og asymmetriske i favør teknologien.

Dessuten kan teknologi-induserte feiltolkninger (jf. Silver 2012) gjøre at forbrukere blir plassert i *feil bås*, mens forslag som baseres på tidligere atferd kan føre til for stor grad av *ensretting* i tjenester og budskap. I fokusgruppene fremkom det at flere ikke ønsket å bli tolket feil, selv om villeding av teknologien kunne bidratt til å redusere det teknologiske kunnskapsovertaket. Dette kan reflektere behovet for å fremstå som «den man er» og bli representert riktig, også i det digitale rom. I materialet ble likevel ikke ensretting sett på som særlig problematisk i kommersiell eller underholdningssammenheng, men ble knyttet til større risiko i relasjon til nyheter og politiske budskap. Konkrete utfordringer som ble nevnt var at få klikk raskt kan lede (andre) brukere til ekstremt eller skadelig innhold, og til stadig bekreftelse av egne meninger uten å bli utfordret av andre syn og perspektiver. Barn og unge ble løftet frem som spesielt sårbare her, samt behovet for økt fokus på kildekritikk som del av den digitale kompetansen – for både voksne og barn.

Sosiale og teknologiske mekanismer – manipulering, diskriminering og algoritmer

Deltakerne i fokusgruppene viste seg å kjenne til flere digitale påvirkningskrefter, som skjult *manipulering* som kan lede forbrukere inn i filterbobler og ekkokamre, men de så i mindre grad *seg selv som sårbare* for slike krefter. Det samme så ut til å gjelde for potensiell *diskriminering*. I fokusgruppene ble eksempelvis prisdiskriminering sett på som noe relativt normalt, og det å skille forbrukere ble vurdert som en naturlig del av markedspraksiser, og at det gjerne ikke var en «villet» diskriminering, men en konsekvens av selskapenes ønske om å tjene penger (jf. March 2019). Samtidig så enkelte deltakere den digitale diskriminering-sutfordringen som et problem på systemnivå, som myndighetene (og ikke den enkelte) burde følge opp. Diskriminering ble ikke vurdert som særlig «farlig» i kommersiell sammenheng, men ble sett som mer problematisk dersom den begrenset enkeltindividers muligheter på andre områder, som i jobbmarkedet.

Selv om manipulering og diskriminering er *sosiale mekanismer* kan de tekniske mekanismene som ligger bak være krevende å forstå. Alle deltakerne kjente til *algoritmer*, men syntes det var krevende å forstå hvordan de fungerer og konsekvenser av algoritmebruk i praksis. Det ble fremhevet at det «ikke er normalt» at vanlige folk, selv om de er skeptiske og relativt teknisk anlagt, skal måtte skjønne og sette seg inn i den fulle rekkevidden av algoritmebruk. Det var likevel bevissthet rundt deler av algoritmebruken, blant annet fordi enkelte følte seg feiltolket og dermed reflekterte rundt hva slags data

algoritmene brukte som grunnlag for tolkning. Det ble dessuten opplevd som irriterende og frustrerende å bli plassert i en bås, og gjentakende feiltolkninger kan tenkes å bidra til en form for fremmedgjøring, fordi man ikke lenger kjenner seg igjen i digitale representasjoner.

I surveyen mente 1 av 3 at det var greit at algoritmer benyttet deres data til å foreslå underholdnings- og sosiale medier-innhold. 6 av 10 så det derimot som problematisk dersom personlige data ble benyttet slik at algoritmene *innsnevret og reduserte variasjonen* i underholdnings- og sosiale medier-forslag. Rundt 5 av 10 fant det problematisk dersom de *ble plassert i en bås de ikke følte seg hjemme i*. Noe overraskende var det færre, litt over 4 av 10, som mente det var problematisk at algoritmer kunne *trekke dem mot stadig mer ekstremt innhold*, med risiko for å havne i ekkokamre og bli utsatt for konspirasjonsteorier. Grunnen til at andelen er lavere her kan være, som fokusgruppene indikerte, at respondentene *ikke anser seg selv* for å være sårbare for denne type påvirkning, selv om de anerkjenner problemstillingen mer generelt.

Målrettet reklame treffer bedre og får tiden til å gå raskere

Det var utstrakt erfaring – men blandede følelser – knyttet til *personrettet markedsføring* i fokusgruppene. Noen var imot mens andre syntes det var like greit å få personrettet reklame som generell reklame. I den landsdekkende surveyen var det rundt 1 av 4 som foretrakk personlig tilpasset markedsføring basert på sporing av egne data fremfor generell markedsføring, mens en større andel, 2 av 5, foretrakk generell reklame. Det fokusgruppe-deltakerne trakk frem som positivt med personrettet reklame var at man uansett «ikke unnslipper reklame», og da kan den like godt *treffe bedre* i forhold til interesser og behov. Den ble også oppfattet som mindre *irriterende*. Dessuten var det flere som *overså mye av reklamen* uansett, og relevante budskap kunne gi følelsen av å få *tiden til å gå raskere*. Som vist tidligere var faktisk eller oppfattet tidsbruk av stor betydning for forbrukerne. Dessuten ble det brukt *strategier for å styre innhold*, enten ved å ignorere eller bla raskt forbi reklamen, og dermed gi signal til algoritmene at reklamen var av liten interesse. Selv om ingen av deltakerne bevisst endret profildata (f.eks byttet kjønn), visste de om flere som gjorde dette for å mislede algoritmene. Enkelte trykket også på innleggsfunksjoner i f.eks Facebook, der de kunne se hva slags data reklameinnholdet ble basert på, for deretter å velge dette bort.

Generell reklame forhindrer innsnevring og er mindre «klein» og «ubehagelig»

Det ble også pekt på fordeler med *generell reklame*, blant annet at denne ville gjøre forbrukere oppmerksomme på nye typer tjenester og produkter de ellers ikke ville tenkt på (det motsatte av ensrettings-mekanismen). Det ble fremhevet at generell reklame er *mindre styrt*, og implisitt gir forbrukerne mer *følelse av kontroll*, samtidig som personrettet reklame oppfattes som mer *klein og ubehagelig* enn generell reklame når man vet at den koples til data om kjønn, alder, bosted og livssituasjon. Selv demografiske variable, som kjønn og alder, kan fremstå som 'intime' avhengig av markedsføringsbudskapet dataene resulterer i.

Som i diskusjonen av data og algoritmer, ble det også her opplevd som frustrerende å *bli satt i bås* av annonsørene, særlig ved nettbasert politisk reklame. Dersom personrettede politiske budskap bommer, enten ved bruk av feil informasjon (politisk farge) eller for lite nyansert informasjon (kun kjønn), kan budskapene stå i motsetning til eget verdigrunnlag og selvoppfatning. Samtidig vil bedre treffsikkerhet med stor sannsynlighet innebære ytterligere innsamling av person- og atferdsdata, noe som kan være uheldig. Personrettet markedsføring ble oppfattet både positivt og negativt i fokusgruppene, men uavhengig av

tolkning, opplevdes den ikke som *særlig risikofylt* for flere av deltakerne. Dette støtter opp om hvordan deltakerne i fokusgruppene generelt ser på kommersiell aktivitet.

5.5. Overvåkning

Føler seg ikke digitalt «overvåket» og «forsvinner i mengden»

Selve begrepet «overvåkning» ble generelt forbundet med noe negativt av deltakerne i fokusgruppene. Men det ga primært assosiasjoner til fysisk/personlig forfølging gjennom video eller lyd, der *mennesker* følger med på hva andre mennesker gjør. Det ble ikke forbundet med digital sporing og monitorering av enkeltpersoner og deres bruksvaner i en maskinstyrt økonomi. Det var heller ikke et begrep deltakerne selv benyttet før forskerne introduserte det. Med andre ord mente de at «overvåkning» ikke var helt dekkende for følelsen de hadde på nett, selv etter refleksjoner rundt aspekter som tilkopling, data, sporing og personalisering/målretting.

Noe annet som så ut til å redusere følelsen av å være overvåket var ideen om at cyberspace er stort, og at man som enkeltperson *forsvinner i mengden*. Det ble hevdet at det ikke føltes så ille fordi ingen klarer å følge med på alle personlig forhold til så mange nettbrukere, og at det derfor heller ikke føltes som «personlig overvåkning». Vi så også tidligere at deltakerne mente at de selv, og deres individuelle data, ikke var så interessante for andre, og i mange tilfeller ikke var så verdifulle. Her fremkommer det at det *vanlige og hverdagslige* de selv kan tilby antas å være uinteressant, noe som understøtter argumentet om at man «ikke har noe å skjule», mens det er nettopp dette «hverdagslige» Zuboff (2019) mener at kommersielle selskaper nå er ute etter.

Kollektive data kan løse samfunnsutfordringer, men «friheten» savnes

Deltakerne så også muligheter i «overvåkningsøkonomien», som det å bidra til å løse store samfunnsutfordringer ved å bruke kollektive data til klimatiltak, i helseapper, til smittesporing, osv. Men det fremkom også en *ambivalens og skepsis* til myndigheters intensjoner. Her ble avveiningen mellom smittesporing og personvern benyttet som konkret eksempel. Dessuten ble det lagt inn forbehold om at deltakelse, der personlige data brukes til samfunnstiltak, må være *frivillig og ikke pålagt*. Data må heller ikke videreselges til kommersielle interessenter og individet må kunne ha *kontroll og «gå inn og skru av ting».* Dessuten må offentlige instanser ivareta innbyggernes interesser. I surveyen mente 4 av 10 at noe personlig datasporing var akseptabelt for å bidra til å håndtere store samfunnsutfordringer innen helse, energi og miljø/klima, mens 2 av 10 ikke ønsket dette.

Selv om begrepet «overvåkning» ikke føltes passende for nettbasert sporing og datainnsamling for flere av fokusgruppedeltakerne, og noe databruk til samfunnsnyttig innovasjon ble sett på som akseptabelt, ble det ytret frustrasjon over det å *ikke kunne unnslippe* denne type digital observasjon. Frustrasjonen ble ikke knyttet til konkret risiko eller skade, men til *ubehag og manglende frihetsfølelse*. Altså noe som rokker ved mer grunnleggende menneskelige og eksistensielle behov om å kunne bevege seg fritt uten å bli registrert, eller at egen atferd skal legge føringer på fremtidig atferd. Med andre ord, det å vite at alt vi gjør nå har en *effekt eller konsekvens* fremover kan gi uheldige *nedkjølings-effekter* og *selvpålagte restriksjoner* på handling og deltakelse (Christl 2017, Lanzing 2019). Det er først sent i fokusgruppediskusjonene at digital overvåkning assosieres med manglende følelse av frihet. I de innledende diskusjonene, der personlig sporing og

datahøsting ble diskutert, fremkom ikke dette ubehaget over manglende frihet frem på samme måte. I surveyen mente 4 av 10 at nettbasert aktivitet ga dem en følelse av å bli «forfulgt» eller «overvåket». Hvorvidt begrepet «overvåkingsbasert markedsføring» stemte med deres følelse av personlig og målrettet markedsføring, var over 6 av 10 enige i. Her ble respondentene mer direkte konfrontert med overvåkningsbegrepet i spørsmålene enn i fokusgruppene.

Fare for økt digital sårbarhet og avhengighet i usikre tider

I fokusgruppene ble også andre negative forhold relatert til digital overvåkning diskutert. Her ble *sårbarhet og avhengighet* trukket frem av deltakerne. Dette ble spesielt fremtredende i relasjon til nye typer usikkerhet i samfunnet, som pandemien, Ukraina-krigen og kinesisk overvåkning – eller såkalte «salience shocks» (Büchi et al. 2022) – store hendelser som kan gjøre forbrukerne mer oppmerksomme. I og med Ukraina-krigen ble deltakerne mer oppmerksomme på muligheter for elektronisk krigføring og sårbarhet for utnytting og misbruk av persondata fra fiendtlige makter/krefter. Denne sårbarheten ble også sett i relasjon til egne myndigheter; misbruk kunne forekomme her til lands mente enkelte, som blant annet var usikre på myndighetenes intensjoner under koronapandemien. Avhengighet ble relatert til hvor nødvendig teknologi og infrastrukturer har blitt i hverdagen, fra elektroniske betalingssystemer til smarthjem. Men avhengighet som dimensjon ble enda tydeligere for deltakerne sett i sammenheng med Ukraina-krigen, og avhengighet ble knyttet tett til ideen om sårbarhet.

Usikkerhet og varierende bekymring for personvern

Helt overordnet står *personvernet på spill* i situasjoner preget av omfattende digital overvåkning; sporing, datahøsting og personalisering kan true individets kontroll, integritet og autonomi (vanOoijen og Vrabec 2018, Clarke 2019). I fokusgruppene så vi variasjon i hvilken grad personvern ble oppfattet som viktig. Enkelte mente at vi virkelig «må kjempe for privatlivet vårt», mens andre ikke var nevneverdig bekymret og stilte spørsmål ved om vi «noen gang har hatt et privatliv på kommersielle tjenester og apper». Oppfatningen av at mye personlig informasjon allerede er offentlig tilgjengelig ser ut til å erodere følelsen av hva som faktisk kan eller bør beskyttes av persondata, i tråd med perspektiver på *personvernapati* (Hargittai & Marwick 2016). I surveyen så vi også at 4 av 10 mente personvernet deres i stor grad var «dødt», fordi mye personlige data allerede ligger ute på nettet, mens 2 av 10 var uenige i dette.

Fokusgruppedeltakernes holdninger til data, overvåkning og personvern var i stor grad preget av *usikkerhet* rundt hva som kan karakteriseres som personlige data, hva slags personlig informasjon selskaper har tilgang til, hva denne informasjonen kan brukes til, og hva dette har å si for dem nå og i tiden fremover. Alle disse lagene av usikkerhet ser ut til å gi en forsterket følelse av *mangel på kontroll* og forvirring rundt hvilke *typer negative konsekvenser* de kan/bør forholde seg til. Det kan fremstå som et paradoks at deltagerne beskriver bekymringer, hvorav mange kretser rundt personvern, men likevel har et avslappet forhold til tilkopling, apper, sporing, data, etc. Utfordringen, viser materialet, er at *bekymringene ikke er så store*, og nytten og underholdningen apper og tjenester tilbyr ser ut til å veie opp for eventuelle usikkerheter og risikoelementer. Enkelte av deltakerne fremhevet at de «må gi for å få», og at de må dele data for sikre seg ønsket bruk og brukervennlige tjenester, og at Google uansett «vet alt». Samtidig ser det ut til at *mangel på konkrete*

negative erfaringer støtter disse praksisene. Dette kan bidra til å forklare det tilsynelatende «personvern-paradokset» (Barth og de Jong 2017) deltakerne signaliserer.

Likevel, når data- og personvernutfordringene ble kontekstualisert, eksempelvis med referanse til russiske hacking under Ukraina-krigen eller kinesisk overvåking og kontroll av befolkningen, ble personvernet aktualisert og fremsnakket som viktig. Dette stemmer overens med funn fra surveyen, som viste at krigen i Europa hadde gjort 4 av 10 mer bekymret for egne digitale data, personlig overvåkning og digital sikkerhet. Et sentralt poeng i fokusgruppene var at deltakernes relativt avslappede forhold til personvern og egne persondata bunnet i en *grunnleggende tillit* til landets myndigheter, institusjoner og den demokratiske orden. Dersom disse forutsetningene endres betraktelig, som krig og krise, mente deltakerne at fokuset på personvern og databeskyttelse nok ville styrkes ytterligere. Et annet sentralt poeng er at personvernet generelt ble oppfattet som viktigere i borgerrelaterte enn i forbrukerrelaterte diskurser.

5.6. Kontroll og regulering

Tillit til myndigheter og selskaper – men ønsker mer oversikt/kontroll med egne data

De fleste deltagerne i fokusgruppene viste seg å ha relativt *høy tillit til myndigheter, men også en viss tillit til kommersielle aktøre*r som dataforvaltere og tjenestetilbydere i den digitale økonomien. Men forventingene var større til at myndighetene ikke utnyttet og videresolgte data, og at data ble brukt til oppsatte formål. Surveyen viste mer konkret at 2 av 10 forbrukere hadde tillit til de store tech-selskapenes håndtering av deres data, mens 5 av 10 hadde tillit til myndighetenes datahåndtering. Samtidig så vi at deltakerne i fokusgruppene følte de manglet oversikt over tilgang til og bruk av dataene deres. De ønsket derfor *mer kontroll over egne data* og *mer kunnskap om hvordan algoritmene utnytter data*. Likevel aksepterte enkelte manglende kontroll, og at dette var en «naturlig» del av det å delta i det digitale samfunnet. I surveyen mente 1 av 4 at et svakere personvern var noe vi måtte regne med fordi persondata er blitt råvaren i den datadrevne økonomien. Dette kan knyttes til teorier om «digital resignasjon» (Turow et al. 2015, Draper & Turow, 2019) eller «personvernkynisme» (Hoffmann et al., 2016; Lutz et al., 2020).

Videre aksepterte mange av fokusgruppedeltakerne at data kreves i en rekke digitale transaksjoner, samtidig som det ble ansett å innebære for mye *arbeid* i seg selv å ha full oversikt og kontroll over alle apper, nettsider, cookies, personvernvilkår, osv. Denne typen «kontrollarbeid» antas å være så tidkrevende at det ikke er forenlig med å «leve et normalt liv i 2022», slik en deltaker formulerte det. Et liv uten digitale plattformer var heller ikke et alternativ for deltakerne, ettersom mye av det «sosiale og praktiske hverdagslivet foregår der», og fordi «digitale plattformer er en del av livet nå», og at man ønsker å «være en del av det teknologiske samfunnet» (jf. Christl 2017). Dermed aksepterte mange sporing av egen atferd og personlige data, og enkelte uttrykte til og med *tilfredshet og trivsel* med måten dette fungerte på, så lenge de ikke ble utnyttet og myndighetene ivaretok deres interesser.

Digitale selskaper ses ikke på som «overvåkningsagenter»

Flere fokusgruppedeltakere mente at digitale selskaper har mye makt og penger, men at de primært er ute etter profitt (jf. Morozov 2019). Bak denne argumentasjonen ser det ut til å ligge en idé om at profittfokuset til kommersielle selskaper delvis «beskytter» forbrukerne mot misbruk (inkludert datamisbruk), i den forstand at deres primære agenda er å tjene mer penger. Da kan ikke hovedmålet være å overvåke, utnytte eller manipulere forbrukerne

(utover det som anses som normalt i markedet) fordi gode og tillitsfulle relasjoner er viktige for å holde på kunder. Selv om de er opptatt av data, er det penger som antas å drive selskapene, og dette genererer i seg selv ikke mistillit hos forbrukerne (jf. Rosen 2020). Surveyen viste på sin side at en relativt stor andel, over 5 av 10, var redde for at store digitale selskaper etter hvert vil vite så mye om dem at de kan bli manipulert eller diskriminert.

I fokusgruppene var enkelte deltagere i mindre grad opptatt av hva slags ansvar bedriftene hadde for å beskytte forbrukernes personvern, og fremhevet at forbrukere selv og myndighetene også måtte ta ansvar. Det som ble lagt på bedriftene var ansvar for å gjøre *personvernerklæringer mer forståelige og lettleste*, og det å gi forbrukere *mer kontroll over egne data*, samt muligheter til å *påvirke algoritmene*, gjerne gjennom styringsknapper på en type 'dashboard' (jf. Datatilsynet 2016).

Lavere tillit til myndigheters beskyttende evne i overvåkningsøkonomien

I relasjon til behovet for regulering og til statens beskyttende rolle, fremkom det i fokusgruppene en forventning og et «håp» om myndigheters tilstedeværelse i den digitale økonomien. Dette ble sett på som viktig for å gi borgere/forbrukere *like muligheter,* forhindre *diskriminering*, og beskytte mot *misbruk av personlige data*. Det ble også forventet større grad av *interaksjon mellom selskaper og myndigheter*, der myndigheter eksempelvis kunne assistere selskaper i utformingen personvernveiledninger. Analysen viste at velfungerende demokratiske institusjoner var avgjørende for deltakernes relativt avslappede holdning til forbrukerovervåkning. Selv om nordmenn generelt har høy tillit til norske myndigheter, viste surveyen at kun 1 av 3 hadde tillit til regulerende *myndigheters evne til å beskytte dem* i overvåkningsøkonomien. Videre mente kun 1 av 10 at de *selv hadde oversikt* over hvilke lover og regler som finnes for å beskytte dem mot omfattende kommersiell overvåkning og misbruk i digitale markeder.

Ønsket om å kunne *velge selv* (agens og samtykke), *slippe å velge* (strengere regulering), eller *å bli valgt for* (maskinbasert beslutningsstøtte) vil nok variere stort blant forbrukere. En sentral utfordring for politikk og regulering ser ut til å stå mellom å legge til rette for at forbrukere får informasjon og valgfrihet nok i digitale systemer, men samtidig unngå at de i for stor grad risikerer å «bli valgt for» av algoritmestyrte systemer som ensretter, manipulerer eller diskriminerer, noe som kan underminere både informasjons- og beslutnings-personvernet deres (jf. Lanzing 2019). Dersom forbrukerens egne data «jobber imot dem» (jf. digital manipulering og diskriminering) kan manglende kontroll over egne data over tid potensielt skape en *negativ relasjon til disse dataene*; de kan fremstå som fremmedgjørende og som suspekte femtekolonister heller enn som verdifulle ressurser forbrukere kan utnytte til egen fordel, vinning og velferd. En utvikling som går mot en *svakere relasjon* og/eller en mer *negativ relasjon* mellom forbrukere og deres egne data vil være uheldig. Samtidig ser dagens «databruksmodell» ut til å ha blitt normalisert og akseptert over tid (jf. Cecez-Kecmanovic 2019), og mangel på selvopplevde negative erfaringer og risiko ser ut til å bidra til at dagens modell møter lite motstand fra forbrukernes selv.

6. Oppsummering og konklusjon

I analysen benytter vi **tilkopling** som første dimensjon til å belyse fenomenet forbruker-overvåkning. Flere smarte og nettverkstilkoplede produkter (utover datamaskiner, nettbrett og mobiler) bidrar til å *øke antallet inngangsporter* som muliggjør sporing, datainnhenting og personretting av budskap og tjenester. Dermed *øker sårbarheten* for mulige negative overvåkningseffekter. Fraværet av skjermer og berøringspunkter på mange nye typer tilkoplede produkter (jf. Holloway 2019) kan bidra til å ytterligere *redusere forbrukernes refleksjon* over tilkoplingsomfanget, ettersom de i mindre grad interagerer direkte med produktene i hverdagen. I materialet knyttes omfattende tilkopling til mulig tap av *styring og kontroll*, uro over *personvern og sikkerhet*, og antakelser om teknisk *merarbeid og komplikasjoner*. Samtidig assosieres tilkopling med nytteeffekter som *tidsbesparing, kostnadsreduksjoner, forenkling, bekvemmelighet, trygghet* og *kontroll*. Vi ser dermed, i tråd med perspektiver på «teknologiparadokser» (jf. Mick og Fournier 1998), at tilkopling kan gi følelsen av *både* mer og mindre kontroll, kan bidra til *både* forenkling og merarbeid, og kan *både* true sikkerhet og bidra til trygghet. Dette gjør forbrukervurderinger krevende, fordi tilkopling ikke fremstår som enten positivt eller negativt, men som *både positivt og negativt*. Slike avveininger er spesielt krevende i forbindelse med systemteknologier (som skybaserte, nettverkstilkoplede enheter med tilgang til et vidt tjenestespekter).

I materialet er forbrukerne dessuten «tilkoplet» gjennom en rekke mobilapper, og mange er overrasket over antallet apper de har lastet ned. Hver app innebærer tilkopling til et nytt selskap, en ny brukeravtale, og dermed en ny sårbarhet for sporing, datainnhenting og personretting. Hundrevis av apper på en enkelt mobil gir et krevende utgangspunkt for aktiv og kritisk refleksjon rundt tilkopling og sårbarhet. I materialet fremkommer det at en viss *moderasjon og nøysomhet* anses som fornuftig. Det å *redusere antall apper*, spesielt de som er unødvendige og lite tillitsvekkende, assosieres med *mer kontroll og mindre sårbarhet*. Slik moderasjon anser forbrukerne i materialet som sitt ansvar; her klandres ikke avhengighets-strukturer eller markedsmanipulasjon. Refleksjonsøvelsene i undersøkelsen bidro til økt vilje til å «rydde opp», mens enkelte mente at frakopling ikke ville hindre informasjonen deres i å fortsette å flyte «der ute». Uansett, analysen viser at uklarhet om antall nettilkoplede enheter og overraskelse over antall mobilapper indikerer *begrenset forbrukeroversikt* over hvor tilkoplet man faktisk er. Større bevissthet om den enkeltes/husstandens tilkoplingsomfang fremstår som fornuftig, og kan gi økt refleksjon rundt *hvor tilkoblet man bør være* (om «alt» trenger å være tilkoplet), og hva *cyberhygiene og appmoderasjon* kan bidra til for å styrke forbrukerkontrollen og redusere overvåkningsrelatert sårbarhet.

Videre muliggjør nettilkoplet utstyr, tjenester og apper omfattende innsamling og utnyttelse av forbrukerdata om forbrukere. I materialet oppleves **data** som noe *diffust, immaterielt og uhåndgripelig* som det er vanskelig å *knytte følelser eller bygge sterke relasjoner til*. Dette gjør at enkelte forbrukere ikke klarer å relatere til data på samme måte som til fysiske gjenstander. Det fremvises stor grad av *usikkerhet* rundt hva som anses som personlige eller sensitive data, hva slags data selskaper har tilgang til, hva data kan brukes til, og hva konsekvensene av databruk kan være i tiden fremover.

Forbrukernes svake relasjon til egne data gjør det *utfordrende å foreta fornuftige risiko-vurderinger*, fordi det er uklart hva som skal beskyttes og hva eventuelle konsekvenser av manglende beskyttelse kan bli. Få har opplevd *negative hendelser med datamisbruk*, og mangler dermed også noe konkret å relatere risiko til. De ulike typene risiko som forbruker-data (og overvåkningsøkonomien generelt) representerer, knyttes dessuten gjerne til mer overordnende utfordringer rundt kontroll, frihet, avhengighet, og hvordan vi ønsker å leve våre liv. Nytten av skreddersydde tjenester og budskap basert på personlige data kan derimot oppleves som umiddelbare og mer konkrete og håndgripelige.

I tillegg til svake datarelasjoner og mangel på negative erfaringer fremheves det i materialet at mye *personlig informasjon allerede ligger offentlig tilgjengelig på nett*, og mange føler de uansett har *mistet kontrollen over egne data*. Flere opplever dessuten det å bytte data mot tjenester som en *rimelig og rettferdig byttehandel*. Personlige data har med andre ord over tid blitt normalisert som valutaen man benytter for å «betale» for tjenester og innhold. Forbrukerne i materialet ser heller ikke den store verdien i egne data, mens alternativer til den eksisterende «databyttemodellen» oppleves som fraværende. I sum ser disse faktorene ut til å lede til en avslappet eller resignert holdning, og dermed lite motivasjon til å styrke vernet om egne data. Likevel uttrykkes det ønske om *bedre kontrollmuligheter for egne data*, men samtidig mener flere dette vil resultere i *stadig mer «kontrollarbeid».*

En sentral utfordring fremover ser ut til å være å *forsterke relasjonen mellom forbrukere og deres egne data*. Det kan tenkes at selskaper, innovatører og myndigheter bør utvikle løsninger for å *visualisere og konkretisere data* på en bedre måte for forbrukerne, slik at de ser hva data «er» i praksis, hvordan data konverteres til produkter, og hvilke konkrete konsekvenser data(mis)bruk kan få for den enkelte. Her kan alt fra avansert 3D-visualisering av data til kritiske dokumentarer rundt datamisbruk være nyttige. Visualisering av data kan også bidra til å «avmystifisere» data slik at de fremstår som mindre abstrakte og uhåndgripelige og samtidig mer verdifulle. Bevisstgjøring om at personlige data – som forbrukernes «digitale representant» – er jevnbyrdig med deres fysiske «jeg», kan bidra til å styrke interessen for å verne om personlige data. Økt forbrukerbevissthet, forbrukerkontroll og innovative datasynlighets-løsninger må gå sammen med regulering som begrenser datainnsamling og sikrer akseptabel datahåndtering.

Data om forbrukere anskaffes primært gjennom identifisering og **sporing** av digitale enheter og tjenester. Materialet viser at sporing i stor grad *aksepteres som «normalen»* i en datadrevet verden, og få motarbeider den eksisterende modellen. Enkelte forsøker å begrense sporingen, men «gir opp» etter gjentakende cookie- og samtykkeforespørsler. Det er heller «ingen» som leser brukervilkår eller personvernerklæringer. De som forsøker å redusere sporingen, opplever gjerne å bli «straffet» for slike strategier ved at *bruker-opplevelsen blir dårligere* eller at *tjenester slutter å fungere*. Denne «utmattingen» av forbrukere ser ut til å forverres av *manipulerende designteknikker* (dark patterns) og av oppfatninger om at «*verdifull tid» kastes bort* ved å gjøre de riktige tingene. I tillegg viser materialet at forbrukere benytter strategier der de *selv «åpner» for sporing* for å gi signal til algoritmene om at de ønsker målrettet reklame for bestemte produkter.

Fra et forbrukerperspektiv er det problematisk at de som aktivt benytter strategier og verktøy for å forhindre sporing til slutt må gi etter grunnet endeløse og gjentakende forespørsler, dårligere tjenester og brukervennlighet, eller designteknikker som lurer dem til å la seg spore. Forbrukere bør gis alternativer til sporing for å kunne opprettholde samme kvalitet på digitale tjenester og funksjoner. Samtidig er det uheldig at forbrukere aksepterer «å bli et produkt» ved å bevisst la seg spore i bytte mot relevant markedsføring. For den enkelte

forbruker kan dette fremstå som «rasjonelt» fordi nytten vurderes som høyere enn kostnaden. Dette viser at kunnskap om risiko og mekanismene i «overvåknings-infrastrukturen» likevel kan lede til tilsynelatende paradoksal eller uheldig forbrukeratferd.

Materialet viser at mekanismen for å generere **personrettet** innhold, basert på sporing av personlige data, også er kjent blant forbrukerne. Slik personalisering, skreddersøm og målretting oppfattes som positivt av mange fordi det gir dem *relevante forslag*, *tilpassede tjenester og innhold*, og bidrar til *tidsbesparing og forenkling*. Men personalisering gir også en følelse av ubehag dersom *teknologien husker for mye*, tar i bruk for *personlige eller intime data*, eller resulterer i for *nærgående budskap og reklame*. Algoritmiske feiltolkninger som *plasserer forbrukere i feil bås*, oppleves dessuten som problematisk og kan bidra til en følelse av fremmedgjøring fordi man *ikke kjenner seg igjen* i de digitale representasjonene som skapes. Samtidig ses *ensrettede budskap og tjenesteforslag* som utfordrende fordi det forhindrer mangfold og friksjon, som er viktig for refleksjon. Materialet viser videre at påvirkningsmekanismer, som *manipulering og diskriminering*, er kjent blant forbrukere. Disse mekanismene vurderes som «vanlige» og mindre «farlige» i kommersiell sammenheng, men anses som mer problematiske dersom de anvendes politisk eller på andre samfunns-områder. Algoritmer (som bidrar til manipulering og diskriminering) oppleves i materialet som krevende, og det fremheves at det ikke kan forventes at den jevne forbruker skal forstå den fulle rekkevidden av algoritmebruk.

I forlengelsen av personretting, viser materialet at **målrettet markedsføring** får blandet mottakelse. Flere anser den for å være *mindre irriterende* og *bedre tilpasset interesser og behov* enn mer generell markedsføring. I tillegg fremheves det at den kan gi en følelse av at *tiden går raskere*. Det benyttes også strategier for å *signalisere til algoritmene* hva man ønsker/ikke ønsker ved å interagere med markedsføringsbudskap på ulike måter. På den annen side viser materialet at personrettet markedsføring kan oppleves som mer *styrt og ensrettet* enn generell markedsføring, og dessuten mer *klein og ubehagelig* fordi den knyttes til personlige data og informasjon om forbrukeres livssituasjon. Det å *bli satt i bås* av annonsører blir også her sett på som uheldig, spesielt ved nettbasert politisk reklame. Begrepet «overvåkingsbasert markedsføring» stemmer dessuten overens med flertallet av survey-respondentenes assosiasjoner til målrettet markedsføring. Likevel, målrettet markedsføring oppleves ikke som spesielt risikofylt for forbrukerne.

En sentral utfordring ved personalisering og målretting er den relativt positive mottakelsen slik personretting får blant forbrukere, slik skreddersøm og personlig oppfølging også kan ha i tradisjonell handel. For å adressere de problematiske sidene, må det *synliggjøres for forbrukerne at det er deres data* som er danner grunnlaget for personrettingen, og at dette kan utnyttes på ulike måter, for eksempel til mer omfattende *diskriminering og manipulasjon*. I tillegg bør eventuelle alternative modeller kunne erstatte den *tilpasningen, relevansen og forenklingen* forbrukerne opplever med dagens modeller, og samtidig minimere forbrukeres ubehag knyttet til *bruk av personlige/intime data, for nærgående budskap, og upresis båssetting*. Materialet viser også at algoritmebruk, og mekanismer som fører til ensretting, manipulering og diskriminering, i større grad bør reguleres fra myndighetssiden, og ikke overlates primært til forbrukernes kompetanse.

Materialet viser at refleksjoner rundt tilkopling, data, sporing og personretting ikke nødvendigvis gir assosiasjoner til **digital overvåkning** (med unntak av målrettet reklame) Overvåkningsbegrepet relateres primært til menneskelig og *ikke maskinstyrt overvåkning*, og til bruk av video/lyd og *ikke digitale data*. Med andre ord ser det ut til at sporing av personlige data og logging av digital atferd *ikke oppfattes som personlig og materielt nok til å gi sterke overvåkningsassosiasjoner*. Her kan andre begrep, som *«dataveillance»* (Clarke 1988, van Dijck 2014), ha større relevans. Dette begrepet («data» og «surveillance» slått sammen),

beskriver den kontinuerlige overvåkningen av forbrukernes handlinger og kommunikasjon på tvers av digitale plattformer. Det å være underlagt dataveillance kan få forbrukere til å begrense sin digitale kommunikasjonsatferd. En slik nedkjølende effekt kan resultere i selvsensur, der risikoen ligger i at forbrukere over tid undergraver egen autonomi og velvære (Büchi et al. 2022). Dette er likevel ikke noe som trekkes eksplisitt frem i materialet.

Videre ser følelsen av å bli digitalt overvåket ut til å minimeres av oppfatninger som at man *«forsvinner i mengden»* og at man *«ikke har noe å skjule».* I sum ser det ut til at overvåkningen *ikke føles nær eller truende* nok til å ta grep for å redusere negative overvåkningseffekter. Likevel ytres det frustrasjon over å *ikke unnslippe digital observasjon*, fordi det gir en *følelse av å miste frihet.* Generelt preges materialet i stor grad av *følelser* (jf. Ruckenstein og Granroth 2020) rundt de ulike overvåkningsrelaterte problemstillingene, heller enn av konkrete risiko-vurderinger eller erfaringer. Det være seg 'skepsis' til sosiale medier og apper, 'usikkerhet' rundt hva data er og kan brukes til, 'ubehag' ved å ikke vite hvor mange som sitter på personlig informasjon, 'klein og ubehagelig' markedsføring, irrelevant reklame som 'irriterer', 'ukomfortable' tanker om datalekkasje til ukjente som kan lede til 'flauhet og skamfølelse', 'frustrasjon' over å bli satt i feil bås av algoritmer, og manglende 'frihetsfølelse' ved å ikke slippe unna sporing og overvåkning.

Analysen viser videre høy **tillit** til norske myndigheters håndtering av forbrukerdata i offentlige tjenester. I materialet artikuleres det dessuten en viss *vilje til å la seg spore* dersom egne databidrag kan hjelpe til med å *løse store samfunnsutfordringer* – så lenge borgerinteresser ivaretas, databidragene er frivillige, og dataflyten kan kontrolleres av brukerne. Samtidig fremvises det en *relativt høy tillit til kommersielle selskaper* som tjenestetilbydere. Disse *anses ikke primært som overvåkningsagenter*, men som profittorienterte selskaper med mål om å tjene penger heller enn å misbruke forbrukerdata. Denne profittorienteringen ser ut til å redusere skepsisen til kommersielle aktørers intensjoner, og bidrar til aksept for at en viss manipulasjon (reklame) og diskriminering (segmentering) er normalt i markedspraksiser. I materialet fremvises likevel en bekymring over at digitale selskaper gradvis får mer *styring og kontroll over forbrukernes informasjon*, og at store selskaper *over tid vil sitte på svært mye data (og makt),* slik at mer omfattende manipulering og diskriminering kan forekomme.

I overvåkningsøkonomien står spesielt **personvernet** sentralt. Overvåkning truer personvernet direkte, og dermed individers behov for å opprettholde et «privat rom» som er fritt for påvirkning fra andre. I materialet gis denne dimensjonen ulik vekt og prioritet, og varierer mellom ideen om personvern som *noe vi må kjempe for*, til at personvernet *uansett er dødt* i det digitale rom. En annen utfordring materialet fremviser er at eventuelle bekymringer rundt personvern *ikke er store nok* til å aktivere gode personvernstrategier blant forbrukerne. Denne utfordringen forsterkes av at *persondata i stor grad aksepteres som råvaren* i den datadrevne økonomien. Materialet viser også at personvernet ser ut til å oppfattes som viktigere i borger- eller samfunnskontekster enn i forbruker- eller markedssammenheng. Usikre tider, som krig, pandemi og statlig (kinesisk) overvåkning, forsterker likevel inntrykket av at *økende avhengighet* til digitale systemer gir *økt sårbarhet for individet*. Denne type diskurser *re-aktualiserer viktigheten av personvern* i materialet, ettersom det «avslappede» forholdet til sporing, data, personvern og digital forbruker-overvåkning bunner i en grunnleggende tillit til norske myndigheter og til en stabil, demokratisk orden.

En mer ustabil verden tilbyr derfor muligheter for å knytte forbrukere tettere til eget forbruker- og personvern, ettersom det blir tydeligere – også for forbrukere – at digital avhengighet

skaper sårbarheter der deres kontroll kan svekkes, integritet kompromitteres, og autonomi utfordres. Forbrukere inngår i dag som sentrale noder i et sammenflettet digitalt økosystem, og dersom de selv kompromitteres kan samfunnssystemet også påvirkes negativt. Personvernet bør derfor i større grad vektlegges som et *konkurransefortrinn* i utviklingen av både offentlige og kommersielle tjenester, heller enn å ses på som en kostnadskrevende nødvendighet. Samtidig ser vi at *forståelsen av personbegrepet* er i endring.

Rettstenkningen, som har formet personbegrepet, forutsetter en viss bestandighet og at en person bør være den samme hele tiden. Dette utfordres av digital dataeksponering, og av at mange opptrer med ulike fysiske, digitale og virtuelle representasjoner av seg selv. Forståelsen av bestandighet og konsistens kan endres, og dermed påvirke hva personvernet skal omfatte i fremtiden, hva vi skal verne om, men også hvordan vi skal definere selve personbegrepet (jf. Neumann 2005). Samtidig dreier digital overvåkning seg om mer enn personvern. Det handler om hva det vil si å være menneske i et fullstendig sammenkoplet samfunn, og hva slags samfunn vi ønsker å leve i.

I materialet er også **kontroll** et viktig aspekt for forbrukerne. Flere ønsker seg bedre «styringsverktøy» for data og algoritmer. Likevel mener andre at det å skaffe seg *kontroll over egen informasjon er nytteløst* i dagens digitale økonomi, at slik informasjon uansett blir *værende igjen «der ute*», og at *full styring vil bli for arbeidskrevende*. Dermed uttrykkes det en viss aksept for *ikke å ha full kontroll,* og det kan oppstå *trade-off*-situasjoner der kontroll avgis i bytte for bekvemmelighet. Sporing og deling av data anses dessuten som *«naturlig» og «prisen man betaler»* for å være del av det teknologiske samfunnet. Mange uttrykker dessuten *tilfredshet og trivsel* med den digitale hverdagen, en tilfredshet som reduserer sannsynligheten for et «forbrukeropprør» mot dagens forbrukerovervåkning. Denne *normaliseringen og rutiniseringen* av datadeling gjør at digitale praksiser kan være krevende å endre, selv med kunnskap om risiko og utvikling av alternative modeller. Etablerte rutiner som fungerer godt, og som mange er fornøyde med, må avlæres og erstattes av nye rutiner og modeller som må innarbeides over tid. Disse må i tillegg tilby tilsvarende bekvemmelighet, forenkling, nytte og relevans som dagens overvåkningsbaserte forretningsmodeller.

For å støtte forbrukere i den digitale hverdagen kreves fornuftig og langsiktig **regulering**. Selv om tilliten til norske myndigheter generelt er høy, inkludert til deres evne til data-forvaltning, viser materialet at tilliten er langt lavere til *myndigheters evne til å beskytte forbrukere* i overvåkningsøkonomien. Det forventes eller «håpes» likevel at myndigheter er tilstedeværende for å sikre like muligheter, forhindre diskriminering, og beskytte mot datamisbruk. GDPR[27] og den kommende Digital Services Act (DSA)[28] skal gi borgere/ forbrukere bedre kontroll og makt over egne data gjennom styrkede rettigheter, samtykke, bevisstgjøring, og mer effektiv sanksjonering. Men fremdeles hviler et stort ansvar på forbrukerne i å navigere og håndtere overvåkningsutfordringen. Her er *kritisk refleksjon* og *digital forbrukerkompetanse* sentrale verktøy. Utfordringen er at forbrukere allerede er overlesset med «arbeid» (jf. samtykke- og informasjonsinnhentingskrav), delvis grunnet regulering som krever at de holder styr på data, sporingskilder, samtykkeforspørsmål og vilkår. Samtidig er det få som har oversikt over hvilke lover og reguleringer som faktisk beskytter dem i overvåkningsøkonomien. I og med at forbrukerovervåkningen er

[27] General Data Protection Regulation

[28] Ref: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

allestedsnærværende, eroderer dessuten skillet mellom forbrukere (som økonomiske aktører) og innbyggere (som samfunnsaktører) (jf. BEUC 2021). Samtidig kan erfaring fra forbrukerrollen og markedsarenaen være nyttig og overførbar til andre samfunnsarenaer. Uansett vil ytterligere sektoroverskridende samordning av regulering, ansvar og kompetanse-bygging være nødvendig i tiden fremover.

Oppsummert kan vi si at forbrukere utfordres av informasjonsoverflod, oppmerksomhetsjag, samtykketrøtthet, data-fatigue, algoritmeforvirring, personvernapati og digital resignasjon – men også av normalisering, aksept, rasjonalisering og tilfredshet med dagens overvåknings-baserte systemer. Samtidig kan forbrukerne ledes til å tro at de har tilgang til *nøytral og ufiltrert informasjon* eller at de tar *frie og upåvirkede beslutninger*, mens de i realiteten utsettes for ulik grad av *filtrering, manipulering og diskriminering* med bakgrunn i data markedet sitter på om dem. En relatert utfordringer er, som materialet indikerte, at mange *ikke anser seg selv* for å være sårbare for ulike typer påvirkning, selv om de anerkjenner mekanismene og problemstillingene mer generelt. Den konstante overvåkningen kan likevel gi forbrukere en eksistensiell *følelse av å miste frihet,* fordi de hele tiden blir sett, vurdert, kalkulert, predikert og påvirket. Tap av *oversikt, kontroll og frihet* kan svekke evnen og viljen til *å reflektere og beskytte seg* selv i digitale rom, mens *langsiktige negative effekter* av digital overvåkning er krevende å overskue for den enkelte.

Omfattende *dataakkumulering* kan over tid bidra til at *maktforholdet* mellom forbrukere og markedsaktører forskyves ytterligere i forbrukernes disfavør. Resultatet kan bli *svekket forbrukeragens* (jf. Cinnamon 2017) og sterkere *teknologisk strukturering og styring* av forbrukernes *informasjon, valgmuligheter og beslutninger*. Dette er svært uheldig for forbruker- og personvernet og utfordrer forbrukernes *autonomi, integritet, verdighet og velferd*. Vi kan derfor, som Dencik og Cable (2017), anta at forbrukere (og myndigheter) står overfor en type «overvåkningsrealisme»; en uro over datainnsamling og samtidig en aktiv normalisering av overvåkning, som begrenser mulighetene til å tenke nytt om medborgerskap og fornuftige alternativer til overvåkningsøkonomien. Teknologisk akselerasjon og utvikling av kunstig intelligens kan ytterligere intensivere forbruker-overvåkningen og samtidig gjøre forbrukere mer avhengige av autonom teknologi. Dette vil samtidig gjøre dem mer sårbare for negative digitale overvåkningseffekter.

Litteratur

Andrejevic, M. (2014). The big data divide. *International Journal of Communication, 8,* 673–1689.

Barth, S & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics, Vol. 34,* Iss. 7, pp. 1038-1058.

BEUC (2021). *EU CONSUMER PROTECTION 2.0: Structural asymmetries in digital consumer markets.* Brussels, March 2021. Report.

Berg, L. (2016). *Hvordan mestrer unge voksne forbrukerrollen? En fortelling basert på fjorten informanters vurderinger og funderinger*. Oppdragsrapport 1-2016 Oslo: SIFO.

Berg, L. og A. Dulsrud (2018). *Tillit og sårbarhet på nett. Forbrukeres praksiser og vurderinger etter innføringen av den nye personvernforordningen (GDPR) i Norge 2018*. SIFO oppdragsrapport nr.9-2018.

BFD (2017). *Framtidas forbrukar – grøn, smart og digital*. Meld.St.25 (2018-2019).

boyd, d. & Crawford, K. (2012). Critical questions for Big Data. *Information, Communication & Society 5*(15): 662-679

Büchi, M., Festic, N. og Latzer, M. (2022). The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda. *Big Data & Society*, Jan–June, 2022, pp 1–14.

Cecez-Kecmanovic, D. (2019). The resistible rise of the digital surveillance economy: A call for action. *Journal of Information Technology 2019, Vol. 34*(1) 81–83

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior, 81,* 42-51.

Christl, W. (2017). *CORPORATE SURVEILLANCE IN EVERYDAY LIFE: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions*. Report.

Cinnamon, J. (2017). Social injustice in surveillance capitalism. *Surveillance & Society, 15*(5), 609-625

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM. 31* (5): 498–512.

Clarke, R. (2019). Risks inherent in the digital surveillance economy: A research agenda. *Journal of Information Technology, Vol. 34*(1), 59–80

Consumer Federation of America (2021). *Surveillance Advertising: What is it?* Ref: https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-what-is-it/

Datatilsynet (2015). *Det store datakappløpet.* Rapport.

Datatilsynet og Teknologirådet (2016). *Personvern 2016 – tilstand og trender*. Rapport

Dencik, L., & Cable, J. (2017). The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication, 11,* 763-781.

Draper, N. A. & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society, 21*(8), 1824-1839.

Dulsrud, A. og F. Alfnes (2017). *Når stordata blir Big Business*. SIFO oppdragsrapport nr.10-2017.

European Commission (2022). *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation*. Final Report.

Forbrukerrådet (2018). *Every step you take*. Rapport.

Forbrukerrådet (2021). *Time to ban surveillance-based advertising*. Rapport.

Grant, M. J. & A. Booth (2009). A typology of reviews: an analysis of 14 review types and associated methodologies, *Health Information and Libraries Journal, 26*, 91–108.

Haga, A. W. (2017). ”*Jeg er mindre paranoid enn jeg innerst inne hadde hatt lyst til å være” En studie av personvernet og nettbrukeres forhold til nettaktørers innsamling og bruk av personlige data*. Masteroppgave, Institutt for medier og kommunikasjon, UiO.

Hargittai, E., & Marwick, A. (2016). “What can I really do?” Explaining the privacy paradox with online apathy. *International Journal of Communication, 10*, 3737-3757.

Heilmann, S. (2016). Leninism upgraded: Xi Jinping’s authoritarian innovations. *China Economic Quarterly, 20(*4), 15–22.

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(4), article 7.

Holloway, D. (2019). Surveillance capitalism and children’s data: the Internet of toys and things for children, *Media International Australia, 170*(1) 27–36

Kamleitner, B., & Mitchell, V. W. (2018). “Can consumers experience ownership for their personal data? From issues of scope and invisibility to agents handling our digital blueprints”. In J. Peck & S. Shu (Eds.), Psychological ownership and consumer behavior (pp. 91–118). Cham: Springer.

Kjørstad, I., T. G. Rosenberg, A. Storm-Mathisen & D. Slettemeås (2017). *Barn og internettkoblede leker og teknologier – IoT*. SIFO oppdragsrapport nr. 8 - 2017.

Kotras, B. (2020). Mass personalization: Predictive marketing algorithms and the reshaping of consumer knowledge. *Big Data & Society*, July–December: 1–14

Lanzing, M. (2019). 'Strongly Recommended' Revisiting Decisional Privacy to Judge Hypernudging in Self-Tracking Technologies. *Philos. Technol., 32:* 549–568

Luguri, J. & L. J. Strahilevitz (2021). Shining a light on dark patterns. *Journal of Legal Analysis, 2021, Vol 13*, pp. 43-109

Lutz, C., Hoffmann, C. P., & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media & Society, 22*(7), 1168-1187.

Mick, G. & Fournier, S. (1998). Paradoxes of Technology: Consumer Cognizance, Emotions, and Coping Strategies. *Journal of Consumer Research, 25,* 123-143.

Morozov, E. (2019). *Capitalism's new clothes*. The Baffler, February 2019.

Nesta (2017). *Me, my data and I: The future of the personal data economy*. Decode project report, Sept. 2017.

Neumann, I. B. (2005). Begrepet «person» står ikke stille. I G. Apenes, *Fra tillit til kontroll. Tolv samtaler om politikk, teknologi og personvern*, ss. 25-33. Oslo: Pax forlag.

Ogura, T. (2006). Electronic government and surveillance-oriented society. In *Theorizing surveillance: The panopticon and beyond,* ed. David Lyon, 270–295. Portland, OR: Willan.

Orwell, George (1949). *1984.* London: Secker & Warburg.

Puntoni, S., R. W. Reczek, M. Giesler & S. Botti (2021). Consumers and Artificial Intelligence: An Experiential Perspective. *Journal of Marketing, 85*(1) 131-151.

Rosen, Michael M. (2020). Review: Why We Choose Surveillance Capitalism. *The New Atlantis, No. 61 (*Winter 2020), pp. 106-113

Ruckenstein, M. & Granroth (2020). Algorithms, advertising and the intimacy of surveillance. *Journal of Cultural Economy, Vol. 13*, No. 1, 12–24

Sandoval, M. (2013). A Critical Empirical Case Study of Consumer Surveillance on Web 2.0. In eds Fuchs et al, *Internet and Surveillance - The Challenges of Web 2.0 and Social Media*. New York, Routledge

Silver, N. (2012). *The signal and the noise. The art and science of prediction*. London: Penguin Books.

Slettemeås, D. (2009). RFID – the next step in consumer-product relations or Orwellian nightmare? Challenges for research and policy. *Journal of Consumer Policy,* 32, 3, pp. 219-244.

Slettemeås, D. (2018). *Forbrukernes digitale hverdag. Kunnskapsoppsummering forbrukerpolitikk 2018.* SIFO-rapport.

Slettemeås, D.(2018b). Big Data og Tingenes Internett – om den «oppkoplede forbruker» og nye markedsføringsrelasjoner. I *Markedsføring og forbrukerinteresser i det 21. århundret – samfunnsvitenskapelige perspektiver*. Oslo: Universitetsforlaget, kap 4.

Slettemeås, D. (2019). *Smart technologies in connected homes – A 2019 Norwegian consumer survey.* SIFO project note 6, 2019.

Slettemeås, D. & A. Storm-Mathisen (2021). Digitalisert forbruk. I Jensen, et al (red.), *Forbrukersosiologi. Bærekraft, digitalisering, identitet og makt.* Ch. 20. Bergen: Fagbokforlaget

Su, H. (2020). *Theory and Practice Towards a Decentralized Internet*, B.S. Computer Science, Interactive Media Arts, New York University Shanghai.

Throne-Holst, H. og I. Kjørstad (2016). *Hva koster gratis? Kommersiell bruk av personopplysninger og forbrukerdata.* SIFO oppdragsrapport nr. 11-2016.

Turow, J., McGuigan, L., & Maris, E. R. (2015). Making data mining a natural part of life: Physical retailing, customer surveillance and the 21st century social imaginary. *European Journal of Cultural Studies, 18(*4-5), 464-478.

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society,12* (2).

van Ooijen, I & H. U. Vrabec (2019). Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. *Journal of Consumer Policy (2019)* 42:91–107

Zuboff, S. (2015). "Big other: surveillance capitalism and the prospects of an information civilization". *J. of Information Technology, 30*, 75-89.

Zuboff, S. (2019). *The age of surveillance capitalism. The fight for a human future at the new frontier of power*. London: Profile Books Ltd.

Vedlegg 1 – Intervjuguide fokusgruppe1

Prosjekt om forbrukeres digitale hverdag og målretting av innhold, reklame og tjenester basert på personlige data

Tema 1: Hverdagsbruk av digitalt utstyr og tjenester

- Vi går gjennom spørsmålene deltakerne fikk i oppgave å notere ned i forkant av fokusgruppen:
    - I hjemmet:
    - Hvilke internettilkoblede enheter har du hjemme? Lag en liste. Noter hvilke enheter som er felles for familien, og hvilke som er personlige (både dine og de andres).
    - På mobilen:
    - Hvor mange apper har du på mobilen? (noter antall).
    - Hvor mange av disse appene har du sjekket brukervilkår og personverninnstillinger for (noter antall)?
    - Hvor mange apper er du usikker på med tanke på om personvernet ditt er godt nok beskyttet (noter antall)?
    - Velg én app du er usikker på og tenk gjennom: hva slags app er det? Hvorfor lastet du den ned?
- Hva tenker dere etter å ha gjort oppgavene? Lært noe nytt, gjort noen refleksjoner?

Tema 2: Forbrukerdata som samles inn på internett

- Det samles inn store mengder data fra stort sett alt vi gjør på internett – om vi shopper, er på sosiale medier, søker på Google, ser filmer på Netflix, lytter til sanger på Spotify, eller bruker smarthjem-utstyr.
    - Er dette noe dere tenker over – at store mengder data samles inn – ofte på tvers - av ulike nettjenester?
        - Typer data? (persondata, atferdsdata, lokasjonsdata, ting/sensordata?)
        - Bevisst/ubevisst? (forskjell på data vi frivillig legger ut i SoME, bruker bevisst i en tjeneste som Fitbit, må gi fra oss for tilgang til gratis tjeneste, eller skjult datasamling til reklame)?
        - Personlige data mer enn «persondata»? (navn, personnr., tlf, status, etc) – men mange datatyper ikke personlige/private – men gir til sammen komplett bilde av dere som person. Hva tenker dere om det?
        - Husstandsdata vs persondata: mye av datahøsting skjer i hjemmet – familiens data blandes sammen og er ikke lenger «persondata» men «husstandsdata» (og forsvinner ut av hjemmet). Hva tenker dere om det?
    - Fordeler – ved at så mye data samles inn om dere og hva dere gjør?
    - Farer/risiko – ved at så mye data om dere sirkulerer «der ute»?
    - Vanskelig for å se verdi av data (valuta, råvare, handelsvare)?
        - Bedre å betale for nettjenester med penger enn med data?
        - Vanskelig - begrepet «data»? (abstrakt, usynlig, immaterielt?)
        - Derfor vanskelig å se farer/alvorlighetsgrad ved misbruk av data?
        - Opplevd negative konsekvenser selv (misbruk, avveie, irritasjon)?

- I dag; Big data, algoritmer, KI - alle typer data interessante, jakter nye mønstre, mange forskjellige formål (som vi ikke vet om). Positivt med ny kunnskap (bedre tjenester, samfunnsgevinster?) eller bør data brukes kun til oppgitt formål? (formålsglidning)
- Data kan brukes til å forutsi interesser, preferanser og svakheter hos brukere? Ok eller problematisk? (utnyttelse av sårbarheter).
- Dataselskaper vet mye om oss og vi lite om dem? Ok eller problematisk? (maktasymmetri).
- Store mengder personlige data lagres i eksterne systemer, fare for hacking, misbruk. Er dette et problem? (datasikkerhet)

<u>Tema 3</u>: Sporing av brukere i hverdagen

- For å få tilgang til gode og nok data trenger digitale selskaper å spore forbrukerne på nett. Det brukes en rekke sporingsteknikker i tillegg til at forbrukere også «selvsporer» (wearables, søkemotor, sosiale medier) + at mye data er offentlig tilgjengelig.
  - Kjenner dere til noen sporingsteknikker som brukes?
    - (cookies, IP-adresse, GPS, søkelogg, annonse-ID (Apple, Google), sensorer i wearables).
    - Benytter dere metoder for å redusere sporing/datainnsamling? (slå av cookies, bruke adblocking, incognito browsing/DuckDuckGo, slå av annonse-ID, kryptert skylagring (vs Dropbox), etc.
  - Hva tenker dere om at det er så mange måter å spore forbrukere på?
  - Er det ubehagelig å bli sporet, eller en del av «gamet»? (nødvendig for tjenester)
  - Føles digital «sporing» mindre farlig enn å bli sporet eller fulgt «fysisk»?
  - Forskjell å bli sporet av Big Tech enn norske mediehus (SPiD) eller offentlige myndigheter (smittestopp)?
    - Forsikring: Hva med sporing som kan gi direkte fordel? For eksempel sanntidssporing av kjøremønster for lavere forsikringspremie (belønne god atferd)?
    - Sikkerhet: sikkerhetstjenester mot svindel online eller bolig (invaderende teknologi)?
    - Selvforbedring: selvsporingsteknologi til personalisert feedback og atferdsendring (sporingsteknologi styrer forbruker)?

<u>Tema 4</u>: Personalisering, skreddersøm og målretting

- Hovedmålet med å samle inn data ved å spore er å lære å forstå oss bedre, for å kunne «personalisere» eller «skreddersy» innhold og tjenester – og til slutt målrette dem til oss der vi er til enhver tid i ulike digitale kanaler. Personaliserte tjenester linkes til personlige identifikatorer (epost, IP, mobilnr) slik at vi gjenkjennes på tvers av plattformer og tjenester. Informasjon og tilbud fremstår da som unike for hver bruker og skal øke relevans/nytte?
- Kan slik personalisering, skreddersøm og målretting være nyttig?
  - Men; vanskelig å sjekke/etterprøve hva andre har fått av informasjon, tilbud eller tjenester – kan både inkludere og ekskludere. Er det greit? (diskriminering)
  - Men; kan individualisere markedet og hindre oss i å handle kollektivt? Tap av fellesskap og forbrukermakt? (Isolasjon)

- Men; data, algoritmer, manipuleringsverktøy kan påvirke beslutninger og valg og avsløre når vi er mest sårbare/tilbøyelige til å handle mer (overforbruk) eller unyttige ting, eller til å velge ting som ikke er bra for oss (velferd) (manipulering)?
    - Eks. Facebook/Cambridge Analytica – data ulovlig høstet fra Facebook profiler til millioner av brukere brukt til politisk mikromålretting, som kan ha påvirket det amerikanske presidentvalget i 2016 og Brexit-avstemningen i 2016.
- Men; data, KI og analyse – utstrakt testing? Får raskere forbedringer eller blir vi forsøksdyr? (eksperimentering)
    - Eks Facebook 'mood experiment' på brukere - manipulerte emosjonelt, positive/ negative poster i news feed for å se hvor mye positive/negative poster brukere selv la ut.
- Men; mer personlig, men innsnevret/ensrettet, innhold basert på tidligere atferd (ekkokammer, filterbobler)?
- Men; mer personlig, men mindre privat – følges, spores og eksponeres (transparente forbrukere)?

<u>Tema 5</u>: Målrettet (overvåkingsbasert) markedsføring

- Personalisering er kanskje mest merkbart i reklame (såkalt; målrettet/atferds-/prediktiv markedsføring.) Mål: målrette personlig reklame på tvers av plattformer og tjenester.
- «Prediktiv» markedsføring; prøver å forutsi hva vi ønsker oss før vi gjør det.
- Eksempel; søk på sko – dukker opp i diverse FB-feeder, Instagram etc. Hva tenker dere?
    - Mye av markedsføringen er «usynlig» – ledet av Adtech industrien (ukjent for forbrukere?) – som sporer, lager forbrukerprofiler, matcher forbrukere med reklame basert på profiler, og plasserer reklamen i relevante kontekster. Hva tenker dere om det?
    - Brukerprofiler kjøpes og selges på enorme børser gjennom automatiserte auksjoner i løpet av millisekunder uten deres viten. Hva tenker de om det?
    - Fatigue: konstant bombardement av annonser på digitale arenaer bryter gradvis ned forsvaret mot overtalelse og manipulasjon. Men har deltakerne opplevd manipulasjon? Og hvordan tolkes dette mot lovlig nudging?
    - Paradoks: kamp om 'oppmerksomhet' - må masseutsende eller målrette for å få 'kontakt' (men ofte BEGGE deler). Hvordan oppleves dette maset/støyen?
    - Kontekstuell reklame ses om alternativ; plasserer relevant reklame etter tema/ innhold på nettsiden. Krever ikke sporing av bruker eller atferd. Hva tenker dere om dette?
    - FR: studie – folk vil ikke spores og profileres for reklame. Stemmer det?
        - (FR-studie: ikke vurdert opp mot hvilke gratis tjenester de får som er reklamefinansierte)
    - Er målrettede annonser kun irriterende eller mulig alvorligere konsekvenser?

<u>Tema 6</u>: Overvåkingsøkonomi

- Overvåkingsbasert annonsering – den antatt drivende faktoren i veksten av det noen kaller 'overvåkingsøkonomien' – der kommersiell overvåking av forbrukere er blitt normen på internett (forstå, predikere, manipulere, forme atferd).
- Det omtales 'overvåking' fordi vi 'følges kontinuerlig' om vi er på nett eller ikke, på tvers av utstyr og tjenester, i hverdagen og i markedet.

- Tenker dere at 'overvåking' er riktig begrep å bruke på utviklingen?
    - Avansert og rimelig teknologi muliggjør «dataveillance» - og big data, algoritmer og KI gir nye muligheter – derfor samle så mye data som mulig.
    - Gir forbrukern**ytte:** bekvemmelighet, tidsbesparelse og friksjonsløs handel. Er det bra? Hva tenker dere?
        - Google Maps; Teknologi som muliggjør overvåking → også sentral i å levere tjenester til oss. Vi forventer at Google vet hvor vi er (og skal) for å gi oss trafikkinfo, distanse, kø, korteste kjørevei)?
    - Paradoks: vi ønsker oppmerksomhet, men ønsker også sterkt personvern/beskyttelse av privatliv?
    - Er vi medskyldige i overvåking? Både brukergenerert + egenovervåking + innhentede brukerdata → er vi med på å samprodusere data?
    - Føles det forskjellig å bli 'overvåket' digitalt vs 'fysisk'?
    - Folk kan begrense egne handlinger og meninger dersom de vet de overvåkes (chilling effect). Stemmer det?
    - Folk kan oppleve resignasjon i møte med å bli sporet, analysert og manipulert. Kan rasjonalisere med at man ikke har noe å skjule, eller ikke kan gjøre noe? (psykisk nummenhet)

<u>Tema 7</u>: Autonomi og kontroll – negative effekter for person

- Data, sporing, personalisering og overvåking → skal gjøre hverdagen enklere/ effektiv/ relevant/ behagelig for forbrukerne. Men mulig manipulasjon, diskriminering og utnyttelse av sårbarheter → påvirker forbrukers valgfrihet og autonomi og følelse av kontroll.
    - Gjør outsourcing til teknologiske systemer og bedrifter at vi mister makt/kontroll (negativt), eller gir det oss mer kontroll (positivt) fordi systemene hjelper oss å rydde og sortere i informasjonsoverfloden + støtte oss i beslutninger?
    - Dagens smarthjem, skybaserte og produsentkontrollerte løsninger – eierskap og data styres utenfra. Enkelt og billig – men mister vi kontroll? Er det noe risiko?
    - Det hevdes at regulering ligger på etterskudd ift. tech-utviklingen og at «personvernet er dødt». Stemmer det med deres oppfatning?
    - Forbruker og personvernlovgivning → i stor grad basert på samtykke:
        - Er det for mye ansvar på forbrukere (fordekt som frihet)? Bør myndigheter beskytte forbrukere bedre?
        - Samtykketrøtthet: for mange forespørsler/godtar uten å sjekke?
        - Kontrollparadokset: samtykke gir følelse av kontroll og reduserer personvernbekymringer + øker villigheten til å publisere sensitiv informasjon?
    - Umistelig gode: Er ikke personvern et umistelig gode? Kan det balanseres/byttes mot andre (samfunnsmessige) goder?

<u>Tema 8</u>: Utfordringer for forbrukere og samfunn i tiden fremover (17.40-17.50)

- Basert på det vi har diskutert omkring data, sporing, personalisering og overvåking; kan en si at dette ikke kun omfatter markedsføring, men kan omfatte hele hverdagslivet, der vi har gått fra et fritt og delende informasjonssamfunn (brukermakt) til overvåkingssamfunn (plattformmakt)?

- Normalisering av overvåking - normaliserer overvåkingskultur ved å gjøre overvåking (tidligere uvanlig) til noe vanlig og ubemerkelig? Hva med langtidskonsekvensene?.
- Total visshet (etter 9/11, Google kunne tilby dette): kvantifisere og algoritmestyre - organisere og justere samfunn minimere risiko/maksimere nytte. Hva tenker dere om dette?
- Trygghet vs frihet: Det å maksimere trygghet/fjerne risiko/maksimere nytte kan bety å fjerne individuell frihet. Tanker? Kan det forsvares med samfunnsbehov; takle store utfordringer innen helse, klima, terror?
- Mer atferdsmodifisering: i retning av mer premiering av riktig atferd, straff for feil atferd (som med fitbit, men i større skala). Er det ok? Må dette til for å takle store utfordringer (klima/strømforbruk, etc)?
- Mer manipulering: systemene/prosesser er lukkede/usynlige – mens vi forbrukere blir mer åpne/eksponerte – gjør det oss mer utsatt for manipulasjon?
- Barn mer utsatte: langvarig datainnsamling, er det en utfordring og er de for unge til å forstå implikasjoner?

Vedlegg 2 – Intervjuguide fokusgruppe 2

Prosjekt om forbrukeres digitale hverdag og målretting av innhold, reklame og tjenester basert på personlige data

Tema 1: Hverdagsbruk av digitalt utstyr og tjenester

- Dere fikk en liten oppgave til i dag – veldig fint om den er skriftlig så vi kan samle den inn på slutten:
- Hva tenker dere etter å ha gjort oppgavene? Lært noe nytt, gjort noen refleksjoner?
    - I hjemmet:
    - Er det noen som vil starte med å si hvilke internettilkoblede enheter dere har hjemme? Hva er felles for husholdningen og hva er personlig?
    - Har dere noen refleksjoner rundt dette? Ble dere overrasket over antallet?
    - På mobilen:
    - Hva med antallet apper? Noen tanker rundt dette?
    - Er det noen apper dere er usikre på personvernmessig?
    - Håndsopprekking – hvor mange har lest terms and conditions for en eller flere apper? Hvilken app var det?

Tema 2: Forbrukerdata som samles inn på internett

- Hva tenker dere på når vi sier at data samles inn? Hva slags informasjon er det snakk om? (persondata, atferd, lokasjon, ting/sensor)
- I hvilke situasjoner samles det inn data om oss på internett (shopping, sosiale medier, Google-søk, Netflix, Spotify, smarthjem-utstyr)? Er dette noe dere tenker over?
- Hva kan fordelene ved slik datainnsamling være?
- Hva kan ulempene være?
- Hva brukes disse dataene til?
- Har dere opplevd at deres data blir misbrukt? Eller havnet på avveie?
- Hvor mye tror dere dataene våre verdt nå?
- Hva tenker dere om å kunne betale for nettjenester med penger i stedet for data?
- Burde vi ha mer kontroll selv og kunne bestemme hvordan dataene våre skal brukes?

Tema 3: Sporing av brukere i hverdagen

- Hvilke teknikker brukes til å samle inn data?
- Hva tenker dere om at det samles inn så mye data?
    - Har dere hatt følelsen av å bli forfulgt på nett? Hvordan føles det?
    - Er det en forskjell på om det er private selskaper eller offentlige myndigheter?
    - Er det noen formål som det er mer akseptabelt å samle inn data til enn andre?

Tema 4: Personalisering, skreddersøm og målretting

Hovedmålet med å samle inn data ved å spore er å lære å forstå oss bedre, for å kunne «personalisere» eller «skreddersy» innhold og tjenester – og til slutt målrette dem til oss og vi gjenkjennes på tvers av plattformer og tjenester

- Kan slik personalisering, skreddersøm og målretting være nyttig?
- Hva er eventuelt ulempene med det?

Eks. Facebook/Cambridge Analytica – data ulovlig høstet fra Facebook-profiler til millioner av brukere brukt til politisk mikromålretting, som kan ha påvirket det amerikanske presidentvalget i 2016 og Brexit-avstemningen i 2016.

Tema 5: Målrettet markedsføring

- Personalisering kanskje mest merkbart i reklame.
- Hvilke erfaringer har dere med markedsføring i sosiale medier?
- Hva synes dere om markedsføring i sosiale medier?
- Hender det at dere får noen type reklame/markedsføring som dere liker / synes er gøy/interessant/nyttig?
- Hender det at dere får noen type reklame/markedsføring som dere synes er irriterende/kjedelig/uinteressant?
- Har dere noen gang blitt litt overrasket over en reklame dere har sett på sosiale medier?
- Bruker dere noen teknikker/triks for å styre markedsføringen dere får?
- Hvordan fungerer slik reklame? (hvordan bestemmes hva dere skal se?)
- Hva er fordelene og ulempene?
- Bør man ha personrettet reklame? Eller finne alternativer?
- Er det noen andre måter vi får målrettet informasjon, med unntak av reklame?

Tema 6: Overvåkingsøkonomi

- Hva tenker dere når vi sier «overvåkning»?
- Er det en riktig måte å beskrive innsamlingen av oss forbrukere på tvers av ulike produkter, tjenester og plattformer?
- Hvem her bruker Google Maps eller en annen kart og lokasjonstjeneste?
    - Hva synes dere om Google Maps?
    - Hva slags informasjon om oss tror dere Google får gjennom Maps? Hva brukes den informasjonen til?
    - Er byttehandelen jevn her? Informasjonen Google får om oss mot hva vi får igjen i Google Maps?
- Hvilket ansvar har vi forbrukere når vi er med på å produsere data? Føler dere at vi bidrar til overvåkning av oss selv?
- Hender det at dere oppfører dere annerledes for å unngå at informasjonen deres samles inn/deles?

Tema 7: Autonomi og kontroll

- Mange store aktører som påvirker hverdagen gjennom alle tingene og plattformene vi bruker – har vi forbrukere mistet kontrollen?
    - Et eksempel: et smartlys-selskap i USA stengte ned uten å advare kundene sine. Det førte til at smartlys, dimmere, lysbrytere og sensorer brått sluttet å fungere fordi de ikke kunne kommunisere med serveren til produsenten. Hva tenker dere om det?
- Hva tenker dere om at noen aktører som Google og Facebook vet så mye om oss? Hva vet vi om dem?
- Når vi besøker en nettside eller tar i bruk en ny app må vi samtykke til deres vilkår. Hvordan håndterer dere dette? Er det en god måte å håndtere personvern på?
    - Er det noen grupper som har større utfordringer med dette enn andre?
- Bør vi ha personvern? Hva skal personvern være?

<u>Tema 8</u>: Utfordringer for forbrukere og samfunn i tiden fremover

- Hvor mye makt har de kommersielle/private selskapene? For eksempel Google, Facebook, Apple, Amazon. Kan de ha noe å si for demokratiet slik det er i dag?
- Har vi mulighet til å påvirke retningen samfunnet går i?
- Hvem burde ha ansvaret for dette?
- Smittevernappen som ble rullet ut under Korona-pandemien krevde at en god del av befolkningen lastet den ned og delte sin lokasjon med appen for at den skulle ha noen positiv effekt på smittesporing og bekjempelse av pandemien. Hva tenker dere om dette med individuell frihet mot kollektiv trygghet?
- Et annet eksempel: Hvis algoritmer kan brukes til å manipulere oss mennesker til å handle mer klima-vennlig og på den måten bidra til å minske klima-utfordringene vi står overfor. Er det greit?

Vedlegg 3 – Spørsmålsskjema websurvey

INFOITEM:

De siste årene har hverdagen vår blitt svært digitalisert, og bedrifter og myndigheter er på konstant jakt etter data og informasjon fra borgere og forbrukere som de kan analysere og benytte til å kommunisere oftere og tettere med oss, utvikle mer personlige produkter og tjenester, og spisse reklamebudskap etter våre interesser og livssituasjon. Dette innebærer at «hele» vårt digitale liv er interessant, og at vi spores og overvåkes digitalt nesten kontinuerlig av en lang rekke aktører og plattformer. Vi ønsker å vite litt om hvordan du oppfatter denne situasjonen, og om du har erfaringer og meninger om denne tematikken.

1. I hvor stor grad føler du at **hverdagen din er preget av digitalisering** og bruk av n**ettbaserte tjenester**?
    - 1 I svært liten grad
    - 2
    - 3
    - 4
    - 5 I svært stor grad
    - Usikker / vet ikke

2. Utover PC, nettbrett og telefoner, har du tilgang til **nett-tilkoblede eller smarte produkter**?
    - Ja, mange
    - Ja, noen
    - Ja, kun noen få
    - Nei, ingen
    - Vet ikke

IF Q2=1-3

3. Har du **opplevd problemer eller ubehag** med noen av de tilkoblede tingene knyttet til personvern eller sikkerhet o.l.?
    - Ja
    - Nei
    - Vet ikke

4. Hva tenker du om **utviklingen der flere og flere ting blir nett-tilkoblet / smarte**?
    - 1 Svært negativt
    - 2
    - 3
    - 4
    - 5 Svært positivt
    - Usikker / Ingen formening

5. Kjenner du til **selskapene som står bak appene** du har lastet ned på telefonen din?
    - Ja, alle
    - Ja, de fleste
    - Ja, noen
    - Kun noen få
    - Nei, ingen

6. Setter du deg stort sett i inn i **brukeravtalene til appene** og hvordan de samler inn og bruker informasjon om deg og app-bruken din?
    - Ja, alltid
    - Ja, ofte
    - Ja, av og til
    - Nei, sjeldent
    - Nei, stort sett aldri

7. Er det noen **apper du er usikker på** eller mangler tillit til, men som du fortsatt har på telefonen din?
    - Ja, mange
    - Ja, noen
    - Nei, kun noen få
    - Nei, ingen

8. Har du hatt **problemer eller ubehag med noen av appene** på telefonen din knyttet til personvern eller sikkerhet?
    - Ja
    - Nei
    - Vet ikke

9. Det samles i dag inn store mengder data fra det meste vi gjør på internett – om vi søker, netthandler, er på sosiale medier, ser på serier, eller bruker smarte produkter hjemme.

    Reflekterer du over at det samles inn data om det meste du gjør digitalt i hverdagen?
    - Ja, ofte
    - Ja, av og til
    - Nei, sjelden
    - Nei, aldri

10. I hvilken grad synes du det er greit at dine data samles inn for å **tilpasse tjenester, forbedre funksjonalitet, og skreddersy innhold** til deg og dine antatte behov?
    - 1 I svært liten grad
    - 2
    - 3
    - 4
    - 5 I svært stor grad
    - Usikker / vet ikke

11. I hvilken grad synes du det er greit at dine data samles inn for å **for å skreddersy og målrette markedsføring** til deg og dine antatte behov – og dermed gjøre tjenester gratis?
    - 1 I svært liten grad
    - 2
    - 3
    - 4
    - 5 I svært stor grad
    - Usikker / vet ikke

12. Personlig og målrettet markedsføring har også fått betegnelsen **«overvåkingsbasert markedsføring».** I hvilken grad føler du at dette stemmer med din opplevelse?
    - 1 I svært liten grad
    - 2
    - 3
    - 4
    - 5 I svært stor grad
    - Usikker / vet ikke

13. Det finnes mange forskjellige **typer personopplysninger / personlige data**. I hvor stod grad mener du å ha **oversikt over hva som utgjør dine personlige data**?
    - 1 I svært liten grad
    - 2
    - 3
    - 4
    - 5 I svært stor grad
    - Usikker / vet ikke

14. I hvor stod grad mener du å ha **kontroll over dine egne data og hva de brukes til** på internett?
    - 1 I svært liten grad
    - 2
    - 3
    - 4
    - 5 I svært stor grad
    - Usikker / vet ikke

15. Har du selv opplevd **negative konsekvenser** ved at data eller informasjon om deg har blitt brukt uten ditt samtykke, eller har kommet på avveie?
    - Ja
    - Nei
    - Vet ikke

16. For å samle inn data fra forbrukere benyttes forskjellige sporingsteknikker, f.eks. cookies i nettleseren, apper på smarttelefonen eller innhenting av informasjon vi deler om oss selv. **Reflekterer du over at du blir sporet** av de fleste nettsteder når du er på internett?
    - Ja, ofte
    - Ja, av og til
    - Nei, sjelden
    - Nei, aldri

17. I hvor stor grad gir det å bli **sporet** når du driver med nettbasert aktivitet deg en følelse av å bli **'forfulgt' eller 'overvåket'**?
    - 1 I svært liten grad
    - 2
    - 3
    - 4
    - 5 I svært stor grad
    - Usikker / vet ikke

18. Hva gjør du vanligvis når du går inn på en nettside og en cookie-forespørsel dukker opp?
    - Trykker «godta alle cookies»
    - «Godtar kun nødvendige» eller prøver å avhuke alle cookies jeg kan
    - Benytter alternativer for å ikke blir sporet, som Incognito-modus, krypterte søketjenester som DuckDuckGo, VPN eller andre metoder

19. Synes du at det er vanskelig å finne og velge alternativer som **i liten grad innebærer sporing** av din aktivitet på nett?
    - Ja
    - Nei
    - Usikker / vet ikke

20. Hva **tenker du om å bli sporet** på denne måten, der hensikten er å samle inn data om deg og dine hverdagslige handlinger?
    - Greit, har ikke noe spesielt å skjule
    - Greit, sporing er nødvendig for å gi nettstedene data til statistikk, tjenesteutvikling og personrettet informasjon
    - Ikke helt greit, men jeg aksepterer at dette er normalen i en datadrevet verden og at alternativene er få
    - Ikke greit, men jeg gjør ikke noe spesielt med det
    - Ikke greit, jeg prøver som oftest å unngå å bli sporet

21. Mye av grunnen til at du spores og persondata samles inn er for å kunne skreddersy innhold og tjenester og målrette disse direkte til den enkelte forbruker.

    Hvor enig eller uenig er du i følgende påstander?
    CARUSEL GRID (TEXT AT END: Klikk på neste-knappen for å gå videre)
    RANDOMIZE
    - Jeg foretrekker **personlig tilpasset innhold og tjenester** heller enn mer **generelt innhold og tjenester**.
    - Jeg foretrekker **personlig tilpasset markedsføring** heller enn **generell markedsføring**.
    - Det er greit at mine data benyttes slik at algoritmene kan foreslå serier, musikk, nyheter og sosiale medier-innlegg som jeg har vist interesse for tidligere.
    - Det er problematisk at mine data benyttes dersom algoritmene snevrer inn forslagene og gir meg for lite variasjon i serier, musikk, nyheter og sosiale medier-innlegg
    - Det er problematisk at mine data benyttes fordi jeg kan bli tolket feil, satt i en bås der jeg ikke føler meg hjemme i, og som det er vanskelig å komme ut av
    - Det er problematisk at mine data benyttes fordi algoritmene kan trekke meg mot stadig mer ekstremt innhold, og jeg kan havne i ekkokammer der f.eks. konspirasjonsteorier florerer.
    - Jeg er redd for at store digitale selskaper etter hvert vet så mye om meg at jeg kan bli manipulert eller diskriminert mot uten å vite det.

    Scale:
    - 1 Helt uenig
    - 2
    - 3
    - 4
    - 5 Helt enig
    - Usikker / vet ikke

22. Hvor enig eller uenig er du i følgende utsagn?
    CARUSEL GRID (TEXT AT END: Klikk på neste-knappen for å gå videre)
    RANDOMIZE
    - Jeg føler at personvernet mitt i stor grad er «dødt» fordi det ligger så mye data og informasjon om meg ute på nettet, hos offentlige og private selskaper, og i sosiale medier og på andre digitale plattformer.
    - Mindre personvern er noe vi må regne med, fordi alle typer data, inkludert våre personlige data, er råvaren i en global datadrevet økonomi
    - Jeg er villig til å akseptere en del sporing av mine data for å bidra til å håndtere store samfunnsutfordringer innen helse, energi og miljø/klima
    - Jeg har tillit til at store selskaper som Facebook, Google, Amazon, Apple, etc. håndterer mine data på en forsvarlig måte og ikke utnytter eller misbruker informasjonen de sitter med.
    - Jeg har tillit til at norske myndigheter som tilbyr offentlige tjenester håndterer mine data på en forsvarlig måte og ikke utnytter eller misbruker informasjonen de sitter med.
    - Krigen i Europa gjort meg mer bekymret for mine digitale data, personlig overvåking, og digital sikkerhet.
    - Jeg har tillit til at regulerende myndigheter og tilsyn i Norge beskytter meg i den datadrevne eller overvåkingsbaserte økonomien
    - Jeg har oversikt over hvilke lover og regler som finnes for å beskytte meg mot omfattende kommersiell overvåking og misbruk i digitale markeder.

    Scale:
    - 1 Helt uenig
    - 2
    - 3
    - 4
    - 5 Helt enig
    - Usikker / vet ikke

Forbruksforskningsinstituttet SIFO ved OsloMet – storbyuniversitetet har et spesielt ansvar for å bidra til kunnskapsgrunnlaget for forbrukerpolitikken i Norge og skal utvikle ny kunnskap om forbruk, forbrukerpolitikk og forbrukernes stilling og rolle i samfunnet.

SIFOs kjerneområder er:

- Bærekraftig forbruksutvikling
- Klær
- Markedsbasert velferd
- Teknologi og digitalisering
- Mat, matkultur og ernæring

Forbruksforskningsinstituttet SIFO,
OsloMet ISBN: 978-82-7063-546-7
www.oslomet.no/om/sifo