Bacheloroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Det humanistiske fakultet
Institutt for kunst- og medievitenskap

Benedikte Aune Olsen

Personvern på lokasjonsbaserte tjenester i dagens overvåkingssamfunn

Bacheloroppgave i Medievitenskap
Veileder: Gunn R. Bekken
Mai 2020

NTNU
Kunnskap for en bedre verden

Benedikte Aune Olsen

Personvern på lokasjonsbaserte tjenester i dagens overvåkingssamfunn

Bacheloroppgave i Medievitenskap
Veileder: Gunn R. Bekken
Mai 2020

Norges teknisk-naturvitenskapelige universitet
Det humanistiske fakultet
Institutt for kunst- og medievitenskap

NTNU
Kunnskap for en bedre verden

Innholdsfortegnelse

Sammendrag

I denne oppgaven har jeg undersøkt om den konstante overvåkingen vi står overfor i dagens samfunn skaper bekymringer hos brukerne av lokasjonsbaserte tjenester, og på hvilke områder. Formålet med oppgaven var å få en bredere forståelse av dagens overvåkingskultur, og om de bekymringene som dannes av brukerne resulterer i en endring av bruken av lokasjonsbaserte tjenester eller ikke. Oppgaven har analysert funn fra Teknologirådets rapport fra 2004 som tar for seg holdninger knyttet til elektroniske spor og personvern. Problemstillingen er diskutert med utgangspunkt i begrepene personvern, overvåking som makt og kontroll og flytende overvåking, i tillegg til at sentrale teorier som panoptikonprinsippet, frivillig panoptikon og personvernsparadokset har hatt stor innvirkning på diskusjonen. For å diskutere problemstillingen ble overvåkingssamfunnet gjort rede for og diskutert opp mot de bekymringer som brukerne har uttrykt når det kommer til bruken av lokasjonsbaserte tjenester, før det til slutt ble satt lys på om bruken av disse tjenestene har endret seg eller om de har forblitt de samme til tross for disse bekymringene. Oppgaven ble konkludert med at bruken av lokasjonsbaserte tjenester har forblitt de samme til tross for de bekymringer som har oppstått. Det viser seg at selv om brukerne i lys av de uttrykte bekymringene ønsker å endre bruken for å kunne opprettholde personvernet, men i praksis veier tjenestenes muligheter opp for de eventuelle konsekvensene knyttet til personvernet, og dermed endres ikke bruken av lokasjonsbaserte tjenester.

Abstract

In this paper I have investigated whether the constant surveillance we face in today's society is causing concerns for users of location-based services, and in what areas. The purpose of this assignment was to gain a broader understanding of today's surveillance culture, and whether or not the concerns raised by users result in changed use of location-based services. The thesis has analyzed findings from the Technology Councils report from 2004 that address attitudes related to electronic tracks and privacy. The issue is discussed based on the concepts of privacy, surveillance as power and control and liquid surveillance, as well as key theories such as the panopticon principle, voluntary panopticon and the privacy paradox have had a major impact on the discussion. To discuss the issue, the surveillance community was accounted for and discussed against the concerns expressed by users when it comes to using location-based services, before finally exploring whether the use of these services has changed or whether they have remained the same despite these concerns. The thesis concluded that the use of location-based services has remained the same despite the concerns that have arisen. It turns out that, in light of the concerns expressed, users want to change usage to maintain privacy, but in practice, the services capabilities outweigh the potential consequences associated with privacy, and thus the use of location-based services does not change.

1 Innledning

I løpet av de siste årene har samfunnet endret seg radikalt. Vi har vært vitne til en teknologisk utvikling vi aldri har sett maken til og som i stor grad har påvirket måten vi lever på. Dagens teknologiske utvikling fører til økt innsamling, lagring og sammenkobling av informasjon av samfunnet (NOU 2009:1, s.11). Teknologien blir stadig smartere og hjelper oss med mer og mer. Samtidig kommer den nærmere inn i livene våre, og den lærer seg å kjenne våre vaner, ønsker og følelser (Teknologirådet, 2020). De teknologiske enhetene og systemene er designet til å følge med, spore handlinger eller rett og slett bare være oppmerksomme på hvor vi befinner oss til enhver tid (Nissenbaum, 2010, s.21). Slike teknologiske enheter kan vi definere som lokasjonsbaserte teknologier, altså mobile enheter som gjennom GPS, Wi-Fi eller triangulering av radiobølger som kan lokalisere seg selv og dermed gi brukeren stedsspesifikk informasjon (de Souza e Silva & Frith, 2012, s.6). Den lokasjonsbaserte mobile enheten vi kjenner best til i dag er smarttelefonen, og vi kan på mange måter hevde at dette er vår beste kilde til lokasjonsbaserte tjenester. Den hyppige bruken av smarttelefonen gir muligheter for at nye typer data, som sporing, skal kunne bli samlet inn. Ifølge Marianne Barland har brukerens posisjon blitt særlig viktig å følge med på, og dermed får mange tjenester nå innarbeidet funksjonalitet som drar nytte av vår bruk av smarttelefonen (Barland, 2016). Dermed ser vi at kombinasjonen av brukerens konstante bruk av smarttelefonen og populariseringen av lokasjonsbaserte tjenester åpner opp for nye former for overvåking i dagens samfunn.

Overvåkning som fenomen er ikke noe nytt som har oppstått de siste årene, men noe vi kan spore tilbake til bibelske referanser (Bauman & Lyon, 2013, s.100). Gjennom bibelen blir det skildret at Gud skal passe på alle, men det innebærer også at Gud ser deg til enhver tid. Selv om utøvelsen av overvåkning har endret seg siden den gang, kan vi fortsatt se likheter mellom bibelens skildringer og vårt samfunn i dag. Overvåking blir oftest assosiert med sikkerhet, og et ønske om å opprettholde dette. I dag er sikkerhet en viktig prioritering i og på tvers av mange land, og selvfølgelig en massiv motivator i overvåkningsverden. Det virker som om de framtredende virkemidlene for å skaffe sikkerhet er nye overvåkningsteknikker og teknologier. Dermed kan vi hevde at ting har endret seg den siste tiden, både for de som blir sett på og de som ser (Bauman & Lyon, 2013, s.100-101).

Nyutviklingen av overvåkning kan på mange måter sammenlignes med det den kanadiske medieforskeren David Lyon omtaler som flytende overvåkning, hvor overvåkingsenhetene har blitt såpass modernisert at de virker «usynlige» og at brukeren derfor ikke legger merke til innsamlingen av informasjon, og utøver dermed ingen motstand (Bauman og Lyon, 2013, s.2). Den amerikanske sosiologen Gary Marx har uttrykt stor bekymring når det kommer til konsekvenser knyttet til den teknologiske endringen i overvåkingsfeltet, og hevder dermed at eldre former for regulering sårt trenger en oppdatering (Bauman & Lyon, 2013, s.132). Ut i fra Helen Nissenbaum kan vi forstå at personvernet som en reguleringsform sårt trenger en oppdatering da bekymringene rundt personvern har blitt multiplisert siden 1960-tallet både i type og omfang. Teknologien har siden 1960-tallet gjennomgått radikale transformasjoner for å bli de systemene som vi kjenner til i dag (Nissenbaum, 2010, s.1). Adriana de Souza e Silva og Mimi Sheller hevder at engasjementet rundt lokasjonsbaserte tjenester ofte resulterer i implikasjoner for vår følelse av personvern (de Souza e Silva & Sheller, 2015, s.5).

Lokasjonsbaserte tjenester vekker større bekymring når det kommer til personvern og makt i det offentlige rom enn noen andre typer mobile teknologier (de Souza e Silva & Frith, 2012, s.11). Dette er trolig på grunn av at det gjennom lokasjonsbaserte tjenester

er enklere enn noensinne for vanlige brukere å finne informasjon om andre mennesker knyttet til lokasjon, bilder, videoer og statusoppdateringer. Gjennom de mulighetene lokasjonsbaserte tjenester tilbyr vil det være viktig å forsikre seg om at personvernet klarer å holde tritt. Adriana de Souza e Silva og Jordan Frith hevder at gjennom veksten av teknologiske tjenester blir personvernet stadig viktigere å beskytte, da det siden oppfinnelsen av World Wide Web har skjedd en eksepsjonell økning i mengden informasjon registrert om oss (de Souza e Silva og Frith, 2012, s.113). Lokasjonsbaserte tjenester presenterer en ny kontekst for informasjonsdeling som brukere av sosiale medier ikke har måtte takle tidligere (de Souza e Silva & Frith, 2012, s.114). Gjennom bruken av lokasjonsbaserte tjenester legger vi som brukere igjen mange digitale spor, og vi har ikke nødvendigvis oversikt over hvem som vet hva om oss (Teknologirådet & Datatilsynet, 2018, s.35). Tenker vi over hvor det blir av de store mengdene med informasjon som vi gjennom disse tjenestene gir fra oss hver dag, og hvem som har tilgang til denne informasjonen? (Overland, 2018).

1.1 Motivasjon for oppgaven

Vi står i dagens samfunn overfor en form for allestedsnærværende overvåking som vi ikke kommer foruten, samtidig har også brukeren selv blitt tildelt en rekke flere muligheter enn tidligere når det kommer til å ta del i denne overvåkingen. Brukerne kan dermed overvåke hverandre slik kun bedrifter og statlige institusjoner tidligere gjorde. Jeg ønsker med denne oppgaven å undersøke om denne konstante og brukertilgjengelige overvåkingsformen skaper bekymringer hos brukere av lokasjonsbaserte tjenester i dag når det kommer til overvåking og personvern, og om bruken av disse tjenestene kan sies å ha endret seg. Ser vi en endring i bruken av lokasjonsbaserte tjenester eller er bruken den samme til tross for disse bekymringene?

1.2 Problemstilling og oppgavens struktur

På bakgrunn av motivasjonen for denne oppgaven har jeg formulert følgende problemstilling; *Hvilke bekymringer knyttet til personvern og overvåkning oppstår i dagens samfunn omringet av allestedsnærværende overvåking? Spiller disse bekymringene noen rolle når det kommer til bruken av lokasjonsbaserte tjenester?*

Jeg vil basere denne oppgaven på teori knyttet til personvern, overvåkning som makt og kontroll og flytende overvåkning. Disse teoriene ser jeg på som relevante i denne konteksten da det er innenfor disse lokasjonsbaserte tjenester kan sies å skape bekymringer blant brukerne. Som skrevet innledningsvis utgjør lokasjonsbaserte tjenester en bekymring innenfor personvern, men disse tjenestene kan også forsterke eller omforme maktforhold blant brukerne. Det vil dermed også være relevant å se på lokasjonsbaserte tjenester i lys av overvåkning som makt og kontroll, hvor jeg blant annet vil trekke inn panoptikonprinsippet da prinsippet blir sett på som en metafor for det moderne overvåkingssamfunnet vi står overfor i dagens samfunn.

For å være i stand til å undersøke omkring folks bekymringer og holdninger til dagens lokasjonsbaserte tjenester har jeg valgt å benytte meg av Teknologirådets rapport fra 2004 som omhandler holdninger knyttet til elektroniske spor og personvern. Dette mener jeg vil legge et godt grunnlag for videre diskusjon og analyse rundt brukernes bekymringer knyttet til overvåkning og personvern på lokasjonsbaserte tjenester. Har disse bekymringene resultert i at bruken av lokasjonsbaserte tjenester har endret seg eller har den forblitt den samme til tross for disse bekymringene?

2 Teori

Det er noen faktorer jeg anser som viktige for å forstå bekymringene knyttet til dagens overvåkingssamfunn. Disse synspunktene er i høy grad relevant for å få en bredere forståelse for temaet og for å kunne besvare problemstillingen. Dermed har jeg tenkt å starte med å gjøre rede for begrepet personvern, før jeg skal se på overvåking som makt og kontroll i lys av panoptikonprinsippet, før jeg til slutt vil ta for meg begrepet flytende overvåking.

2.1 Personvern

Personvern som et allment begrep ble først tatt i bruk i Norge i første halvdel av 1970-tallet og avløste det som tidligere ble omtalt som personlighetsvern (Hannemyr, Liestøl, Lüders & Rasmussen, 2015, s.110). Ifølge Helen Nissenbaum er personvern et rotete og komplekst emne å studere, hvor det ikke finnes en enkel begrepsdefinisjon (Nissenbaum, 2010, s.67). Det vi derimot kan hevde er at det finnes to tilnærminger når det kommer til å definere begrepet personvern, hvor den ene karakteriserer personvern som en begrensning av tilgang, mens den andre karakteriserer personvern som en form for kontroll (Nissenbaum, 2010, s.69-70). Innenfor denne konteksten vil jeg ta for meg den tilnærmingen som karakteriserer personvern som en form for kontroll. Jordan Frith hevder at man gjennom personvernet ønsker å kunne kontrollere hvem som får tilgang til informasjonen deres og hvor langt informasjonen om dem reiser (Frith, 2015, s.112). Personvern er ikke en statisk konstruksjon. Det er ikke en iboende egenskap til spesiell informasjon eller innstilling. Det er en prosess der mennesker søker å ha kontroll over en sosial situasjon ved å håndtere inntrykk, informasjonsstrømmer og kontekst (Boyd, 2014, s.76).

2.1.1 Lokasjonsbasert personvern

Bruken av lokasjonsbaserte mobile teknologier kan signalisere en endring i vår forståelse av personvern. I forbindelse med lokasjonsbaserte tjenester er personvernspørsmål nært knyttet til ideer om kontroll. Betydningen av lokasjonsbasert personvern påvirkes direkte av muligheten til å kontrollere lokasjonsinformasjonen vår (de Souza e Silva & Frith, 2012, s.113). Vi lever i en verden hvor smarttelefoner med innebygd GPS er en stor del av hverdagen vår, noe som gir enorme muligheter for overvåkning gjennom mobiltelefonen. Selv om folk ikke blir aktivt overvåket, påvirkes personvernet fortsatt av den enorme innsamlingen av informasjon fordi de ikke kan finne ut hvilken informasjon forskjellige enheter har. Selv når lokasjonsdata brukes til det sosialt beste, som for eksempel til å forbedre trafikkstrømmen eller å spore sykdommer, bør folk gjøres oppmerksomme på hvem som har tilgang til dataene dine og hvordan de blir analysert (Frith, 2015, s.122). Lokasjonsbasert personvern kan deles inn i to ulike grupper; institusjonelt og sosialt. Forskjellen ligger i den at institusjoners evne til å samle inn og lagre brukerinformasjon er annerledes enn når det er brukerne selv som samler inn informasjon om hverandre gjennom sosiale medier (Frith, 2015, s.113). Jeg har spesifikt valgt å kun ta for meg sosialt lokasjonsbasert personvern da det ses på som mest relevant i denne konteksten hvor det er brukerbasert overvåking som skal gjøres rede for og drøftes rundt. Det er også her store deler av bekymringene som dannes rundt bruken av lokasjonsbaserte tjenester stammer fra.

2.1.2 Sosialt lokasjonsbasert personvern

Denne sosiale formen for personvern referer til at det er brukerne selv som bevisst har kontroll over andre brukeres lokasjon. Dermed skiller den seg fra institusjonelt personvern

da overvåkingen foregår horisontalt snarere enn vertikalt og sentrerer seg rundt andre mennesker i stedet for institusjoner (de Souza e Silva & Frith, 2012, s.125). Sosialt lokasjonsbasert personvern bør betraktes som en forhandling om ulike sosiale sammenhenger. På visse tidspunkter, i visse situasjoner, kan det være lurt å dele sin beliggenhet med medlemmer av et sosialt nettverk. Det betyr ikke at de vil at alle skal vite hvor de befinner seg, og det betyr heller ikke at de ikke bryr seg om deres lokasjonsbaserte personvern. Å legge til lokasjon i sosiale nettverk betyr at folk må navigere i et endret informasjonslandskap. De må utvikle måter å dele stedsinformasjon samtidig som at de opprettholder en følelse av privatliv, akkurat som de utvikler taktikker for å dele andre typer informasjon på sosiale nettsteder (Frith, 2015, s.123).

2.2 Personlig informasjon

Begrepet personlig informasjon blir definert som informasjon om en identifiserbar person, altså alt av informasjon som kan identifiseres til en bestemt person, både direkte og indirekte. Dette kan både være ved henvisning til et identifikasjonsnummer eller til en eller flere faktorer som er spesifikke for vår fysiske, fysiologiske, mentale, økonomiske, kulturelle eller sosiale identitet. Personlig informasjon kan altså være bilder, video, meldinger, bankkortopplysninger, passord, lokasjonshistorikk og lignende (Nissenbaum, 2010, s.4).

2.3 Overvåking som makt og kontroll

David Lyon definerer overvåking som all innsamling eller behandling av personopplysninger, uansett om de kan identifiseres eller ikke, med det formål om å påvirke eller administrere dem som det blir samlet inn informasjon om (Lyon, 2001, s.2). Humphreys hevder at i henhold til definisjonen av overvåking er makt eller innflytelse sentral. En del av overvåkingsmakten er at personer hvor personopplysninger blir samlet inn eller observert ikke vet når eller om de blir overvåket (Humphreys, 2014, s.110).

Forståelsen om overvåkning som en form for makt og kontroll handler om at jo mer informasjon en part får kontroll over, jo mer makt får de. Dersom vi ser på personvern ut fra et makt- og kontrollperspektiv blir det ofte snakket om at personvern er noe som man kan miste kontroll over (Boyd, 2014, s.60). Det er ikke noe nytt å se på personvern gjennom et makt- og kontrollperspektiv, da dette er noe som har eksistert over lengre tid og som vi kan se tilbake på. Michel Foucault tar i bruk panoptikonprinsippet i det han beskriver overvåkning som et maktforhold der overvåkeren har makt over den som blir overvåket (Foucault, 1977, s.203).

2.3.1 Panoptikonprinsippet

Jeremy Bentham designet på slutten av 1700-tallet et fengselssystem hvor vokteren hadde mulighet til å se alle fangene i cellene deres fra et vakttårn, mens fangene verken kunne se vokteren eller vite om han så på dem (Bentham, 2018). Fangen er sett, men han ser det ikke. Han er objekt for informasjon, men aldri subjekt for kommunikasjon. Ved at rommet vender ut mot vakttårnet, tvinges han til å være synlig langs en akse. Men bygningskjedens inndelinger, disse klart adskilte cellene, impliserer at han ikke kan ses fra siden, og denne usynligheten garanterer at det hersker orden. Slik oppnås den panoptiske hovedvirkning: At den innsatte stadig skal være og vite seg synbar – for dermed fungerer makten automatisk (Foucault, 1977, s.180). Dersom fangene hadde en overhengende følelse av å alltid bli overvåket, mente Bentham at fangene ville internalisere denne frykten

for å bli tatt i å gjøre noe ulovlig, og derfor vokte seg selv for å unngå straff (Bentham, 2018).

Foucault brukte panoptikon som en maktmekanisme og en metafor for det moderne overvåkingssamfunnet. Foucault argumenterer for at Benthams prinsipper er videreført i datidens samfunn som følge av kulturelle skifter og teknologiske fremskritt. Ifølge Mathiesen fungerer samfunnets disiplinering gjennom trusselen om overvåkning på samme måte for samfunnsmedlemmene som for fangene (Mathiesen, 1997, s.218). Foucaults teori om panoptikon har blitt mye brukt i samfunnskritikk mot en økende grad av overvåkning, og blitt bygd videre på i andre teorier. Overvåkningskameraer, mobiltelefoner og internett har blitt kommentert som panoptiske elementer da de alle har potensiale til å «avsløre» oppførsel som ikke samsvarer med samfunnets lover (Bauman & Lyon, 2013).

2.3.2 Lateral panoptikon

Den australske medieprofessoren Mark Andrejevic tar i bruk begrepet *lateral panoptikon* for å få en bedre forståelse på panoptiske prosesser i dagens mediesamfunn. Han mener at alle overvåker alle i form av rapporteringsfunksjoner, og at sosiale medier gjør oss alle til spioner (Andrejevic, 2006, s.392). Teorien omfatter hvordan mennesker spionerer på andre mennesker i hverdagen, og at de bruker ulike former for overvåkning til å observere sine venner, familiemedlemmer og kjærester. Andrejevic mener dette fører til en normalisering av hverdagslig overvåkning, og fremhever hvordan dette tilrettelegger for folk som ønsker å finne informasjon om andre (Andrejevic, 2004, s.488-489).

2.4 Flytende overvåkning

Flytende overvåkning er mindre en komplett måte å spesifisere overvåkning og mer en orientering, en måte å lokalisere overvåkningsutviklingen i den flytende og urolige moderniteten i dag (Bauman & Lyon, 2013, s. 2). David Lyons teori om flytende overvåkning handler om hvordan systemer med potensiale for overvåkning fungerer autonomt i samfunnet. Han hevder at informasjonsutveksling av brukeres personlige informasjon er såpass innvevd og dagligdags gjennom ulike digitale systemer som også samhandler med hverandre: transaksjoner mellom butikker og banker, informasjonsutveksling mellom arbeidsgiveren og skatteetaten og internettleverandørens tilrettelegging av nettjenester for å nevne noen. Alle disse systemene trekker ut en viss mengde av informasjonen til sine brukere for å fungere. Slike prosesser fungerer autonomt og «usynlig» for brukerne av dem. Lyon hevder at jo mer usynlig denne flytende overvåkningen er, jo lettere er det for brukeren å «glemme den», å ikke tenke over den (Bauman & Lyon, 2013). Adriana de Souza e Silva og Jordan Frith hevder at gjennom å ta i bruk GPS-teknologi blir overvåkningen mindre åpenbar og mer konstant (de Souza e Silva & Frith, 2012, s.12).

3 Empiri

Jeg har nå tatt for meg teori knyttet til personvern, overvåkning som makt og kontroll og flytende overvåkning. Videre skal jeg se på innsamlingen av det empiriske datamaterialet. Datamaterialet jeg skal presentere er basert på rapporten til Teknologirådet som tar for seg holdninger knyttet til elektroniske spor og personvern.

3.1 Teknologirådets rapport om elektroniske spor og personvern

Teknologirådet har som oppgave å følge den teknologiske utviklingen og stimulere til debatt om de muligheter og konsekvenser som ny teknologi skaper for samfunnet og det enkelte individ (Teknologirådet, 2004, s.3). Med bakgrunn i de senere års kraftige økning i bruken av informasjons-og kommunikasjonsteknologier (IKT) har Teknologirådet gjennomført intervjuer av fokusgrupper for å få et inntrykk av hvordan lekfolk (ikke-eksperter) ser på personvernkonsekvenser knyttet til bruk av slik teknologi (Teknologirådet, 2004, s.5).

Rapporten tar opp ulike arenaer hvor man kan legge fra seg elektroniske spor og hvor personvernet kan spille en viktig rolle, og ser på hva de ulike fokusgruppene legger vekt på når det kommer til bruken av disse. Teknologirådet var spesielt interessert i brukernes tanker omkring elektroniske spor og personvern (Teknologirådet, 2004, s.4). Deltakerne til fokusgruppene kom fra Oslo og Bodø. Fire grupper bestod av ungdom mellom 17 og 19 år, og to grupper var med voksne i alderen 30-40 år. Temaer som ble diskutert var brukervaner knyttet til informasjons- og kommunikasjonsteknologier, samt holdninger til personvern og bevissthet omkring elektroniske spor og deres konsekvenser (Teknologirådet, 2004, s.5).

Noe av det Teknologirådet ønsket å vite var om deltakerne hadde gjort seg opp noen tanker når det kom til elektroniske spor på nett, altså spor som kan inneholde opplysninger om hva man har gjort, hvor man har vært og til hvilken tid. Blant deltakerne var de voksne mer bekymret for elektroniske spor enn de unge. De unge deltakerne var avslappet til igjenleggelse av elektroniske spor. Men under diskusjonen ble også de unge deltakerne mer bekymret enn det de opprinnelig var i utgangspunktet. De voksne understreket av det var ubehagelig at man la igjen elektronisk informasjon om seg selv, og at man i liten grad hadde kontroll over det på grunn av teknologiens egenskaper som gjør det vanskelig for brukeren å ha kontroll over hvor ens egne elektroniske spor havner og hvem som har tilgang til dem (Teknologirådet, 2004, s.14).

Et annet tema som ble tatt opp under intervjuet var mobiltelefon og lokasjonsbaserte tjenester. Digitalisering av data har gjort det enklere å samle og oppbevare opplysninger fordi mobiltelefonen avgir posisjonsopplysninger og gir mulighet til å spore bruker geografisk. Økt bruk av GPS-systemet kan gi nøyaktige lokaliseringsmuligheter av brukeren, og dermed gi oversikt over hvor mobilbrukere til enhver tid befinner seg. Deltakerne var enige i at det var ubehagelig at det innebar at noen ville ha oversikt over hvor de befant seg til enhver tid. Mobilen oppfattes på mange måter som en del av den private sfære og det kan dermed føles ekstra ubehagelig at andre har oversikt over hvor man befinner seg (Teknologirådet, 2004, s.18-19).

4 Diskusjon

I denne delen av oppgaven skal jeg sette oppgavens empiriske materiale opp mot det teoretiske grunnlaget som ble lagt tidligere i oppgaven. Videre skal jeg diskutere rundt bekymringene som oppstår blant brukerne når det kommer til overvåking og personvern på lokasjonsbaserte tjenester, og om disse bekymringene har noe å si for bruken av disse tjenestene.

4.1 Nye overvåkningsformer og bekymringer knyttet til disse

Dagens tilbud av teknologiske systemer muliggjør en overvåkingsform som blir integrert inn i livene våre, denne overvåkingsformen kaller David Lyon for flytende overvåking. Denne flytende formen for overvåking resulterer i at overvåkingen nærmest blir usynlig for brukeren og siden vi ikke blir gjort bevisst på at overvåkingen finner sted kan vi ikke utøve noen form for motstand mot den. Overvåkingen blir flytende i den forstand at tilstedeværelsen av overvåkingsenheten ikke kan skilles fra den originale teknologiske enheten som den er plassert i (Lyon, 2014, s.76). Dermed føler vi ikke at denne formen for overvåking blir for påtrengende, da overvåkingen skjer gjennom teknologiske enheter som vi allerede ser på som hverdagslige og som vi tar i bruk på en daglig basis (Zurawski, 2014, s.33). Smarttelefonen kan ses på som en slik hverdagslig enhet som gjør overvåking av brukeren mulig uten å virke for påtrengende. De fleste av oss går rundt med avanserte datamaskiner i form av en mobiltelefon i lommen, det er noe vi har på oss og omgir oss med konstant uten at vi tenker noe over det (Hannemyr et al., 2015, s.201). Gjennom bruken av smarttelefonen trenger vi ikke lengre å koble oss opp på internettet da vi konstant har den på og med oss (de Souza e Silva & Sheller, 2015, s.4). Internett blir gjennom smarttelefonen forvandlet til en konstant følgesvenn for gjennomsnittsforbrukeren og dermed blir overvåkingen nesten uunngåelig for brukeren (Zurawski, 2014, s.32).

Selv om bruken av smarttelefonen i dagens samfunn blir sett på som hverdagslig, er det likevel enkelte som har uttrykt bekymring knyttet til bruken av smarttelefonen som en enhet som muliggjør overvåking. Dette kommer frem gjennom rapporten som Teknologirådet ga ut i 2004. I rapporten kommer det frem at de unge deltakerne vanligvis har en avslappet holdning til overvåkingen som skjer gjennom smarttelefonen, men under diskusjonen snus dette og deltakerne blir mer og mer bekymret enn det de opprinnelig var. De voksne derimot understreket at de synes det skapte et ubehag fra første stund, da man i liten grad har kontroll over overvåkingen som finner sted på grunn av teknologiens egenskaper som usynliggjør overvåkingen for brukeren (Teknologirådet, 2004, s.14). Resultatene av undersøkelsen til Teknologirådet viser at den flytende formen for overvåking skaper bekymringer hos brukerne. Vi vet ikke hvem som overvåker, hvordan de gjør det, hvilken informasjon de tar eller hvordan de bruker den (Berg & Lysgård, 2019). Vi mister kontrollen over hvilken informasjon som blir lagret gjennom bruken av smarttelefonen. Den flytende overvåkingen resulterer i at brukeren blir mindre oppmerksom på at overvåkingen finner sted, og brukeren får dermed lite kontroll over hvilken informasjon som blir samlet inn om den, og hvem som får tilgang til denne informasjonen.

Adriana de Souza e Silva og Jordan Frith skriver om personvern i deres bok *Mobile Interfaces in Public Spaces,* og at forventningene knyttet til personvern handler om kontroll, og da ofte om kontroll over hvilken personlig informasjon man deler med de teknologiske tjenestene. Dersom brukeren mister kontrollen over hvilken informasjon man har delt med tjenesten vil man føle på at personvernet har blitt svekket og kan ofte skape en frykt hos brukeren for hva annet tjenestene kan «stjele» av informasjon om brukeren (de Souza e Silva & Frith, 2012, s.120). Frith understreker at vi som brukere ønsker å kunne kontrollere hvem som får tilgang til informasjonen vår og hvor langt informasjonen reiser (Frith, 2015, s.112). Brukeren ønsker å ha kontroll over hvilken informasjon som innhentes av de lokasjonsbaserte tjenestene og at informasjonen som blir hentet kun blir brukt til det som var tiltenkt. Dermed kan personvernet bli utfordret gjennom lokasjonsbaserte tjenester i den grad at det ikke finnes noen garanti for at brukeren kan

kontrollere hvilken personlig informasjon som deles med tjenestene. Det gis heller ingen garanti for at informasjonen kun blir brukt til det som først var tiltenkt. Dermed skapes det store bekymringer hos brukerne gjennom denne flytende formen for overvåking, men kan vi i lys av disse bekymringene se en endring i bruken av tjenester som tilbyr denne flytende overvåkingen?

4.2 Ny overvåkingskultur

Vi kan ikke komme utenom overvåking i dagens moderne samfunn, det er noe vi må lære oss å leve med og dermed har også aksepten for å bli overvåket måttet endre seg de siste årene. Der hvor vi tidligere ønsket å unngå alt som hadde med overvåking å gjøre er ikke mulig i dag. Nå er det i luften vi puster, bygningene der vi jobber, gatene vi går i, butikkene hvor vi handler, bilene vi kjører, telefonene vi bruker for å holde kontakten med hverandre og selvfølgelig i sosiale medier (Lyon, 2014, s.73). Vi lever i en tid hvor vi til enhver tid omringes av teknologier som muliggjør overvåking, dermed må hver enkelt av oss lære at overvåking ikke er noe som er mulig å unngå. På bakgrunn av dette har det oppstått en normalisering blant folket når det kommer til overvåking i samfunnet vårt da det ikke finnes noen mulighet til å komme foruten det (Rettberg, 2014, s.80). Noe som også har endret seg de siste årene er at overvåking ikke lengre er noe som kun kan utøves av politi og andre styremakter, men er noe alle kan ta del i og utføre på hverandre. Gjennom bruken av internett og lokasjonsbaserte tjenester har vanlige mennesker nå lignende teknologiske evner til å drive med overvåking av hverandre, noe som tidligere ble holdt eksklusive for bedrifter og statlige enheter. Nå kan innbyggerne selv overvåke hverandre, og søke etter informasjon om andre borgere uten deres viten eller tillatelse (Humphreys, 2014, s.111). Mark Andrejevic hevder at dagens bruk av sosiale medier har gjort mennesker til hverdagsspioner. Vi tar i bruk overvåkingsenheter for å spionere på og å holde et øye med venner, familiemedlemmer eller kjæreste (Andrejevic, 2006, s.392). Dagens tilbud av lokasjonsbaserte tjenester tilbyr oss brukere et bredt spekter av muligheter når det kommer til å holde et øye med våre sosiale nettverk og kan, dersom vi ønsker det, få vite hvor venner og familie befinner seg til enhver tid. Eksempler på dette fra dagens mye brukte tjenester kan være den innebygde kartapplikasjonen til Snapchat, «Snapmap», og Apple sin «Find My».

William G. Staples diskuterer i sitt arbeid med sosial kontroll og overvåking hvordan overvåking i dagens samfunn har blitt allestedsnærværende, normalisert og akseptert. Han tar opp blant annet Reality-TV som for eksempel «Big Brother» og populariseringen av dette som gjør at vi kan se på overvåking som en form for underholdning. Vi omringes av sikkerhetskameraer på butikker og i gater og blir tilbudt spesialtilbud i bytte mot vår personlige informasjon på internettet (de Souza e Silva & Frith, 2012, s.119). Uten denne normaliseringen av overvåking ville vi ikke vært like aksepterende når det kommer til å la venner og selskaper få tilgang til informasjonen knyttet til egen lokasjon, hevder Adriana de Souza e Silva og Jordan Frith (de Souza e Silva & Frith, 2012, s.119).

4.3 Panoptikonprinsippet i dagens medier

Panoptikonprinsippet blir i lys av dagens overvåkingssamfunn ofte beskyldt for å være utdatert og lite relevant, til tross for dette kan vi fortsatt hevde at det fortsatt eksisterer likhetstrekk mellom Foucaults idé om panoptikon knyttet til overvåking og den overvåkingen vi står overfor i dagens samfunn. Zygmunt Bauman og David Lyon skriver i sin bok *Liquid Surveillance* at den gamle, panoptiske planen (du skal aldri vite når du blir sett på) enda konsekvent og tilsynelatende ustoppelig blir tatt i bruk gjennom dagens digitale medier (Bauman & Lyon, 2013, s.23). I vår tid har panoptikonprinsippet blitt

gjenfødt gjennom dagens bruk av sosiale medier og innhentingen av informasjon som muliggjøres gjennom dem (Hannemyr et al., 2015, s.155). Panoptikonprinsippet har gjennom dagens sosiale medier modernisert seg og gjennom smarttelefonen og sosiale medier har det oppstått nye panoptiske elementer som er blitt til det vi kan kalle for personlige panoptikoner. Gjennom disse personlige panoptikonene videreføres den originale ideen om å overvåke fangene individuelt og at «de få kan se de mange». Panoptikonprinsippet har dermed gått vekk fra overvåking gjennom et vakttårn til overvåking gjennom individuelle enheter som smarttelefonen.

Gjennom lokasjonsbaserte tjenester står vi overfor en overvåkingskultur som er lik den overvåkingen som var tiltenkt gjennom panoptikonprinsippet, altså «fangen er sett men ser ikke, man kan verken se vokteren eller vite om han ser på deg» (Bentham, 2018). Som brukere av lokasjonsbaserte tjenester er vi ikke blitt tildelt muligheten til å se hvem som overvåker oss og vet heller ikke om vi faktisk blir overvåket av andre. Likevel vet vi at muligheten er tilstede for at vi kan bli overvåket av andre. Foucault tar i bruk panoptikon som en maktmekanisme og mente at gjennom panoptikon fungerer makten automatisk – da den «innsatte» stadig er bevisst og vet at muligheten for å bli overvåket er der (Foucault, 1977, s.180). Denne maktmekanismen som vi oppnår gjennom panoptikonen kan vi hevde at vi fortsatt ser gjennom bruken av dagens sosiale medier.

Selv om vi gjennom panoptikon vet at overvåking muliggjøres har det i senere tid oppstått en underkategori som innebærer at brukeren selv lar seg frivillig overvåkes. Denne kategorien kan vi kalle for frivillig panoptikon. Ifølge Lee Humphreys skiller frivillig panoptikon seg fra eldre overvåkingssystemer ved at brukeren selv gir samtykke til å bli overvåket av andre (Humphreys, 2014, s.111). Når det kommer til lokasjonsbaserte tjenester ser vi at det først og fremst er opp til brukeren om man ønsker å ta i bruk tjenesten. Dersom man velger å ta i bruk tjenesten må man på de fleste tjenester selv logge inn og akseptere å dele lokasjonen sin med den valgte tjenesten. Adriana de Souza e Silva og Jordan Frith hevder at dersom lokasjonsbaserte applikasjoner skal kunne fungere, er de nødt til å få vite hvor brukeren befinner seg (de Souza e Silva & Frith, 2012, s.124). Selv om det er brukeren selv som godtar å ta i bruk tjenesten og skaper en følelse av kontroll, er det ingen garanti for at brukeren ikke står i fare for å miste kontroll over egen informasjon. Lokasjonsbaserte tjenester er som tidligere nevnt en av tjenestene som tilbyr flytende overvåking og gjennom å ta disse tjenestene i bruk står brukerens personlige informasjon og personvernet i fare.

Et eksempel på frivillig panoptikon ser vi gjennom EUs personvernsforordning (GDPR) som trådte i kraft i juli 2018. GDPR er et tiltak som har blitt innført for å gi forbrukerne mer makt over hvilken informasjon de deler og hvem de deler den med. Forordningen går ut på at brukeren selv må akseptere at tjenestene skal få lov til å innhente informasjon om brukeren (Berg & Lysgård, 2019). Dermed tilegnes brukeren en form for frivillig panoptikon gjennom denne forordningen, da man selv har makten til å velge hvem som skal få tilgang til egen personlig informasjon og hvem som ikke skal få det. Likevel ser vi at denne formen bringer med seg konsekvenser for brukeren i det forordningen skal utøves i praksis; de fleste brukerne aksepterer uten å sette seg inn i hva det faktisk innebærer. Ifølge Sintef-forskeren Petter Bae Brandtzæg har GDPR bare ført til at man må trykke på «Jeg aksepterer» hele tiden. Det er ingen som orker å faktisk gå gjennom og lese disse tingene. Gjennom GDPR mener Brandtzæg at problemene blir sendt videre til forbrukerne. I stedet for at selskaper holdes ansvarlig, må vi selv ta ansvaret og det er ikke en realistisk løsning (Berg & Lysgård, 2019).

4.4 I lys av disse bekymringene, ser vi en endring i bruken av lokasjonsbaserte tjenester?
Selv om enkelte medieforskere og Teknologirådets rapport viser til bekymring når det kommer til personvern og det å miste kontroll over hvilken personlig informasjon man gir til blant annet lokasjonsbaserte tjenester gjennom bruken av dem, mener andre forskere at bruken av disse tjenestene fortsetter slik den alltid har gjort til tross for disse bekymringene.

David Nguyen, Alfred Kobsa og Gillian Hayes er noen av de som har forsket og sett på at bruken av lokasjonsbaserte tjenester ikke har endret seg til tross for den uttrykte bekymringen knyttet til bruken av disse. De har funnet ut at selv om folk uttrykker bekymringer rundt det å miste kontrollen over personlig informasjon og at personvernet står i fare, driver de samme folkene med en motstridende praksis i det de fortsetter å benytte seg av tjenester som resulterer i at deres personlige informasjon sirkulerer rundt i databaser på nett. De hevder at dette trolig skjer på grunn av at de fleste mener og tror at fordelene ved å ta i bruk slike tjenester oppveier de mulige konsekvensene som kan komme av å benytte seg av disse tjenestene (de Souza e Silva & Frith, 2012, s. 114). Det at brukerne til tross for bekymringene til overvåking og personvern fortsetter å benytte seg av lokasjonsbaserte tjenester kan vi se på i lys av det David Barnard-Wills definerer som personvernsparadokset. David Barnard-Wills hevder at ideen om et personvernsparadoks dreier seg rundt en tilsynelatende motsetning mellom tro og oppførsel når det kommer til utøvelsen av personvern. Det går ut på at enkeltpersoner eller grupper uttrykker en bekymring for personvernet, eller kritiserer teknologier for personvernsinngripelse. Likevel oppstår paradokset når de samme personene eller gruppene driver med personvernreduserende atferd, for eksempel gjennom å frivillig gi fra seg personlig informasjon, bli medlem av et sosialt nettverk hvor det er dårlig kontroll over personvernet, eller å godta en gratis tjeneste i bytte mot målrettet reklame basert på dine personlige opplysninger (Barnard-Wills, 2014, s.174). Dermed ser vi at Barnard-Wills på lik linje som David Nguyen, Alfred Kobsa og Gillian Hayes hevder at bekymringene som folk uttrykker over bruken av lokasjonsbaserte tjenester ikke resulterer i endret bruk av tjenestene.

I nesten alle situasjoner der mennesker må velge mellom privatliv og omtrent hvilket som helst annet gode, velger de det andre godet. Folk velger alternativene som tilbyr bekvemmelighet, økonomiske besparelser, rask tilkobling og sikkerhet i stedet for de som tilbyr personvern. Personvernet er tross alt ikke av stor verdi; eller i det minste ikke av sammenlignbar verdi som andre tjenester (Nissenbaum, 2010, s.105). Uansett hva folk sier om deres ønske om privatliv, avslører de gjennom bruken av for eksempel lokasjonsbaserte tjenester at de tar lite hensyn til personvernet (Nissenbaum, 2010, s.107). Dermed ser vi at i «konkurransen» mellom det å skulle ta hensyn til personvernet og andre tilbud som tjenestene tilbyr, kommer personvern dårligst ut av situasjonen. Brukerne opplever at fordelene ved å ta i bruk en lokasjonsbasert tjeneste ofte veier opp for konsekvensene av bruken. De fleste lokasjonsbaserte tjenestene tilbyr en fordel brukeren får i det de benytter seg av tjenesten, og ofte velger brukeren å velge godet som tilbys fremfor å verne om personvernet og privatlivet sitt. Dersom vi skal se på dette i lys av bruken av lokasjonsbaserte tjenester ser vi ofte at brukerne gir opp deler av personvernet sitt for å kunne følge med og å overvåke andre brukere til enhver tid. Vi gir altså opp privatlivet vårt for å kunne spionere på andre sitt privatliv. Det blir dermed selvmotsigende av brukerne å uttrykke stor bekymring rundt bruken av lokasjonsbaserte tjenester når de likevel utøver en praksis hvor de til tross for disse bekymringene fortsetter å ta de lokasjonsbaserte tjenestene i bruk. Da på det grunnlag at de mener fordelene ved

å ta i bruk lokasjonsbaserte tjenester veier opp for konsekvensene som resulterer i å svekke personvernet og å miste kontrollen over egen personlig informasjon.

5 Oppsummering og konklusjon

I denne teksten har jeg undersøkt hvilke bekymringer brukerne av dagens lokasjonsbaserte tjenester har uttrykt når det kommer til overvåking og personvern i dagens samfunn, og om disse bekymringene har spilt en rolle når det kommer til bruken av disse tjenestene. Spesifikt ønsket jeg å undersøke om vi gjennom disse bekymringene har endret bruken av lokasjonsbaserte tjenester eller om bruken har forblitt den samme til tross for disse bekymringene. Dersom bruken ikke har endret seg og forblir den samme, hva er det som gjør at vi trosser bekymringene knyttet til personvern og risikerer å miste kontrollen over personlig informasjon på nett?

Jeg startet teksten med å drøfte omkring bekymringer knyttet til den flytende formen for overvåking vi står overfor i dagens samfunn. Denne formen for overvåking har blitt integrert inn i enheter vi bruker i hverdagssammenheng og det blir derfor vanskeligere å legge merke til at overvåkingen finner sted, vi finner ikke denne overvåkingen for påtrengende og utøver derfor ingen motstand mot den. Ifølge Teknologirådets rapport skaper denne formen for overvåking bekymring for brukerne når det kommer til å kunne kontrollere egen personlig informasjon. Gjennom flytende overvåking mister brukeren kontroll over hvilken informasjon som blir tatt og hvem som får tilgang til denne informasjonen. Brukeren blir mindre oppmerksom på at overvåkingen tar sted og har dermed ingen mulighet til å kontrollere hva som blir tatt og av hvem. Den flytende overvåkingen resulterer dermed i at personvernet og brukerens kontroll over egen informasjon står i fare, da vi ikke har noen garanti for å kunne verne om eget personvern eller informasjon knyttet til brukeren.

Denne flytende overvåkingen er et resultat av den nye overvåkingskulturen vi nå lever i, hvor overvåking i stor grad har blitt mer normalisert og akseptert blant befolkningen. Vi har lært at overvåking ikke er noe vi slipper unna og dermed må vi lære oss å leve side om side med det. Dagens sosiale medier har gjort at det ikke lengre kun er politi og andre styremakter som kan overvåke innbyggerne, nå kan alle innbyggerne ta del i å overvåke hverandre. Sosiale medier har dermed gjort alle til hverdagsspioner, hvor vi tar i bruk overvåkingsenheter for å spionere og overvåke venner og familie. Vi står gjennom lokasjonsbaserte tjenester overfor et bredt spekter med muligheter når det kommer til å holde et elektronisk øye med våre sosiale nettverk gjennom disse tjenestene. Likevel blir det gjennom Teknologirådets rapport uttrykt bekymring knyttet til denne overvåkingen da man har liten kontroll over det å vite at man blir overvåket og av hvem. Vi vet at muligheten er der for å konstant bli overvåket, noe som også skaper ubehag hos brukerne.

Her ser vi at panoptikonprinsippet spiller inn og at det dermed kan trekkes linjer mellom Foucaults idé om overvåking og den overvåkingen vi står overfor i dag. Det har i lys av panoptikonprinsippet oppstått nye panoptiske elementer i dagens samfunn som vi kan kalle for personlige panoptikoner, smarttelefoner og internett, og dermed kan vi hevde at den originale ideen om overvåking har blitt videreført til dagens teknologiske enheter. Vi har gjennom disse personlige panoptikonene ikke muligheten til å se om noen faktisk overvåker oss og vi får heller ikke vite om vi blir overvåket, men vi vet at gjennom bruken av disse finnes det en mulighet for å kunne bli overvåket. Begrepet frivillig panoptikon er noe vi har sett utvikle seg de seneste årene og blir gjennom eksempelet om GDPR, sett på

som en redning når det kommer til brukerens kontroll over hva som deles på de lokasjonsbaserte tjenestene da det er brukeren selv som aksepterer hvem som skal få tilgang til informasjonen. Likevel har vi sett at dette også skaper en del ulemper, blant annet i form av at alt ansvaret tillegges brukeren og siden ikke mange brukere orker å sette seg inn i hva som aksepteres har dette lite virkning på kontrollen over informasjonen og personvernet.

Det kommer tydelig frem at bruken av lokasjonsbaserte tjenester ikke har endret seg selv om folk uttrykker store bekymringer knyttet til disse tjenestene. Dette ble synliggjort gjennom David Nguyen, Alfred Kobsa og Gillian Hayes og deres forskning på dette, hvor det viser seg at selv om brukerne uttrykker bekymringer viser bruken av disse tjenestene noe helt annet. På samme vis trekkes personvernsparadokset frem, hvor Barnard-Wills hevder enkeltpersoner uttrykker en bekymring for personvernet, likevel driver de samme personene med personvernreduserende atferd gjennom bruken av lokasjonsbaserte tjenester. Dermed ser vi at i «konkurransen» mellom tilbudet av lokasjonsbaserte tjenester og det å kontrollere informasjon og personvernet, er det personvernet og kontrollen som kommer dårligst ut.

Til slutt vil jeg konkludere med at bruken av lokasjonsbaserte tjenester ikke har endret seg til tross for de bekymringene som har oppstått gjennom bruken av dem i dagens samfunn. Brukerne fortsetter å ta disse tjenestene i bruk selv om de er bevisste på at kontrollen over personlig informasjon og personvernet står i fare. Ut i fra den frivillige panoptikonen, GDPR og personvernsparadokset forstår jeg det slik at vi som brukere aksepterer risikoen om å miste kontrollen over hvilken personlig informasjon som deles med andre og hvem som får tilgang til denne gjennom lokasjonsbaserte tjenester. I nesten alle situasjoner hvor vi må velge mellom privatliv og omtrent hvilket som helst annet gode, velger vi det andre godet. Vi velger det vi føler vi tjener mest på i den konteksten, og i denne konteksten spiller kontrollen over privat informasjon og personvern en liten rolle. Vi ser gjennom GDPR at ansvaret om å verne om eget personvern på nett blir tildelt fullt og helt til brukeren, og skal vi forstå dette i lys av David Nguyen, Alfred Kobsa, Gillian Hayes og Barnard-Wills vil det å legge alt ansvaret over på brukeren ikke være et lurt valg dersom man har et ønske om å opprettholde et visst nivå av privatliv i dagens overvåkingssamfunn. Da må brukerne endre prioriteringene sine når det kommer til bruken av lokasjonsbaserte tjenester, og det kjapt.

6 Litteraturliste:

Andrejevic, M. (2004). The Work of Watching One Another: Lateral Surveillance, Risk, and Governance.

Andrejevic, M. (2006). The Discipline of Watching: Detection, Risk, and Lateral Surveillance

Barland, M. (2016, 28.januar). Slik blir du overvåket. Hentet fra https://teknologiradet.no/slik-blir-du-overvaket-2/

Barnard-Wills, D. (2014). The Non-Consensual Hallucination: The Politics of Online Privacy. I A. Jansson og M. Christensen (red.), *Media, Surveillance and Identity* (s.165-182). New York: Peter Lang Publishing.

Bauman, Z. & Lyon, D. (2013). *Liquid Surveillance: A conversation.* UK: Cambridge; Malden, MA: Polity Press.

Bentham, J. (2018). *Panopticon.* Farmington Hills: Gale Ecco.

Berg, A. & Lysgård, M., F. (2019, 11. november). Forsker: -Det finnes ikke privatliv på internettet. Hentet fra https://www.abcnyheter.no/nyheter/norge/2019/11/11/195625746/forsker-det-finnes-ikke-privatliv-pa-internettet

Boyd, D. (2014). *It`s complicated: The Social Lives of Networked Teens.* New Haven: Yale University Press.

de Souza e Silva, A. & Frith, J. (2012). *Mobile Interfaces in Public Spaces: Locational Privacy, Control and Urban Sociability.* New York: Routledge.

de Souza e Silva, A. & Sheller, M. (2015). *Mobility and Locative Media: Mobile communication in hybrid spaces.* New York: Routledge.

Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison.* New York: Pantheon Books.

Frith, J. (2015). *Smartphones as locative media.* UK: Polity Press.

Hannemyr, G., Liestøl, G., Lüders, M., & Rasmussen, T. (2015). *Digitale medier: Teknologi, Anvendelser og Samfunn* (3.utg). Oslo: Universitetsforlaget.

Humphreys, L. (2014). Mobile Social Networks and Surveillance: Users`Perspective. I A. Jansson og M. Christensen (red.), *Media, Surveillance and Identity* (s.109-126). New York: Peter Lang Publishing.

Lyon, D. (2001). *Surveillance Society: Monitoring in everyday life.* Buckingham: Open University Press.

Lyon, D. (2014). The Emerging Surveillance Culture. I A. Jansson og M. Christensen (red.), *Media, Surveillance and Identity* (s.71-88). New York: Peter Lang Publishing.

Mathiesen, T. (1997). "The Viewer Society: Michel Foucault`s Panopticon Revisited". *Theoretical Criminology,* 1 (2), s.215-234. https://doi.org/10.1177/1362480697001002003

Nissenbaum, H. (2010). *Privacy in context: Technology, Policy and the Integrity of Social Life.* Stanford: Stanford University Press.

NOU 2009:1. (2009). *Individ og integritet: Personvern i det digitale samfunnet.* Oslo: Fornyings- og administrasjonsdepartementet.

Overland, J., A. (2018, 02.juli). Digital dømmekraft. Hentet fra https://ndla.no/subjects/subject:14/topic:1:185701/resource:1:114171

Rettberg, W., J. (2014, 15.desember). «Angsten for medienes umenneskeliggjørende virkning»: Fremtidsmedier sett gjennom science fiction. – En respons til Jon Bing. *Norsk medietidsskrift.* Hentet fra https://www.idunn.no/nmt/2014/04/angsten_for_medienes_umenneskeliggjoerende_virkning_fremt

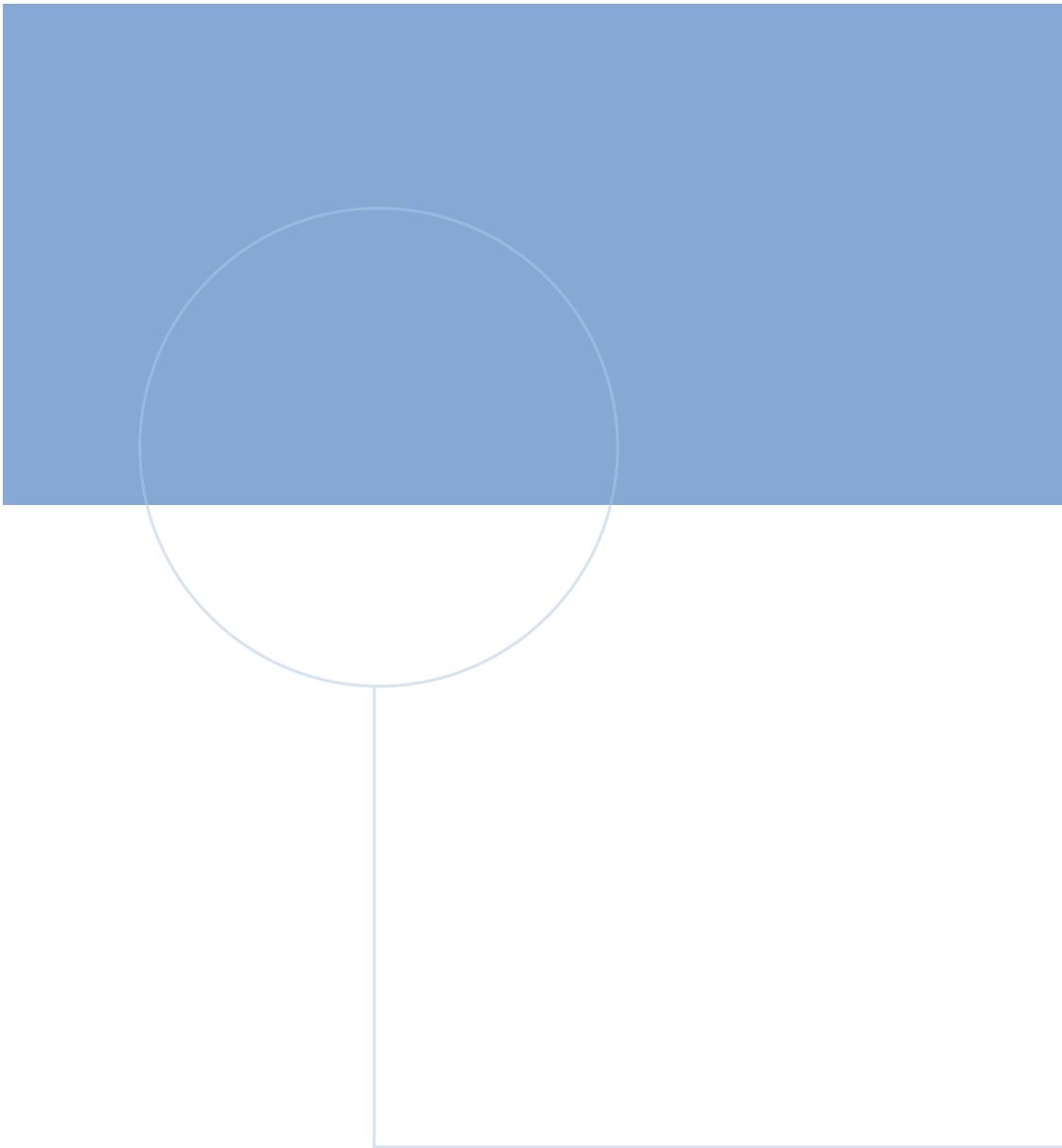
Rettberg, W., J. (2014). *Seeing Ourselves Through Technology.* UK: Palgrave Macmillian.

Teknologirådet. (2004). *Holdninger til personvern. Rapport fra fokusgrupper om elektroniske spor og personvern.* Oslo: Teknologirådet.

Teknologirådet. (2020). Demokrati og personvern. Hentet fra https://teknologiradet.no/category/personvern/

Teknologirådet & Datatilsynet. (2018). *Personvern 2018. Tillit og følelser.* Oslo: Teknologirådet.

Zurawski, N. (2014). Consuming Surveillance: Mediating Control Practices Through Consumer Culture and Everyday Life. I A. Jansson og M. Christensen (red.), *Media, Surveillance and Identity* (s.32-48). New York: Peter Lang Publishing.



NTNU

Kunnskap for en bedre verden