«Prisen å betale»

En studie av hvordan unge voksne forholder seg til personvern på nett.

Terje Sandkjær Hanssen

Masteroppgave i Medievitenskap

Institutt for informasjons- og medievitenskap

Universitetet i Bergen

Våren 2019

Sammendrag

Denne studien tar for seg hvordan unge voksne vurderer eget personvern på nett, og hva som påvirker disse vurderingene. Med oppgaven ønsker jeg å få en videre forståelse for hva denne «digitale» generasjonen tenker og føler rundt temaet personvern. Dette skal utforskes i lys av tre grupper av aktører: statlige institusjoner, medieplattformer og andre brukere. Jeg skal også ta for meg to case-eksempler: Google Maps og Snapmap.

Aldersgruppen 19 til 23 år er valgt med tanke på at de er unge nok til å ha vokst opp med internett og sosiale medier, og gamle nok til å ha reflektert bevisst over egen aktivitet og forhold til personvern på nett over tid. Ved hjelp av 11 kvalitative dybdeintervjuer har jeg utforsket informantenes mediebruk og forståelse for personvern på nett. Prosjektet startet ut med en åpen tilnærming for å undersøke hvordan unge voksne forholdt seg til personvern i sosiale medier.

Det benyttes flere teoretiske perspektiv i oppgaven for å forklare funnene. Kontekstuell integritet er en teoretisk personvernsmodell utformet av Helen Nissenbaum som kan brukes til å analysere og forklare hvordan sosiale kontekster, forventninger og normer påvirker hvordan mennesker opplever tillitsbrudd på nett. Andre teorier baserer seg blant annet på Michel Foucaults makt- og kontrollperspektiv om panoptikon.

Forord

Jeg har ofte forestilt meg hvordan livet hadde vært om jeg hadde vært like effektiv i studier og jobb som jeg er i innspurter, og for masteroppgaven gjelder dette trippelt opp. Jeg tror likevel ikke jeg har tenkt å gjøre masterskriving til en vane. En ting jeg har fått smertefullt erfare i prosessen er at mastertåka eksisterer, og jeg gleder meg til å tre ut av den nå snart. Men det har vært en utrolig givende prosess for meg å se at ting gradvis tar form, og at det bygger seg opp til å bli en konkret oppgave jeg kan levere. Det har vært en lærerik prosess, og jeg ville ikke vært den foruten.

En stor takk til min veileder Hallvard Moe for all hjelp og tilbakemelding på min oppgave. Du har alltid vært der når jeg har trengt deg, og har vist deg å være en tålmodig og forståelsesfull støttespiller. Takk til førsteamanuensis Ankica Babic for all varmen og omtenksomheten du gir til oss studenter.

Takk til Ida, Maja og Hilde på lesesal 635, jeg hadde ikke holdt ut dette året uten dere her. Takk til mine foreldre som er stolte av meg uansett hva. Takk til Kristian og min søster Gro for korrekturlesing og hjelp med oppgaven i innspurten.

Og ikke minst takk til alle informantene som stilte opp for intervju. Uten dere hadde dette prosjektet bokstavelig talt ikke blitt til.

Terje Sandkjær Hanssen

31.05.2019

Innholdsfortegnelse

1 Innledning

Personvern og viktigheten av å beskytte sitt eget privatliv ble tidligere sett på som en kampsak mellom folket og staten. Dystopiske fremtidsvisjoner som romanen «1984» av George Orwell beskriver hvordan totalitære stater kunne bruke overvåkning til å knuse all form for motstandsbevegelser (Orwell 1949). Uttrykket «Big Brother» fra denne romanen har siden blitt brukt for å beskrive statlig undertrykking gjennom overvåkning. Selve ordet «overvåkning» viser til en hierarkisk maktforståelse der overvåkeren kontrollerer den som blir overvåket. I nyere tid har markedskreftene forstått verdien av å «overvåke» folket. Arkivering og analyse av brukeratferd og kjøpshistorikk gir selskaper mulighet til å forstå og forutse sine kunders behov. Digitale medieplattformer som Facebook og Google har tilrettelagt for mye av denne målrettede markedsføringen ved å la selskaper benytte seg av plattformenes informasjon om sine brukere. Medieforsker David Lyon omtaler denne innsamlingen av brukerinformasjon som en *flytende overvåkning* som brukerne ikke legger merke til, og derfor heller ikke gjør motstand mot (Bauman og Lyon 2013).

De siste årene har det også vokst frem en større internasjonal interesse for personvern på nett. Etter Facebooks innblanding i skandalen med Cambridge Analytica, analyseselskapet som hadde fått urettmessig tilgang til Facebooks brukere og ble beskyldt for å påvirke det amerikanske presidentvalget, har direktør Mark Zuckerberg lovet å forbedre sine brukeres sikkerhet gjennom en ny «personvern-fokusert sosial plattform» (Wong 2019). Nye personvernlover som EUs GDPR har også blitt utformet for å verne om individets personvern på nett. Med en stadig forandrende medieutvikling er det likevel ikke sikkert disse personvernlovene utformes raskt nok, eller at de klarer å fange opp alt av menneskers personvernproblematikk på nett.

Med fremveksten av sosiale medier har de tradisjonelle forestillingene om personvern også forandret seg på andre måter. Snapchat-brukere har mulighet til å vise sine kontakter hvor de befinner seg til alle tider på en innebygd kartfunksjon. Apper som installeres henter mye av informasjonen rett fra brukerens smarttelefon eller Facebook-profil. Tjenester som Facebook og Google har også gjort det lettere enn noensinne for vanlige brukere å finne informasjon om andre mennesker gjennom bilder, videoer, kommentarer og statusoppdateringer. Medieforskere som Anders Albrechtslund poengterer likevel viktigheten av å ikke se oss blinde på farene knyttet til personvern og overvåkning på nett, men at vi i forskningsprosesser også benytter anledningen til å tenke nytt rundt hva overvåkning er (Albrechtslund 2008).

Her i Norge har innbyggerne høy sosial mobilitet, et godt utbygd mobil- og nettilbud og lett tilgang til internett. Vi har også stor tillit til staten og styresmaktene. I denne settingen ønsker jeg å studere hva slags forhold unge voksne som har vokst opp med internett har til personvern på nett. Unge voksne som har vokst opp med internett og sosiale medier har en antakelig en annen forståelse for personvern på nett enn hva eldre generasjoner har. De kommende digitale generasjonene kommer også til å sette dagsorden, utforme kommende lovverk og påvirke prosesser for hvordan medieteknologi kommer til å bli utviklet. Jeg ønsker derfor å undersøke hva slags forståelser unge voksne har rundt personvern på nett. Hva har de av forestillinger, holdninger, preferanser og motforestillinger? Hva er det motstand mot, og hva er det mangel på motstand på? Hva spiller inn i hvordan de bedømmer sikkerhetssituasjoner på nett? Hvorfor er de eventuelt ikke opptatt av å beskytte seg selv, sitt innhold og sin informasjon?

Dersom personvern virkelig hadde vært den viktigste faktoren i menneskers liv, hadde ingen vært på internett, ingen hadde betalt med kort i butikker og ingen hadde ønsket å oppholde seg i byområder med kameraovervåkning. Alle gir opp enn viss grad av personvern når vi benytter oss av disse tjenestene i samfunnet i bytte for digitale tjenester på internett, kontantløs betaling og forhåpentligvis tryggere byområder. På tilsvarende vis er det for bruk av medieplattformene i denne studien. Informantene bruker ikke medieplattformene fordi de tilbyr de beste måtene å sikre deres personvern på, de er der først og fremst på grunn av tjenestene de tilbyr: Sosiale medietjenester, videotjenester, internettsøk og lokasjonstjenester. Jeg ønsker derfor å se på hvordan unge voksne tar personvernvurderinger ut fra disse forutsetningene – hvordan andre faktorer i medielandskapet og utenfor det påvirker hvordan vurderingene de tar, og hvordan personvernhensyn spiller inn i dem.

I resten av dette kapittelet vil jeg først skrive om tidligere forskning og hvilken relevans dette har for denne studien. Jeg vil så definere problemstillingen min og forklare hvordan jeg har valgt å løse den. Jeg vil så kort vise hvilke avgrensninger jeg har tatt i studien, og avslutningsvis oppgavens struktur.

1.1 Tema og problemstilling:

For å finne ut hvilke forståelser som informantene har om personvern på nett, har jeg valgt en todelt problemstilling som jeg mener vil belyse dette på best mulig måte, og utvide forståelsen av hvordan unge voksne forholder seg til personvern på nett.

1. Hvordan vurderer unge voksne personvern på nett? Hvilke faktorer påvirker personvernvurderingene?

Med vurdering av personvern menes det her hvordan informantene tar avgjørelser i å verne om sin personlige informasjon på nett. Vurderinger og avgjørelser informantene tar på nett mener jeg er en god måte å vise hvordan informantene tenker og resonnerer rundt eget personvern, og slik vise deres forståelser rundt tematikken. For å besvare problemstillingen har jeg valgt å vise hvilke personvernvurderinger de tar overfor tre grupper av aktører: statlige institusjoner, medieplattformer og andre brukere.

Vurderingene jeg har valgt for å besvare denne første delen i problemstillingen er:

a) Akseptering eller ikke akseptering av statlig overvåkning (Kapittel 4)
b) Kapittel 5: Bruk eller ikke-bruk av medieplattformer (Kapittel 5)
c) Kapittel 6: Vurderinger rundt innholdsdeling, blokkering av andre brukere, hvilke brukere som kan legges til som kontakter, avgrensing av kontekster og personverninnstillinger (Kapittel 6)
d) Kapittel 7: Bruk eller ikke-bruk av lokasjonstjenestene Google Maps og Snapmap. (Kapittel 7)

Siden vurderingene jeg skal ta for meg i oppgaven er påvirket av flere faktorer enn bare personvern, har jeg også valgt å beskrive hvilke andre faktorer som påvirker informantenes vurderinger. Den andre delen av problemstillingen, hvilke faktorer som påvirker hvordan informantene tar personvernvurderinger, skal derfor utforskes for hvert tema der dette er mulig. Dette er tatt med for å få et bedre bilde av de komplekse og sammensatte prosessene som personvernvurderinger er, og for å få en bedre forståelse av hvordan personvernhensyn vektes i de forskjellige vurderingene som blir beskrevet.

Akseptering av at statlige institusjoner har mandat til å overvåke borgerne sine er eksempelvis en «renere» personvernvurdering enn vurderingen om å bruke eller ikke bruke medieplattformer, siden det er færre faktorer som påvirker denne vurderingen. Fortsatt bruk av medieplattformene har mange og sammensatte grunner, i likhet med vurderinger overfor andre brukere. I oppgaven skal jeg derfor ta opp hva jeg anser som de viktigste og mest interessante faktorene som påvirker informantenes vurderinger. Alle påvirkningene spiller i større eller mindre grad inn i personvernvurderingen rundt fortsatt bruk, enten for eller imot. På tilsvarende vis har også case-eksemplene med Google Maps og Snapmap faktorer som påvirker bruk eller ikke-bruk av tjenestene.

I kapitlet om andre brukere er det også snakk om tilsvarende vurderinger som å legge til eller ikke legge til en spesifikk bruker, men også andre vurderinger som er mindre definerbare, som hva slags innhold som legges ut i hvilke kontekster, og hvordan de reagerer når det har oppstått en ubehagelig situasjon. Disse vurderingene er sammensatte også, men for enkelhets og helhetens skyld kan ikke alle slike påvirkninger tas med i dette kapitlet. Dette kommer riktignok litt til syne i case-eksempelet om Snapmap i kapittel 7.

Gjennom kapitlene benytter jeg meg også av ulike teoretiske perspektiv som skal bidra til å forklare og utdype forståelser rundt informantenes personvernvurderinger og faktorer som påvirker disse. Studien har en temabasert struktur, og analysen av datamaterialet slås sammen med teoretisk drøfting for hvert tema. Jeg vil i kapittel 5, 6 og 7 også ha en avsluttende drøfting der temaene for hvert kapittel sees i sammenheng.

1.2 Avgrensninger

Avgrensningen unge voksne satt jeg i utgangspunktet fra 18 til 23 år. Dette gjorde jeg for det første fordi jeg var interessert i en ung nok aldersgruppe som hadde vokst opp med internett og sosiale medier. Jeg valgte dem også fordi jeg gikk ut fra at denne gruppen ville hatt mer tid og modenhet til å reflektere over egen nettbruk og personvern enn hva ungdom under 18 år muligens kunne. Med studien ønsker jeg å bidra til en økt forståelse for hvordan det å ha vokst opp med internettilgang og sosiale medier har påvirket synet på personvern på nett.

1.3 Tidligere forskning

Personverndebatter relatert til informasjonsteknologi, overvåkning og sporing og lagring av massive databaser med informasjon om privatpersoner startet i USA på 1960- og 1970-tallet (Nissenbaum 2010, 36). Debattene er fortsatt aktuelle i dag i tråd med fortsatte teknologiske nyvinninger som innsanker informasjon om sine brukere.

Det meste av forskningen på personvern og nettbruk i dag gjennomføres hovedsakelig innenfor rettsvitenskap og informasjonsvitenskap. De vektlegger hovedsakelig tekniske og juridiske aspekter ved personvern, og påpeker ofte hvor sårbart og lett tilgjengelig enkeltindividers personinformasjon er på nett. Forskere som Thomas Mathisen hevder at organisasjoner og stater har fått overdrevent mye tilgang til brukeres personinformasjon, og at mediefokuset på terrorisme har skapt en ufortjent bred aksept av overvåkning på nett og i det offentlige rom (Mathiesen 2013).

I denne diskursen er det også vanlig å påstå at spesielt unge brukere er skjødesløse når det kommer til deling på nett og ikke bryr seg om personvern:

> Some researchers have suggested that social network users are uniquely unconcerned about privacy; that over time, regular use of social media without any major negative experiences may lessen their concerns about sharing information. (Madden 2012, 4)

David Lyon er en av de mest kjente forskere innenfor personvern på nett. Lyon argumenterer for at en av grunnene til at forskning innenfor personvern ikke klarer å forklare hvorfor folk tilsynelatende deler mer informasjon enn de bør og ikke er mer opptatt av personvern på nett, er fordi forskerne ikke prøver å forstå folkene og hvordan deres hverdagsliv påvirker deres oppfatning av personvern og de digitale tjenestene de bruker. Spesielt nå som overvåkning er sammenvevd i folks liv i større grad gjennom internett fremhever Lyon viktigheten av å forstå folks meninger og holdninger til personvern på nett (Bauman og Lyon 2013). Dette er det lite forskning på for øyeblikket, og i tråd med en forandrende verden i form av teknologiske fremskritt som hverdagsliggjøring av smarttelefoner og nye sosiale medier, mener jeg det er kontinuerlig behov for mer kunnskap om dette feltet.

Det finnes likevel en del studier studier som tar opp hvordan mennesker forholder seg til nettopp personvern på nett. Et av de mest kjente er produsert av medieforsker danah boyd. Boyd gjennomførte en kvalitativ forskningsstudie gjennom et tiår om hvordan amerikanske tenåringer brukte sosiale medier i hverdagen, og publiserte funnene i boken «It's complicated – The social lives of networked teens» (boyd 2014). En stor del av studien omhandler hvordan tenåringene boyd intervjuer forholder seg til personvern, og Boyd finner at tenåringene i høy grad bryr seg om eget personvern og å verne om egen informasjon, selv om det ikke virker slik utad (boyd 2014).

Kommunikasjonsforskeren Lee Humphreys utforsket menneskers forhold til personvern og overvåkning i sin studie om brukere av den mobile tjenesten *Dodgeball* mellom 2005 og 2006 (Humphreys 2013, 113). Dodgeball var en mobilapplikasjon som knyttet brukere i nettverket sammen gjennom såkalte «check-ins» der brukerne kunne kunngjøre beskjeder og meldinger om hvor de var til Dodgeball-brukere i nærheten (Humphreys 2013, 112). Tjenesten hadde flere likheter med nåtidens sosiale medieapplikasjon Jodel. Humphreys fant at brukerne hadde minimale bekymringer for eget personvern, at de mente at de sendte meldinger på deres egne vilkår, og at de beskyttet eget personvern ved å avgrense hvem de la til som venner (Humphreys 2013, 114). Denne studien skal jeg komme tilbake til i løpet av oppgaven.

Christine M. Mæland forsker i sin masteroppgave «Ikke-bruk av Facebook og ubehaget bak» på mennesker mellom 25 og 35 år som ikke bruker Facebook. Et viktig funn i denne kvalitative studien er hvordan åtte av ti informanter fortalte om ubehagelige erfaringer med sosiale medier, noe hun kobler sammen med deres ikke-bruk (Mæland 2017, 63). Noen av disse ubehagelige erfaringene som Mælands informanter tok opp var relatert til personvern: Enkelte av informantene hadde en skepsis til hvordan Facebook ivaretok deres personvern (Mæland 2017, 98–99). Andre hadde opplevd ubehagelige situasjoner med ukjente mennesker på Facebook som føltes skremmende og ubehagelige (Mæland 2017, 69). Disse informantene hadde altså vurdert å ikke bruke Facebook delvis på grunn av personvernhensyn. Oppgaven hennes viser til hvordan det å ikke bruke medieplattformen Facebook har sammensatte årsaker, noe som jeg skal ta med meg i kapittel 5 om påvirkninger på fortsatt bruk (Mæland 2017).

Ut fra tidligere forskning legger jeg opp til at denne studien kan bidra til mediebruksforskningen på dette området: gjennom å få en utvidet forståelse for hva norske, unge voksne som har vokst opp med internett har av holdninger til personvern i mylderet av sosiale medieplattformer, smarttelefoner og internett generelt. Bryr de seg om eget personvern? Hva er de bekymret for på internett? Hvor mye vet de om personvern, og har dette innvirkning på holdningene og vanene deres? Det er også interessant å finne ut om det er motstand mot overvåkning blant disse unge voksne, og hvilke former de eventuelt tar.

1.4 Oppgavens struktur

I kapittel 2 vil jeg ta for meg teoretiske perspektiver jeg skal bruke gjennom oppgaven, samt begreper og definisjoner på personvern og personlig informasjon.

I kapittel 3 presenterer jeg metode jeg har brukt for studien, som intervjuguide, rekruttering av informanter, transkribering og analysering av datamaterialet.

I kapittel 4 om statlige institusjoner skal jeg se på om informantene aksepterer en potensial overvåkning av statlige institusjonene eller ikke, og hva som påvirker denne vurderingen.

Kapittel 5 om medieplattformer tar for seg vurderingene om å fortsette å bruke de forskjellige medieplattformene og la dem få tilgang til personinformasjon og brukeratferd. Jeg skal her også se på hva som påvirker disse vurderingene.

I kapittel 6 om andre brukere skal jeg se på hva slags typer personvernvurderinger informantene tar overfor andre brukere. Jeg skal også se på hvordan ulike faktorer som påvirker deres vurderinger.

I kapittel 7 skal vi ta for oss karttjenestene Google Maps og Snapmap som case-eksempler på hvordan informantene vurderer personvern både overfor medieplattformer og andre brukere.

I kapittel 8 skal jeg oppsummere hva jeg har funnet i en konklusjon, og se på veien videre for videre forskning.

2 Teoretisk rammeverk

Jeg skal her gå gjennom forskjellige teoretiske perspektiv jeg skal benytte meg av i oppgaven. Aller først skal jeg se på personvern og hvordan det kan bli definert.

2.1 Personvern

Aristoteles var en av de første som skrev om skillet mellom livet i den politiske sfæren og den private sfæren i hjemmet (van den Hoven mfl. 2018). Personvern ble første gang beskrevet i en publikasjon i 1890. Louis Brandeis og Samuel Warren skrev en artikkel i Harvard Law Review som omtalte «retten til å bli latt være i fred» som en reaksjon på innpåslitne journalister (Warren og Brandeis 1890). Personvern har derfor hatt en tydelig verdi i historisk kontekst, men det er altså de siste 130 årene at begrepet har blitt tydeligere definert og blitt en vesentlig del av demokratisk lovgivning.

Det strides riktignok fortsatt om hvordan personvern skal defineres, spesielt innenfor lovgivning, politikk og informasjonsteknologi. Siden det viktigste i denne oppgaven er å få frem hvordan informantene i studiet selv vurderer personvern på nett, er det like viktig å tydeliggjøre hva slags personvernsdefinisjoner som samsvarer med deres forståelser. Jeg har derfor tatt utgangspunkt i personvernsdefinisjoner som er mest mulig relevante for besvarelsene, som kan utdype deres posisjoner og som muligens kan beskrive enkeltes ambivalente forhold til personvern lettere.

Det engelske begrepet *privacy* kan sees på som et videre begrep enn det norske begrepet *personvern*, idet det kan tolkes som å omfatte flere aspekter av privatliv enn hva personvern gjør. Men i konteksten med personvern i digitale arenaer blir privacy og personvern brukt til å beskrive det samme behovet for vern av privatliv og personlig informasjon.

Helen Nissenbaum fremholder at det viktigste i personvernforskning ikke nødvendigvis er å definere personvern, men å analysere og forutsi situasjoner der individet *opplever* at dets personvern har blitt krenket (Nissenbaum 2010). På tilsvarende vis skal jeg gå frem for å utforske hvordan informantene vurderer personvern, med tanken om at de selv definerer hva personvern er gjennom situasjonene de har erfart og vurderingene de tar ut fra dem.

I oppgaven brukes derfor begrepet personvern som et løst begrep for å beskrive *personlig, digital informasjon som er viktig å verne om*. På denne måten kan jeg romme alle forståelser som informantene har kommet med om personvern på nett.

Begrepet *personlig informasjon* skal bli brukt som et samlebegrep i oppgaven til å definere innhold som inkluderer bilder, videoer, meldinger, betalingskortopplysninger og passord, i tillegg til brukeratferd som kjøpshistorikk, nettleserhistorikk, lokasjonshistorikk og tilsvarende. Informantene definerer hva som er viktigst for dem ut fra mange forskjellige variabler, så jeg har valgt å beholde en noe flytende definisjon. Jeg vil trekke frem en mer spesifikk betegnelse av informasjon når det er behov for det.

Jeg skal nå over til ulike andre perspektiver på personvern som vi skal bruke for å forstå informantenes vurderinger og påvirkningene av vurderingene bedre.

2.1.1 Normativt og nøytralt perspektiv på personvern

En normativ forståelse av personvern går ut fra at personvern er et gode og et ideal i seg selv, og at det alltid bør strebes mot. Dette er et viktig utgangspunkt for utforming av personvernlovverk, der personvern blir sett på som en menneskerett (Nissenbaum 2010, 72).

En *nøytral forståelse* av personvern legger åpent for at mindre personvernsrettigheter noen ganger kan være bedre enn mer. Med en nøytral forståelse kan det argumenteres hvorvidt en funksjon, nettverk eller tjeneste på nett gir mer fordeler til samfunnet enn ulemper ved å veie individets rett til personvern opp mot eventuelle samfunnsgoder som tjenesten tilbyr. Nissenbaum mener en nøytral personvernsforståelse kan argumentere for de største fordelene i en gitt problemstilling uten å holde hverken liberalistiske eller sosialdemokratiske prinsipper som moralske ledetråder (Nissenbaum 2010, 68).

Ved å utforske hvordan informantene vurderer personvern, kan dette også innebære at de definerer dette forskjellig. Jeg skal derfor definere personvern og informasjonen som personvern belyser ut fra to forskjellige teoretiske tradisjoner. De to mest brukte teoritradisjonene innenfor akademisk forskning tar utgangspunkt i at personvern enten er en form for kontroll eller maktutøvelse, eller en begrensning på tilgang til informasjon (Nissenbaum 2010, 70). I analysen av datamaterialet benyttes det forskjellige teorier innenfor begge disse teoritradisjonene, i tillegg til andre perspektiv utenfor disse. Jeg skal nå gå i gang med å beskrive dem.

2.2 Overvåkning som makt og kontroll

Denne forståelsen handler om at jo mer informasjon en part får kontroll over, jo mer makt får de. Forskning som baserer seg på å se på personvern ut fra et makt- og kontrollperspektiv snakker ofte om personvern som noe som man kan miste kontroll over (boyd 2014, 60). Andre perspektiv beskriver hvordan mennesker kan komme i en maktposisjon ved å få tilgang til informasjon. Denne forståelsen blir derfor oftest tillagt et normativt perspektiv, at personvern er et ideal i seg selv og noe man må verne om for ikke at andre skal få makt og innflytelse over en. Michel Foucault beskriver overvåkning som et maktforhold der overvåkeren har makt over den som blir overvåket (Foucault 1977). Overvåkning og innsanking av personinformasjon vil med dette perspektivet sees på som en form for makt og kontroll, for eksempel som at myndigheter og selskaper havner i en maktposisjon jo mere de vet om brukernes og innbyggernes nettatferd og interesser. Flere personvernsteorier forholder seg til dette perspektivet, som vi skal se nærmere på senere i kapittelet.

2.2.1 Overvåkningsprinsippene til panoptikon

Jeremy Bentham designet et fengselssystem på slutten av 1700-tallet der vokteren hadde mulighet til å se alle fangene i cellene deres fra et vakttårn, mens fangene hverken kunne se vokteren eller vite om han så på dem (Bentham 2018). Med dette fengselssystemet mente han det trengtes færre voktere, siden fangenes usikkerhet om de ble iakttatt eller ikke ville hindre dem fra dårlig oppførsel som rømningsforsøk og vold. 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). Michel Foucault beskriver Benthams prosjekt slik:

> He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection (Foucault 1977, 202–3)

Bentham mente dette prinsippet med subjekters internalisering av overvåkning kunne videreføres til samfunnsinstitusjoner som skoler, sykehus, sinnssykehus og fabrikker for å forbedre produksjon, effektivitet og færre overvåkere (Bentham 2018). Michel Foucault tok utgangspunkt i Benthams idè om panoptikon da han utviklet sin sosiologiske teori om overvåkning, makt og kontroll i sin avhandling «Discipline and Punish, the birth of the

prison» (Foucault 1977). Foucault brukte Panoptikon som en maktmekanisme og en metafor for det moderne overvåkningssamfunn. Foucault argumenterer for at Benthams prinsipper er videreført i datidens samfunn som følge av kulturelle skifter og teknologiske fremskritt. Samfunnenes disiplinering gjennom trusselen om overvåkning fungerer ifølge Mathisen på samme måte for samfunnsmedlemmene som for fangene.

> It is the normalizing gaze of panopticism which presumably produces that subjectivity, that self-control, which disciplines people to fit into a democratic capitalist society. (Mathiesen 1997, 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, idet de alle har potensiale til å "avsløre" oppførsel som ikke samsvarer med samfunnets lover (Bauman og Lyon 2013).

Som en forklaringsmodell for maktmekanismer i det moderne overvåkningssamfunnet har modellen som Foucault argumenterer for fått mye kritikk. Den mest vesentlige problematikken i forhold til denne teorien er at den var ment for et fengselssystem på 1700-tallet. Lyon og Bauman argumenterer for at teorien fortsatt kan være relevant i miljøer som tilsvarer utgangspunktet; fengsler, flyktningeleirer, byområder med høy kriminalitet og tilsvarende, men at den er uegnet til å forklare mye om det vestlige, postmoderne internettsamfunn (Bauman og Lyon 2013). Teorien kan også være aktuell i «digitale diktatur» der regimer overvåker sine innbyggere, i tillegg til å beskrive hvordan for politi og etterretningstjenester sporer opp kriminelle ved hjelp av overvåkning og digitale spor. Et eksempel på dette er Kinas nye digitale poengsystem for sine borgere. Dette nettbaserte, sosiale poengsystemet er ment å differensiere mellom borgere som er lovlydig og pliktoppfyllende, og borgere som ikke er det (Ma 2018). «Negativ oppførsel», som det å få bøter for å kjøre for fort, røyke i områder det ikke er lov å røyke, og å kjøpe mange dataspill trekker ned den sosiale poengsummen, og fører til at borgerne mister fordeler som muligheten til å reise ut av landet (Ma 2018). Dette kan argumenteres for å være et eksempel på hvordan myndigheters digitale overvåkning kan tolkes ut fra makt- og kontrollperspektivet til Foucault. For å beskrive en mediehverdag for norske brukere som som er beskyttet av lovgivning og egne sikkerhetstiltak er derimot teorien mindre aktuell. Norske myndigheter og selskaper er underlagt strenge lover og reguleringer, og det er derfor begrenset hva den innsamlede personinformasjonen og nettatferden kan brukes til. Det vil likevel være områder der et panoptisk perspektiv vil komme til nytte i oppgaven, i tillegg til at flere av modellene

som tar utgangspunkt i Panoptikon være interessante å anvende. Vi skal nå ta for oss de mest relevante for dette perspektivet.

2.2.2 Lateral Panoptikon

Mark Andrejevic introduserer begrepet *Lateral Panoptikon* som en teori for å bedre forstå panoptiske prosesser i dagens mediesamfunn (Andrejevic 2006). Han mener med dette at alle overvåker alle i form av rapporteringsfunksjoner, og at sosiale medier gjør oss alle til spioner. Teorien forsterker derfor Foucaults opprinnelige panoptikon-teori ved å forsterke ovenfra og ned-overvåkningen til nasjonale byråer for sikkerhet, som amerikanske FBI og norske PST. I tillegg kan teorien omfatte digitale medieplattformer som utformer retningslinjer ved at brukerne oppfører seg som individuelle overvåkere som rapporterer inn profiler, innlegg og oppførsel som ikke er forenlig med plattformens regler. Andrejevic argumenterer for at disse mekanismene for tilbakemelding både forbedrer de digitale plattformenes overvåkningsfunksjoner, og bidrar til at brukerne føler at de selv er med på å ivareta deres egen sikkerhet. (Andrejevic 2006)

Teorien kan også omfatte hvordan mennesker spionerer på andre mennesker i hverdagen, 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 ut informasjon om andre (Andrejevic 2004).

2.2.3 Synoptikon

Begrepet *Synoptikon*, også kalt polyoptikon, har sitt opphav fra den norske sosiologen Thomas Mathisen (2013). Mathiesens teori bygger på idèen om Panoptikon, men i motsetning til panoptikon-metaforen der en vokter passer på mange fanger, snur Mathisen på det og hevder at "de mange vokter de få". Denne teorien utelukker ikke at panoptikon-prosesser eksisterer i samfunnet, men er ifølge Mathiesen ment å beskrive prosesser som supplerer den. Mathiesen mener det norske samfunnet har flere elementer av panoptiske prosesser: økende overvåkning av fanger, løslatte i samfunnet, potensiale lovbrytere i databaser, oversikt i psykiatrien, skoler, medisiner blant annet. Alle disse er verktøy som har mulighet til å å fange opp problematiske, kriminelle elementer i samfunnet, og Mathiesen mener disse verktøyene må sees i sammenheng med den synoptiske modell han presenterer (Mathiesen 2013, 36–45).

Synoptikon legger også opp til at overvåkerne kan bli overvåket og korrigert, for eksempel gjennom hvordan nyhetsmediene som blir omtalt som «den fjerde statsmakt» passer på de tre øvrige statsmakter i samfunnet. Og disse kan igjen bli overvåket og korrigert, som vi har sett i den nylige VG-skandalen hvor det ble mistenkt at en VG-journalist fabrikkerte et sitat for å sverte AP-politikeren Trond Giske (Fossheim, Sørsdahl, og Fremstad 2019). Synoptikon legger derfor opp til en to-veis overvåkningsperspektiv, der både institusjoner med makt og vanlige folk overvåker hverandre.

Tv-serien "How to make a murderer" er et eksempel på hvordan disse to systemene komplementeres. Serien fikk et enormt mediefokus, noe som førte til at «de mange» utøvde kritikk av det amerikanske rettsvesenet og politivesenet som etterforsket saken (Judah 2016). Dette førte til at saken ble tatt opp igjen i rettssystemet (*BBC News* 2019). Det må riktignok sies at dette er en røff forklaringsmodell for hvordan slike prosesser i overvåkningssamfunn kan fungere. I tillegg kan prosesser som synoptikon beskriver også føre til en mobb-kultur der lov og rett på ingen måte blir representert, i tillegg til å bli manipulert av aktører fra næringslivet og lobbyorganisasjoner. Dette gjør slike bevegelser sårbare og uforutsigbare.

2.3 Kontekstuelle personvernsmodeller

Kontekstuelle personvernsmodeller ser på personvern ut fra en forståelse om at tilgang til personinformasjon[1] og omstendighetene rundt dette er hovedårsaken til personvernskonflikter på nett (Nissenbaum 2010). Med dette perspektivet er altså ikke innsanking og arkivering av nettatferd og informasjon i seg selv nok til å definere ujevne maktforhold eller maktmisbruk, men også aspekter som hvem som får tilgang til informasjonen, på hvilken måte tilgangen ble gitt og i hvilken kontekst, blant annet. Begrensning av tilgang er derfor i fokus i teorier som Kontekstuell integritet av Helen Nissenbaum (2010).

Personvernskonflikter oppstår i denne sammenheng når parter som brukerne enten ikke har visst om eller ikke har gått med på å gi tilgang til plutselig får tilgang til informasjonen deres. Dette kan være basert på at brukerne ikke visste om hva som ble hentet inn og brukt av informasjon da de lagde profilen sin, enten ved at brukerne ikke undersøkte dette godt nok eller at informasjonen rundt dette var obskur. Det kan også være snakk om tilfeller der tilgangen til brukerinformasjonen deres blir tilegnet på ulovlig vis (Nissenbaum 2010).

[1] Med informasjon menes alt av personinformasjon, brukeratferd, innhold delt og sendt, et cetera.

Cambridge Analytica-saken er et godt eksempel på dette, der brukere av appen Cambridge Analytica benyttet seg av på Facebook ga firmaet tilgang til nettatferd og personinformasjon til brukernes Facebook-venner som ikke hadde godkjent dette (Cadwalladr og Graham-Harrison 2018). Christopher Wylie, tidligere medarbeider ved Cambridge Analytica, forteller hvordan selskapet bearbeidet denne brukeratferden til å utnytte kunnskapen om brukernes «indre demoner» til å overtale dem (Cadwalladr og Graham-Harrison 2018).

Et annet eksempel er saker der hackere får tilgang til selskapers databaser med brukerpassord, og tilbyderen av den digitale tjenesten vanligvis får skylden for ikke å ha sikret seg godt nok mot dette. Et eksempel på dette er saken fra 2017 med Yahoo. Et sikkerhetsbrudd hadde oppstått fra Yahoos side da de ba brukerne sine om å bytte passord, og hackere fikk derfor tilgang til passordene til selskapets 3 milliarder brukere (Larson 2019). Som med denne saken, blir selskapene ofte beskyldt for dårlig sikkerhet i media, selv om dette ikke nødvendigvis har vist seg å være negativt for selskapers omdømme i et langtidsperspektiv.

Denne personvernforståelsen utvider derfor forståelsen av menneskers oppfatning av personvern og sikkerhet på internett både i sosiale, mellommenneskelige kontekster og med hensyn til folks reaksjoner til informasjonsnettverk, og tilfører ofte en mer nøyaktig vurdering av saker og konflikter som oppstår rundt personvern på nett. Personvernsforståelse ut fra tilgang omfatter derfor ikke bare forholdet mellom bruker og institusjon, men også bruker til bruker. Sosiale personvernskonflikter på nett kan forklares med den samme terminologien og forståelsen for tilgang, noe vi skal se nærmere på i analyse- og diskusjonskapitlene.

I danah boyds tidligere nevnte forskningsstudie om amerikanske tenåringer fremhever hun hvordan kontekst er viktig for å forstå ungdommenes forhold til personvern, og hvordan de sosiale nettverkene som utspiller seg i de ulike sosiale medieplattformene påvirker ungdommenes forhold til skjerming av eget privatliv (boyd 2014). Boyd argumenterer for at menneskers syn på personvern er avhengig av de sosiale kontekstene og de teknologiske nettverkene de er en del av på nett. Tilgangen til sosiale medier har ført til en dyptgripende endring i personvernsfeltet og har derfor forandret hvordan unge mennesker oppfatter og vurderer personvern. For eksempel kan ikke tenåringene kontrollere at andre ikke videredeler informasjon og innhold av dem selv i slike informasjonsnettverk, spesielt ikke når de teknologiske forutsetninger har gjort dette enklere å utføre enn før (boyd 2014).

Kontekstuelle personvernsmodeller tar altså for seg det sammenknyttede sosiale- og nettverksaspektet ved dagens sosiale mediesamfunn. I bruk kan kontekstuell teori derfor bidra

til å forklare hvordan digitale medieplattformer som Facebook og Snapchat har forandret hvordan unge voksne tilnærmer seg personvern, at de fortsatt har dette i tankene i hverdagen og at de praktiserer det på ulike måter.

2.3.1 Kontekstuell integritet

Kontekstuell integritet er en teoretisk modell for analysering og evaluering av hvordan sosioteknologiske kontekster påvirker personvernsforståelsen til de som bruker dem (Nissenbaum 2010). Teorien omhandler hvordan folk oppfatter at det har oppstått brudd på deres forventninger til eget personvern i spesifikke kontekster. Dette kan også innebære at personvernlover har blitt overtråkket samtidig, men ikke nødvendigvis. Teorien kan derfor være et godt redskap til å redegjøre for når systemer eller kontekster legger opp til personvernskonflikter, hvor det bør bli utviklet personvernslovverk, eller hvordan eksisterende lovverk kan bli utvidet. Den er også et bra verktøy for å analysere informantenes vurderinger rundt personvern (Nissenbaum 2010).

Sosioteknologiske systemer blir beskrevet av Nissenbaum som «sosial» teknologi som knytter mennesker sammen på nye og revolusjonerende måter, slik som telefonen, fjernsynet, datamaskinen og til og med biler gjorde (Nissenbaum 2010, 4–6).I oppgavesammenheng er internett det et eksempel på et slikt sosioteknologiske system, men sosiale nettverksplattformer som Facebook og Snapchat kan naturligvis også sees på som sosioteknologiske systemer.

Appropriering av informasjonsstrøm

Nissenbaum definerer personvern gjennom kontekstuell integritet som retten til å appropriere informasjonsstrøm i forskjellige sosiale kontekster (Nissenbaum 2010, 126). For eksempel kan dette gå ut på hvordan digitale aktører lagrer og benytter seg av brukeres atferd på sine nettsider. Dersom en bruker søker etter ølbryggingsutstyr en dag, og så plutselig ser masse annonser om slikt utstyr etter dette, kan det oppleves som ubehagelig av brukeren.

Et mer dramatisk eksempel på en slik personvernskonflikt oppstod med butikkjeden Targets målrettede markedsføring i USA. Target benyttet seg av algoritmer for sine brukeres nettaktivitet, i dette tilfellet var det ut fra hva tenåringsdatteren i huset tidligere hadde søkt på på deres nettside. Kjeden sendte derfor rabattkuponger på babyprodukter til henne i posten før faren var klar over at hun var gravid, noe som resulterte i at han fant ut av det (Hill 2012).

Dette viser at selv om alle personvernlover overholdes, kan det altså oppstå situasjoner som brukerne opplever som ubehagelige og negative (Pole i Hill, 2012).

Personvern gjennom rett til appropriering av informasjon kan også gå ut på forventninger i sosiale kontekster om at innhold ikke tas ut av konteksten og at andre ikke videresender dette. Det som vises til den nære familien blir kanskje ikke vist til venner og bekjente. Nære venner kan ha flere forskjellige grupper der de sender meldinger og deler bilder de ikke vil ha delt i andre grupper. Brukere av sosioteknologiske tjenester som Facebook forventer også at denne informasjon blir beskyttet fra andre brukere gjennom sikkerhetstiltak, og at ikke det slurves med sikkerhetsbrister og beskyttelse mot hacking. Med andre ord har brukere på internett visse forventinger om hvordan ting bør være. Nissenbaum kaller disse forventingene for informasjonsnormer, noe vi skal se nærmere på senere (Nissenbaum 2010, 127).

Rammeverket til kontekstuell integritet

Nissenbaum baserer sin teori med utgangspunkt i Ruth Gavisons anerkjente tekst «Privacy and the limits of law» (Gavison 1980). Gavison argumenterer for at privacy/personvern er en begrensning av tilgang som andre personer får til et individ (Gavison 1980, 428). Hun lister opp tre premisser for når et individ opplever at sitt personvern blir innskrenket eller tapt (Gavison 1980, 429–33):

- **Hemmelighold** (En part får informasjon om et individ)
- **Anonymitet** (En part gir oppmerksomhet til et individ)
- **Ensomhet** (En part får fysisk tilgang til et individ)

Premisset for Nissenbaums teori er at folks opplevelse av personvern på nett ikke baserer seg på hverken hemmelighold, Gavisons første premiss, siden hun mener premisset for å delta på nettet forutsetter en gjensidig utveksling av informasjon mellom bruker og tjenesteleverandører. I likhet med Gavison mener Nissenbaum at kontrollbaserte personvernsteorier heller ikke er relevante for å forstå sosiale kontekster på nett. Og siden fysisk tilgang til individer ikke er aktuelt i sammenheng med personvern på nett, gjenstår anonymitet: oppmerksomhet gitt til et individ (Nissenbaum 2010, 68). Nissenbaum argumenterer for at det er uproblematisk for folk at ens aktivitet på nett blir arkivert og analysert, iallfall at dette er en aktivitet som folk går med på når man bruker internett, lager profiler og kjøper varer på nett. Derimot blir approprieringen av informasjonsflyten området som det kan oppstå konflikter rundt, hvordan denne aktiviteten og informasjonsflyten blir

brukt av aktører i forskjellige kontekster, eller hvordan konteksten i seg selv legger opp til personvernbrudd. Nissenbaum kaller disse konfliktene for brudd i den kontekstuelle integriteten, eller det kortere begrepet *integritetsbrudd*, og mener at grensene for dette varierer fra kontekst til kontekst. (Nissenbaum, 2010:127)

For å bruke det teoretiske rammeverket i oppgaven, må visse parametere for å analysere når en informasjonsnorm har blitt brutt først bli presentert og forklart.

Kontekstuell integritet veksler mellom flere typer offentligheter i stedet for den vanlige privat/offentlig-dikotomien. Nissenbaum mener at offentlig/privat-problematikken er en veldig forenklet og ufullstendig forklaring på hvordan sosiale kontekster oppfattes på nettet, at man enten er privat eller offentlig. Hun argumenterer heller for at det eksisterer en mengde ulike sosiale *kontekster* med hver sine normer og regler for å håndtere informasjonsflyt (Nissenbaum 2010, 141). Ut fra dette oppstår det mange forskjellige offentligheter med ulikt tilgangsnivå og spesifikke forventninger. Nissenbaum kaller disse for kontekster og informasjonsnormer.

Idèen om kontekst som en ansamling forståelser, handlinger, roller/utøvere og regler som utgjør en felles forståelse av et sosialt område eller felt. Dette oppstår i alt av det sosiale liv: akademia, journalistikk, næringslivet og lignende (Nissenbaum 2010, 131–32). På nettet kan eksempler på kontekster inkludere alt fra Facebook-grupper, meldingstråder på Facebooks meldingstjeneste Messenger, kontaktnettverket til en sosiale-mediebruker eller kommentarfeltet til en avis.

Nissenbaum mener ulike kontekster har ulike *normer* og forventninger til oppførsel. Dersom normene i en gitt kontekst overskrides, erfarer brukeren dette som et brudd på den kontekstuelle integritet: et brudd på forventingene til hvordan brukeren selv, brukerens innhold eller brukerens personinformasjon blir videreformidlet eller brukt i sammenhenger brukeren ikke ønsker (Nissenbaum 2010, 127). Aktører, systemer eller praksiser kan alle overskride slike *informasjonsnormer*. Nissenbaum viser til Cristina Bicchieri, som skiller mellom to hovedtyper av informasjonsnormer (Bicchieri 2000, 156):

- **Injunktive normer -** normer: Normer som folk mener burde bli fulgt, atferd som bør eller ikke bør gjøres, etc.
- **Deskriptive normer** – Normer som ikke trengs å følges, men som de fleste andre følger.

Nissenbaum skiller mellom tre ulike *aktører*: Den som sender informasjonen, den som mottar informasjonen, og den informasjonen handler om(informasjonssubjektet). Sender og subjekt kan være det samme (Nissenbaum 2010, 141).

Egenskapene ved informasjonen som blir sendt bestemmer også viktigheten av informasjonen. Det kan være snakk om en bankutskrift, en kvittering fra et kjøp, et bilde sendt i melding, eller en video publisert på Instagram. Informasjon med visse type egenskaper er akseptabelt å sende til visse typer aktører.

Overføringsprinsipper omhandler hvordan informasjonsflyten skal og ikke skal foregå (Nissenbaum 2010, 140). Eksempler på ulike typer overføringsprinsipper omfatter:

- Konfidensialitet – mottaker får ikke lov til å dele informasjonen mottatt med andre.
- Resiprositet – utveksling av informasjon har en fordel for både sender og mottaker.
- Dessert – en aktør fortjener å motta informasjon.
- Entitlement – en aktør mener han har krav på å motta informasjon.
- Compulsion – en aktør føler for å sende informasjon.

Disse teoretiske prinsippene skal jeg hovedsakelig bruke i analysen av informantenes vurderinger av personvern på nett. Men det trengs også andre teorier til å analysere datamaterialet, som jeg skal ta for meg nå.

2.4 Flytende overvåkning og fryktfaktoren

David Lyons tidligere nevnte teori om flytende overvåkning handler om hvordan systemer med potensiale for overvåkning fungerer autonomt i samfunnet. Lyon forklarer hvordan 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 arbeidsgivere og skatteetaten, internettleverandørers tilrettelegging av nettjenester, og tilsvarende. Alle disse systemene trekker ut en viss mengde av informasjon fra sine brukere for å fungere. Slike prosesser fungerer autonomt og «usynlig» for brukerne av dem. Lyon mener at jo mer usynlig denne *flytende overvåkningen* er, jo lettere er det for brukerne å «glemme den», å ikke tenke over den. (Bauman og Lyon 2013)

David Lyon, i likhet med sosiolog Thomas Mathiesen (Mathiesen 2013), mener frykten for terror og kriminalitet fører til at mennesker i større grad aksepterer overvåkningstiltak på bekostning av eget personvern. Lyon kaller dette for *fryktfaktoren* (Bauman og Lyon 2013). Lyon mener at denne aksepten i verdenssamfunnet har økt etter terrorangrepet mot World Trade Center i 2001, blant annet med økte sikkerhetskontroller på flyplasser og en økende aksept av statlige etaters innsyn i digitale mediekontoer. (Bauman og Lyon 2013). Detten mener han kan bidra til å forklare hvorfor statlig overvåkning generelt aksepteres i frykt for terror.

3 Metode

I dette kapittelet skal jeg beskrive de akademiske forskningsmetodene jeg har brukt, hvordan jeg har kommet frem til problemstilling, hvordan jeg har gått frem i utvalget av informanter, utforming av intervjuguide, gjennomføring av intervjuer og etiske hensyn jeg har forholdt meg til. Først skal jeg fortelle om kvalitativ metode og hvorfor jeg valgte å bruke det i studien.

3.1 Valget om å bruke kvalitativ metode

I utgangspunktet var jeg interessert i å skrive om personvern på sosiale medier etter all negativ kritikk som de store medieselskapene Facebook, Google og Snap Inc. hadde fått i mediene. Jeg vurderte først tekstanalyse av nyhetsartikler om personvern på nett, men etter å ha lest gjennom en del artikler var mitt inntrykk at det var et uforholdsmessig skjevt fokus på skandaleoppslag i tilknytning til problematikken. I tillegg var perspektivet både i nyhetsartikler og forskningsartikler hovedsakelig fokusert på tekniske aspekter: hva brukerne aksepterte i brukervilkårene, hvor mye personinformasjon som ble videresolgt, hva som ble arkivert og så videre. Mye av forskningen artiklene baserte seg på var såkalte *kvantitative studier,* studier som baserte seg på spørreundersøkelser og surveys, gjerne besvart over nett. Dette ble gjerne etterfulgt av fagpersoner som ikke kunne forstå hvorfor folk tillot dette. Jeg syntes med andre ord personvern på nett ble fremstilt ganske endimensjonalt i media, og at det oftest ble tatt opp som en reaksjon på at noe galt hadde skjedd. De kvantitative metodene i forskning det ble tatt utgangspunkt i, synes jeg heller ikke forklarte særlig mye om motivasjonen som lå bak de ulike besvarelsene. Jeg savnet med andre ord dypere og grundigere studier av mediebrukeres personvernsforståelse innenfor akademisk forskning; forskning som tydeligere forklarte årsaker og grunner til mediebrukernes nettvaner, og som ut fra dette forklarte hvordan og hvorfor brukerne av nettjenester forholdt seg til nettopp personvern på nett.

3.2 Kvalitativ metode

Kvalitativ intervjuform er en forskningsmetode som muliggjør en åpen og utforskende tilnærming til temaet (Bryman 2016, 466–67). Metoden legger opp til ganske åpne spørsmål med spesifikke «topics», og en samtaleform på intervjuet (Gentikow 2005). Planen var å

gjennomføre intervjuene først og siden ta tak i hva jeg oppfattet som interessant eller spesielt, og formulere en problemstilling ut fra funnene. Kvalitativ intervjuform ga meg også mulighet til å ta tak i hva som var interessant og bruke såkalt *boreteknikk*, en teknikk der intervjueren spør mer om og går dypere i interessante saker som intervjuobjektet har snakket om (Gentikow 2005, 40). Gentikow argumenterer for hvordan ansikt-til-ansikt intervjuer er spesielt fruktbare i denne sammenheng fordi både intervjuer og intervjuobjekt er i en fysisk, umediert tilstedeværelse sammen. Dette kan gjøre det mer naturlig å bruke «boreteknikk» i en samtale, det kan også gjøre det lettere å se helheten av et svar enn i for eksempel kvalitative telefonintervju, der intervjuer ikke ser ansiktsmimikk, kroppsspråk, og lignende. Å være i samme rom og få med seg denne informasjonen kan bidra til å unngå misforståelser rundt besvarelser (Gentikow 2005, 84).

Kvalitativ metode byr riktignok også på utfordringer i forskningsprosessen, spesielt når det kommer til bearbeiding av datamaterialet. Erfaringen jeg ønsker å få informantene til å formidle verbalt er ifølge Gentikow «pre-refleksiv […], den er ikke gjennomtenkt og den er ikke formulert i ord» (Gentikow 2005, 67). Det kan derfor by på utfordringer å få informantene til å ta stilling til saker, emner og problematikk som de ikke har reflektert rundt i forkant (Gentikow 2005, 67–68). Dette har vært viktig for meg både i utforming av intervjuguide, gjennomføring av intervjuene, og i analysearbeidet av datamaterialet. Dette inkluderer blant annet å sette spørsmålstegn til om informantene vet hva de svarer på, og om intervjusituasjonen får informantene til å svare forhastet. Kommentarer i løpet av intervjuet som på overflaten ser ut som om informanten motsier seg selv og sine meninger, kan også vise seg å handle om forskjellige ting, bare at informanten kanskje har formulert seg litt uheldig (Gentikow 2005).

Med *semistrukturerte intervju* menes det at forskeren forholder seg til en intervjuguide med enten spesifikke spørsmål eller forskjellige temaer. En del fleksibilitet er mulig gjennom at forskeren ikke trenger å følge den samme spørsmålssettingen eller rekkefølgen slavisk for hver informant, men passer på å spørre de ulike informantene om de samme temaene eller spørsmålene i løpet av hvert intervju. Muligheten for at informantene kan snakke om temaer som er utenfor intervjuguidens rammer, som opptar dem spesielt og som potensielt kan berike datamaterialet, blir sett på som positivt i denne sammenheng (Bryman 2016, 428).

Intervjuguiden i denne oppgaven ble utformet med tanke på å legge opp til uformelle samtaler om utvalgte temaer knyttet til personvern, sosiale medier og digitale medieselskaper. Muligheten til å ha en fleksibel rekkefølge på temaer i intervjuet viste seg å være praktisk for

meg de gangene informantene begynte å snakke om nær beslektede temaer på egen hånd. Ved å la dem gjøre dette uten å avbryte dem, følte jeg at flyten gikk mye lettere i hvert intervju, i tråd med hva Thomas Lindlof kaller for «en konversasjon med en hensikt» (Lindlof 1995, 163) Samtalen har et formål, den er strukturert, men den innehar også den sosiale samtales spontanitet, dynamikk og flyt (Gentikow 2005, 88).

3.3 Forskningsdesign

Den åpne tilnærmingen til tematikken preget utformingen av intervjuguiden i stor grad. Jeg jobbet ut fra den midlertidige problemstillingen «Hvordan forholder informanter seg til personvern i sosiale medier», og ønsket som problemstillingen sier å finne ut hva slags holdninger og meninger unge, norske sosiale mediebrukere hadde til personvern i sosiale medier.

Etter to runder med pilotstudier endte jeg opp med seks forskjellige hovedspørsmål som jeg utformet intervjuguiden ut fra. Disse var bygd på generell forskning rundt personvern, personvernsteorier, forskningsartikler om unge voksne og personvern på nett, nyhetsartikler og erfaringen etter prøveintervjuene.

Temaer i intervjuguiden:

- Bakgrunn til informanten

  Dette var mest for å komme i gang med intervjuet og for å få muligheten til å bli kjent med informanten, som i vanlige sosiale situasjoner.

- Informantens medievaner

  Her ønsket jeg å få en oversikt over hvilke medier informantene bruker i hverdagen, spesielt sosiale medier. Dette var for å bedre forstå hver enkelt informants digitale kompetanse og interesse for sosiale medier.

- Hvor informerte er informantene om personvern knyttet til sosiale medier?

Her ønsket jeg å finne ut mer om hver enkelt informants kompetanse og kunnskap om personvern[2].

- Hva er informantenes holdninger til store medieselskaper som Facebook, Google og Snap Inc?

  Her ønsket jeg å undersøke om informantene var positivt eller negativt disponerte overfor selskapene bak de største sosiale medieplattformene i Norge. Ser de på medieplattformene mest som systemer eller aktører?

- Hva er informantenes holdninger til overvåkning?

  Her ønsket jeg å finne ut hvordan informantene forholdt seg til begrepet *overvåkning*, om de noensinne følte seg overvåket selv, og hvordan personvern spiller inn i dette.

- *Hva slags opplevelser har informantene hatt som har vært negative på nett?*

  Hvem legger informantene skylden på for de negative opplevelsene? Hvordan resonnerer de over slike opplevelser?

- *Hvordan vil informantene reagere på problematiske aspekter ved personvern i sosiale medier? Lese og diskutere.*

  Dette ble representert gjennom 3 artikler som informantene leste på slutten av intervjuet. Jeg prøvde å velge ut artikler som ikke moraliserte for mye, men som relativt nøytralt beskrev fenomener på nett mellom medieselskaper og brukere som det kan problematiseres rundt. Her er en oversikt over og kort beskrivelse av artiklene:

  - «I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets" (Duportail 2017)

    Artikkelen i The Guardian tok opp problematikken med at medieselskapene bak tjenester som Tinder og Facebook lagrer all mulig informasjon om sine brukere, gjerne informasjon om atferd som brukeren ikke er klar over.

[2] Eksempler: Leser informantene brukervilkårene før de installerer digitale produkter, kjenner de til personvernlovverk som GDPR, vet de hva de digitale medieselskapene og myndighetene har mandat til å gjøre med brukerdataen deres.

- «Google may be quietly tracking everywhere you go – here's how to turn it off» (Price 2017)

  Artikkelen i Business Insider beskriver hvordan Google Maps arkiverer hvor brukeren befinner seg geografisk til alle tider, hvordan dette kan vises på en tilleggsfunksjon på Googleprofilen, og hvordan man kan slå den av.

- «Gay? Conservative? High IQ? Your Facebook likes can reveal traits» (Boyle 2013)

  Den siste artikkelen i NBC News demonstrerte hvordan en gjennom Facebook-likes kan lage psykologiske profiler over hver bruker, og hvor eksakt denne teknikken var. Teknikken, kalt *psykometri* av psykologiforsker Michal Kosinski har i senere tid blitt koblet til innblanding i det nyligste amerikanske presidentvalget og Brexit-avstemningen i Storbritannia (Sjøberg 2019). Artikkelen som ble valgt beskriver fenomenet relativt nøytralt, og viser potensialet for hvor mye selskapene kan finne ut om brukerne sine med relativt lite informasjon. For det første ville jeg med denne artikkelen finne ut om informantene husket disse sakene, og kunne se sammenhengen mellom dem. Dersom de ikke husket dem, ønsket jeg å se hva de syntes om en slik teknologi, og hva slags formål den kan bli brukt til.

Som hovedspørsmålene viser, hadde jeg et fokus på hva informantene mente om personvern overfor medieplattformer og statlige institusjoner. Hva som kom frem i intervjuene ble også til et ekstra tema i oppgaven:

- Hvordan vurderer informantene personvern ut fra andre brukere på nett?

Dette temaet kom frem i løpet av intervju- og analyseprosessen ut fra hvordan informantene fokuserte på personvern som noe de gjorde overfor andre brukere. Dette vurderte jeg som såpass viktig for hvordan informantene ser på personvern at jeg ga det større plass i oppgaven og tok det med som en del av problemstillingen.

I tillegg tok informantene opp flere historier knyttet til personverntematikken som omhandlet medieplattformene Google og Youtube. Selv om det er en del forskjeller mellom hvordan informantene vurderer personvern overfor sosiale medier og Googles og Youtubes tjenester, er det mange andre ting som overlapper. Jeg har valgte derfor også å inkludere disse to medieplattformene i tillegg til de sosiale medieplattformene. Googles tjenester vil bli mest

omtalt i oppgaven og Youtube vil bli brukt i noen eksempler informantene tar opp. Det er fortsatt et større fokus på de sosiale medieplattformene gjennom oppgaven, siden tjenestene disse tilbyr omfattet flest personvernvurderinger for informantene.

3.4 Erfaringene etter pilotstudiene

Etter å ha gjennomført pilotstudier med 4 prøveintervjuer, gjorde jeg en del viktige forandringer på intervjuguiden. Et tidlig fokus på identitet ble forlatt til fordel for et fokus på de sosiale medieplattformene og negative sider ved nettbruk. Bruken av såkalte *assosiasjonsord*, der informantene skulle komme med tre assosiasjoner for hvert ord, ble også forlatt (Gentikow 2005, 92). Jeg syntes ikke dette fungerte bra nok, og det ødela litt flyten i samtalen å plutselig stoppe opp og komme med disse assosiasjonsspørsmålene.

Artiklene som problematiserte personvernstematikk ble også lagt til som en del av intervjuene. Jeg valgte å la informantene lese artiklene til slutt for at informasjonen i artiklene ikke skulle farge resten av intervjuet. Artiklene var ment å fange opp meninger og holdninger informantene kanskje ikke hadde fått frem i intervjuet, for å se hva slags reaksjoner de muligens ville fremkalle, og for å vite om de visste om noe av hva som kom frem i artiklene.

En annen erfaring jeg fikk etter prøveintervjuene var at informantene ikke nødvendigvis hadde en klar, statisk forståelse av personvern. De snakket om personvern, sikkerhet og privatliv på nett som om dette var dynamiske aspekter av mediebruk på nett, som noe som var oppe for diskusjon og redefinering, og som noe som kunne byttes bort mot enkelte goder. Jeg utformet derfor intervjuguiden med dette i bakhodet. Guiden ble som sagt tilpasset en semistrukturert intervjuform, med ulike temaer og eksempelspørsmål under hvert tema.

Utvalget av temaer i intervjusituasjonen kunne ideelt sett vært nærmere den endelige problemstillingen for å få mer utfyllende svar. På den annen side ville jeg ikke kommet frem til problemstillingen om ikke jeg hadde valgt en bred problemstilling i utgangspunktet, så dette ser jeg på som et nødvendig ledd i arbeidet med oppgaven.

3.5 Informantene

Gentikow anbefaler minst 10 informanter for en kvalitativ studie. Jeg endte opp med 11, som er innenfor denne anbefalingen (Gentikow 2005, 77). Som tidligere nevnt syntes jeg gruppen jeg valgte var interessant på grunnlag av at de mer eller mindre har vokst opp med sosiale

medier og internett, og at det ikke har blitt utført så mye medieforskning på hva dette alderssegmentet mener om personvern på nett. Avgrensingen av alder med en spredning på 5 år valgte jeg også på et generelt grunnlag for å mest mulig demme opp for aldersspesifikke forskjeller i en studie med et såpass lite antall informanter. Jeg ønsket i utgangspunktet å få med noen informanter som var i arbeid og ikke studerte, men lykkes ikke med dette, og utvalget består derfor utelukkende av studenter. Dette hadde nok vært viktigere i et kvantitativt studium, der demografiske forskjeller, sammenhenger og representative utvalg er viktigere å undersøke enn i kvalitativ forskning, der dypdykk inn i tematikken og rike besvarelser er viktigere. Det er heller ikke nødvendigvis noen grunn til å tro at unge voksne som jobber ville hatt noe spesielt annerledes syn på personvern på nett enn hva studenter i samme alderssegment har.

3.5.1 Rekruttering av informanter

Jeg postet først innlegg om studiet på Facebook og Instagram. Overskriften til posten var «Er du mellom 18 og 23 år, bor i nærheten av Bergen og har vokst opp med sosiale medier? I så fall vil jeg gjerne bruke deg som informant til mitt masterprosjekt!» Videre forklarte teksten i innlegget om at intervjuet ville handle om sosiale medier, personvern og innholdsdeling, samt praktiske detaljer som intervjusted og hvor lang tid samtalen ville ta. I tillegg fikk jeg hjelp av venner og medstudenter i rekruttering av informanter. Etter en stund ble det vanskelig å få tak i nok informanter, og etter samtale med veileder om dette gikk jeg over til å spørre Facebook-brukere som hadde felles venner med meg direkte om de ville være med i studiet mitt.

Med unntak av de to første intervjuene som ble honorert, stilte deltakerne i studiet opp uten å få kompensasjon for dette. Utenom en genuin interesse for sosiale medier, personvern og innholdsdeling, kan dette også vise til en god sans for samfunnsengasjement og interesse for fellesskapet, noe jeg opplevde gjaldt alle informantene under intervjuene. Dette kan også anses å være en av studiens svakheter: de som var mest interessert i sosiale medier, personvern og innholdsdeling og mest kunnskapsrike om dette antakelig var de som tok kontakt og sa seg villige til å bli med i studiet. Andre svakheter er at utvalget ikke er representativt for befolkningen hverken ut fra alder eller bosted. Det er derfor viktig å vurdere informantenes holdninger og meninger i denne oppgaven ut fra disse forutsetningene.

3.5.2 Kort beskrivelse av informantene

Tabellen nedenfor viser en oversikt over informantenes demografi: navn (pseudonym, ikke deres ekte navn), alder, hjemsted, nåværende studie og hvilke sosiale medier de bruker til daglig. Alle bruker Google, så det er ikke tatt med. Bruk av Facebook Messenger regnes som Facebook i denne oversikten. For at enkelte informanter ikke skal bli gjenkjent, har jeg valgt å ikke spesifisere i hvilket årskull av studiet de er i.

Navn	Alder	Kommer fra	Nåværende studie	Medieplattfomer, daglig bruk
Jonas	21 år	Mindre by på østlandet	Folkehøyskole	Facebook, Instagram, Snapchat.
Mette	23 år	Mellomstor by på vestlandet	Bioingeniør	Facebook, Instagram, Snapchat.
Linda	20 år	Stor by på østlandet	Engelsk	Facebook, Instagram, Snapchat.
Nina	21 år	Liten by på vestlandet	HR og personalledelse	Facebook, Instagram, Snapchat.
Silje	21 år	Stor by på sørlandet	Psykologi	Facebook, Instagram, Snapchat.
Anders	19 år	Stor by på østlandet	Rettsvitenskap	Facebook, Instagram, Snapchat.
Frida	20 år	Liten by på vestlandet	Rettsvitenskap	Facebook, Instagram, Snapchat.
Anette	20 år	Stor by på vestlandet	Sosiologi	Facebook, Instagram, Snapchat.
Petter	23 år	Liten by på østlandet	Pedagogikk	Facebook, Instagram, Snapchat, Youtube.

Gunnar	21 år	Liten by i Nord-Norge	Historie	Facebook, Instagram, Snapchat.
Mari	22 år	Liten by i Midt-Norge	Musikk	Facebook, Instagram, Snapchat, Telegram (meldingstjeneste).

3.5.3 Om utvalget av informanter

Avgrensningen av utvalgets alder var viktig for meg ganske tidlig, jeg ønsket å intervjue såkalte *digitalt innfødte,* med andre ord unge voksne som har vokst opp med sosiale medier, nettjenester, nettbrett og smarttelefoner (Prensky 2001). Det at informantenes meninger om personvern var uutforsket, iallfall i forhold til tidsperiode og land, var noe av det som appellerte til meg med prosjektet. Jeg vurderte å inkludere yngre informanter på et punkt, men på grunn av intervjuenes sensitive natur i forhold til potensial tematikk som kunne bli tatt opp i forhold til deling av nakenbilder, valgte jeg å begrense utvalget til over 18 år. NSD ville krevd at informanter under 18 år måtte også få samtykke av foreldre i denne sammenheng, noe som ville vært et ekstra hinder i intervjuprosessen («NSD personverntjenester: Barnehage og skole» 2018). Jeg planla derfor å avgrense utvalget til mellom 18 og 23 år, men siden jeg ikke fikk tak i noen 18-åringer, ble utvalget avgrenset til mellom 19 og 23 år. Denne aldersgruppen vurderte jeg som unge nok til at internett og sosiale medier har spilt en stor rolle i oppveksten deres, og modne nok til å reflektere over dette. Jeg så det som en fordel å avgrense informantene til et utvalg som har vokst opp i relativt lik tidsperiode for å muligens finne ut noe om alderssegmentet. Dette kan som sagt også være en svakhet.

I Norge har 98 % av innbyggerne mellom 9 og 79 år tilgang til internett, ifølge Medienorges oversikt («Medienorge: Andel med tilgang til internett» 2019). Aldersgruppen jeg har tatt utgangspunkt i har den største andelen av internettbruk en gjennomsnittsdag (98 % bruker internett på en gjennomsnittsdag i 2017), i tillegg til at de er blant de to gruppene som bruker mest tid på internett hver dag: 16-19 år bruker 261 minutter på internett en gjennomsnittsdag i 2017, mens 20-24 år bruker 245 minutter («Medienorge: Internett-bruk en gjennomsnittsdag» 2019). Informantene har også vokst opp med internett og etter hvert sosiale medier fra tidlig alder, og jeg var derfor interessert i perspektivene som denne oppveksten kan ha medvirket til. I og med at ungdomstiden er en tid der de fleste er opptatt av det sosiale, kan man gå ut ifra at sosiale medier spiller en større rolle for denne gruppas sosiale liv enn for eldre generasjoner

som opplevde overgangen fra fasttelefon til smarttelefon, fra tiden før internett, Google Maps og sosiale medier til nå. For denne aldersgruppen kan det derfor muligens være et større sosialt press til å fortsette å ha en tilstedeværelse på de sosiale mediene, at de kanskje føler seg «låst» til å bruke dem selv om de er negative til selskapenes retningslinjer, eller at de ikke ser på det å kutte sosiale medier som en mulighet. I tillegg vil en oppvekst hvor man er vant til å bruke internett, apper og etter hvert sosiale medier uten å ha opplevd en alternativ hverdag også muligens ha noe å si for valget om å fortsatt bruke dem. Siden oppgaven er et kvalitativt studium om hvordan unge voksne vurderer og praktiserer personvern, vil ikke dette utgangspunktet og motivasjonen for å intervjue utvalget være noe som kan testes og etterprøves her. Eventuelt kan tendenser og funn jeg kommer frem til i oppgaven brukes i utformingen av kvantitativ forskning, med et større fokus på sammenligning mellom alderssegment.

Informantene kommer fra ulike deler av Norge, men hovedsakelig fra vestlandet og østlandet. Flertallet bor i Bergen for tiden, og intervjuene ble holdt i Bergen i januar og februar 2018.

3.6 Etiske hensyn

Etiske hensyn er spesielt viktig i sammenheng med kvalitativ forskning, der intervjusituasjonen legger opp til visse utfordringer. Som nevnt i utvalget av informanter, valgte jeg å avgrense utvalget av informanter delvis på grunn av etiske hensyn rundt sensitiv tematikk som kunne oppstå i intervjusituasjonen, som nakenbilder og deling av disse på nett. Gentikow beskriver hvordan informert samtykke, konfidensialitet og lojalitet er nødvendig i forskningsprosesser som omfatter kvalitative intervju, noe vi skal se nærmere på i sammenheng med egen oppgave (Gentikow 2005, 64).

Informantene har gitt informert samtykke i form av et informasjonsskriv på en side de leste gjennom og underskrev før intervjuet begynte. Denne inkluderte informasjon om masteroppgavens fokus, lengde på intervjuet, at intervjuet skal bli tatt opp, transkribert, og brukt i oppgaven, samt muligheten til å trekke seg når som helst. En problematikk Gentikow nevner i sammenheng med informert samtykke er om man skal kontakte informantene dersom problemstillingen forandrer seg (Gentikow 2005, 64–65). Jeg gjorde likevel en vurdering av å ikke kontakte og oppdatere informantene, siden jeg mener den nye problemstillingen hovedsakelig er mer spisset i sitt fokus og ikke tar opp noen nye temaer som informantene ikke var klar over.

Konfidensialitet for informantene går på at de ikke skal bli gjenkjent av andre personer i deres kretser (Gentikow 2005, 65). Alle informantene har fått pseudonymer i stedet for deres egentlige navn. Jeg har også valgt å ikke inkludere hvilket årskull informantene er på i utdanningsløpet deres for at ikke de skal kunne bli gjenkjent i denne sammenheng. I tillegg har enkelte sitater blitt utelatt som potensielt kunne identifisert informantene. For eksempel kan dette omhandle steder eller klubber informantene har tilknytning til eller spesifikke ansvarsstillinger de har som kan være med på å identifisere dem.

Som intervjuer og forsker havner man i en tillitssituasjon, og det er derfor viktig å bevare lojaliteten overfor menneskene som setter av sin tid til å bli med på dette prosjektet. Lojalitet overfor informantene omfatter blant annet å utelate sensitive opplysninger om dem og ikke å fremstille dem på en dårlig måte. Men lojalitetsprinsippet omfatter også å være lojal mot den akademiske praksis og være åpen om funnene som kommer frem av intervjuene (Gentikow 2005, 66).

Enkelte utsagn som noen av informantene har kommet med kan ha virket som om de ikke samsvarer med resten av intervjuet. Dette er riktignok noe av hva jeg er på utkikk etter av funn, men i enkelte av disse sitatene kan informantene virke uinformerte, uinteresserte eller på andre måter kan de stille dem i negativt lys. Jeg har i disse situasjoner gjort en avveiing av intervjuet med informanten i sin helhet, prøvd å være lojal mot det bildet jeg har fått av hver spesifikk informant, og ikke valgt ut enkelte sitater fra sammenhengen som kan ha vært sagt uten å tenke, eller som kan ha blitt sagt uten å forstå spørsmålet mitt. Samtidig har jeg bevart de sitatene som har hatt en klar sammenheng og relevans til problemstillingen min, og som mest mulig har virket som om informantene kan stå for.

3.7 Forskningsprosessen

Jeg skal nå se på forskningsprosessen i arbeidet med oppgaven. Aller først skal jeg ta for meg gjennomføring av intervjuene med informantene.

3.7.1 Gjennomføring av intervjuer

Etter intervjuene valgte jeg å innlemme de to informantene fra andre pilotstudie i studiet på lik linje som de andre informantene, siden jeg syntes informantene hadde god innsikt og verdifulle perspektiver for studiet. Siden det meste som skilte daværende intervjuguide fra den siste intervjuguiden var de tre eksempelartiklene jeg ikke hadde tatt med enda, så jeg det som

relativt uproblematisk å ta dem med, så lenge jeg så bort fra temaene jeg hadde snakket med dem om som var tatt bort i siste revisjon av intervjuguiden.

Et praktisk problem var at informantene innimellom begynte å diskutere temaer som jeg hadde planlagt å snakke om senere i intervjuet. Det ble derfor litt utfordrende å holde oversikt over hva som hadde blitt snakket om og hva som ikke hadde blitt snakket om til tider. Etter å ha opplevd dette i et par intervjuer, begynte jeg derfor å huke av temaer de hadde snakket om for å lettere holde oversikten.

Som tidligere nevnt angående den kvalitative intervjusituasjonen som pre-refleksiv metode, der informantene må ta stilling til saker de ikke har reflektert grundig nok over i forkant, kan dette ha ført til andre svar enn hva en skriftlig spørreundersøkelse eller en mediedagbok ville gitt (Gentikow 2005, 98). Svarene kan også ha blitt formet mer enn jeg trodde av informasjonen i utlysningsteksten og samtykkeskrivet. Informantene som oppsøkte meg og sa seg villige til å bli med kan ha vært ekstra bevisst personvern og egen sikkerhet på nett enn hva andre informanter ville vært dersom utlysningsteksten var mindre informativ. Dette er riktignok potensiale skjevheter som man kan forvente seg i denne type kvalitative studier, siden hovedmålet med semistrukturerte intervjuer er å få et rikt datamateriale og detaljerte svar, og ikke nødvendigvis et representativt utvalg (Bryman 2016, 467). Jeg har derfor vurdert dette som innenfor, så lenge man har denne potensiale påvirkningen i bakhodet når man skal vurdere informantenes meninger og holdninger.

3.7.2 Spissing av problemstilling

I utgangspunktet hadde jeg mest fokus på sosial mediebruk enn generell nettbruk i intervjuene. Men siden nærmest samtlige av informantene snakket om sine erfaringer med personvern rundt generell internettbruk uavhengig av spørsmålssettingen, valgte jeg å fokusere på nettbruk generelt i problemstillingen.

Jeg ønsket også å undersøke mer hva informantene mente om de store digitale medieselskapenes ansvar rundt personvern og brukernes sikkerhet. Men siden de aller fleste viste seg å være lite interesserte i dette og penset fort over på andre mennesker på nettet, vinklet jeg problemstillingen til å inkludere dette.

3.7.3 Transkribering

I arbeidet med transkriberingen lot jeg være å inkludere de fleste fyllord som eh, mm, og lignende, som Gentikow anbefaler å gjøre (Gentikow 2005, 117). Jeg lagret interessante kommentarer i egne dokumenter mens jeg transkriberte intervjuene. Da jeg var ferdig leste jeg over alle intervjuene fra starten av, og begynte arbeidet med dataanalysen. Etter jeg hadde skrevet en god del av analysen ferdig, leste jeg over alle intervjuer en siste gang, for å se om det var deler av dem som kunne utbrodere teoriene og funnene jeg hadde kommet frem til.

3.7.4 Dataanalyse

I denne prosessen benyttet jeg meg av hva Tove Thagaard kaller en «temasentrert» analysemetode der jeg undersøkte jeg spesifikke sitater som var relevante for de ulike temaene jeg ønsket å belyse gjennom alle de transkriberte intervjutekstene. (Thagaard 1998, 125) Disse sitatene ble samlet i egne dokumenter for hvert tema for å lettere se sammenhengene eller forskjellene i de ulike besvarelsene.

Jeg begynte så med hva Geertz kaller for *Thick description*, med andre ord forskerens egen kontekstualiserte analyse og fortolkning av datamaterialet (Geertz 1973). Under arbeidet med analysen jobbet jeg med thick description og integrering av teori i analysen vekselvis, ut fra et såkalt nedenfra-perspektiv og ovenfra-perspektiv. Nedenfra-perspektiv vil si å lese hva det faktiske datamaterialet forteller i seg selv, den tidligere nevnte thick description. Man lar empirien snakke for seg selv for å komme med ny innsikt (Geertz 1973). Ovenfra-perspektiv vil si å fortolke materialet i lys av ulike teoretiske metoder, at man bruker tidligere teorier til å bedre forstå og analysere materialet (Bryman 2016). I begynnelsen av analysearbeidet var ovenfra-perspektivet mitt preget av de tidligere nevnte makt- og individfokuserte teoretiske perspektivene. Det positive med å veksle mellom ovenfra og nedenfra-perspektiv i denne sammenheng var at jeg med nedenfra-perspektivet innså at ovenfra-perspektivet var for smalt, for lite dekkende til å forklare alle aspekter av datamaterialet. Dette fikk meg til å lete etter flere og mer dekkende teorier som kunne forklare informantenes besvarelser på en mer utfyllende måte.

3.7.5 Bearbeiding og analyse av funn, integrering av teori i analysen

I arbeidet med analyse og teori brukte jeg først mange ulike tradisjonelle personvernsmodeller og teorier som legger opp til et individualistisk perspektiv. Dette fungerte til en viss grad, men

jeg følte de ikke forklarte godt nok informantenes oppfatning av personvern på nett, det var noe som jeg ikke fanget opp med disse teoriene. Informantene snakket mye om rollen andre brukere hadde i deres syn på personvern på nett, både som faremoment, hjelpere og støttespillere, og som hovedmotivasjon for deres nettbruk. Informantenes personvernsbevissthet bestod av komplekse og sammensatte prosesser, og det virket som det sosiale samspillet var vesentlig for å forstå disse prosessene best mulig. Jeg savnet derfor teoretiske modeller som trakk inn det sosiale elementet i en større grad. Etter hvert fant jeg frem til kontekstuelle personvernsmodeller, modeller som baserer seg på sosiale nettverk og kontekster. Jeg syntes Helen Nissenbaums teoretiske modell om kontekstuell integritet var et bra perspektiv til å drøfte informantenes syn på personvern ut fra kontekst, og valgte derfor å inkludere denne. I tillegg valgte jeg å bruke teorier basert på Michel Foucaults teori om panoptikon for å vise hvordan informantene fremholdt at statlig overvåkning i informasjonssamfunnet hadde en tradisjonell makt- og kontrollfunksjon i sin beskyttelse av borgerne. Jeg kunne brukt flere personvernsteorier for å forklare nyanser av informantenes oppfattelse av personvern, men jeg prioriterte et fokus på hva jeg anså som de viktigste funnene i analysen.

4 Statlige institusjoner

Informantenes oppfatning av statlige institusjoner vil strukturere diskusjonen i dette kapitlet. Aller først skal jeg ta for meg hvordan informantene vurderer personvern overfor statlige institusjoner, jeg vil siden se på faktorer som påvirker disse.

4.1 Personvernvurderingen overfor statlige institusjoner

Vurderingen informantene tar overfor statlige institusjoner har jeg valgt å formulere gjennom *aksept eller ikke-aksept* av at statlige institusjoner kan få tilgang til informantenes personinformasjon. Under samtalene kom det frem at alle informantene aksepterte en potensial innsikt inn i informantenes sosiale medieprofiler, internettrafikk og personlig informasjon.

Da informantene ble spurt om de noensinne følte seg overvåket av statlige institusjoner, mente enkelte av dem at uttrykket *overvåkning* heller kunne bli brukt i sammenheng med statlige institusjoners etterforskning av kriminelle og terrortrusler. Mari forklarer hvordan hun selv definerer overvåkning:

> Det er vel mer hvis jeg begynner å søke på, hvordan lage bomber, hvordan sånn og sånn og sånn, og det begynner å bli sånn, begynner å søke opp de ingrediensene til å kjøpe inn, og sånt, begynner å handle på nettet, at man blir overvåka.

Mange av informantene tar opp at de ikke føler seg overvåket i denne sammenheng fordi de ikke gjør noe ulovlig. De føler ikke denne overvåkningen gjelder for dem, som Nina her:

> […] jeg er veldig positiv til overvåkning, altså, jeg er jo ingen plasser som er hemmelige i den forstand, altså… ja. Så jeg har liksom ingenting å skjule. Har ikke vært på noen ulovlige plasser, eller… Som regel så vet jo folk hvor jeg er til enhver tid uansett.

Dette synet på statlige institusjoners rolle som beskytter er derfor en viktig faktor for aksept som vi skal nå se nærmere på nå.

4.2 Påvirkninger på informantenes aksept

Vi skal nå se nærmere på de viktigste faktorene som påvirker vurderingen informantene har tatt om å akseptere en potensial statlig overvåkning.

4.2.1 Statens rolle som beskytter av borgerne som positiv påvirkning på aksept

Da informantene ble spurt om de var bekymret for statlig overvåkning, tar som sagt flere av dem opp hvordan *terrortrusler og kriminalitet* legitimerer eventuelt innsyn inn i deres atferd på nett. Siden informantene mente statlige institusjoner som politiet og PST har dette som formål med overvåkning på nett, forklarer de statlig overvåkning som et nødvendig onde. Anders forklarer hvorfor han tar denne posisjonen:

> […] slik situasjonen og konflikter er i dag, så er det noe sånn terror og sånt, som er fryktelig uforutsigbar, så må man, bare for å sikre, sikkerheten til alle sammen, så må man innskrenke litt friheten, da.

Anders forklarer hvordan han er villig til å innskrenke litt av egen frihet for å bli beskyttet mot terrortrusler. David Lyons *fryktfaktor*, frykten for potensiale terrorhandlinger, spiller derfor muligens inn i informantenes aksept av den statlige overvåkningen (Bauman og Lyon 2013).

Statens rolle som beskytter kom også opp på andre måter enn gjennom vern fra terror. To av informantene tok opp i intervjuene hvordan politiet kunne bedre beskytte borgernes personvern og deres fysiske sikkerhet med hjelp av overvåkning. Nina så på det som positivt at politiet kan få tilgang til lokasjonsinfo dersom hun skulle bli kidnappet:

> […] jeg er litt sånn katastrofetenker, så hvis jeg liksom blir kidnappet eller forsvinner, så kan det brukes til å finne meg. […] For det, jeg vet jo at politiet kan jo spore telefonen ganske lenge. Eh, men da er det jo ganske mulig å finne informasjon.

Frida trakk frem saken om håndballspilleren Nora Mørk som hadde fått spredt nakenbilder mot sin vilje. I saken fant politiet de som hadde videresendt bildene, og de ble dømt til å betale erstatning for dette (NRK 2018).

> Men det har jo jeg lest etter den saken om Nora Mørk, og de bildene, at det… det at folk faktisk de, bare de som sender bildene videre, er faktisk, at det, du kan få straff for det, liksom. Det er flere som har fått bøter og sånn. […] Og det er jo bra. At det kommer frem. For kanskje at mindre folk gjør det, da.

Det at lovene overholdes, signaleffekten de gir og hvordan etterforskningen av saken omfattet statlig overvåkning, ble av Frida tatt opp som påvirkninger for hvorfor hun aksepterte at statlige institusjoner kunne få innsikt i hennes personinformasjon.

Siden informantene er villige til å la sitt eget personvern vike for samfunnets sikkerhet, har de i denne sammenheng et nøytralt perspektiv på personvern. De veier behovet for sitt eget personvern som mindre viktig enn samfunnsnytten. Hvordan selve innsynet i sosiale mediekontoene, de konkrete lovbestemmelsene rundt statlig overvåkning og hvordan eventuelle juridiske prosesser foregår er det riktignok delte meninger om blant informantene.

Med mindre det er mistanke om at informantene bryter norsk lov, forventer informantene at staten ikke bruker informasjonen deres i andre sammenhenger enn i konteksten rundt terror og kriminalitet. Siden informantene aldri har opplevd noen negative konsekvenser av statens overvåkning på nett, føler de at denne kontekstuelle integriteten blir ivaretatt. Siden denne overvåkningen ikke legges merke til av lovlydige borgere, er dette er også i tråd med David Lyons teori om *flytende overvåkning*: jo mer usynlige overvåkningsprosessene foregår, jo lettere er det å akseptere dem (Bauman og Lyon 2013).

4.2.2 Tillit til myndighetene som positiv påvirkning på aksept

En generell *tillit til samfunnet* er med på å bidra til at informantene stoler på at statlig overvåkning ikke misbrukes på noen måte, og er til støtte for innbyggerne. Flere av informantene forklarte under intervjuene om hvordan de har tillit til den norske stat. Anders tok opp dette her:

> Det handler om å ha tillit også til, myndighetene, da. Bare, hvis, eller, at jeg ikke kommer til å gjøre noe gæernt, og ja. Da er det jo bare litt sånn, ja, å ha tillit til dem, da. Vite at det er i god tro og sånn. […] Særlig når vi bor, det å vite at vi bor i Norge. Hadde vært et helt annet land, så er det helt annet tilfelle.

Når informanter som Anders beskriver sin tillit til myndighetene, kan dette også innebære en tillit til de demokratiske prosesser som utformer lover og reguleringer som beskytter sine borgeres krav på personvern. Ut fra hvordan Anders og andre informanter omtaler denne tilliten og sammenligner den med andre land, kan vi gå ut fra at dette er en forutsetning for å akseptere at statlige institusjoner har mulighet til å overvåke borgerne i landet. Selv om alle ikke uttalte seg like direkte om dette, er det grunn til å tro at de andre informantene også hadde denne forståelsen. Norge er en nasjon med en sterk grad av rettssikkerhet og ytringsfrihet, noe som vekker tillit hos informantene. Når man bor i et samfunn hvor kritikk av styresmakter er dagligdags og akseptert, er det nok lettere å stole på et myndighetsapparat som blir utsatt for et stort moralsk press og mediefokus.

Vi kan forstå informantenes tillit til myndighetenes overvåkning bedre ut fra Mathisens teori om Synoptikon. Borgernes mulighet til å kritisere og melde fra om maktmisbruk fra maktpersoner eller statlige organisasjoner tvinger disse til å oppføre seg. Synoptikon kan i denne sammenheng beskrive dette som en politisk og sosial maktfordelingsmekanisme som holder de statlige overvåkerne i sjakk. Som Mathisen sier det, «de mange overvåker de få» (Mathiesen 2013). I en stat der ytringsfriheten står veldig sterkt, er denne maktmekanismen utøvd blant annet gjennom journalistikk, vanlige personers leserinnlegg, protester, politianmeldelser og så videre.

5 Medieplattformer på nett

I dette kapitlet skal vi se på personvernvurderinger relatert til medieplattformers innsamling av brukerinformasjon på nett. Hva jeg ønsker å finne ut med dette kapitlet er hvordan personvern spiller inn i informantenes fortsatte bruk av medieplattformer, og hva annet som påvirker disse vurderingene. Vurderingene om å fortsette å bruke medieplattformene er såklart hovedsakelig påvirket av at informantene får tilgang til tjenestene der. Men jeg er interessert i å utforske hvordan informantene resonnerer rundt for hvorfor de fortsatt bruker medieplattformene ut fra et personvernperspektiv, hvordan de forklarer hva som er grunnene til at de er der *på tross* av at de samler inn hva de kan av brukeratferd og personinformasjon.

5.1 Vurderingen om å fortsette å bruke medieplattformene

I det forrige kapitlet om statlig overvåkning tok alle informantene den samme personvernvurderingen ved å akseptere den statlige overvåkningen. I denne delen skal jeg ta for meg vurderingen informantene tar om å fortsette å bruke medieplattformene og la dem få tilgang til personinformasjonen deres.

Ut fra hvordan vurderingen er formulert, kommer spørsmålet opp om dette er en vurdering informantene teknisk sett tar hver gang de bruker en medieplattform, eller en vurdering de tok da de laget en profil på plattformene der dette behøves[3]. Mest sannsynlig er dette variabelt for hver informant. Petter oppga at han vurderte å slutte med sosiale medier delvis ut fra personvernhensyn, noe som innebærer at han har tenkt på det ved flere anledninger. Andre informanter som var bekymret for personvern oppga at de har vært inne på tanken til tider, men at påvirkningene vi skal ta for oss senere i kapitlet gjorde at de fortsatte å bruke dem. Andre informanter igjen oppga at de hadde tenkt på å avslutte å bruke sosiale medieplattformer, men ikke ut fra personvernhensyn. Et par av informantene hadde aldri tenkt på å slutte å bruke noen av medieplattformene.

I Christine Mælands studie om ikke-brukere på Facebook, hadde alle informantene tatt vurderingen om å ikke bruke Facebook, delvis på grunn av personvernhensyn (Mæland, 2017). I denne studien har alle tatt vurderingen om å fortsatt bruke medieplattformene, delvis på tross av personvernhensyn. For å vise hvordan personvernhensyn spiller inn i den

[3] De sosiale medieplattformene krever at man oppretter en profil, mens Youtube og Googles tjenester kan brukes uten profil.

sammensatte vurderingen av å bruke eller ikke bruke medieplattformene, er det derfor viktig å også vise hvilke andre faktorer som påvirker denne vurderingen. Dette gjelder for medieplattformene mest, men også for de andre vurderingene vi har tatt opp og skal ta opp.

Som vi også så i Mælands studie, var andre brukere ofte grunnen til hvorfor informantene hennes sluttet å bruke Facebook, og ikke bare på grunn av personvernhensyn (Mæland 2017). På tilsvarende vis har informantene i denne studien også opplevd ubehagelige erfaringer med andre brukere, og oftere knyttet til personvernkonflikter enn i hennes studie. Dette kan ha sin årsak i at intervjuguiden i denne studien vektla temaer knyttet til personvern mer enn Mælands studie gjorde, i tillegg til at Mælands utvalg prioriterte ikke-brukere av Facebook. Andre brukere er uansett også en påvirkning i vurderingen om informantene skal fortsette å bruke eller ikke bruke de sosiale medieplattformene, noe som skal tas opp i kapittel 6.

Da informantene fikk spørsmål om målrettet markedsføring under intervjuene, tok de hovedsakelig opp de digitale medieplattformene Facebook, Google, Youtube, Snapchat og Instagram som eksempler. Informantene så på disse aktørene som de som hovedsakelig sanket inn brukeratferd og personinformasjon om brukerne sine. Personvernvurderingene i denne delen er derfor i utgangspunktet knyttet til disse fem aktørene som informantene forholder seg mest til. Ved eksempler på andre aktører, som andre medieplattformer eller selskaper som samler inn brukerinformasjon, blir de navngitt i teksten.

De fleste informantene ser på medieplattformene som *systemer* for informasjon og kommunikasjon, og ikke som aktører som kan ansvarliggjøres for å ta dårlig vare på brukernes personlige informasjon. Dette henger sammen med tre faktorer:

a. Informantene omtalte personvern hovedsakelig som noe de selv aktivt gjorde inni medieplattformene for å verne sin personlige informasjon fra andre brukere.

b. Synet deres på personlig informasjon begrenser seg i denne sammenheng til innhold som kan misbrukes av andre brukere, som meldinger, bilder og videoer.

c. Informantene går ut fra at deres brukeratferd, kjøpshistorikk og metainformasjon blir analysert sammen med mengder av andres informasjon, og blir derfor gjort enda mindre personlig.

Informantene mente systemene kunne være gode eller dårlige til å tilrettelegge for personverntjenester, men de så ikke på medieplattformene som aktører som hadde et selvstendig ansvar overfor informantene. Fire av informantene så på dem både som systemer

og aktører, og tilla deler av ansvaret på personvern på dem. Av disse mente tre av dem at medieplattformene stort sett gjorde hva de kunne for å sikre sine brukeres personvern, siden det var i plattformenes interesse at brukerne var fornøyde. Petter mente at medieplattformene «tok for seg» og var kyniske i sin innsamling.

Alle informantene aksepterte at medieplattformene fikk tilgang til deres brukeratferd og personinformasjon. Informantene omtalte dette som en *byttehandel* mellom dem selv og medieplattformene, der informantene fikk tilgang til medieplattformenes tjenester i bytte mot at selskapene brukte brukeratferden og personinformasjonen deres til målrettet reklame siktet mot informantene. Informantene fremstår også med dette tilfellet med et nøytralt perspektiv på personvern idet de veier negative og positive påvirkninger for å bruke medieplattformene frem og tilbake.

Selv Petter, den mest kritiske til medieplattformene, fortalte at han mislikte at de sosiale medieplattformene samlet inn informasjon om ham:

> *…vanligvis er det jo sånn at dersom man ikke stoler på et sosiale medie-nettverk så pleier folk å slutte, da. Så jeg vil jo gå ut fra at du stoler på de nok til å ikke slutte, iallfall.*
>
> Ja, jeg har noen betenkeligheter, og liksom…
>
> *Du er på vippen?*
>
> Ja. Det er jeg. Men jeg vil jo samtidig fortsatt bruke disse sosiale mediene, da. Fordi de har noen goder ved seg, også. Og da er det litt av prisen jeg må betale.

Det virket som om flere av informantene omtalte denne byttehandelen som noe de hadde tenkt over tidligere, de snakket ikke om det som om det var noe nytt de tenkte seg frem til der og da. Det er ikke nødvendigvis sikkert at de hadde reflektert over alle aspektene ved det, men at de tidligere hadde innsett at dette var noe de måtte forholde seg til.

Ut fra det kontekstuelle integritetsperspektivet kan vi påstå at informantene gir selskapene tilgang til egen informasjon i bytte mot tilgang til tjenester ut fra en nøytral forståelse av personvern. De legger på denne måten en pris på sitt eget personvern, og betaler den hver gang de bruker tjenestene ved å bli eksponert for reklame, og ved å bli sporet og analysert. Denne utvekslingen mellom medieplattform og bruker omfatter overføringsprinsippet *resiprositet*, en utveksling av informasjon som både sender og mottaker har fordel av. Forståelsen informantene har av denne utvekslingen av goder og tjenester kommer tydelig

frem gjennom intervjuene, blant annet gjennom hvordan Mari forsvarer de sosiale medieplattformenes målrettede reklame:

> …de må jo tjene penger på en måte, og Facebook er jo gratis, og det meste av sosiale medier er jo gratis, og for at de skal tjene penger, så må de jo få det gjennom reklame, om de, jeg vet ikke om jeg synes det er så greit, alltid, men det gir mening at de gjør det sånn.

Ut fra kommentaren «jeg vet ikke om jeg synes det er så greit, alltid» viser Mari hvordan hennes nøytrale perspektiv på personvern kommer til syne: ved å legge til side sitt eget personvernbehov og preferanser til fordel for at plattformen kan fortsette å tilby brukerne sine tjenester.

Selve vurderingen om å fortsette å bruke medieplattformene er riktignok ikke bare påvirket av personvern, og det var heller ikke alle informantene som følte at de ga opp deler av eget personvern i byttehandelen.

Jeg skal nå over til hva informantene mener påvirker deres fortsatte bruk av medieplattformene.

5.2 Påvirkninger på fortsatt bruk av medieplattformene

I løpet av intervjuene forklarte nesten alle av informantene at personvern var viktig for dem, og trakk frem flere eksempler på hvordan de sosiale medieplattformene *ivaretar brukernes personvern*, og hvordan dette påvirker informantenes vurdering om å fortsette å bruke disse plattformene eller ikke. Jeg skal derfor se på forskjellige måter informantene opplever at de sosiale medieplattformene tilrettelegger for og ivaretar brukernes personvern. Denne påvirkningen for fortsatt bruk var ikke i like stor grad gjeldende for Google og Youtube, der profil ikke var nødvendig å bruke.

5.2.1 Tillit til medieplattformene som en viktig påvirkning

Flere informanter trekker inn hvordan *tillit* til at de sosiale medieplattformene ivaretar deres personlige informasjon er vesentlig for fortsatt bruk. Tilliten som informantene har til myndighetene, som omtalt i forrige kapittel, kan også overføres til selskapene gjennom myndighetenes evne til å regulere og lovpålegge medieplattformene. Anders beskriver her hvordan han har tillit til at reglene som utformes av myndighetene beskytter dem:

> Hvis det er et lite selskap som er i USA, da vet jeg at, da er det ikke så internasjonalt selskap, og da er det sikkert bundet av amerikansk lovgivning, og, regelverk. Personlig så er ikke jeg så særlig fan av akkurat det, så de har jeg ikke så mye tillit til. Men når det er sånn Facebook, det er ikke et amerikansk selskap lenger, det er internasjonalt, samme med Google og alt det, jaja, de har hovedkvarter der, men, de er internasjonalt forpliktet av ulike lover og reglementer og sånt.

Her snakker Anders om tillit til hvordan internasjonale lover og regler, og underforstått norske lover og regler spiller inn i hvordan han vurderer Facebooks hensyn til brukernes personvern på nett. Anders ser på norske og internasjonal jurisdiksjon som garanti for at selskapene ikke misbruker tilgangen de har til brukernes personinformasjon. Vi kan påstå at Mathisens *synoptiske maktprosesser* spiller inn i Anders sitt syn på Facebooks ivaretakelse av brukeres personinfo, forestillingen om at «de mange ser de få» (Mathiesen 2013). Anders studerte rettsvitenskap, noe som forklarer hvorfor han vinklet problematikken opp mot lover og reguleringer. Gunnar snakket også om en tilsvarende bevissthet da han tok opp problematikken med den negative publisiteten Facebook hadde hatt i sammenheng med brukernes personvern:

> …med Facebook har det liksom vært så mye nå, så hvis ikke de har så god sikkerhet som de kan, liksom, optimalt ha, så tror jeg det at folk kan, liksom, vende seg mot dem […] Hvis det kommer sånn ut, at Facebook tar ikke vare på informasjonen til brukerne sine.

Gunnar mener Facebook generelt ikke har vært gode nok til å ivareta personvernet til sine brukere i den siste tiden, og at dersom denne tilliten forsvinner, mener han at brukerne vil straffe dem ved å slutte å bruke tjenestene. De fleste av informantene omtalte i denne sammenheng personlig informasjon som bilder delt mellom brukere, samtaler og tilsvarende innhold. De brydde seg mindre om informasjon som nettatferd, brukerhistorikk, metadata eller lokasjonshistorikk, som vi også har sett eksempler på tidligere.

5.2.2 Sikkerhetstiltak på plattformene som positiv påvirkning

De sosiale medieplattformenes mulighet til å la sine brukere *endre på personverninnstillinger* som ga dem bedre personvern spiller inn i forutsetningen for å fortsatt bruke disse plattformene. Med muligheter til å forbedre eget personvern, mente informantene de lettere kunne beskytte seg fra *ukjente brukere* på nett, noe som nesten alle informanter fortalte de hadde negative erfaringer med. Gunnar forklarer hva han synes om dette:

> …man kan jo selv velge på Facebook hvor mye man vil vise da, for en person som ikke er vennen din. Så jeg syns det at hvis man vil ha, liksom, optimalt, da, så har det skjedd det at det

> fins en del profiler der man kun kan se navnet, og man kan ikke engang sende en sånn venneforespørsel. Så, jeg syns det at det fins ganske mye sikkerhet for dem som vil ha det, liksom, ifra folk med dårlige intensjoner, liksom.

Mange av informantene tok opp hvordan de sosiale medieplattformene Facebook, Instagram og Snapchat tilrettela for at brukerne selv kunne redigere personverninnstillinger, og hvordan det derfor var brukernes *eget ansvar* å gjøre dette. Disse mulighetene ga informantene en følelse av at de selv kunne bidra med å justere og verne om deres eget personvern fra andre brukere. Vi skal se nærmere på personverninnstillinger i neste kapittel om andre brukere.

Rapportering av andre brukere var et annet sikkerhetstiltak på sosiale medieplattformer og fora som informantene ga flere eksempler på. Nina forklarer hva hun synes om dette:

> […] mitt inntrykk er at det er veldig bra at det er mange som styrer det (Facebook), fordi at jeg merker det, hvis jeg rapporterer en profil, som for eksempel er falsk, så er jo det gjort på 12 timer. Så får jeg beskjed om at det er sletta eller hva som er gjort med den. Da vet jo jeg at da sitter det jo noen der som faktisk gjør noe og prøver å slette upassende innhold og upassende profiler og, det gjør jo at jeg føler jo at det er litt tryggere enn om bare det var en app som var utviklet.

Når Facebook tar Ninas rapportering seriøst og håndterer det raskt, føler hun seg derfor tryggere på at det er mange folk som bidrar med å sikre brukernes personvern, og tilliten hennes til at medieplattformen ivaretar hennes personvern styrkes. Andrejevics *laterale panoptikon (2006)* påpeker hvordan slik rapportering kan gi brukerne følelsen av å bidra i overvåkningsarbeidet på plattformen, og slik gi en følelse av trygghet og samarbeid ved å delta i denne «opprenskningsprosessen». Gunnar tok opp et eksempel på en sosial medieplattform som hadde mindre av slike sikkerhetstiltak, Formspring.

> Det var en slags sånn der, plattform som kalte seg Formspring, som er sånn, du kan lage en bruker, da, også kan folk stille deg spørsmål helt anonymt, da. Og så var det ofte folk brukte det til å si hva de mislikte, da, med den og den personen. […] Jeg husker det at jeg synes det var litt rart at det var så mange som laga brukere, fordi at egentlig så godt som alle fikk ganske, fikk ganske stygge ting, da.

Formspring ble kritisert i media for at designet på plattformen med offentlige poster og anonyme brukere var lite gjennomtenkt og la opp til mobbing (Berg 2012). På tross av stor vekst hadde ikke medieplattformen ressurser nok til å holde det gående økonomisk, og plattformen ble lagt ned i 2013 (Seifert 2013). Det er nærliggende å tro at denne mangelen på

ressurser også førte til at plattformen ikke hadde like effektive sikkerhetstjenester og moderering som det Nina mener Facebook har.

Vi har med dette sett på personvernhensynene som gjør at informantene føler at personvernet deres blir ivaretatt av medieplattformene. Dette oppgir informantene som viktige faktorer for at de fortsatt skal bruke medieplattformene. Vi skal nå over til faktorer som på forskjellige andre måter påvirker de tidligere nevnte vurderingene om fortsatt bruk av medieplattformene. Her er det viktig å presisere at disse påvirkningene speiler kompleksiteten i informantenes holdninger og meninger, og informantene veier de ulike faktorer for påvirkning forskjellig.

5.2.3 Målrettet reklame som både positiv og negativ påvirkning

Medieplattformenes innsamling av brukerinformasjon er lettere å akseptere for informantene når de ikke merker at informasjonen deres blir trukket ut, at det er en usynlig innsamling av informasjon i tråd med Lyons teorier om *flytende overvåkning* (2013). Begrepet beskriver hvordan utveksling av informasjon foregår som en autonom og nær sagt usynlig prosess mellom informasjonssystemer på nett og brukerne av disse. Da informantene ble spurt om hva de syntes om målrettet reklame, tok flere av informantene opp hvor tydelig det var at det plutselig dukket opp reklame for noe de nettopp hadde søkt om på Google eller fra en butikkside de nettopp hadde kikket på. Anette beskriver hva hun synes om dette:

> Jeg syns det er litt ubehagelig, faktisk, for jeg tenkte, før tenkte jeg aldri over det når det var sånn, popup som det var, kom opp ting så trodde jeg det bare var helt tilfeldig reklame. Men så fant jeg ut at det var jo faktisk ting som du har vært, og sett på. Så de på en måte, overvåker da. Alt av sider og alt du på en måte er inne på. Så det, så det er litt ubehagelig, egentlig.

Når dette skjer blir «illusjonen» om overvåkning som flytende og «usynlig» brutt for informantene, og de blir påminnet om at plattformene benytter seg av brukeratferden deres. Det at selskaper generelt hadde tilgang til informasjon om personinformasjon og brukeratferd gjennom medieplattformenes målrettingsparametere, noe som foregår i det skjulte i tråd med Lyons flytende overvåkning, bekymret de seg over i mindre grad. Det virket å heller å være den synlige konsekvensen av at dette skjedde som vekket ubehag hos enkelte av informantene, som det gjorde hos Anette. Frida hadde en annen reaksjon på samme opplevelse:

> Egentlig så er det litt tåpelig fra Facebook syns jeg, fordi, det eneste de oppnår er jo at jeg blir sånn: å Herregud, dere følger så sjukt masse med på meg, hva er vitsen, liksom. Fordi at, det er, skjer jo ikke, at jeg, trykker på det og liksom, kjøper noe gjennom det…

I Fridas eksempel føler hun at netthistorikken hennes har blitt appropriert til å prøve å overtale henne til å kjøpe produktene, noe hun opplever som at Facebook undervurderer henne. En del av informantene oppga at de ser at målrettet reklame kan være en fordel og en måte å gi brukerne mer relevant innhold når de først skal vise reklame, som Anders beskriver her:

> […] du vet at det kommer reklame før videoen (på Youtube), og hvis du tilfeldigvis trykker på den reklamen, det er jo egentlig positivt at den er målretta, fordi at det er reklame du faktisk kan bry deg om. Jeg har flere ganger sett ting på reklame som jeg faktisk bryr meg om, og jeg litt sånn, ok, det var faktisk et bra tilbud, om det er et tilbud, eller om det bare er produktet i seg selv, bare.

Denne holdningen viser til den tidligere nevnte teknologioptimismen som informantene viste overfor videreutviklingen av medieplattformenes tjenester. Denne gruppen mente at jo bedre medieplattformene ble til å målrette, jo mer relevant og interessant reklame fikk de.

5.2.4 Teknologisk kompetanse og teknologioptimisme som positive påvirkninger

Gjennom intervjuene var det spesielt tre informanter som fremstod som om de følte seg bevisste, kompetente og erfarne med ny teknologi, sosiale medier og internett: Anders, Nina og Silje. Denne kompetansen omfattet også personvern og «nettvett». Selv om disse informantene var de som uttrykte seg mest om denne kompetansen, er det grunn til å tro at dette i større eller mindre grad også gjelder for flere av informantene. Anders beskriver deler av denne kompetansen her:

> *Du føler du ikke er i en situasjon der du trenger å bekymre deg over noe?*
>
> Nei. For nå har jeg bare vennene mine rundt meg som kunne ha vært noe å bekymre seg over på sosiale medier. Og vi er i en såpass alder at, de vet jo når de ikke skal legge til noen, og hva de skal gjøre med fremmede og sånt, og, alle sånne ting.

I det tidligere nevnte Dodgeball-studiet til Lee Humphreys var en av informantene, «Barbara», heller ikke bekymret for statlig eller firmaers overvåkning fordi hun følte seg som en erfaren, kompetent og kunnskapsrik internettbruker (Humphreys 2013). Studien viste at denne kompetansen ikke nødvendigvis var reell, men at den bidrog til en tilsvarende følelse av trygghet for henne, som den hos de tre informantene i denne studien også viser til

(Humphreys 2013). Informantene i denne studien har antakelig en større reell kompetanse enn «Barabara», siden den ble gjennomført i 2005 og 2006 da sosiale plattformer som Dodgeball var relativt nye. Informantene i denne studien har alle brukt flere timer daglig på forskjellige nettaktiviteter over mange år, de har måtte forholde seg til flere teknologiske nyvinninger som smarttelefon, nettbrett og sosiale medier, de har en lenger erfaring med sosialisering på nett og de har erfart mange tilfeller av ubehagelige situasjoner på egne og venners vegne. Men hva vi kan trekke med oss fra Humphreys studie er at denne forståelsen kan føre til at man kan bli overmodig og ta for gitt hvor mye man vet om å beskytte seg selv i personvernsituasjoner. Informantene har også tatt opp eksempler på situasjoner de ikke hadde referanserammer for å unngå.

Det virker som om alle informantene viser til en *teknologioptimisme* i løpet av intervjuene. Noen av dem, som Silje, rasjonaliserer sin egen aksept av selskapenes innsanking av informasjon og brukeratferd på grunnlag av en form for teknologisk utvikling:

> […] jeg er mer skeptisk hvis det er, sånn at de bare skal hente inn informasjon om bruken min [ler]. På en måte. Men jeg begynner å bli mindre og mindre skeptisk til det når… egentlig jo mer jeg studerer, fordi at jeg skjønner jo at man trenger litt sånn, statistikk og sånn, til utvikling.

Alle informantene er veldig positive til nye teknologiske muligheter, og ser ikke på algoritmer som analyserer dem ut fra personinfo og metadata nødvendigvis som noe negativt. Selv etter at de leste artikkelen om psykometri som jeg var redd var for negativt vinklet, virket flertallet mest fascinerte over de teknologiske mulighetene dette innebar, som Petter her:

> Men det var jo sånn, veldig spennende, for en… veldig oppfinnsom måte å samle inn data på [ler] folk på. Det er… genialt. Det er skummelt, men det er… det er helt genialt.

Nina forklarer hvorfor hun mener hun og hennes jevnaldrende forstår internett bedre enn eldre generasjoner:

> For det første har vi mer forståelse for hele opplegget, internett generelt, teknologien. Og så er vi jo yngre, så vi lærer jo fortere. Vi fikk mobiltelefoner tidligere, mange av dem hadde jo ikke tv hjemme når de var på min alder. […] Mens vi som har, på en måte, sånn som jeg fikk mobiltelefon da jeg var 7 år, eh, og da sendte vi jo mp3-filer via bluetooths. Og så kom liksom appene og alt dette her videre, og vi har på en måte følgt det, og, det har vært nytt og spennende og vi har prøvd og testa, og vært med på hele det…

Som Nina sier, har denne generasjonen blitt vant til å vokse opp med nye medieløsninger og ny teknologi. Denne nærmest pragmatiske tilnærmingen til nye teknologiske produkter og digitale løsninger som Nina beskriver kan ha en del å si for at så mange av de andre også viser til en tilsvarende teknologioptimisme. Da Silje ble spurt om hvorfor hun stolte på at selskapene tok godt vare på informasjonen hennes og ikke misbrukte den, trakk hun frem både teknologioptimisme og teknologikompetanse i svaret:

> […] jeg føler jo liksom at jeg klarer å se fordelene med det, da, og klarer å se aspektet, og jeg tror det er veldig mange som, for eksempel altså Google Glass ble på en måte gitt ut, og alle er sånn: Å, de synes det er så kult, så, bra idè, og vil at vi liksom skal komme dit at alle har for eksempel en AI, da. Men, så ser de på en måte ikke alle de stegene en må ta for å komme dit, og det tror jeg er litt det som drives med nå, er liksom det å, det er jo det å tilrettelegge, skreddersy alt sånn av reklame og tjenester for å liksom, ja, finne ut av hvordan det liksom kanskje kan nå et høyere nivå. Det tror jeg i hvert fall at det er det som kommer til å skje i fremtiden, at det når et eller annet, et eller annet nytt.

Siljes teknologioptimisme er for det første basert på forventningen om nye og spennende teknologiske fremskritt. I tillegg har hun en forståelse om at veien dit forutsetter en god del prøving og feiling fra utviklernes side, noe som resulterer i en aksept og forståelse for denne «prøveperioden» av blant annet markedsføring, digitale softwareløsninger på nett og teknologisk tidsånd. Dette vitner om et ganske gjennomtenkt og pragmatisk perspektiv fra Siljes side rundt både personverndebatten og en overordnet diskusjon om ny teknologi i møte med sosiale masser.

Når Silje veier viktigheten av personvern fra sak til sak, blir denne bevisstheten tatt med i beregningen; at det teknologiske målet helliger det potensielt personvernovertredende midlet. Ut fra dette perspektivet som Silje belyser, kan vi også spørre oss om flere av informantene ser på overtredelser som en nødvendig del av teknologisk utvikling. At informantene også kanskje aksepterer selskapers innsamling av informasjon i sammenheng med denne utviklingen i bakhodet.

5.2.5 Medieplattformenes «monopol» påvirker fortsatt bruk

Medieplattformene Google, Facebook, Snapchat, Instagram og Youtube er de mest brukte blant informantene. Selv om det finnes andre typer sosiale medieplattformer og søketjenester, har disse blitt de mest etablerte og velkjente i Norge. Hver av plattformene har sin egen nisje de dominerer: videodeling på Youtube, bilder og korte videoer på Instagram, Google er den

mest brukte tjenesten for nettsøk og karttjenesten Google Maps, Snapchat er mest brukt til flyktig innholdsdeling og små gruppechatter, og Facebook har meldingstjenesten Messenger, informasjon om hendelser og som den mest kjente og en av de første seriøse sosiale medieplattformene, har brukerne oftest det største kontaktnettverket på den. Da Nina ble spurt om hvordan hennes oppfatning av Google som et selskap er, svarte hun dette:

> Jeg er veldig positiv til Google, jeg syns det er en ganske genial oppfinnelse, det kan brukes til veldig masse. Samtidig så ser jeg jo det at de har blitt så store at det er på en måte vanskelig å konkurrere mot de, og de er ofte det eneste valget du har, og det skaper jo veldig liten konkurranse i markedet på en måte, så.. ja… Hva skal jeg si? Jeg er jo egentlig positiv til det, men jeg ser jo at det kan være negativt at de er så store…

Nina erkjenner at størrelsen på Google som selskap skaper liten konkurranse, og at det er vanskelig å unngå å bruke medieplattformen.

Enkelte av informantene mente at vennebasen på plattformen ønsket om å være del av et sosialt fellesskap har gjort det vanskelig å søke vært delaktig i at de fortsatte å bruke de sosiale medieplattformene, noe som påvirker vurderingen om å bruke plattformene eller ikke. Mari mener at siden alle vennene hennes er i nettverket, er det vanskelig å la være å bruke det.

> […] du blir jo litt sånn avhengig av det, på grunn av at alle andre er det, og fordi du kjenner folk andre steder enn der du er. Så… hvis jeg kunne sluppet å være så mye på sosiale medier og heller på en måte, da hadde jeg ikke hatt den tanken om at personinformasjonen min kunne blitt misbrukt i det hele tatt, ikke sant.

Andre informanter sa de er avhengig av å bruke Facebook til jobbgrupper for å nå andre medlemmer og gi dem beskjeder, og det å la være å bruke plattformen blir veldig upraktisk for dem, som Silje beskriver her:

> I organisasjonen er det noen som ikke er på Facebook, og da er det jo veldig mye tilrettelegging som må til, for å jobbe seg rundt det. Og liksom, hver gang det legges ut noe så må det sendes separat på mail eller melding til de, og da, da får man liksom opp øya litt for at det er, det hadde nok vært veldig vanskelig å isolere seg helt.

Enkelte av informantene mener at dette «monopolet» spiller inn i deres fortsatte bruk av sosiale medier, og at dette gjør at eventuelle personvernhensyn blir nedprioritert på grunn av dette.

6 Andre brukere

Vi skal nå ta for oss hvordan informantene vurderer eget personvern overfor andre brukere på nett. Andre brukere var hva informantene var mest opptatt av når det kom til personvern, og de tok opp eksempler på mange forskjellige personvernvurderinger rettet mot disse aktørene. Siden informantenes vurderinger er mange, varierte og vanskeligere å definere tydelig, skal jeg i dette kapitlet derfor strukturere funnene litt annerledes. Jeg skal først beskrive de ulike typene personvernvurderinger som informantene tar opp. Jeg skal så beskrive to av de viktigste vurderingene informantene tar gjennom personverninnstillinger og rapportering. Etter dette skal jeg gå over til påvirkninger og under disse temaene ta opp eksempler på forskjellige typer vurderinger. Dette fungerer siden påvirkningene omfatter flere av personvernvurderingene.

Personvernvurderingene vi tok for oss som omhandlet statlig overvåkning og medieplattformers datainnsanking var preget av en dikotomi – aksept eller ikke aksept for statlig overvåkning, bruk eller ikke bruk av medieplattformene og bruk eller ikke bruk av funksjonene i dem. I denne delen, hvor vi skal se på hva slags vurderinger informantene tar overfor andre brukere, er det som sagt snakk om mange og «små» personvernvurderinger og avgjørelser som informantene tar i de sosiale mediene. På samme måte som i delen om medieplattformene, er ikke informantene like i hvilke vurderinger de tar og hva som påvirker dem mest. Informantenes erfaringer og vurderinger med andre brukere er varierte, og innehar en større grad av kompleksitet ved seg enn vurderingene overfor stat og medieplattformer. Vi skal derfor igjen se på de mest interessante funnene ut fra bredden av datamaterialet, og ikke bare konsentrere oss om hva de fleste informantene er enige om.

6.1 Personvernvurderinger overfor andre brukere

Ut fra eksempler som informantene tok opp for å beskrive ulike personvernsituasjoner gjennom intervjuene, er det visse typer personvernvurderinger som går igjen:

a. Hvordan forholde seg til innhold som blir publisert eller videresendt mot subjektets[4] vilje. (nakenbilder, festbilder)

b. Hvordan forholde seg til ukjente brukere som tar kontakt.

[4] Personen(e) innholdet dreier seg om. I dette tilfellet personen som er avbildet.

c. Hvilke brukere som skal legges til som kontakter.

d. Hvilke brukere som skal blokkeres.

e. Hvilke og hvor mange brukere som informanten velger å dele innhold med

f. Vurdering av hva slags innhold som er trygt å dele

Som med vurderingene overfor statlige institusjoner og medieplattformer, er disse vurderingene påvirket av flere faktorer enn personvernhensyn alene, for mange til å gå i detalj på. Jeg skal i dette kapitlet forklare hva slags påvirkninger informantene tok opp for ulike situasjoner de beskrev med andre brukere, se sammenhenger mellom dem og si noe om hvordan de tar disse vurderingene.

Jeg skal se nærmere på flere av disse vurderingene i resten av dette og neste kapittel. Aller først skal jeg ta for meg personvernvurderinger knyttet til konkrete personverntiltak.

6.1.1 Personverntiltak som vurderinger informantene tar overfor andre bruker

Som beskrevet i 5.2 tok flere av informantene opp hvordan de på et punkt innså at de trengte å *justere personverninnstillinger* på de sosiale medieplattformene for å bedre ivareta sitt personvern. Dette omfatter blant annet hvor mye innhold ukjente brukere kan få tilgang til på Facebook og Instagram, hvor lett det er å finne profiler på Snapchat, mulighet til å motta meldinger fra brukere som ikke har knyttet kontakt på Facebook og Instagram og hvem som kan se brukeren på Snapmap. Linda snakket om hvordan vennegjengen hennes fikk øynene opp for hvor synlige innholdet på de sosiale mediekontoene deres var for fremmede:

> [...] det ble mer og mer privat, at det ble mer avgrenset, når kanskje folk, fikk litt øynene sine opp for at, oi, hvem som helst kan se det her. [...] vi ble mer bevisst på det, det er nok grunnen til at såpass mange skaffet seg privatkontoer, det er mange som også har fått avgrenset profilbilde, at man ikke kan gå inn og like eller trykke eller noen ting.

I tillegg til flere kontoer, oppga Linda og andre informanter at de også justerte innstillingene til at kun godkjente kontakter kan se profilen, bildene og videoene de legger ut. Linda oppgir også senere at det å bli mer moden også spiller inn i hvordan vennekretsen hennes vurderte og personvern på nett som viktigere for dem. Når de oppdaget hvor mye innhold ukjente brukere hadde tilgang til, forandret de dette gjennom å innskrenke tilgangen som ukjente brukere hadde til dem.

Det er interessant hvordan Linda ordlegger seg i kommentaren «vi ble mer bevisst på det», og ikke at hun ble mer bevisst på det. Linda forklarte i starten av intervjuet at hun brukte mye tid på sosiale medier og kontakt med venner der, og hvordan dette påvirket hennes nettvaner:

> Bare for noen dager siden var jeg på kino, og jeg kunne ikke gå 30 minutter uten å sjekke mobilen min, for jeg var redd for at, ok, hvem er det som maser nå, nå må jeg bare svare...
>
> *Men er det fra deg som ikke vil gå glipp av det, eller er det fra de som forventer at du må svare?*
>
> Jeg tror det er litt begge deler, fordi nå har det blitt litt sånn at det er litt "Fear of missing out", man vil ikke gå glipp av ting, og man vil spesielt ikke gå glipp av planer og ting som de andre opplever, så da blir man jo bare aktiv hele tiden.

Det kan godt være at Lindas økte verdsetting av personvern kan ha vært en gruppeoppdagelse, at det ble sosialt akseptert innad i gruppen å bry seg mer om personvern og innstillinger for synlighet, og at *sosialt press og gruppetilhørighet* hadde en innflytelse på personvernsvurderingene hennes i denne sammenheng.

Rapportering av andre brukere var et annet sikkerhetstiltak som informantene beskrev under intervjuene for å beskytte seg mot brukere de opplever som truende, ubehagelige eller som svindlere. Da Nina ble spurt om hva hun synes om Facebook som selskap, beskriver hun denne funksjonen her:

> Mitt inntrykk er at det er veldig bra at det er mange som styrer det (Facebook), fordi at jeg merker det, hvis jeg rapporterer en profil, som for eksempel er falsk, så er jo det gjort på 12 timer. Så får jeg beskjed om at det er sletta eller hva som er gjort med den. Da vet jo jeg at da sitter det jo noen der som faktisk gjør noe og prøver å slette upassende innhold og upassende profiler og, det gjør jo at jeg føler jo at det er litt tryggere enn om bare det var en app som var utviklet.

Ved å flagge mistenksomme profiler bidrar denne vurderingen derfor både til å beskytte hennes eget personvern og andres fra de falske profilene.

6.2 Påvirkning på personvernvurderinger

Påvirkninger på informantenes personvernvurderinger overfor andre brukere er i denne sammenheng avgrenset til de mest generelle påvirkninger for å kunne si noe av betydning for

bredden av vurderinger. Vi skal her ta for oss hvordan forestillingen om at alt lagres påvirker vurderinger, og hvordan relasjoner og kontekster påvirker vurderinger.

6.2.1 Forestilling om at alt lagres og alt kan spre seg påvirker vurderinger

Informantene tok opp flere personvernsituasjoner der de gikk ut fra at alt de foretar seg på nett blir arkivert et sted. Denne forståelsen gikk igjen gjennom flere av temaene som ble tatt opp under intervjuene, og virker å ha stor påvirkning på hvordan alle informantene vurderer og personvern overfor andre brukere. Mari tok opp dette i sammenheng med Snapchat og personvern:

> […] det er også noe som jeg er litt skeptisk til, at, eller ikke helt forstår, i forhold til Snapchat, at du sender et bilde, men det forsvinner etter så lang tid, med mindre du lagrer det selv, da. Men, det blir jo lagra et sted. Det må det jo bli. Sånn som med alt annet på nettet, så blir det aldri helt borte.

Praksisen med at samtaler eller bilder blir «liggende på nettet» er noe som informantene mener kan gjøre dem sårbare, spesielt dersom dette innholdet er av en karakter de ikke vil dele med alle. Informantene hadde delte meninger på eksakt hvor mye de mente ble lagret, hvem som lagret det og for hvilke formål. Noen innrømmet også at det var en del de ikke visste om temaet, men de fleste gikk ut fra at alt som kan arkiveres blir arkivert. Informantene ser riktignok ikke på dette som overvåkning, som Mari beskriver her:

> Man blir jo på en måte overvåka, men man blir vel mer, ikke overvåka sånn, enn man blir, ja hvorfor det, eh… forska på, på en måte, ikke forska på, men, hvis du skjønner hva jeg mener. Man blir, observert, mer enn overvåka. For overvåke, da blir det jo at de retter seg spesifikt mot deg hele tiden, mens observering er mer på statistikk, hva er det du gjør, sånn og sånn og sånn, tenker jeg.

Informantene nevner blant annet internettleverandørene, Google, Facebook, Schibsted, cookies fra hjemmesider og lokasjonsinfo til mobilen som noen av aktørene og mekanismene som kan arkivere enten innhold sendt eller brukeratferd. Informantene gikk ut fra at hva selskapene er interessert i å lagre og registrere av personinformasjon var mest upersonlig, statistisk informasjon som brukeratferd, kjøpshistorikk og metadata. Siden dette ikke er innhold som informantene så på som viktige for dem på et personlig plan, var det lettere for dem å avskrive dette som uviktig å bekymre seg over. Da de ble spurt om hva de syntes om at

selskapene hadde tilgang til bildene og meldingstrådene deres, var alle informantene enige om at dette ikke var interessant for selskapene, og derfor ikke noe de gikk og bekymret seg over.

6.2.2 Relasjoners påvirkning på personvernvurderinger

Hva slags relasjon informantene har til de andre brukerne avgjør hvordan de håndterer eller forutser situasjoner som går på bekostning av personvernet deres. Visse typer relasjoner går igjen i situasjonene de beskriver, og vi skal se på de fire mest omtalte relasjoner. Enkelte av relasjonene kan overlappe, en medstudent kan for eksempel også være en nær venn. Ved hjelp av kontekstuell integritet skal vi dele inn de ulike typer aktører ut fra hvordan informantene oppfatter deres rolle er.

Nære venner blir oftest inkludert i mindre kontekster der det deles mye sensitivt innhold, som i chatgrupper og meldinger. Selv om tilliten til denne gruppen av relasjoner er høy, oppgir flere av informantene at det ofte kan oppstå situasjoner som går på bekostning av informantenes personvern med nære venner. Anders beskriver dette her:

> Det er litt oftere at det skjer, at man for eksempel, opplever noe ubehagelig som noe venner kan gjøre mot deg, eller noe. At de prøver å være litt tullete, og den andre personen opplever ikke at det er så gøy, men da pleier det som regel å fikse seg, da. […] Det er ikke en veldig stor, det er ikke en veldig sterk grad heller, da, men det er jo, det er en mild form for ubehagelighet. For det er jo bare å spørre vennen sin, for det er jo vennen sin. Ja, kan du slette det.

Som Anders sier, er ikke slike integritetsbrudd alltid like alvorlige. Ved å bruke begreper fra kontekstuell integritet, ser vi at hva Anders beskriver kan tolkes som to venner med forskjellige *informasjonsnormer* for den aktuelle konteksten, forskjellige forventninger til hva som er greit og ikke greit å poste av personlig innhold.

Ukjente brukere er naturlig nok gruppen som informantene er mest mistenksomme mot i personvernsammenheng. De vurderer det som en større risiko for at innhold blir videredelt fra dem, de er mistenksomme for svindelforsøk og de oppgir at de legger dem vanligvis ikke til som kontakter. Denne mistenksomheten har kommet fra egne og venners erfaring med ubehagelige situasjoner på nett: svindler, seksuell trakassering, hacking av profil og hatmeldinger. Hvordan informantene definerer ukjente brukere kan variere noe.

Kontekstrelaterte brukere er brukere som informantene kjenner fra en spesifikk sosial kontekst. Det kan være medarbeidere på jobben, kolleger i en frivillig organisasjon

medstudenter eller slektninger. Ofte samles disse kontaktene i egne grupper på Facebook eller gruppechatter på Messenger eller Snapchat. Informasjon som blir gitt til disse gruppene eller brukerne er vanligvis ikke personlig for informantene.

Nye relasjoner kan være brukere som informanten nettopp har møtt eller som er bekjente av dem. Informantene pleier å legge til disse kontaktene dersom de får venneforespørsel fra dem, avhengig av kontekst og informantens egen vurdering. Hvordan informantene definerer nye relasjoner varierer også her.

6.2.3 Konteksters påvirkning på personvernvurderinger

Som med hvordan informantene skiller mellom ulike typer aktører, tar de også ulike vurderinger ut fra konteksten de møter dem i. Som beskrevet i teorikapitlet under kontekstuell integritet, blir kontekster her sett på som en samling av forståelser om hvordan man oppfører seg i spesifikke sosiale sammenhenger. På nett formes disse forståelsene om sosiale roller ut fra de digitale møtepunktene for kommunikasjon og innholdsdeling. Dette kan enten være et nettforum, kommentarfeltet på en Facebook-post, en nettdating-app eller en plattform for deling av løpeturer.

For å vise et eksempel på konteksters betydning for hvordan informanter opplever integritetsbrudd og at personvernet deres settes i fare, skal vi se på en erfaring Mari forteller om her:

> […] jeg ble venn med en person på Tinder, snakket med han der og så la han meg til på Snapchat, også la han meg plutselig til på Facebook, også sender meg masse ting som jeg egentlig ikke har lyst til å, eller bry meg om, og plutselig så, «jeg så du var i sundet, spiste med moren din», for jeg posta et bilde av mamma, på Snapchat […] han kjente igjen stedet, ut ifra sånn, ingenting.

Mari beskriver hvordan hun opplevde at vurderingen med å gi en ny relasjon tilgang til hennes Facebook- og Snapchatprofil med ett ble ubehagelig. Nissenbaum argumenterer for hvordan integritetsbrudd ofte oppstår når ulike kontekster overlappes og roller blandes (Nissenbaum 2010, 137). Denne situasjonen handler for det første om forventninger til roller i spesifikke kontekster. Dersom en nær venn eller bekjent hadde sendt den samme meldingen om at han kjente igjen stedet hun og moren var, hadde ikke nødvendigvis Mari fått den samme reaksjonen av ubehag. I tillegg var konteksten Mari la ham til som kontakt at de hadde «matchet» på nettdatingappen Tinder, og vi kan gå ut fra at Mari har andre

informasjonsnormer for dette, andre forventninger til hva slags oppførsel en slik relasjon innebærer.

I teorikapitlet tok vi opp hvordan Helen Nissenbaum argumenterer for at retten til personvern handler om hvordan informasjonsstrøm i forskjellige sosiale kontekster blir appropriert (Nissenbaum 2010, 126). Ifølge dette rammeverket hadde det vært uproblematisk for Mari dersom den nye relasjonen hadde bare fått tilgang til innholdet hun delte og ikke gjort noe med det. Mari har tross alt hundrevis av kontakter på Facebook og Snapchat, og hun tenker ikke over hva disse som hun allerede har tatt en personvernvurdering på og gitt tilgang til ser gjennom av hennes innhold. Det ubehagelige oppstår idet personen hun la til «approprierer» innholdet: hvordan han identifiserer stedet og handler på dette gjennom å videreformidle informasjon om at han vet hvor de har vært, oppleves som et integritetsbrudd for Mari. Hun føler seg overvåket på grunn av at oppmerksomheten hun fikk ikke samsvarer med hennes forventning av relasjonens rolle, og situasjonen oppleves derfor ubehagelig. Dette samsvarer også med Ruth Gavisons andre premiss for når et individ opplever en innskrenking i sitt personvern: Når en part gir oppmerksomhet til et individ (Gavison 1980, 432–33).

Medieforsker danah boyd argumenterer for at selv om sosiale medier er designet for å dele og kommentere innhold, gjør ungdom hva de kan for å oppsøke mer private sfærer i sosiale nettverk (Marwick og boyd 2014). Informantene i denne studien er ikke annerledes, alle har et veldig bevisst forhold til hvor og hvem de deler bilder, videoer, tanker og vitser med. Vi skal se på et par eksempler på vurderinger de tar for å verne innholdet sitt fra visse typer relasjoner ved hjelp av å *avgrense deres sosiale fellesskap* på nett.

Avgrensning av sosiale fellesskap på nett

I mindre kontekster trenger ikke informantene å ta så mange personvernvurderinger om innholdet de deler siden konteksten med venner føles tryggere for dem. I Lindas vennegjeng fikk flere såkalte *privatkontoer* på Instagram i tillegg til deres opprinnelige konto:

> [...] det ble mer og mer privat, at det ble mer avgrenset, når kanskje folk, fikk litt øynene sine opp for at, oi, hvem som helst kan se det her. [...] vi ble mer bevisst på det, det er nok grunnen til at såpass mange skaffet seg privatkontoer, det er mange som også har fått avgrenset profilbilde, at man ikke kan gå inn og like eller trykke eller noen ting.

Disse privatkontoene på Instagram er «lukket for offentligheten», det vil si at andre brukere må få godkjennelse til å knytte kontakt og se postene deres. Ingrid Aarseth Johannessen har

forsket på dette i sin masteroppgave «Selvrepresentasjon og sosial sammenligning blant unge jenter på Instagram» (Johannessen 2016). I studien hennes hadde flertallet av informantene to kontoer for to ulike kontekster: en konto for nære venner og en konto for «offentligheten». Hvordan de fremstod i begge kontekstene var veldig forskjellig, men bevisst fra informantenes side (Johannessen 2016). Kontoene som ble knyttet til hverandre fungerer derfor som mindre, avgrensede offentligheter med få kontakter som kjenner hverandre godt, og et godt eksempel på hvordan unge sosiale mediebrukere oppsøker mer private sfærer i offentlige nettverk (Marwick og boyd 2014).

Med to kontoer blir det også en sterkere definering av de forskjellige sosiale kontekster med forskjellige normer og regler, mindre publikum når det bare er vennegjengen, mindre risiko for å oppleve ubehagelige situasjoner med ukjente brukere, og mindre risiko for at innhold forsvinner i andre kontekster. Likevel er det viktig å presisere at Linda og vennegjengen hennes har privatkonto også fordi det er gøy og uformelt å dele innhold i mindre grupper, og sekundært på grunn av personvernbekymringer. Informantenes behov for å avgrense samtaler, bilder og filmer til spesifikke sosiale kontekster er ikke nødvendigvis bare fordi de ønsker å holde innholdet i seg selv privat, det kan også være for å holde selve den interne, sosiale konteksten privat: For å beholde det interne sosiale fellesskapet som en gøy og uformell kanal, og ikke bekymre seg over hva andre måtte mene om hva de deler av innhold.

Anders forklarer hvordan han ekskluderer folk fra visse sosiale kontekster tilgang til hans Facebookprofil:

> *Du har blokkert noen?*
>
> Ja. Men da er det som regel sånn, da pleier det veldig ofte å være enten sånne familievenner eller noen sånne slektninger. Det er greit at vennene av meg ser det og ler av det og har det gøy, liksom, det bryr jeg meg ikke om, men, hvis slektninger ser det, da er det liksom… Jeg vil ikke at de skal se fyllabilder av meg og sånt, eller videoer. Har liksom et skille mellom hva som er relevant for familien min å vite, og hva venner, liksom.

Anders ønske om å avgrense slektningers og familievenners tilgang til hans Facebook-profil er ifølge ham for at de ikke skal se eventuelle «fyllabilder» og tilsvarende innhold. På denne måten redigerer han sitt eget publikum og Facebook-kontekst ut fra innhold han forventer kan bli postet av ham av vennene sine, et aktivt tiltak for å holde den sosiale konteksten med sine venner og alle normer (eller fraværet av disse) den måtte medføre, avgrenset fra hans mer seriøse sosiale kontekst med familievenner og slektninger. Med dette avgrenser han sitt

publikum i Facebook-konteksten for å skjerme familievenner og slektninger for eventuelt «tullebilder» som vennene hans kan finne på å tagge ham i eller poste på veggen hans. Dette gjøres også for å bevare Facebook-konteksten hans som en sosial sfære der han ikke trenger å bekymre seg over at sensitivt innhold blir delt.

Innholdsdeling i kontekster

Frida tok opp hvordan hun passer på hva hun skriver i meldinger til andre personer for å unngå at det kan bli spredt:

> […] hvis jeg, jeg og liksom en nær venninne av meg eller noe sånt, sånn, på grensa til å, jeg vet ikke, baksnakke, eller liksom, snakke om en person og sånt, på litt sånn, med negativ undertone, så gjør jeg ikke det på Facebook, da gjør jeg det heller face to face. [..] Jeg bare sånn, fordi at, det at jeg vet at det finnes skriftlig en eller annen plass, inni internett. […] Det er ikke sånn, en helt konsekvent ting jeg gjør, men har vært flere ganger at jeg har tenkt: ok, jeg tar det heller når vi møtes om to timer, for jeg vil ikke ha det skriftlig.

Frida beskriver i dette eksempelet en forståelse hun deler med Frida skiller i eksempelet mellom to ulike arenaer eller kontekster for innholdsdeling: nettet og snakke sammen utenfor nettet. Hun vurderer nettet til å være en for usikker kontekst/arena, og deler heller innholdet hennes utenfor nettet der informasjonen hennes ikke lagres.

Som tidligere nevnt snakket flere av informantene om hvordan det alltid vil være en viss risiko for at innhold kan bli spredt, samme hvor bra sikkerhet selskapets servere har eller hvor gode intensjoner mottakere har. Og på bakgrunn av bevisstgjøringen om at alt lagres og alt kan spre seg, tar Frida et aktivt valg om å ikke skrive noe som har potensiale til å komme på avveie.

Handlingen Frida snakker om, å sensurere hva hun selv skriver i meldinger til venner, er altså en måte hun vurderer personvern på. Foucault beskrev prinsippet bak panoptikon som en måte subjektet internaliserte frykten av å bli overvåket og tatt i å gjøre noe ulovlig, og derfor voktet seg selv og hva han gjorde (Foucault 1977). Den tilsvarende internaliseringen om at alt lagres og har mulighet til å spre seg er hva som driver Fridas selvsensur. Forskjellen mellom teorien og eksemplene her er at det ikke er en stor, overordnet maktutøver som er årsak til frykten her, men informantenes sosiale liv – at venner eller bekjente blir sinte på hva de skriver, lei seg, eller skuffet over at de videredeler hemmeligheter. Ifølge Nissenbaums kontekstuell integritet vurderer Frida her risikoen for integritetsbrudd som for stor til å sende informasjonen over nettet. Hemmelighold av denne informasjonsutvekslingen er såpass viktig

at hun velger å omgå internett og sende den verbalt, uten at informasjonen lagres. Frida og Silje har antakelig en sterkere bevissthet på at alt lagres og alt kan spre seg enn de andre informantene, og har kanskje opplevd at egne eller venners meldinger har spredt seg på denne måten.

Flere av informantene tok opp hvordan de redigerte bort innhold og hva ukjente brukere kunne se på profilen deres med tanke på potensiale arbeidsgivere. Anette snakker om dette her:

> Siden jeg vet jo det at i hvert fall arbeidsgiver og sånn går jo ofte inn på Facebook også ser, i hvert fall det de har muligheten til å se. Av bilder ofte på profilen, det vet jeg at mange gjør, før de ansetter folk. Så du passer liksom på å ha noe som du ikke er redd for at, de eventuelt kunne sett, da.

En god del av informantene tok også opp nakenbilder og lettkledde bilder som eksempel på innhold de unngikk å sende, hovedsakelig fordi de vil unngå risikoen for at de kan bli spredt. Nina beskriver dette her:

> […] så er jeg veldig nøye med på en måte, lettkledde bilder og, nakenbilder ville jeg aldri delt på noen sosiale medier. […] bildene kan forsvinne, de kan bli misbrukt, og, ja. Prøve å ha litt kontroll på hvem som ser det.

Den tidligere Nora Mørk-saken som ble tatt opp av Frida, var også et eksempel på hvor lett slike bilder kan bli spredt.

Vi har til nå sett på hvordan informantene vurderer personvern overfor statlig overvåkning, medieplattformer og andre brukere. Vi skal nå se på to ulike case-eksempler der vi skal bruke hva vi har lært gjennom kapitlene til å forstå informantenes personvernvurderinger og påvirkninger på disse enda bedre.

7 Google Maps og Snapmap som case-eksempler

I dette kapitlet skal jeg bruke Google Maps og Snapmap som eksempler på hvordan informantene tar personvernvurderinger overfor medieplattformer og andre brukere. Jeg skal først ta for meg karttjenesten Google Maps.

7.1 Google Maps

Google Maps er en karttjeneste som informasjonsselskapet Google tilbyr til å finne reiseruter og få oversikt over ukjente områder. Funksjonen kan brukes uten å ha en Google-konto, men informantene beskriver visse fordeler med å bruke den med en konto. Som nevnt i metodekapitlet, handlet den ene artikkelen informantene leste på slutten av intervjuet om hvordan Google Maps hadde oversikt over alle steder brukerne hadde bevegd seg ved hjelp av kontoen på smarttelefonen deres, og hvordan dette kunne vises flere år tilbake. Alle informantene som leste artikkelen (8 stykker) brukte Google Maps og hadde konto tilknyttet den. Ingen av informantene ble overrasket over sporingen beskrevet i artikkelen, og ingen av dem så på dette som noe spesielt negativt. Igjen ser vi at informantene ikke bekymrer seg over medieplattformenes innsamling av informasjon, men i dette tilfellet skulle man nesten tro at sporingen av hvor informantene befinner seg til alle tider ville vært mer personlig for dem og viktigere å verne om. Så hvorfor vurderer ikke informantene dette som en begrensning i deres personvern? Fridas kommentar belyser dette:

> […] jeg har ikke så stort problem med at de store selskapene vet hvor jeg er, det er mer sånn folk jeg kjenner vil jeg ikke skal vite, hvor jeg er, eller, om informasjon om meg […]

Ved hjelp av rammeverket til kontekstuell integritet ser vi at selv om informasjonen i seg selv, informantenes fysiske lokasjon, kan være høyst personlig og viktig for informantene, har de tillit til at Googles tilgang til denne informasjonen ikke blir brukt til annet enn markedsføring og forbedring av tjenestene deres. Dette gjenspeiler også funnene fra kapittel 5 om medieplattformene: informantene er innforståtte med at aktørene dette blir delt med er kun kommersielle parter, og egenskapene ved innholdet innebærer at det blir anonymisert og dermed gjort mindre personlig. Så selv om det kan argumenteres for at Google Maps kanskje teknisk sett innskrenker informantenes personvern, så opplever de ikke dette som en veldig stor innskrenking selv. Dette er muligens også på grunn av at de ikke legger merke til det,

som Lyons teori om flytende overvåkning poengterer (Bauman og Lyon 2013), og fordi de har tillit til at Google holder denne lokasjonsinformasjonen skjult fra andre brukere.

Som byttehandelen overfor medieplattformer viste i kapittel 5, kan det på tilsvarende måte være at informantene brydde seg litt om denne sporingen, men ikke nok til at de ville unnvære de praktiske godene som tjenesten tilbyr. Informantenes nøytrale perspektiv på personvern blir i så fall bekreftet med dette eksempelet (Nissenbaum 2010, 68).

7.1.1 Positiv påvirkning på fortsatt bruk av Google Maps

De åtte informantene mente også at denne sporingen bidro til å forbedre tjenestene, at de ble «skreddersydd» brukeren, som Silje her beskriver:

> […] her er det jo mer sånn at den informasjonen lagres for mitt eget beste […] det er jo noe av det som jeg synes er ganske bra med produktet, at det er liksom sånn derre, jeg taster inn, åja, jeg skal spise middag med noen som foreslår et location jeg har vært før, og så er det sånn, åja, der skal jeg, og så står det sånn, ja, det tar ca. 10 minutter å komme seg dit, det er litt mye trafikk nå, det er liksom sånn, [ler] det er veldig sånn, fremtiden, liksom.

Hvordan Silje omtaler Google Maps er et mulig eksempel på en teknologioptimisme som gikk igjen i samtalene med informantene. Denne optimismen ble oftest tatt opp i sammenheng med medieplattformenes andre formål med innsamling av brukerinformasjon på nett: for å videreutvikle medieplattformens tjenester. Den ble også brukt som argument for hvorfor medieplattformene trengte å få tilgang til brukernes personinformasjon, i dette tilfelle lokasjon.

Vi skal nå over til en noe tilsvarende tjeneste som informantene hadde mer delte meninger rundt.

7.2 Snapmap

Snapchats funksjon *Snapmap* viser hvor brukeren og kontaktene som har valgt å slå på funksjonen befinner seg på et kart. Brukerne kan slå av og på at de vises til andre på kartet når som helst. Selv om man ikke vises for andre brukere, kan man se hvor de andre brukerne er. Det er også mulig å redigere hvilke brukere som kan og ikke kan se ens egen posisjon. Eventuelle aktiviteter illustreres også automatisk, som at brukerne er i en bil, fly eller buss, hører på musikk, og lignende aktiviteter.

7.2.1 Ikke-brukerne av Snapmap

Informantene var veldig delt i hva de mente om denne funksjonen. Fem av informantene var ikke synlige på Snapmap. Silje var synlig, men oppga at hun var skeptisk til tjenesten, og derfor bare synlig for moren og romvenninnen hennes.

Påvirkning på ikke-bruk av Snapmap

De seks informantene som var skeptiske til kartfunksjonen foretrakk en større grad av anonymitet enn informantene som viste lokasjonen sin. Frida svarte dette da hun ble spurt om hvorfor hun ikke var synlig på Snapmap:

> […] fordi at folk vet hvor jeg er hele tida, det er jo, ja. Da har jeg jo null privatliv. Det hadde jeg vært veldig ukomfortabel med.

Fridas oppfatning av Snapmap la seg tett opp til et panoptisk syn på overvåkning, idet hun nærmest følte at *andre fikk kontroll over* hvor hun var. Noen av ikke-brukerne tok også opp eksempler på hvordan Snapmap kunne brukes til å *overvåke andre* ut fra et slikt panoptisk perspektiv, som Silje beskriver her:

> [...] jeg har, kjenner noen venninner også, som bruker det på en sånn derre, eh, creepy måte, at det er liksom gutter de begynner å date, også er det sånn, åja, hvorfor er han der og ikke der han sa han skulle være, og da, da begynner jeg å merke at det blir for mye [ler], på en måte.

Da Snapmap ble tatt opp som tema i intervjuet, tok Anette opp hvordan venninner hun kjenner overvåkte kjærestene sine:

> […] det er mange som bruker det til det, det vet jeg. Det har jo jeg, det har jo jeg hørt, liksom, fra venninner og. At de bruker det. Til det.
>
> *Ok? Hva har du hørt for noe?*
>
> Nei, at hun, hun ene var i hvert fall, at hun tok det på, liksom, for hun ville se hvor kjæresten var når han var ute, liksom. På byen og sånn, så ville hun liksom vite hvor han var. Så det, det er, folk bruker det jo litt til det. Det vet jeg.

Nina ga uttrykk for at hun selv ønsker å *bestemme vilkårene* for når andre brukere får vite hvor hun er:

> […] alle bare kan vite hvor du er, uten at jeg har valgt å dele det, det syns jeg er litt sånn… ja, nesten litt ekkelt. Fordi at da føler jeg meg litt sånn overvåket. Eh, og, ja. Da syns jeg det heller er bedre at jeg tar en snap og sier at, å, jeg er der. For da har jeg på en måte bestemt det.

Nina fortalte også at hun var spesielt opptatt av å sikre sitt eget privatliv under samtalen. Silje fortalte om hvordan det innimellom føles ubehagelig å observere folk som kanskje ikke tenkte over at de blir sett på Snapmap:

> [...] så får jeg av og til den følelsen, det er litt ubehagelig å vite det, fordi jeg føler at de ikke er 100 % klar over at de deler sin plassering hele tiden. Og jeg bare har, det føles liksom, ja, kan se at, oi, nå er noen oppe på sykehuset, liksom, så blir det bare litt sånn derre, det blir en litt sånn unødvendig innsikt da, for de som ikke allerede vet at jeg er der, sånn typisk.

Silje ønsket med dette ikke å havne i en overvåkningsposisjon der hun fikk for mye innsikt inn i venners personlige liv, som om hun følte hun brøt en uskreven informasjonsnorm for hvordan folk bør bruke Snapmap.

7.2.2 Brukerne av Snapmap

Fem av informantene hadde slått på funksjonen som viste deres posisjon på Snapmap for alle sine kontakter. Av disse var tre av de fire guttene synlige og to av de syv jentene. I tillegg var Silje som sagt synlig, men bare for to kontakter. Jentenes større skepsis mot tjenesten kan være av frykt for ubehagelig oppmerksomhet, noe flere av dem hadde erfaring med. Brukerne av Snapmap var mindre skeptiske til funksjonen, og så på den ut fra andre perspektiver enn makt og kontroll. De følte seg ikke overvåket da de brukte det, og de trodde heller ikke at kontaktene deres brukte Snapmap til å overvåke andre.

Ingen av disse brukerne tok opp erfaring med venner som hadde overvåket andre, så en mangel på en slik erfaring kan ha spilt inn i synet deres. Petter, informanten som var mest skeptisk til statlig og selskapers overvåkning, hadde slått på denne funksjonen og var heller ikke bekymret over å bli overvåket av vennene sine.

Disse informantene forventet at overføringsprinsippet[5] *anonymitet* ble overholdt til en viss grad: at de andre brukerne ikke brukte informasjonen i Snapmap til å overvåke kontaktene sine. Da Jonas for eksempel ble spurt om han noensinne fikk spørsmål fra vennene sine om hva han gjorde på spesifikke steder, svarte han at:

> […] jeg tror ikke det er så mange som bruker det sånn, til å se hvor hverandre er.

[5] Hvordan informasjonsflyten skal og ikke skal foregå.

Informasjonsnormene som Jonas implisitt beskriver kan knytte seg til både tid (brukere sitter ikke og følger med på andre brukere på Snapmap over lengre tid) og fokus (brukere tenker ikke over hvor en spesifikk bruker beveger seg).

Informantene som ikke ville bruke Snapmap (eller Linda som hadde begrenset synligheten), hadde den samme forventingen til overføringsprinsippet anonymitet som brukerne hadde. Forskjellen var at de hadde opplevd at disse normene var forskjellige, at hva de hadde opplevd eller hørt om styrte hvordan de forholdt seg til tjenesten. Ikke-brukerne av Snapmap hadde erfaring eller større mistanke om at andre brukere i visse kontekster (som sjalu kjærester, evt. stalkere) faktisk brukte både tid og fokus på å overvåke hverandre.

Hvordan brukerne av Snapmap resonnerte rundt Snapmap er ganske likt hvordan informantene i Humphreys studie resonnerte rundt tjenesten Dodgeball, der brukerne kunne overvåke hverandres posisjoner (Humphreys 2013, 112). I Dodgeball-studiet måtte brukerne selv skrive inn hvor de befant seg før vennene kunne finne dem, med Snapmap skjer dette automatisk. Men konseptet er veldig likt, også det at ikke alle velger å vise hvor de er. Noen av informantene i Dodgeball-studiet sa også at de ønsket en automatisert lokaliseringstjeneste tilsvarende Snapmap (Humphreys 2013, 116). Den viktigste likheten mellom brukerne av Dodgeball og brukerne av Snapmap er riktignok hvor lite bekymring det var på sikkerhet overfor andre brukere (Humphreys 2013, 116).

Sosialisering påvirker fortsatt bruk på forskjellige måter

På samme måte som sosiale opplevelser ofte var utgangspunktet for å bruke Snapmap, var s*osialt press og gruppetilhørighet* fra venner og kjærester en faktor som påvirket fortsatt bruk av tjenesten. Linda beskriver hvordan vennegjengen hennes reagerte dersom hun slo av synligheten:

> [...] det er noen ganger jeg slår det av, faktisk, men da får jeg ofte spørsmål: Hvorfor har du slått av? [...] det er ganske forventninger om at man skal på en måte være der. Ehm, og, det gjør jo at alle har kontroll på hvor du er, noe som også kan være en positiv ting, hvis du ikke er aktiv på to timer, liksom, så begynner jo folk å lure.

Linda fremstod gjennom samtalen som sosial, utadvendt og sterkt knyttet til vennene sine. Ved å være synlig på Snapmap har Linda gitt forventinger til andre om at hun pleier å ha denne synligheten slått på, og at dette er en informasjonsnorm for deres kontekst, den rådende forventningen i vennegjengen. Ruth Gavison beskriver dette paradokset med privatliv godt:

> Sometimes we may be inclined to criticize an individual for not choosing privacy, and other times for choosing it (Gavison 1980, 428).

I eksempelet Linda tar opp er det snakk om overføringsprinsippet *entitlement:* vennene hennes mener de har krav på å motta informasjon om hvor hun er. Som Lindas kommentar viser, trenger ikke det sosiale presset for å fortsette å bruke tjenesten nødvendigvis å være negativ, det kan også være en form for *omtanke, trygghet og sikkerhet* der venner passer på hverandre. Mette beskriver også dette her:

> […] jeg vet folk som bruker den for å sjekke om folk har kommet seg hjem på kvelden, for eksempel, at det er, hvis de har hatt, vært ute med en gjeng med folk på byen, så kan de på en måte sjekke at når de kommer hjem og legger seg…

Personvernet hennes føltes på denne måten ikke som begrensende i like stor grad for henne fordi hun selv *bestemte vilkårene* for «overvåkningen». De andre brukerne av Snapmap har muligens den samme innstillingen overfor sine kontakter, og kanskje har de ikke veldig mange kontakter på Snapchat i utgangspunktet. Som vi så i kapitlet om andre brukere og avgrensing av sosiale fellesskap på nett, så vurderer brukerne av Snapmap at kontaktene deres er trygge nok til å se deres lokasjonsinformasjon, og vurderer derfor konteksten som trygg. Siljes personvernvurdering var å begrense antall kontakter som kunne se henne til to stykker, og hun *avgrenset* slik hennes egen Snapmap-kontekst. Av samme grunn som Nina tidligere oppga som grunn til hvorfor hun valgte å ikke være synlig på Snapmap, føler disse brukerne at de selv har valgt termene for hvem og når lokasjonsinformasjon om dem skal vises. De har dermed skapt sin egen kontekst for hvem som de kan bli «overvåket» av.

Det kan også være at disse brukerne ikke vurderer denne lokasjonsinformasjonen som like personlig for dem som ikke-brukerne, eller at de fortsetter å være der av sosialt press, som Linda fortalte om.

7.3 Avsluttende drøfting av Case-eksempler

Vi har sett at alle informantene brukte Google Maps, og at ingen av dem så det som problematisk at Google sporet deres lokasjon til alle tider. Dette var kanskje ikke så overraskende med tanke på informantenes aksept av medieplattformenes innsamling av informasjon. I tillegg kan bevisstheten om at alt lagres som ble diskutert i 6.2.1 også spille inn i aksepten av Google Maps, til at dette også omfatter lokasjonssporing. Aksepten av Google Maps kan også knyttes til hvilke fordeler informantene får med en skreddersydd, personalisert

opplevelse av tjenesten. Det at ingen av informantene reagerte negativt på artikkelen, ikke engang Petter som var mest kritisk til medieplattformenes innsamling av personinformasjon, var litt overraskende. Men kanskje dette understreker det nøytrale perspektivet informantene har på personvern, at de bryr seg om personvern på nett, men ikke nok til å unnvære de digitale godene de har blitt vant til. Selve tjenestens praktiske funksjoner i seg selv utgjør den største påvirkningen på fortsatt bruk, og brukerne av tjenesten tar alle en vurdering om at tjenesten er trygg, at den ikke innskrenker deres personvern.

Med Snapmap hadde brukerne og ikke-brukerne to forskjellige perspektiver å se lokasjonstjenesten på. Ikke-brukerne opplevde at tjenesten var inntrengende og innskrenket deres behov for privatliv. Dette var delvis på grunn av negative erfaringer enkelte av informantene hadde hatt eller hørt om fra venner. Deres opplevelse av tjenesten lå tett opp til et panoptisk maktperspektiv som Foucault argumenterer for (Foucault 1977).

Brukerne av tjenesten opplevde ikke at tjenesten var inntrengende. Tvert imot synes de den var praktisk og morsom. Enkelte av brukerne trakk frem hvordan vennegjenger brukte den til å passe på at alle hadde kommet trygt hjem fra byen. Brukerne fortalte ikke om negative erfaringer med tjenesten. Det var mest gutter som brukte tjenesten, som kanskje ikke var like redde for egen sikkerhet som jenter.

Dersom vi sammenligner reaksjonene på de to tjenestene finner vi at selv om Google Maps faktisk oppbevarer mer informasjon om brukerne enn Snapmap gjør, i form av å lagre informasjon om hvor brukerne har vært til alle tider, er det eksponering mot andre brukere som oppleves som ubehagelig av halvparten av informantene. Dette har også vært gjennomgående gjennom oppgaven. Det interessante er hvordan disse ikke-brukernes holdninger står i så sterk kontrast til Snapmap-brukerne, som verdsatt tjenesten mer enn å skjule sin egen lokasjon fra andre. De negative erfaringene og historiene til flere av ikke-brukerne hadde tydelig påvirket deres ikke-bruk, så det er godt mulig en mangel på negative erfaringer også kan være en påvirkning for brukernes fortsatt bruk. I tillegg var det en overvekt av gutter som brukte tjenesten (tre av fire) enn jenter som gjorde det, (tre av syv) og behovet for sikkerhet og anonymitet kan oppleves større for jenter enn for gutter. Men det er likevel tydelig at det er flere sosiale påvirkninger som spiller inn i hvorfor halvparten av informantene fortsetter å bruke Snapmap. Ikke-brukere som Mette trakk også frem hvordan venner hun kjente brukte tjenesten til å passe på hverandre.

8 Konklusjon

Informantene tok alle vurderingen om å akseptere statlige institusjoners rett til å overvåke dem. Den viktigste påvirkningen på denne avgjørelsen er hvordan informantene oppfatter at statlige institusjoner beskytter borgerne sine. Dette skjer gjennom overvåkningstiltak mot terror og kriminalitet. Politiet kan også bruke lokasjonsinformasjon fra borgeres telefon til å redde mennesker som har forsvunnet og kan avdekke kriminelle aktiviteter gjennom tilgang til netthistorikk, som i Nora Mørk-saken. Denne bevisstheten viser til Lyons teoretiske begrep om fryktfaktoren. Informantene mener at denne samfunnsnytten er viktigere enn deres krav på personvern, og viser derfor til et nøytralt perspektiv på personvern. De mener også at denne overvåkningen ikke gjelder for dem som er lovlydige.

En annen påvirkning på denne tankegangen omfatter en tillit til staten og til lovene som beskytter borgernes personvern fra de statlige institusjoner. Synoptikon kan hjelpe med å forstå denne tilliten ved å rette søkelys på prosessene som beskytter borgerne fra statlige institusjoner.

Alt i alt veide alle informantene sitt eget personvernhensyn som mye lavere enn påvirkningene for å akseptere statlig overvåkning.

Alle informantene tok vurderingen om å fortsette å bruke medieplattformene. De fleste av informantene ser på medieplattformene mest som systemer for informasjon og kommunikasjon, og ansvarliggjør dem heller ikke for personvernkonflikter. Informantene så på utvekslingen av medieplattformenes tjenester mot innsamling av brukernes personlige informasjon som en byttehandel. Dette reflekterte informantenes nøytrale perspektiv på personvern, at personvern kan forhandles om som et gode. De var heller ikke redd for at selskapene var interesserte i innholdet som føltes viktige for dem, og de gikk ut fra at brukeratferden deres ble analysert sammen med mange andres brukeratferd og anonymisert.

En påvirkning for fortsatt bruk er tillit til at medieplattformene tok vare på informasjon deres. Synoptiske maktprosesser kan forklare en av informantenes forståelse om hvordan internasjonale lover gir økt tillit til selskapene.

Informantene mente at de selv var ansvarlige for å sikre sitt eget personvern i medieplattformene, og trakk frem det å endre personverninnstillinger og rapportere ukjente brukere som metoder for dette. En god tilrettelegging av sikkerhetsinnstillinger,

rapporteringsfunksjoner og oppfølging bidrog til denne tilliten som en positiv påvirkning for fortsatt bruk.

Målrettet reklame ble sett på som ubehagelig for noen, og en fordel av andre. Det var derfor både en positiv og negativ påvirkning på fortsatt bruk.

En følelse av teknologisk kompetanse er en positiv faktor for fortsatt bruk som vi finner hos tre av informantene. Informantene forklarer hvordan denne kompetansen får dem til å føle seg trygge i situasjoner de må ta personvernvurderinger.

En gjennomgående teknologioptimisme hos informantene kan ha en påvirkning på hvilket perspektiv de vurderer nye digitale løsninger ut fra. Dette kan påvirke informantene til å se på disse løsningene som positive, og ikke som invaderende i deres personvern.

Informantene mener at de store medieplattformenes «monopol» på markedet gjør det vanskelig å unngå å bruke dem, og er en viktig faktor for fortsatt bruk. Dette gjelder spesielt de sosiale mediene som knytter informantene sammen med vennene deres.

Generelt sett veide informantene sitt eget personvern som en adskillig mindre viktig negativ påvirkning på fortsatt bruk av medieplattformene enn summen av de andre påvirkningene. Bekymring om eget personvern kunne også være en positiv faktor for fortsatt bruk, i form av personverninnstillinger og rapporteringsfunksjoner.

Informantene så på andre brukere som den største risikoen for deres personvern. Situasjonene og eksemplene de tok opp inkluderte flere forskjellige typer personvernvurderinger. Justering av personverninnstillinger omfattet noen slike personvernvurderinger der informantene hadde mulighet til å skjule sin egen tilstedeværelse på nett fra andre brukere. Rapportering av falske profiler var en annen vurdering de tok opp under intervjuene som en måte å beskytte seg selv og andre fra ukjente brukere med dårlige motiver.

Påvirkninger på de forskjellige personvernvurderinger omfattet først en forestilling om at all aktivitet på nett lagres og har mulighet til å spre seg. Relasjoner var en annen påvirkning på vurderinger der informantene skillet mellom nære venner, ukjente brukere, kontekstrelaterte brukere og nye relasjoner.

Kontekster har stor påvirkning på brukeres personvernvurderinger overfor andre brukere. Avgrensing av sosiale fellesskap på nett er en måte informantene tar personvernvurderinger på for å verne sin personlige informasjon både fra ukjente brukere og kontekstrelaterte brukere. Med avgrensing forandrer de hvilke brukere som får tilgang til deres personlige

informasjon og deres tilstedeværelse i konteksten. En av informantene tok opp hvordan vennegjengen hennes hadde to kontoer. En annen informant blokkerte slektninger som prøvde å legge ham til som kontakt på Facebook. Med dette ønsket han å bevare Facebook-konteksten som en kanal der han ikke trengte å bekymre seg over hva spesifikke kontekstrelaterte brukere mente om bildene som ble lagt ut av ham. En annen informant tok opp hvordan hun selvsensurerte seg selv når hun skrev meldinger over nettet, og at hun heller tok sensitive samtaler utenfor nettet for å unngå at det ble lagret. Flere av informantene redigerte også bort innhold på de sosiale medieplattformene med tanke på at potensiale arbeidsgivere ikke skulle se dem. Enkelte av informantene tok også opp nakenbilder og lettkledde bilder som eksempel på innholdsdeling som de passet på å aldri sende.

Informantene har hovedvekten av sine personvernbekymringer knyttet til andre brukere, og som vi har sett har de mange og forskjellige personvernstrategier for å unngå ubehagelige situasjoner på nett.

Case-eksempelet med Google Maps viser oss at alle åtte av informantene som leste artikkelen ikke er redd for å la Google arkivere og kontinuerlig samle inn hvor de befinner seg til alle tider. En eventuell bekymring blir oppveiet av de praktiske fordelene denne tjenesten tilbyr, som er den viktigste påvirkningen for fortsatt bruk. Innhenting av brukernes lokasjonshistorikk blir også forklart som at den forbedrer informantens opplevelse av tjenesten, et mulig uttrykk for teknologioptimisme.

Med Case-eksempelet med Snapmap mente ikke-brukerne av tjenesten at den innskrenket deres personvern i stor grad. Personvernhensyn var derfor den viktigste påvirkningen på informantenes ikke-bruk. Dette kan muligens forstås bedre ut fra et panoptisk maktperspektiv, der informantene mente at andre brukere «fikk kontroll» over hvor de befant seg. Eksempler på dette inkluderte overvåkning av venner og kjærester. En av informantene mente hun heller selv ville bestemme vilkår for å dele hvor hun befant seg, en annen synes det kunne være ubehagelig å overvåke andre, at dette gikk ut over deres personvern.

Ikke-brukernes opplevelse av tjenesten står i kontrast til brukernes opplevelse. Disse opplevde ikke at deres synlighet på Snapmap gikk ut over deres personvern. Dette kan delvis være fordi det var flest gutter som var synlige, det kan også være fordi disse brukerne ikke hadde hatt eller hørt om tilsvarende ubehagelige erfaringer som ikke-brukerne tok opp.

Tjenesten og dets sosiale funksjoner var påvirkninger for hvordan brukerne oppfattet var praktisk og morsom. Brukerne av Snapmap mente de hadde valgt termene for personvern ut

fra *hvem* som skulle få tilgang til deres lokasjon. Ikke-brukeren Nina mente derimot hun selv ville velge termene for eget personvern ut fra *når* hun valgte å fortelle kontaktene hennes hvor hun var. Snapmap-casen lignet på Dodgeball-casen til Lee Humphreys, spesielt i forhold til hvordan Snapmap-brukerne ikke bekymret seg over andre brukere når de brukte funksjonen.

Ut fra brukernes opplevelser viser Snapmap seg som en useriøs og leken kontekst der de sosiale spillereglene blir flyttet på. I tillegg bekrefter case-eksemplene hvordan andre brukere er den største kilde til brukeres bekymringer på nett.

8.1 Veien videre

Snapmap er et mikrokosmos av personvernvurderinger, og et egnet objekt til å utforske videre i mer detalj. For det første står ikke-brukernes sterke meninger mot den i kontrast til brukernes opplevelse av tjenesten. Det hadde vært interessant å utforske brukernes selvbevissthet til tjenesten nærmere, hvordan brukerne «leker» overvåkere av vennene sine, og generelt fått samlet inn flere opplevelser og historier knyttet til den gjennom kvalitative studier.

Det kan også være interessant å utforske personvernholdninger på nett ut fra andre alderssegment for å sammenligne hvordan meninger og holdninger avviker. Er eldre generasjoner like lite bekymret som studiens unge voksne overfor statlig overvåkning og medieplattformers innsamling av personinformasjon? Er de også mest bekymret over andre brukere på nett eller ikke? Som informanten Nina forklarte i delen om teknologioptimisme, har eldre generasjoner andre forutsetninger for å forstå internett og teknologi, og med det også andre holdninger og forventinger om risikomomenter.

9 LITTERATURLISTE

Albrechtslund, Anders. 2008. «Online Social Networking as Participatory Surveillance». *First Monday* 13 (3). https://doi.org/10.5210/fm.v13i3.2142.

Andrejevic, Mark. 2004. «The Work of Watching One Another: Lateral Surveillance, Risk, and Governance». *Surveillance & Society* 2 (4). https://doi.org/10.24908/ss.v2i4.3359.

———. 2006. «The Discipline of Watching: Detection, Risk, and Lateral Surveillance: Critical Studies in Media Communication: Vol 23, No 5». *Critical Studies in Media Communication* 23 (5): 391–407.

Bauman, Zygmunt, og David Lyon. 2013. *Liquid Surveillance: A Conversation*. Cambridge, UK; Malden, MA: Polity Press. http://www.dawsonera.com/depp/reader/protected/external/AbstractView/S9780745676371.

BBC News. 2019. «Making a Murderer Case to Be Re-Examined», 26. februar 2019, pargr. US & Canada. https://www.bbc.com/news/world-us-canada-47380658.

Bentham, Jeremy. 2018. *Panopticon - Jeremy Bentham*. Farmington Hills: Gale Ecco. https://www.bokklubben.no/samfunn-og-kultur-generelt/panopticon-jeremy-bentham/produkt.do?produktId=15921653.

Berg, Ingvild. 2012. «Unge mobbes og rangeres på Formspring». Aftenposten. 2012. https://www.aftenposten.no/article/ap-K3pp6.html.

Bicchieri, Cristina. 2000. «Words and Deeds: A Focus Theory of Norms». I , 153–84. https://doi.org/10.1007/978-94-015-9616-9_10.

boyd, danah. 2014. *It's Complicated: The Social Lives of Networked Teens*. New Haven: Yale University Press.

Boyle, Alan. 2013. «Gay? Conservative? High IQ? Your Facebook 'likes' Can Reveal Traits». NBC News. 12. mars 2013. http://www.nbcnews.com/science/science-news/gay-conservative-high-iq-your-facebook-likes-can-reveal-traits-f1C8805606.

Bryman, Alan. 2016. *Social Research Methods*. 5 edition. Oxford ; New York: Oxford University Press.

Cadwalladr, Carole, og Emma Graham-Harrison. 2018. «Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach». *The Guardian*, 17. mars 2018, pargr. News. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Duportail, Judith. 2017. «I Asked Tinder for My Data. It Sent Me 800 Pages of My Deepest, Darkest Secrets». *The Guardian*, 26. september 2017, pargr. Technology. https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold.

Fossheim, Kenneth, Elin Sørsdahl, og Mads Fremstad. 2019. «Sofie (27) danset med Trond Giske - dette er hennes historie». *TV 2 Spesialer*, 30. mai 2019. https://www.tv2.no/spesialer/sofie-27-danset-med-trond-giske-dette-er-hennes-historie.

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

Gavison, Ruth. 1980. «Privacy and the Limits of Law». *The Yale Law Journal* 89 (3): 421–71. https://doi.org/10.2307/795891.

Geertz, Clifford. 1973. «Thick Description: Toward an Interpretive Theory of Culture». I *The Interpretation of Cultures: Selected Essays*. Bd. 1.

Gentikow, Barbara. 2005. *Hvordan utforsker man medieerfaringer?* Kristiansand: IJ-forlaget.

Hill, Kashmir. 2012. «How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did», 2012. https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#fd9a0a966686.

Hoven, Jeroen van den, Martijn Blaauw, Wolter Pieters, og Martijn Warnier. 2018. «Privacy and Information Technology». I *The Stanford Encyclopedia of Philosophy*, redigert av Edward N. Zalta, Summer 2018. Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/sum2018/entries/it-privacy/.

Humphreys, Lee. 2013. «Mobile Social Networks and Surveillance». I *Media, Surveillance and Identity: Social Perspectives*, New edition edition, 109–26. New York: Peter Lang Inc., International Academic Publishers.
Johannessen, Ingrid Aarseth. 2016. «'Koffor har isje eg det du har?' Selvpresentasjon og sosial sammenligning blant unge jenter på Instagram». Bergen: Universitetet i Bergen. https://bora.uib.no/handle/1956/12379.
Judah, Sam. 2016. «Netflix Documentary Leads to Debate about Convicted Murderer», 5. januar 2016, pargr. Trending. https://www.bbc.com/news/blogs-trending-35234883.
Larson, Selena. 2019. «Every single Yahoo account was hacked - 3 billion in all». *CNN business*, 30. mai 2019. https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html.
Lindlof, Thomas R. 1995. *Qualitative Communication Research Methods*. Sage Publications.
Ma, Alexandra. 2018. «China has started ranking citizens with a creepy 'social credit' system — here's what you can do wrong, and the embarrassing, demeaning ways they can punish you». *Business Insider*, 2018. https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4.
Madden, Mary. 2012. «Privacy Management on Social Media Sites», 20.
Marwick, Alice E., og danah boyd. 2014. «Networked privacy: How teenagers negotiate context in social media». *New Media & Society* 16: 1051–67. https://doi.org/10.1177/1461444814543995.
Mathiesen, Thomas. 1997. «The Viewer Society: Michel Foucault's `Panopticon' Revisited». *Theoretical Criminology* 1 (2): 215–34. https://doi.org/10.1177/1362480697001002003.
———. 2013. *Towards a Surveillant Society: The Rise of Surveillance Systems in Europe*. Waterside Press.
«Medienorge: Andel med tilgang til internett». 2019. medienorge. 2019. http://medienorge.uib.no?cat=statistikk&medium=ikt&queryID=347.
«Medienorge: Internett-bruk en gjennomsnittsdag». 2019. medienorge. 2019. http://medienorge.uib.no?cat=statistikk&medium=ikt&queryID=315.
Mæland, Christine Marie. 2017. «Ikke-bruk av Facebook og ubehaget bak. En studie av norske Facebook-unnvikere mellom 25-35 år og selvrepresentasjon». Bergen: Universitetet i Bergen. https://bora.uib.no/handle/1956/16138.
Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press.
NRK. 2018. «Ni bøtelagt for spredning av Nora Mørk-bilder». NRK. 16. april 2018. https://www.nrk.no/sport/ni-botelagt-for-spredning-av-nora-mork-bilder-1.14009852.
«NSD personverntjenester: Barnehage og skole». 2018. 2018. https://nsd.no/personvernombud/hjelp/forskningstema/barnehage_skole.html.
Orwell, George. 1949. *1984*. Houghton Mifflin Harcourt.
Prensky, Marc. 2001. «Digital Natives, Digital Immigrants Part 1». *On the Horizon* 9 (5): 1–6. https://doi.org/10.1108/10748120110424816.
Price, Rob. 2017. «Google may be quietly tracking everywhere you go — here's how to turn it off». *Business Insider*, 2017. https://www.businessinsider.com/google-location-history-maps-everywhere-you-go-how-to-turn-it-off-2017-4.
Seifert, Dan. 2013. «Social question and answer site Formspring to shut down on March 31st». The Verge. 15. mars 2013. https://www.theverge.com/2013/3/15/4110196/social-question-answer-site-formspring-shut-down-march-31st.
Sjøberg, Jeanette. 2019. «Michal Kosinski: – Retten til et privatliv slik vi kjenner det er definitivt over». *Aftenbladet*, 30. mai 2019. http://www.aftenbladet.no/article/sa-5aXvW.html.
Thagaard, Tove. 1998. *Systematikk og innlevelse: En innføring i kvalitativ metode - Institutt for sosiologi og samfunnsgeografi (ISS)*. https://www.sv.uio.no/iss/forskning/publikasjoner/boker/1990-1999/systematikk.html.
Warren, Samuel D., og Louis D Brandeis. 1890. «The Right to Privacy». *Harvard Law Review* 4 (5): 193–220.
Wong, Julia Carrie. 2019. «Facebook's Zuckerberg Announces Privacy Overhaul: 'We Don't Have the Strongest Reputation'''». *The Guardian*, 30. april 2019, pargr. Technology.

https://www.theguardian.com/technology/2019/apr/30/facebook-f8-conference-privacy-mark-zuckerberg.

Vedlegg 1: NSD godkjenning

NSD

Hallvard Moe
Fosswinckelsgate 6
5007 BERGEN

Vår dato: 13.11.2017 Vår ref: 56792 / 3 / BGH Deres dato: Deres ref:

Forenklet vurdering fra NSD Personvernombudet for forskning

Vi viser til melding om behandling av personopplysninger, mottatt 25.10.2017.
Meldingen gjelder prosjektet:

56792	*Sosiale medlebrukeres holdinger til personvern.*
Behandlingsansvarlig	*Universitetet i Bergen, ved institusjonens øverste leder*
Daglig ansvarlig	*Hallvard Moe*
Student	*Terje Sandkjær Hanssen*

Vurdering

Etter gjennomgang av opplysningene i meldeskjemaet med vedlegg, vurderer vi at prosjektet er omfattet av personopplysningsloven § 31. Personopplysningene som blir samlet inn er ikke sensitive, prosjektet er samtykkebasert og har lav personvernulempe. Prosjektet har derfor fått en forenklet vurdering. Du kan gå i gang med prosjektet. Du har selvstendig ansvar for å følge vilkårene under og sette deg inn i veiledningen i dette brevet.

Vilkår for vår vurdering

Vår anbefaling forutsetter at du gjennomfører prosjektet i tråd med:

- opplysningene gitt i meldeskjemaet
- krav til informert samtykke
- at du ikke innhenter sensitive opplysninger
- veiledning i dette brevet
- Universitetet i Bergen sine retningslinjer for datasikkerhet

Veiledning

Krav til informert samtykke

Utvalget skal få skriftlig og/eller muntlig informasjon om prosjektet og samtykke til deltakelse. Informasjon må minst omfatte:

- at Universitetet i Bergen er behandlingsansvarlig institusjon for prosjektet
- daglig ansvarlig (eventuelt student og veileders) sine kontaktopplysninger
- prosjektets formål og hva opplysningene skal brukes til

Dokumentet er elektronisk produsert og godkjent ved NSDs rutiner for elektronisk godkjenning

NSD – Norsk senter for forskningsdata AS Harald Hårfagres gate 29 Tel: +47-55 58 21 17 nsd@nsd.no Org.nr. 985 321 884
NSD – Norwegian Centre for Research Data NO-5007 Bergen, NORWAY Faks: +47-55 58 96 50 www.nsd.no

- hvilke opplysninger som skal innhentes og hvordan opplysningene innhentes
- når prosjektet skal avsluttes og når personopplysningene skal anonymiseres/slettes

På nettsidene våre finner du mer informasjon og en veiledende mal for informasjonsskriv.

Forskningsetiske retningslinjer
Sett deg inn i forskningsetiske retningslinjer.

Meld fra hvis du gjør vesentlige endringer i prosjektet
Dersom prosjektet endrer seg, kan det være nødvendig å sende inn endringsmelding. På våre nettsider finner du svar på hvilke endringer du må melde, samt endringsskjema.

Opplysninger om prosjektet blir lagt ut på våre nettsider og i Meldingsarkivet
Vi har lagt ut opplysninger om prosjektet på nettsidene våre. Alle våre institusjoner har også tilgang til egne prosjekter i Meldingsarkivet.

Vi tar kontakt om status for behandling av personopplysninger ved prosjektslutt
Ved prosjektslutt 15.01.2018 vil vi ta kontakt for å avklare status for behandlingen av personopplysninger.

Gjelder dette ditt prosjekt?

Dersom du skal bruke databehandler
Dersom du skal bruke databehandler (ekstern transkriberingsassistent/spørreskjemaleverandør) må du inngå en databehandleravtale med vedkommende. For råd om hva databehandleravtalen bør inneholde, se Datatilsynets veileder.

Hvis utvalget har taushetsplikt
Vi minner om at noen grupper (f.eks. opplærings- og helsepersonell/forvaltningsansatte) har taushetsplikt. De kan derfor ikke gi deg identifiserende opplysninger om andre, med mindre de får samtykke fra den det gjelder.

Dersom du forsker på egen arbeidsplass
Vi minner om at når du forsker på egen arbeidsplass må du være bevisst din dobbeltrolle som både forsker og ansatt. Ved rekruttering er det spesielt viktig at forespørsel rettes på en slik måte at frivilligheten ved deltakelse ivaretas.

Se våre nettsider eller ta kontakt med oss dersom du har spørsmål. Vi ønsker lykke til med prosjektet!

Vennlig hilsen

Marianne Høgetveit Myhren

Belinda Gloppen Helle

Kontaktperson: Belinda Gloppen Helle tlf: 55 58 28 74 / belinda.helle@nsd.no