
INGENTING Å SKJULE?

*En kvalitativ studie av to generasjoners holdninger til personvern
i sosiale nettverkstjenester*



HANNA KVAMME

VÅR 2023

Masteroppgave i Medier og Kommunikasjon

v/ Universitetet i Bergen, Institutt for informasjons- og medievitenskap

Sammendrag

Denne masteroppgaven tar for seg personvern i sosiale nettverkstjenester (SNS), og utforsker hvilke holdninger til personvern som eksisterer blant ulike generasjoner. Det er mange utfordringer på dette området. Vilkårene er komplekse og personvernsinnstillingene kan være vanskelig å forstå – og att på til, er de i stadig endring. Hvordan brukerne navigerer mellom private og offentlige sfærer i SNS, vil også være avgjørende for hvor sterkt personvern de har. Det kreves derfor mye av dagens mediebrukere for å skulle håndtere alt dette.

Ved å ta utgangspunkt i tre-komponentmodellen for holdninger, belyser denne studien hvordan tolv informanter tilhørende Boomer-generasjonen og Generasjon Z forstår, handler og føler i møte med personvernet på Facebook og Instagram. Datagrunnlaget bygger på kvalitative forskningsintervju, kombinert med en tenke høyt-metode. Sentrale forankringer er blant annet Erving Goffman (1959) sin teori om selvrepresentasjon. Helen Nissenbaum (2010) sitt bidrag om kontekstuell integritet, er også av betydning for å analysere krenkelser av personvernet.

Tittelen – Ingenting å skjule? – gjenspeiler en utbredt holdning blant informantene, som ser ut til å prege deres oppfatning av personvernet. Resultatene antyder at det er mye forvirring om hva et personvern er, og hvorfor det er viktig. Flere overser også at personvernet er noe som kan bidra til kollektive gevinster for samfunnet. Funnene viser imidlertid til noen interessante generasjonsforskjeller. Generasjon Z viser til en generelt høyere kritisk medieforståelse, enn Boomerne, som ser ut til å undervurdere den massive datainnsamlingen og konsekvensen av selvavsløring i SNS. Det betyr likevel ikke at Boomerne er helt frakoblet – de er bare en annen type brukere enn Generasjon Z, noe som kommer tydelig frem i denne studien.

Forord

Det siste året kommer til å gå inn i minneboken som en av de bedre. Det har vært lærerikt og givende på mange plan. Samtidig skal jeg ikke legge skjul på, at det har vært noen krevende og frustrerende timer underveis. Nå skal masterboblen straks sprekkes, og jeg er klar for å ta hverdagen tilbake. Før den tid kommer, er det er rekke som fortjener en takk.

Først og fremst vil jeg rette oppmerksomheten til min dyktige veileder, Torgeir Uberg Nærland. Takk for gode råd, fleksible veiledninger og at du holdt meg på sporet. Videre vil jeg takke Mediebruksgruppen, med Hallvard og Brita i spissen - for påfyll både på faglige områder og i kaffekoppen. Evnen dere har til å løfte frem masterstudenter er unik, og jeg har fått mye ut av forskningsgruppens aktiviteter. I denne forbindelse vil jeg rette en takk til både Irene Costera Mejier og Ranjana Das, for deres inspirerende tilbakemeldinger.

En stor takk til Medietilsynet og Fritt Ord for masterstipend. Det har vært svært motiverende å vite at dere ser aktualiteten av tematikken, og ønsket å satse på mitt prosjekt.

Til alle på lesesal 635 – takk for gøyale stunder, lange lunsjer og prokrastinering mellom slagene. Vi kom i mål til slutt. Takk til mamma for korrekturlesing, og gode heia-meldinger fra venner og familie. Dette masterprosjektet har vært gjenstand for påfallende mange gode samtaler, med både kjente og ukjente - og det er gøy å se at det vekker engasjement. Dette er tydeligvis et tema som må snakkes høyere om.

En spesiell takk til samboer, for tålmodighet og beroligende ord, når knekkene kom.

Den største takken bør uavhengig tilhøre mine flotte informanter. Takk for at dere tok dere tid fra deres travle hverdager for å delta i studien, og delte deres erfaringer med en fremmed. Det er dere som utgjør masteroppgaven - jeg har bare satt det i system.

Hanna Kvamme

Bergen, 31.05.2023

Innholdsfortegnelse

Sammendrag	i
Forord	ii
KAPITTEL 1 – Introduksjon	1
1.1 Forskningsspørsmål og analytiske dimensjoner	2
1.1.1 Operasjonalisering av sentrale begreper	3
1.1.2 Analysespørsmål (AS) – Kognitiv, Atferd og Affektiv	6
1.2 Oppgavens Struktur	7
KAPITTEL 2 – Bakgrunn	8
2.1 Personvernets fremvekst: Et skille mellom privat og offentlig	8
2.2 Definisjon av personvernsbegrepet	9
2.3 Nye forretningsmodeller	10
2.4 Tidligere forskning på personvern	12
KAPITTEL 3 - Teoretiske Perspektiver	13
3.1 Privatlivsparadokset	13
3.2 Personvernets betydning for individ og samfunn	15
3.2.1 Et individuelt gode	15
3.2.2 Et kollektivt gode	15
3.2.3 Personvern som egenverdi og kjerneverdi	16
3.3 Kontekstuell Integritet	17
3.4 Navigering av privatliv på SNS	18
3.4.1 Handlingsmuligheter (Affordances) på SNS	19
3.4.2 Selvrepresentasjon: Inntrykkskontroll, forestilt publikum og kontekstkollaps	19
3.4.3 Taktikker: selvavsløring og selvensur	20
3.4.4 Kritisk medieforståelse og kommunikativ handlekraft (agency)	21
3.5 Teoretisk oppsummering	22
KAPITTEL 4 – Metode	23
4.1 Valg av kvalitative metoder	23
4.1.1 Kvalitative forskningsintervjuer	24
4.1.2 Tenke høyt-metode	25
4.2 Planlegging av studien	26
4.2.1 Utvalgsriterier	26
4.2.2 Intervjuguide	27
4.2.3 Pilotstudie	28
4.3 Gjennomføring av datainnsamlingen	29
4.3.1 Etske hensyn	29
4.3.2 Rekrutteringsprosess	30
4.3.3 Studiens utvalg	31
4.3.4 Datainnsamling	32
4.4 Analyse av datamaterialet	33
4.4.1 Forberedelse av datamaterialet: Transkribering	33

4.4.2 Koding av datamaterialet: Bearbeiding	34
4.4.3 Kategorisering av datamaterialet: Analysetemaer	34
4.5 Metodiske refleksjoner.....	35
KAPITTEL 5 - Den Kognitive Komponenten.....	38
5.1 Overordnet kunnskap om personvern.....	38
5.1.1 Kunnskapsnivået preges av informantenes yrkesbakgrunn.....	39
5.1.2 Lav kjennskap til personvernsforordningen (GDPR).....	40
5.2 Kunnskap om Meta sin behandling av personopplysninger.....	41
5.2.1 Meta sin datainnsamling: Boomerne viser til en lavere kritisk medieforståelse	41
5.3 Kognitiv vurdering av privatliv og personvern	43
5.3.1 Blitt mer bevisst på personvern over tid.....	43
5.3.2 Privatliv betyr mer for Boomerne enn for Generasjon Z	45
5.3.3 Mange hevder at de ikke har noe å skjule	47
5.4 Oppsummering av den kognitive holdningskomponenten.....	48
KAPITTEL 6 - Atferdskomponenten.....	49
6.1 Periodiske personvernshandlinger.....	50
6.1.1 Boomerne trykker rett på godta – Gen Z forsøker å tilpasse personvernet.....	50
6.2 Statistiske personvernshandlinger (tenke høyt-øvelse).....	51
6.2.1 Boomerne er redde for å stille inn feil – Gen Z er skeptiske til stedstjenester.....	52
6.3 Dynamiske personvernshandlinger.....	56
6.3.1 Boomerne bruker grupper – Gen Z bruker flere kontoer	57
6.3.2 Boomerne har vanskeligere for å blokkere andre brukere, enn Gen Z.....	58
6.3.3 Boomerne «skriver dagbok» og Gen Z «skaper fotoalbum»	60
6.3.4 Selvsensur gjennom ulike taktikker	61
6.4 Oppsummering av komponenten for atferd.....	63
KAPITTEL 7 - Den Affektive Komponente.....	64
7.1 Følelser knyttet til det institusjonelle personvernet på Meta	64
7.1.1 Boomerne føler på en viss kontroll – Gen Z føler seg helt maktesløse.....	64
7.1.2 Boomerne spekulerer – Gen Z er overbevist over at de overvåkes.....	66
7.2 Følelser knyttet til det sosiale personvernet på Meta	69
7.2.1 Alle kjenner noen som har blitt kontokapret den siste tiden: Frykt, Ubehag, Kynisk.....	69
7.2.2 Bildedeling uten samtykke: Ubehag, Sinne, Sårbar, Vantro.....	71
7.3 Oppsummering av den affektive komponenten	74
KAPITTEL 8 - Oppsummerende Diskusjon og Konklusjon	75
8.1 Ingenting å skjule – en utfordrende holdning for personvernet.....	77
8.2 Konklusjon	83
8.3 Veien videre.....	85
Referanser	87
Vedlegg 1 – Intervjuguide	92
Vedlegg 2 – Vurdering fra Sikt	94

KAPITTEL 1 – Introduksjon

Hva betyr privatliv for deg? Er det noe du ønsker å beskytte? Eller tenker du, «jeg har jo ingenting å skjule?». Uavhengig hva du forteller deg selv, så har vi gjerne noe vi ønsker å holde tettere til brystet. I hverdagen lukker vi vanligvis døren når vi går på toalettet. Døren fungerer som et *personvern*. Døren skjerner oss fra andre som går forbi. Vi gjør nødvendigvis ikke noe ulovlig der vi sitter, men vi ønsker bare et privat øyeblikk som ingen andre har noe med å gjøre. Datatilsynet (2019a) forklarer at personvern handler om *retten til privatliv* og til å bestemme over egne *personopplysninger*. Dette innebærer alt som kan identifisere deg – slik som navn, mobilnummer, adresse etc. Personvern er noe hver og en av oss har rett på – en *menneskerett*¹. En beskyttelse, som er nedfelt i mange demokratiske grunnlover rundt om i verden, inkludert vår egen (Grl.§102).

I dagens digitale mediesamfunn kan det imidlertid være vanskeligere å skille mellom hva som er privat og offentlig. *Sosiale nettverkstjenester* (SNS), slik som Facebook og Instagram, har ført til at vi deler mer om oss selv en noen gang tidligere. Samtidig er det der vi holder kontakten med venner; finner informasjon og deltar i samfunnsdebatter; kjøper og selger; og konsumerer underholdning. For de fleste nordmenn vil det være umulig å ikke ha noen form for tilstedeværelse på SNS, uten å melde seg ut av samfunnet (NOU 2022: 11, s. 150). En betydelig konsekvens av at teknologi smelter sammen med medier og vår identitet, er dog at *personvernet* svekkes. Her gir vi først og fremst fra oss personopplysninger gjennom å avsløre oss selv, og et sentralt poeng er at personvernet er innebygget i hvert stadium av brukerreisen på SNS. Om vi ønsker å bli medlem av Facebook, må vi først godkjenne selskapets *personvernserklæring* og bruk av *informasjonskapsler*. I neste steg, lager vi en profil med opplysninger om oss selv – slik som fødselsdato, bosted og et passende profilbilde. Deretter må vi ta beslutninger for hvem vi ønsker skal kunne se denne informasjonen. Skal profilen være åpen for alle eller lukket? Når vi først kan ta i bruk Facebook, må vi også kontinuerlig vurdere å dele - eller ikke dele - informasjon og bilder av oss selv og andre.

Parallelt med det som skjer skjermen vår, foregår det i tillegg tap av personvern hver gang vi berører den. All vår aktivitet - alle våre klikk, 'svipes' og 'likes' - lagres, analyseres og selges videre til tredjeparter (Mejias og Couldry, 2019). Det er nettopp disse underliggende strukturene

¹ EMK artikkel 8 (Retten til respekt for privatliv og familieliv)

av SNS – drevet av kunstig intelligens og kraftige algoritmer – som utvinner *brukerdata* om vår atferd og personlighet (Kalsnes og Pettersen, 2019). Høsten 2022, kom det imidlertid to innsiktsfulle utredningsarbeid, som belyser personvernproblematikken i norsk kontekst. I utredningen, *En åpen og opplyst offentlig samtale*, mener Ytringsfrihetskommisjonen at den massive innsamlingen av data har konsekvenser for brukernes personvern og kan føre til at folk blir forsiktige med å ytre seg (NOU 2022: 9). Personvernkommissjonen forteller i, *Ditt personvern – vårt felles ansvar. Tid for en personvernpolitikk*, at dagens forbrukere har svært begrensede muligheter til å forstå omfanget av datainnsamlingen som skjer på tvers av apper, nettsider og 'tingenes internett'. Det er mange aktører å holde styr på, teknologien er kompleks og vilkårene er vanskelig å lese. De understreker at det er på høy tid at diskusjoner om personvern «løftes ut av ekspertssirkelene» og gjøres til et relevant spørsmål i samfunnsdebatten (NOU 2022: 11). De to utredningene har vært en viktig inspirasjon for dette prosjektet.

Den nåværende samtalen om personvern på nett, fokuserer imidlertid nesten utelukkende om trusler mot personlig informasjon, og overser hvordan brukere opplever og drar nytte av personvern på internett (KR&I, 2022). Vi må forstå menneskene som bruker teknologien - ikke bare teknologien i seg selv - for å kunne ta tak i personvernsutfordringene. Et vesentlig gap i forskningen er at eldre voksne har fått lav prioritering. Denne generasjonen utgjør imidlertid en økende brukergruppe på SNS, og har blant annet ført til en 'eldre-boom' på Facebook (Lervik, 2018). Vi trenger å få bedre innsikt i denne generasjonens møte med personvern på nett. Samtidig er det interessant å kunne se hvordan de skiller seg fra yngre brukere. Gjennom tolv semistrukturerte forskningsintervjuer og tenke høyt-protokoller, utforsker jeg hvilke personvernsholdninger som eksisterer blant to generasjoner i møte med SNS - og ønsker dermed å bidra med ytterligere empiri til den stadig mer aktuelle personverndebatten.

1.1 Forskningsspørsmål og analytiske dimensjoner

I denne studien er målet å avdekke ulike generasjoners holdninger knyttet til personvern i sosiale nettverkstjenester (SNS). Denne masteroppgaven er slikt sett en mediebruksstudie med fokus på utforskning av medieerfaringer (Gentikow, 2019). I denne masteroppgaven undersøker jeg konkret to generasjoner på hver sin side av aldersspekteret, og deres personvernsholdninger til Facebook og Instagram (Meta). Herunder ser vi på generasjonen omtalt som *Babyboomers* (Boomers, 57-67 år), og den yngre *Generasjon Z* (Gen Z, 15-26 år). Formålet er å sammenligne

disse to generasjonene, og utforske potensielle ulikheter, avvik eller hvor de sammenfaller. Det overordnede forskningsspørsmålet for studien er:

Hvilke holdninger har ulike generasjoner til personvern i sosiale nettverkstjenester?

Dette empiriske forskningsspørsmålet deles inn tre analyse spørsmål, som tar for seg hvordan Boomers *forstår*-, *handler*-, og *føler* om personvernet på Meta, i forhold til Generasjon Z. Disse analytiske dimensjonene blir ytterligere presentert under operasjonaliseringen av viktige begreper.

I denne studien skal jeg diskutere dette i lys av tidligere forskning og sentrale teorier, om hvordan brukere navigerer skillet mellom offentlig og private sfærer i SNS. Jeg fokuserer her på hvordan brukerne *fremstiller* seg selv, gjennom å vurdere hva de velger å *avsløre* om seg selv. Dette knyttes til Erving Goffman (1959) sine teorier om *selvrepresentasjon*. Evnen de har til å håndtere dette, blir koblet til deres *kritiske medieforståelse* og *kommunikative handlekraft* (Ytre-Arne og Das, 2020). Herunder vil det såkalte *privatlivsparadokset* (Barnes, 2006) bidra til å nyansere både deres forståelse og handlinger. Andre viktige aspekter knyttet til deres følelser, er Helen Nissenbaum (2010) sitt rammeverk for *kontekstuell integritet*, som bidrar med å analysere opplevde personvernbrudd på SNS. Intensjonen er dermed å gi et helhetlig bilde av brukernes personvernholdninger.

1.1.1 Operasjonalisering av sentrale begreper

For å kunne besvare forskningsspørsmålet, er det noen grunnleggende elementer som bør avklares i form av en operasjonalisering. Herunder hva denne studien mener med: *personvern*, *brukere*, *holdninger*, *generasjoner* og *sosiale nettverkstjenester*.

Når det kommer til **personvern**, skilles det mellom retten til respekt for privatliv og retten til beskyttelse av personlig data (personopplysningsvern) (NOU 2009: 1). Begrepet benyttes i vid forstand i denne studien, og fenomenet utypes nærmere i Kapittel 2 og 3. Videre benyttes termen **brukere** om individer som produserer, konsumerer og distribuerer innhold på digitale tjenester (Lomborg og Mortensen, 2017).

Generasjoner referer til de som ble født rundt den samme tiden, og som opplevde mye av den samme kulturen når de vokste opp (Twenge, 2023, s. 2). Psykologiprofessor, Jean Twenge

(2023), mener at den æraen vi ble født i, har en betydelig innflytelse på våre holdninger og verdier. Tidligere var det imidlertid utfordrende å skille mellom hvor og hvordan generasjoner skilte seg ut - men med stordata hevder hun at dette ikke lenger er tilfellet. Herunder består den vestlige befolkningen for øyeblikket av: *Den stille generasjonen* (f.1925-1945); *Babyboomers* (f.1946-1965); *Generasjon X* (f.1965-1979); *Millennials* (f.1980-1994); *Generasjon Z* (f.1995-2012) og den nyeste generasjonen har fått navnet *Generasjon Alfa* (f.2013-).

Boomers, har fått sitt tilnavn etter den store økningen i fødselsraten etter den andre verdenskrig. De har også vært vitne til en enestående teknologisk fremgang på mediefeltet – og opplevd utviklingen fra de tradisjonelle mediene (radio og TV), til å måtte sette seg inn i nye interaktive medier i relativt voksen alder (Twenge, 2023). *Generasjon Z* (eller Gen Z) har på sin side hatt tilgang til internett og moderne teknologier store deler av livet. De blir av den grunn ofte omtalt som *digitalt innfødte*. Denne unge generasjonen har dermed et annet grunnlag for teknologisk kompetanse, og er vant til å tilpasse seg nye medier (Mitchell, 2020). Bakgrunnen for valget av akkurat disse to generasjonene, er for å skape et bredt aldersspenn og bidra til tydeligere *generasjonsforskjeller*. Det skal imidlertid kommenteres at forskning på generasjoner har blitt debattert, spesielt i forhold til definering av aldersgrenser. Enkelte argumenter for at generasjoner er sosialt og kulturelt definert og produsert, og kan som resultat overse andre viktige faktorer ved individet (Buckingham og Willett, 2013). Jeg tror at det finnes en middelvei, gjennom å anse generasjoner som en interessant faktor, som kan knyttes til personvern og krysningen mellom teknologi, medier og identitet. Men samtidig anerkjenne at det er andre individuelle aspekter som også påvirker våre holdninger til dette.

Sosiale nettverkstjenester (social network sites, heretter SNS) er en undersjanger av sosiale medier. I følge Ellison og Boyd (2013) kjennetegnes en SNS gjennom at brukeren må kunne ha en unik profil, som består av brukergenerert innhold. Videre må en SNS kunne offentliggjøre brukerens nettverk, slik som en liste over «Venner». Brukeren må også kunne konsumere, produsere og samhandle med brukergenerert innhold på plattformen – med andre ord en nyhetsstrøm (feed).

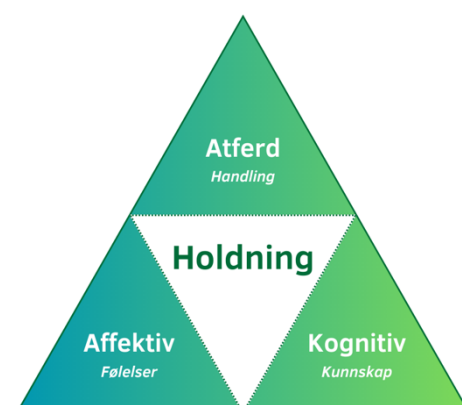
Siden de første SNS vokste frem på begynnelsen av 2000-tallet, er det i dag et stort utvalg med ulike formål og mot ulike målgrupper. For å avgrense studien, ble det besluttet å fokusere på SNS tilknyttet selskapet, *Meta*. Dette er et amerikansk teknologiselskap, som ble grunnlagt av Mark Zuckerberg i 2004. Selskapet eier og driver *Facebook*, der brukere kan poste

kommentarer, dele bilder og lenker til nyhets- eller annet interessant innhold på nettet (Bucher, 2021). Meta eier også *Instagram* som ble lansert i 2010 - som fokuserer på foto- og videodeling. Heretter anvendes 'Meta', når jeg snakker om Facebook og Instagram under ett. Ferske tall viser at Facebook er mest utbredt blant Boomerne, og Generasjon Z er mest aktiv på Instagram (Ipsos, 2023). Et viktig poeng er at de to generasjonene har erfaringer med de to plattformene over tid. Studien ønsker slik å koble et tettere bånd mellom brukernes medieerfaringer og personvernsholdninger.

Holdninger hjelper oss å definere hvordan vi ser på situasjoner, og hvordan vi oppfører oss i disse situasjonene – men de kan være utfordrende å avdekke empirisk (Allport, 1935; Pickens, 2005). Mange kvalitative studier skorter nettopp på operasjonalisering (Gentikow, 2019, s. 90). Tradisjonelt sett har *holdning* blitt definert, som en lært predisposisjon til å opptre på en konsistent positiv eller negativ måte i forhold til et objekt (Allport, 1935) – i denne sammenheng, personvern.

I denne studien finner jeg inspirasjon fra den såkalte *tre-komponentmodellen* (Rosenberg og Hovland, 1960). Modellen teoretiserer at holdningene våre består av tre komponenter: (i) *kognitiv* (kunnskap og meninger), (ii) *affektiv* (følelser) og *atferd* (handling) (Pickens, 2005). Med andre ord er våre holdninger en respons til noe (en person, sosiale problemer etc.) – der vi responderer gjennom våre meninger, atferd og følelser (Breckler, 1984). Holdningsendringer kan også starte i hver av disse komponentene. Det må imidlertid påpekes at tre-komponentmodellen er en forenkling av holdning, der komponentene kan overlape eller være motsigende. En kan eksempelvis være klar over at å røyke er skadelig (kognitiv), men gjør det likevel (atferd). For å dempe virkningen på den manglende konsistensen – eller den *kognitive dissonansen* – kan det medføre at personen ikke engasjerer seg så sterkt (affektiv) i spørsmål rundt røyking (Gentikow og Østbye, 2009, s. 24).

Figur 1: Tre-komponentmodellen for holdninger fritt illustrert, basert på Pickens (2005).



1.1.2 Analyse spørsmål (AS) – Kognitiv, Atferd og Affektiv

Tre-komponentmodellen for holdninger bidrar i denne studien, som en ramme for å forstå datamaterialet. Modellen er utgangspunktet for tre analyse spørsmål (AS), som sammen skal svare på; *hvilke holdninger ulike generasjoner har til personvern i sosiale nettverkstjenester*. Slik kan informantenes holdninger dekket i vesentlig grad, gjennom å operasjonalisere holdningsbegrepet i mer håndfaste dimensjoner:

AS1 (Kognitiv) Hvordan *forstår* Boomers personvern i forhold til Generasjon Z?: Den kognitive komponenten vil utforske informantenes kunnskap og forståelse av personvernet på Meta. Konkret innebærer dette å undersøke hvordan de to generasjonene forstår personvernsbegrepet og deres kjennskap til deres rettigheter; oppfatninger om hvordan Meta samler inn personopplysninger; og hvordan de vurderer eget forhold til privatliv på SNS.

AS2 (Atferd) Hvordan *handler* Boomers når det kommer til personvern på Meta, i forhold til Generasjon Z?: Holdningskomponenten for atferd omfatter verbale uttalelser om informantens handlinger og intensjoner i møte med personvernet. Det inkluderer også faktiske handlinger i møte med personvernsinnstillingene, som utforskes gjennom en *tenke høyt-øvelse*. Dette innebærer å se på deres periodiske-, statiske- og dynamiske personvernshandlinger.

AS3 (Affektiv) Hva *føler* Boomers om personvernet på Meta i forhold til Generasjon Z?: Den affektive komponenten referer til en emosjonell respons, og samles inn gjennom verbale utsagn om følelser knyttet til personvernet på Meta. Dette inkluderer følelser rundt kontroll og tillit til Meta som behandlingsansvarlig for personopplysninger. Her undersøkes også ulike krenkelser av privatlivet på SNS (kontokapring og publisering av bilder uten samtykke), og hvordan de ulike generasjonene føler om dette.

1.2 Oppgavens Struktur

Masteroppgaven består av åtte kapitler. Disse vil ta leseren gjennom en rekke elementer og forhåpentligvis bidra til å øke å dens innsikt i personvernsholdninger:

Kapittel 2 skaper et bakteppe for tematikken, og forteller om hvordan behovet for privatliv har vokst frem i takt med en større offentlighet. Det juridiske og teknologiske perspektivet ved personvern vil utdypes her – både med tanke på begrepets definisjon og nye forretningsmodeller som utfordrer personvernet. Herunder ser vi også på tidligere forskning på området.

Kapittel 3 ser på ulike teoretiske tilnærminger til personvernsholdninger. Hensikten er å skape en grunnleggende innsikt i hvorfor personvern er viktig og hvordan personvern kan analyseres kontekstuellt. Teorier fra medie- og samfunnsvitenskap, vil også stå sentralt for å belyse hvordan brukere navigerer mellom det private og offentlige på SNS.

Kapittel 4 vil redegjøre for selve forskningsprosessen. Herunder metodiske beslutninger og refleksjoner.

Kapittel 5 er det første av tre analysekapitler, og tar for seg AS1 (kognitiv) om informantenes meninger og kunnskap om personvern på SNS. Her belyses mellom annet informantenes kritiske medieforståelse.

Kapittel 6 tar for seg AS2 (atferd) om informantenes personvernshandlinger på Facebook og Instagram. Her vil funn fra tenke høyt-metoden illustrere faktisk atferd. Teori om selvrepresentasjon vil stå sentralt for å belyse informantenes kommunikative handlingskraft i møte med personvern.

Kapittel 7 ser på AS3 (affektiv) informantenes følelser, både fra et institusjonelt og sosialt perspektiv (Raynes-Goldie, 2010). Herunder deres opplevelse av Meta sin datainnsamling. I kapitlet vil Nissenbaum (2010) sin teori knyttes til krenkelser av privatlivet på SNS.

Kapittel 8 bringer klarhet over de viktigste funnene. Herunder settes de tre holdningskomponentene sammen, og en oppsummerende diskusjon vil herunder bidra til å samle trådene før oppgaven konkluderes i sin helhet.

KAPITTEL 2 – Bakgrunn

Dette kapittelet skal gjøre tematikken mer håndgripelig. Vi begynner med å gi et historisk innblikk, da personvernet har vært en viktig beskyttelse for individet i møte med utviklingen av det moderne samfunnet. Deretter presenteres en generell tilnærming til personvern, som legger grunnlag for begrepet i denne studien. Dette blir etterfulgt av tidligere forskning knyttet til personvernsholdninger hos ulike aldersgrupper.

2.1 Personvernets fremvekst: Et skille mellom privat og offentlig

Privatliv og behovet for å verne om det, kan knyttes helt tilbake til antikken. Her skilte Aristoteles mellom to livssfærer, *polis* og *oikos*. Polis beskrev bystaten og dens borgere (offentligheten) og oikos var den private intimsfære i hjemmet (Gripsrud, 2017, s.17). To sentrale filosofer som har bidratt med innsikt i skillet mellom det private og det offentlige, er Jürgen Habermas og Hannah Arendt. De forteller at det er først i det moderne samfunnet, at disse skillene blir synlige. Habermas (1991) argumenterer for at *offentligheten* oppstod på 1700-tallet, som en sfære av privatpersoner som kom sammen for å diskutere saker av offentlig interesse. Offentligheten var en arena der borgerne kunne utøve politisk frihet, noe som ikke var mulig under føydalismen. Arendt (1958) ser imidlertid det private rom, som et *nødvendig* grunnlag for det offentlige. Uten en privat sfære, så kan ikke det offentlige fungere optimalt.

Personvernets historie kan slikt sett spores til ulike tidsepoker, der hver periode bidro til en forståelse av behovet for å beskytte individets privatliv. Sarah Igo (2018, s. 13) beskriver hvordan sammenstøtet mellom viktorianske anstendighetsnormer og fremveksten av medieteknologier på 1800-tallet – slik som fotografiet – førte til et økende behov for et privatliv. Påtrengende journalister tok riktignok bilder og invaderte folks privatliv – noe som resulterte i at Brandeis og Warren (1890) oppfordret til en lov om *retten til å få være i fred*. Dette var et viktig vendepunkt, hvor kravet om beskyttelse av personlig informasjon ble en del av den offentlige diskusjonen (Igo, 2018).

I senere tid argumenterte Alan Westin (1967) for at personvern burde anses som en *kontroll* over hva og hvordan, vi deler informasjon med andre. Irwin Altman (1975) mente også at personvern burde inkludere å kunne *begrense* denne informasjonen. Selv om dette er ulike tilnærminger – så kan de likevel relateres fordi begge gjelder grensen som går mellom seg selv og andre – det private og det offentlige (Altman, 1975 i Acquisti, Taylor og Wagman, 2016, s.

443). Enkelt personer navigerer slik sett grensene mellom offentlig og privat hele tiden. Mediene har på sin side vokst frem som en *balansegang* mellom det offentlige og private, der mediene presenterer det offentlige rommet inne i privatlivet. Fra radioen og TV plassert i det private hjem, til sosiale medier i lommen (Gripsrud, 2017, s. 44).

Det er imidlertid når privatlivet først nedfelles i lov, at vi snakker om et *personvern* – og er en rettsdisiplin som først har vokst frem etter andre verdenskrig (Wessel-Aas og Ødegaard, 2018). Lovverket har imidlertid hatt en tendens til å ligge bak den teknologiske utviklingen. Da digitaliseringen av samfunnet begynte på 1960-tallet, var det allerede fra start en bekymring om at *elektronisk databehandling* ville krenke folks privatliv (Schartum, 2020, s. 16). Denne uroen spredte seg utover flere land, og ble en sterk motivasjon for å samles om felles reguleringer på feltet. Dette er noe av bakgrunnen for *Personvernsforordningen* som ble innført i 2018 – omtalt som *GDPR* (General Data Protection Regulation). Formålet er å beskytte brukere i EU og EØS gjennom å regulere hvordan personopplysninger samles inn, behandles og deles i organisasjoner (Schartum, 2020). Nå har GDPR fått fem år å modne på - og det jobbes i skrivende stund for å innføre nye regelverk, der hensikten er å skape en tryggere digitalsfære, hvor personvernet får en enda sterkere posisjon (*Digital Services Act* og *Digital Market Act*).

2.2 Definisjon av personvernsbegrepet

Personvern betyr ulike ting for ulike personer og fagdisipliner. Fremfor alt er personvern et særnorsk begrep, som har vært preget av terminologisk uklarhet og forvirring (NOU 2009: 1, s. 29). Innen akademisk litteratur fra engelsktalende land, bruker de eksempelvis det beslektede begrepet, «privacy» - som både kan forstås som privatliv og personvern. Dag Wiese Schartum (2020), gir imidlertid en definisjon, som vil brukes som utgangspunkt i denne studien. Han forklarer at personvern gjelder et vern av de *private sfærer* som mennesker befinner seg i. Her operer han med fem ulike sfærer; *psykisk-, kroppslig-, geografisk-, kommunikasjon-,* og en *personopplysningssfære*. Innenfor hver av disse sfærene, må det være *autonomi* og *integritet*. Dette innebærer at hver person skal kunne få bestemme selv, og at de blir respektert for sine valg. Dersom noen *krenker* vårt privatliv, betyr det at vi enten ikke kan få bestemme selv eller bli respektert innenfor disse sfærene.

Schartum (2020, s. 13) forstår personvern som en tilstand der det «råder stor grad av autonomi og integritet innenfor private sfærer», og vil være utgangspunktet for denne studien. Den

psykiske sfæren omfatter vår selvfølelse, og kan bli krenket dersom noen mobber oss. Den *kroppslige* sfære kan på sin side bli krenket om noen utnytter kroppen vår uten samtykke. En *geografisk* sfære er derimot private områder, der vi forventer å være i fred. Den fjerde sfæren handler om kommunikasjon mellom mennesker, og at de kanalene vi bruker for å kommunisere blir beskyttet. Om en postmann åpner et brev som er sendt til deg, vil dette være en krenkelse av din *kommunikasjonssfære*. Den siste beskrives av Scharthum som en *opplysningsssfære*, og handler om den enkeltes rett til å bestemme over egne opplysninger. Samt krav på respekt og beskyttelse av disse opplysningene (2020, s. 14).

En viktig bemerkning er at lovgivninger, slik som GDPR, *ikke* regulerer fysiske overtredelser – slik som brevbrudd. Scharthum understreker at loven er avgrenset til behandling av *personopplysninger* som er i digital form – og som kan være gjenstand for automatisk behandling (2020, s. 13). Vi åpner imidlertid mobilen med ansiktet vårt (kroppslig sfære) og deler lokasjonen vår med en rekke mobilapper (geografiske sfære). Store deler av vårt liv i det moderne samfunnet er nettopp digitalisert, og selve behandlingen av slike digitale opplysninger blir derfor helt avgjørende for personvernet.

2.3 Nye forretningsmodeller

Siden år 2000 har det vokst frem mektige teknologikonglomerater, slik som Meta og Alphabet (Google), som har livnæret seg på innovative *forretningsmodeller* (Evans og Schmalensee, 2016). Fremfor alt tjener de penger på å vise reklame for potensielle kjøpere - slik aviser og TV har gjort i alle år. Teknologiselskapene spiller imidlertid i en helt annen inntektsliga. Meta dro inn beskjedne 28,65 milliarder dollar bare i første kvartal av 2023 – hvorav 98% av dette kom fra annonsesalg (Resvoll, 2023). Inntektene kommer hovedsakelig av *atferdsbasert markedsføring*, som innebærer å bruke *data* om brukerens atferd til å forutsi og påvirke deres fremtidige handlinger – slik som kjøp eller klikk (NOU 2022: 11, s. 148).

Mejias og Couldry (2019) forklarer at det skjedd en såkalt *datafisering* av våre liv. Dette innebærer at nesten alle aspekter av hverdagen vår – fra sosiale interaksjoner, læring og lesing til andre forbruksvaner – nå kan spores, lagres, analyseres og utnyttes for kommersielle formål. Denne datafiseringen er selve kjernen i det Shoshana Zuboff (2019) kaller *overvåkningskapitalisme* - et økonomisk system der teknologiselskaper samler inn persondata for å lage detaljerte profiler av brukerne. Zuboff sammenligner selskapene med de spanske

conquistadorene - som gikk i land, plantet flagget på stranden og proklamerte eierskap på alt de så (2019, s. 12). På samme måte har teknologigigantene hentet ut og tatt eierskap på brukernes data uten samtykke - og blitt styrtrike i prosessen. Cambridge Analytica-skandalen er praktksemeplet, der selskapet med samme navn, brukte informasjon om millioner av Facebook-brukere for å påvirke presidentvalget i USA i 2016 (Cadwalladr og Graham-Harrison, 2018). Meta har imidlertid blitt bøtelagt gang på gang for å bryte med GDPR. Senest en bot i milliardklassen (Bodoni, 2023).

Når det kommer til forretningsmodellen, så er en vanlig misoppfatning at det er *rådataene* som blir solgt videre. Realiteten er at varen de selger, er en *predikasjon* om hvem brukeren er, hvilke vaner den har og hva den interesserer seg for. Dette kalles for en *digital tvilling* og er en sammensatt 'profil' av hvem Meta tror bruken er (Hareide, 2021, s. 116). Disse predikasjonene sammenstilles ved hjelp av komplekse algoritmer og automatiserte systemer i form av kunstig intelligens (Bucher, 2012 i Kalsnes og Pettersen, 2019). Meta gjør med andre ord antagelser om våre behov, og selger dem videre til alle som ønsker å påvirke oss.

Evans og Schmalensee (2016) beskriver at Facebook fungerer som en *flersidig plattform* - hvor ulike aktører, brukere, annonsører og tjenesteleverandører samhandler. På den ene siden tilbyr Facebook gratis tjenester til sine brukere, samtidig som de generer inntekter gjennom å selge tilgang til predikasjoner til annonsører. Facebook har med andre ord en avansert forretningsmodell, hvor de høster inntekter fra 'flere sider', ved å eksponere brukere for målrettet innhold (Bucher, 2021). For å illustrere hvordan Facebook fungerer, kan en også se for seg *to informasjonsstrømmer* - der den ene er sosial og *synlig*, og den andre er teknisk og *usynlig* (Rasmussen, 2016, s. 56). Den synlige informasjonen handler om vår sosiale interaksjon på plattformen – det vi deler, liker og kommenterer av innhold. Den usynlige informasjonsstrømmen, holder derimot til under panseret på plattformen - den tekniske biten som brukerne aldri får øye på – som sender oss målrettet innhold i retur. Det er en kontinuerlig runddans ved at våre digitale fotavtrykk blir samlet inn, analysert og sendt tilbake til oss gjennom nytt innhold. Dataene sirkulerer slikt sett i en løkke (loop) fra brukerne til plattformen og tilbake igjen (Mathieu og Vengerfeldt, 2020).

2.4 Tidligere forskning på personvern

Å forske på hvordan brukere tilnærmer seg personvern på nett er ikke noe nytt, og det finnes en rekke studier, spesielt med kvantitative tilnærminger. Datatilsynets personvernsundersøkelse (n=1501) avdekker blant annet at mange brukere endrer atferd, fordi de er usikre på hvordan deres opplysninger faktisk blir brukt (2020). Denne selvreguleringen som oppstår som en konsekvens av overvåkingsfrykt, kalles *nedkjølingseffekt* (Marder *et al.*, 2016). Her oppga fire av fem nordmenn at de var opptatt av personvern – likevel opplevde tre av fem at de følte seg maktesløse når det gjaldt å ha kontroll over personopplysninger på internett.

Det er dog ikke mange kvalitative studier å oppdrive på norsk jord, som ser på personvernsholdninger mellom ulike aldersgrupper. En mindre studie utført ved Southern Illinois University, indikerer imidlertid at yngre voksne generelt er mindre bekymret enn eldre voksne, for om selskaper har informasjon om dem (Aguirre, Woodward og Martin, 2018). Medienes dystre fremstilling av personvernbrudd (hacking), skaper følelser hos eldre, om at digitale medier er risikabelt, og kan medføre at de er motvillige til å ta det i bruk (Elueze og Quan-Haase, 2018). Selv om mange eldre er nå aktive på sosiale medier, viser det seg dog at deres forståelse av disse nettstedene er begrenset (Quan-Haase *et al.*, 2018). Unge voksne er på sin side 'avhengig' av digitale medier, og vil derfor kunne ha en bedre forståelse for personvern på nett (Dhir *et al.*, 2017). De unge stiller også inn personvernsinnstillingene i større grad enn eldre voksne (Madden og Smith, 2010). Medietilsynet (2021) bekrefter herunder at aldersgruppen 16-34 år vurderer seg som mer kompetente til å håndtere personvernsutfordringer på internett enn eldre grupper - spesielt de over 60 år (n=2084).

En utfordring med personvernsforskning er at personvern har ulike definisjoner, og vernet oppfattes ulikt mellom nasjoner. Europeiske land har eksempelvis hatt et sterkere personvern etter GDPR ble innført, i forhold til USA. Et annet aspekt er at når det oppstår en endring i våre sosiale strukturer eller teknologi - vil også vårt syn på privatliv, og derav personvern endre seg (Svendsen, 2014). Det er derfor viktig å studere brukernes personvernsholdninger med jevne mellomrom over tid. Det vi oppfatter som privat i dag, kan oppleves som offentlig i morgen. Dette er noe av bakgrunnen for at vi trenger mer empiri som er basert på nasjonal kontekst, og er en motivasjon for mitt avhandlingsarbeid. Dette bakgrunnskapittelet har herved hatt som formål å gi en grunnleggende innføring i juridiske og tekniske aspekter, for at du som leser skal kunne ha noen knagger å henge personvernstatistikken på. I neste kapittel skal vi se nærmere på den teoretiske forankringen som legger grunnlaget for de kommende analysekapitlene.

KAPITTEL 3 - Teoretiske Perspektiver

Det teoretiske personvernslandskapet brer seg over fagdisipliner, slik som statsvitenskap, jus, økonomi, media, psykologi og informasjonsteknologi. Uansett tilnærming, er den røde tråden at personvern er et omfattende, rotete og komplekst emne. For å besvare på forskningsspørsmålet om *hvilke holdninger ulike generasjoner har til personvern i sosiale nettverkstjenester*, skal vi i dette kapitlet legge et teoretisk grunnlag for analysene. Denne studien baserer seg dermed ikke på én klassisk hovedteori – men forsøker å samle ulike perspektiver, som har som formål å skape en *helhetlig* forståelse for tematikken.

Først skal vi se nærmere på hvordan personvernet har endret meningsinnhold siden SNS kom på markedet, og presenterer det såkalte *privatlivsparadokset*. Videre tar vi for oss noen filosofiske ideer som forklarer hvorfor personvern er viktig, og hvilke verdier det har både for individet og samfunnet. Deretter presenteres en sentral teori om *kontekstuell integritet* av Helen Nissenbaum. Siste delkapittel ser på sosiologiske og medievitenskaplige tilnærminger som belyser hvordan brukere anvender *handlingsmuligheter* for å presentere eller tilsløre seg selv i SNS. Her er Erving Goffman sin forståelse av selvrepresentasjon og inntrykkskontroll sentral, samtidig som vi tar i betraktning at dette påvirkes av brukerens *kritiske medieforståelse* og *kommunikative handlekraft*.

3.1 Privatlivsparadokset

Personvern har blitt tilegnet mange betydninger. Noen har vi sett på allerede – slik som at det kan anses som å *kontrollere* eller *begrense* informasjonen som vi deler (Westin, 1967; Altman, 1975). Ved fremveksten av SNS, har det kommet nye aspekter som supplerer og utfordrer synet på personvern. Et fenomen som går igjen er, *privatlivsparadokset* (privacy paradox) (Acquisti, Taylor og Wagman, 2016; Kokolakis, 2017). Det paradoksale er at mange sier at de bryr seg om eget privatliv, men har en atferd som ikke reflekterer disse påstandene (Barth og de Jong, 2017; Marwick og Hargittai, 2019). Susan Barnes (2006) brukte eksempelvis paradokset for å begrunne hvorfor tenåringer frivillig gav fra seg personlig informasjon i sosiale medier. Statistikk viser herunder at kun et fåtall leser *personvernserklæringen*, før de godtar den (Pew Research Center, 2019). Mange har siden forsøkt å løse dette privatlivsparadokset.

En forklaring har vært at brukere gjør bevisste kalkuleringer om de skal avsløre personlig informasjon eller ikke – også kalt *privacy calculus* (Dinev og Hart, 2006). Det viser seg at mange

avslører ting om seg selv, når opplevde fordeler er større enn ulempene - med andre ord en *personvernsvurdering* (Dienlin og Metzger, 2016). Westin (1967) skilte eksempelvis mellom å være en *pragmatiker*, *fundamentalist* eller *ubekymret* i møte med personvern. Personvernspagmatikerne var en mellomting mellom fundamentalister og de likegyldige – der de var bekymret for sin personlige informasjon, men tok rasjonelle beslutninger. Nora Draper (2017) mener dog at slike diskurser fremstiller selvavsløring som en strategisk beslutning gjort av *informerte forbrukere* - der personvern bunner ned i et valg mellom å delta eller isolere seg fra sosiale fellesskap. En annen forklaring på paradokset kan dermed være at brukerne ikke har tilstrekkelig forståelse for måten deres informasjon blir samlet inn og brukt (Park, 2013).

Vi avslører imidlertid mye om oss selv uten at vi gjerne er klar over det, gjennom å engasjere oss på plattformene. Det har også blitt kjent at menneskehjernen frigjør lykke -og kjærlighetshormonene, dopamin og oxytocin når andre «liker» våre innlegg på SNS (Ritvo, 2012). Dette kan lede til avhengighet, overdreven deling av informasjon, samt tap av personlige data. Det kan derfor tyde på at brukerne ikke kan gjøre en *rasjonell* personvernsvurdering for å ta kontroll, når de ikke har innsikt i hele risikobildet og hvordan de faktisk påvirkes.

Neil Richards (2022, s. 92-96) peker på at kontroll er en *illusjon* – og ville vært overveldende for brukeren. Tenk bare på hvor mange passord vi må huske på. Han vektlegger at det er selskapene som bestemmer hvordan personvernsinnstillingene er utformet, og hvilke bokser vi kan huke av. Selskapene kan herunder bruke *tilsløringstaktikker* for hvordan de håndterer brukerdata. Draper og Turow (2019, s. 1830) beskriver dette som *obfuscation* - bevisste handlinger for å gjøre noe vanskelig å forstå. Dette kan innebære å *berolige brukeren* gjennom å forsikre at deres personvern blir tatt vare på. Selskapene kan også bruke *distraheringer* eller *komplisert språk* i personvernserklæringene. Richards (2022) argumenterer for at brukere ikke har den nødvendige kompetansen til å ta en reell kontroll over sine egne persondata, om de så fikk full tilgang. Denne følelsen av å ikke ha mulighet til å beskytte eget personvern kan lede til en *digital resignasjon*, der brukeren gir opp forsøket om å kontrollere personvernet (Draper og Turow, 2019). Forskerne argumenterer for at resignasjon er en helt rasjonell respons på forbrukerovervåking – ikke at de nødvendigvis er likegyldige og ikke bryr seg (Westin, 1967). Personvernsholdninger er muligens ikke så paradoksale som mange kan ha det til. Denne problematikken skal vi komme tilbake til senere i oppgaven.

3.2 Personvernets betydning for individ og samfunn

En ting, er å vite *hva* personvern er - men det er vel så viktig å vite *hvorfor* privatlivet er viktig å beskytte. I de neste avsnittene blir det trukket frem ulike verdier som har blitt koblet til vern av privatliv - der det ikke bare handler om å beskytte seg selv, men også å beskytte *hverandre*. Denne tilnærmingen kommer fra en lang filosofisk og rettslig tradisjon, som er tett sammenbundet med tanken om den *liberale rettsstaten*.

3.2.1 Et individuelt gode

Personvernet er først og fremst et *individuelt* gode, i form at vi har rettigheter innenfor våre private sfærer (Schartum, 2020). James Moor (1997) tar imidlertid for seg hvordan privatlivet er noe av stor betydning og viktig å verne. Samtidig peker han på at dette styres av individuelle preferanser, at det er kulturelt relativt og vanskelig å rettfærdiggjøre generelt. Moor referer videre til en filosofisk distinksjon mellom *instrumentelle-* og *iboende egenverdier*. Som en instrumentell verdi, kan personvernet sees på som et middel til å oppnå andre verdier eller mål – slik som å opprettholde individets autonomi og integritet.

Oxford-professoren, Carissa Véliz, forklarer at det å ha et privatliv handler om å kunne holde enkelte intime ting for oss selv – våre egne tanker, samtaler og planer (Véliz, 2020, s. 3). Det som er essensen i å ha et privatliv, er at det gjør det mulig å ta avstand til noen – for å danne nærmere bånd med andre. Å avsløre ulike personlige sider ved oss selv, er grunnlaget for å skape relasjoner (Moor, 1997; Svendsen, 2014). Det innebærer at visse sider holdes private, for å bevare distinkte forhold til ulike mennesker i vårt liv - slik som ektefeller eller bekjente.

3.2.2 Et kollektivt gode

Personvernet er mer enn en individuell rettighet, og har i tillegg en instrumentell verdi i form av at det fører til *kollektive* goder for fellesskapet. I det digitaliserte samfunnet henger vårt eget personvern ofte uløselig sammen med andres personvern (NOU 2022: 11). På samme måte som vi er knyttet til hverandre gjennom våre gener, så er vi også bundet sammen på utallige og usynlige måter, som gjør oss sårbare for hverandres personvernskrenkelser (Véliz, 2020, s. 92). Hvis du eksempelvis avslører informasjon om hvor du bor, så eksponerer du også dine naboer. Dersom du gir et selskap tilgang til mobilen din, så eksponerer du også alle dine telefonkontakter. Vi er alle sammenvevd og gjensidig avhengige når det kommer til personvern.

Véliz (2020, s. 93) hevder også at konsekvensene av tap av personvern, blir opplevd kollektivt. Et robust personvern er instrumentelt for å sikre både ytringsfrihet, informasjonsfrihet og

meningsdannelse – og en bærebjelke for et funksjonelt demokrati (NOU 2022: 11). Dette handler om at mennesker trenger et privatliv for å utforske nye ideer, og å gjøre oss opp en mening (Véliz, 2020, s. 3). Personvernet er derfor en sentral komponent i å skape maktbalanse mellom individet og staten, og individet og private foretak – og tjener som et viktig rom for utvikling av kritiske perspektiver og holdninger (Arendt, 1958; NOU 2022: 11, 2022).

Dette kan knyttes Michel Foucault (1977) sin bruk av begrepet *panoptikon*. Panoptikonet var et arkitektonisk fengselskonsept, utviklet av Jeremy Betham på slutten av 1700-tallet. Fengselet var sirkulært, med et sentralt vaktårn - hvor vaktene kunne overvåke cellene, uten at fangene visste om vaktene så på dem eller ikke. Når de var klar over at vokteren kunne *se* dem til enhver tid, ville de bli disiplinert (Hareide, 2021, s. 35). Foucault så panoptikon som en metafor for det moderne samfunnet, hvor makten er desentralisert og borgerne overvåker og regulerer sin egen oppførsel i frykt for å bli sett på. I sammenheng med personvern, kan panoptikon illustrere en *selvregulering*, hvor overvåkning blir internalisert og bidrar til kontroll av individets atferd – og på den måten begrenser individets personlige frihet (Marder *et al.*, 2016).

Ytringsfrihet og personvern kan overfladisk sett fremstå som motsetninger – men begge to sikrer tre avgjørende verdier for mennesker i samfunnet: selvstendighet, sannferdighet og demokrati (Hareide, 2021, s. 81). For et demokratisk samfunn skal fungere optimalt, trenger samfunnet at borgerne er selvstendige og *tenker selv* (Véliz, 2020). Det er derfor *alle* har en stemme ved politiske valg, for at vi kan si våre meninger uten å være redd for å bli straffet. Ekstreme eksempler der dette ikke er tilfellet, er kommunistmakten i Kina, med sin masseovervåkning av innbyggerne (Solvang, 2018). Å være seg selv, betyr at man må kunne *være for seg selv*.

3.2.3 Personvern som egenverdi og kjerneverdi

Personvernet er altså et instrumentelt redskap, som beskytter andre grunnleggende rettigheter. Moor (1997) hevder i tillegg at personvern har en iboende *egenverdi*, som er verdifullt i seg selv – helt uavhengig av de andre verdiene det kan fremme. I praksis er ikke dette like enkelt. Både ytringsfrihet og personvern ansees eksempelvis som *likeverdige* rettigheter, og er vanskelig å balansere. Grensen for hva vi kan ytre før det krenker andres personlige sfærer kan utvilsomt variere. Moor (1997) konkluderer dermed at personvern bør innarbeides som en *kjerneverdi* i samfunnet. Noe felles grunnleggende, som tilstrebes i alle kulturer – som lykke og trygghet. Selv om personvern ikke har denne statusen i dag, så er det likevel et uttrykk for

en tilsvarende kjerneverdi, *sikkerhet*. Uten beskyttelse så vil arter og kulturer verken blomstre eller overleve. Moor kobler det sammen ved å hevde at etterhvert som samfunnet blir større, mer interaktive og mindre intime – så blir personvern et naturlig uttrykk for behovet for sikkerhet (Moor, 1997, s. 29).

3.3 Kontekstuell Integritet

Kontekstuell integritet er et juridisk rammeverk, utviklet av Helen Nissenbaum. I boken «Privacy in Context» (2010) ser hun på personvern innenfor spesifikke sosiale sammenhenger, fremfor å behandle det som en abstrakt verdi. Hun argumenterer for at personvern ikke bare handler om kontroll over vår personlige informasjon, men også om en hensiktsmessig informasjonsflyt. Denne flyten kaller hun for *kontekstrelative informasjonsnormer* (Nissenbaum, 2010, s. 129) – som karakteriseres av fire nøkkelementer; *konteksten, aktørene, type informasjon og overføringsprinsipper* (2010, s. 140-147). Hensikten er ikke å forby selskaper om å behandle informasjon om brukerne – men at dette gjøres på en anstendig måte. En person sin kontekstuelle integritet er dermed ivaretatt når informasjonsnormene er respektert, og krenket når de brytes.

Kontekst, referer til situasjonen eller omgivelsene der informasjonen blir delt. Innenfor en kontekst er det både ulike roller, aktiviteter og normer i spill (Nissenbaum, 2010, s. 133). Det vil eksempelvis være akseptabelt å ta av seg skjorten (norm) for at legen (rolle) kan lytte på hjertet (aktivitet) til pasienten (rolle). Om den samme personen tok av seg skjorten under en Gudstjeneste, ville dette dog være et brudd på normene i den aktuelle konteksten. Det bunner ned i akseptabel oppførsel i den spesifikke situasjonen.

Når det kommer til *aktører*, skiller Nissenbaum mellom avsender, emne og mottaker av informasjon (2010, s. 141). Relasjonen mellom aktørene bestemmer hvor mye informasjon som er akseptabelt å gi til hverandre. Vi forteller ikke alt til alle. Derfor kan det være relevant å vite om aktøren er statlig eller privat, med tanke på hvilke interesser de kan ha for informasjonen.

Hvilken *type informasjon* det gjelder, er også relevant for Nissenbaum (2010, s. 143). Ulik informasjon har ulik grad av sensitivitet. Helseopplysninger, politisk oppfatning eller seksuelle forhold er gjerne personopplysninger av høyere sensitivitet (Datatilsynet, 2019b). Informasjon som vi ikke anser som sensitiv, er imidlertid lettere å dele i flere kontekster. Dette dreier seg

om forventinger. Når vi eksempelvis deler kredittopplysninger med banken, så er dette akseptabelt. Problemet oppstår om de krever å få vite din seksuelle legning. Da skjer det et brudd på informasjonsnormen, da typen informasjon ikke er akseptabel å dele i den konteksten.

Nissenbaum (2010, s. 145) trekker også frem *overføringsprinsipper* som begrenser informasjonsflyten. Dette er en friksjon i hvordan informasjonen distribueres, formidles og overføres – fra en aktør til en annen i en kontekst. Et eksempel på dette er *konfidensialitet*, som betyr at den som mottar informasjon har et forbud om å dele den med andre. Det kan også innebære *tvang* – der den ene aktøren blir tvunget til å dele informasjonen sin. Mange brukere av SNS kan kjenne på dette, når de må godkjenne personvernserklæringen for å kunne bruke tjenestene.

Å ta vare på personvernet betyr i følge Nissenbaum (2010) å respektere den sammenhengen som informasjonen er delt i; hvem informasjonen er ment for; og forventningene til hvordan disse opplysningene blir brukt. I et digitalt samfunn er det imidlertid lett for at informasjonen flyter over ulike kontekstgrenser, og det kan derfor være utfordrende å anvende en teori som er så sterkt avhengig av slike veldefinerte kontekster. Til tross for dette er det bred enighet om at Nissenbaum sitt arbeid er et viktig bidrag til forståelsen av personvern, og vil bidra som et bakteppe for hvordan krenkelser tolkes i denne studien.

3.4 Navigering av privatliv på SNS

Det er nesten umulig å delta i sosiale nettverkstjenester (SNS), uten å ta noen valg om hvordan man ønsker å *fremstå*, og hva en ønsker å *avsløre* om seg selv. I dette delkapittelet ser vi nærmere på hvordan brukere kan navigere denne representasjonen av egen identitet og hvilke taktikker som benyttes. For å forstå hvordan brukere representerer seg selv i SNS, må vi også forstå helt menneskelige behov. Vi ønsker å bli likt og akseptert. Samtidig handler det om å forstå hvordan plattformene er lagt opp og hvordan selskapene bak plattformene prøver å oppmuntre til disse behovene på en lønnsom måte. I de neste avsnittene går vi inn på SNS sine *handlingsmuligheter* (affordances), og hvordan disse kan skape både *kontekstkollaps* og *tidskollaps* for brukerne. Erving Goffmans teori om *selvrepresentasjon* vil være sentral for disse aspektene. Hvordan brukerne mestrer denne navigeringen kan også knyttes til deres *kritiske medieforståelse* og *kommunikative handlingskraft* (communicative agency).

3.4.1 Handlingsmuligheter (Affordances) på SNS

Vårt personvern på SNS, preges av plattformens *handlingsmuligheter* (affordances). Dette innebærer alle funksjoner og egenskaper som en plattform tillater - slik som å produsere, reagere, distribuere eller interagere med innhold (Kalsnes, 2019, s. 82-86). Vi har eksempelvis mulighet til å legge ut et bilde på «historier» som forsvinner etter et døgn, eller å publisere et bilde på profilen vår, som varer evig.

SNS har herunder fire egenskaper som påvirker hvordan vi navigerer kontekstene og skillet mellom offentlig og private sfærer (boyd, 2010). *Vedvarenhet* refererer for det første til at innhold ofte blir liggende på plattformene, og at man må aktivt inn å fjerne det. Dette legger til rette for *søkbarehet*, hvor innhold kan søkes opp igjen flere år etter det ble lagt ut (Aalen og Hoem Iversen, 2021, s. 35). *Reproduserbarhet* innebærer i sin tur at digitalt innhold er enkelt å kopiere og distribuere, noe som skaper utfordringer i å kontrollere spredning og gjenbruk (boyd, 2010, s. 47). På bakgrunn av at digital informasjon er så enkel å lagre, kopiere og dele – er også potensialet stort for at mange kan se innholdet. *Skalerbarheten* viser dermed til at innhold kan nå et stort publikum på kort tid – slik som når en video går *viralt*. Disse fire egenskapene skaper utfordringer for personvernet, spesielt dersom sensitiv informasjon blir liggende.

3.4.2 Selvrepresentasjon: Inntrykkskontroll, forestilt publikum og kontekstkollaps

Den kanadiske samfunnsforskeren, Erving Goffman (1959) har hatt stor innflytelse på hvordan vi forstår *selvrepresentasjon*. Han forteller at vi viser ulike sider av oss selv, alt etter hvem vi er sammen med. Det finnes dermed ingen *ekte* eller *falske* versjoner av oss (Aalen og Hoem Iversen, 2021, s. 72). For å forklare hvordan vi konstant justerer oppførselen vår, presenterer Goffman begrepet *inntrykkskontroll*. Herunder trekker han analogier til teateret, der han bruker *frontstage* og *backstage*, for å forklare oppførsel i ulike situasjoner. Dette dreier seg om at vi kontrollerer hvilket inntrykk vi gir - alt etter om vi er *på* eller *av* scenen. En butikkansatt kan eksempelvis virke hyggelig når hun sitter i kassen (frontstage), men baksnakke kundene når hun går bak på lageret (backstage).

Det er dog ikke like enkelt å skille mellom frontstage og backstage på SNS, da publikummet består av mange ulike relasjoner (Vitak og Kim, 2014, s. 471). Alice Marwick og dana boyd (2011) bruker derfor begrepet *imagined audience* for å illustrere den gruppen av mennesker vi ser for oss at vi kommuniserer med, når vi deler noe på SNS. Problemet med dette *forestilte* publikummet er at det ikke alltid stemmer overens med det *faktiske* publikummet (Marwick og

boyd, 2011). Utfordringen er at SNS har en større rekkevidde enn vi ofte innser (skalerbarhet), der våre innlegg kan nå ut til mennesker langt utenfor vårt forestilte publikum. Dersom et innlegg som var ment for vennegjengen, blir sett av en arbeidsgiver - så kan det føre til misforståelser. Dette kan føre til en *kontekstkollaps* – noe som Marwick og boyd beskriver som en sammensmelting av forskjellige publikum (2011, s. 122). Dette kan oppstå når ulike personer fra ulike deler av livet vårt (bekjente, kolleger og familie) samles i samme Venneliste. Å skille mellom de ulike kontekstene, er en kunst i seg selv (Palen og Dourish, 2003).

I disse Vennelistene på Facebook har det gjerne samlet seg opp ulike bekjentskaper over mange år. Brandtzaeg og Chaparro-Domínguez (2020, s. 166) bruker begrepet *tidskollaps* som referer til hvordan konteksten i SNS blander sammen grensene mellom fortid og nåtid. Det er ingen klar begynnelse eller slutt på samtaler - og innhold vi legger ut kan være tilgjengelig for alltid (vedvarenhet). Statuser og bilder på Facebook fra 2010, representerer gjerne ikke den personen vi er i dag. Når innhold fra ulike tidspunkter i livet vårt blir blandet med nåtiden, så kan det skape et forvirrende bilde av hvem vi er. Dette henger sammen med hvordan vår identitet har utviklet seg over tid og hvordan vi representerer oss selv i ulike situasjoner. Overgangen fra barn til ungdom og voksen alder, innebærer en utforskning av identitet, og overgangen mellom ulike identiteter (Arnett, 2000). Generasjon Z, er den første generasjonen som har levd ut disse overgangene gjennom sosiale medier. Aalen og Hoem Iversen (2021, s. 73) trekker frem at det vil være umulig for de unge å forutse hvordan dagens selvrepresentasjon, kan påvirke dem senere i livet - i en annen tid og kontekst. En slik selvrepresentasjon henger tett sammen med handlingsmulighetene i SNS, og at disse bidrar til å forme normene på den aktuelle plattformen. Summa sumarum, kan Goffman sine begreper bidra til et språk for å snakke om selvrepresentasjon på SNS, og hvordan dette er helt situasjonsavhengig.

3.4.3 Taktikker: selvavsløring og selvsensur

Når sosiale kontekster kollapse kan det skape indre spenninger, og i enkelte situasjoner oppleves dette som personvernskrenkelser. Marwick og boyd (2011, s. 122) påpeker at personvernsinnstillingene ikke er nok for å sette en demper på spenningen. Fremfor å styre personvernet gjennom *innstillinger* - viste deres studie at tenåringer anså personvern som en *evne* til å kontrollere hvordan de ble oppfattet. For å styrke personvernet brukte de en rekke *taktikker*; i forsøk på å gjenvinne kontroll over informasjonen som ble konsumert og hvordan den ble tolket (Marwick og boyd, 2014, s. 1056). Dette kan innebære å opprette flere profiler. Dersom en blir tagget i et bilde, kan en også fjerne koblingen mellom innholdet og egen profil

(Brandtzaeg og Chaparro-Domínguez, 2020). Noen fjerner også følgere, for å dempe på spenningen. Slike taktikker knyttes til behovet for *selvavsløring* (self-disclosure) – prosessen med å dele informasjon om seg selv til andre (Masur og Scharkow, 2016). Noen er imidlertid mer komfortable å dele personlig informasjon på nett enn andre – og enkelte plattformer oppfordrer til mer selvavsløring enn andre.

Den vanligste taktikken er likevel en form for *selvsensur*. Ofte kan dette komme av at det *forestilte* publikummet er blitt så mangfoldig, at en ikke vet hva som er akseptabelt å legge ut om seg selv. Da iscenesetter mange en representasjon av seg selv med et mål om å unngå konflikter. Dette preges av det *minste felles multiplum* (Hogan, 2010), som handler å dele innlegg som ikke støter *noen*. Herunder er det mange vurderinger å ta i betraktning. Noen brukere kan derfor unngå å legge ut mye innhold, i frykt for å kjede følgerne sine; eller å avstå fra å dele tragiske hendelser i frykt for å fremstå som selvmedlidende (Aalen og Hoem Iversen, 2021, s. 93). Det å la være å dele synspunkter innen kontroversielle emner, også være en måte å selvsensurere seg. *Taushetsspiralen* beskriver eksempelvis en prosess der personer som tror de har en upopulær mening, unngår å uttrykke meningen i offentligheten av frykt for sosial isolasjon. Denne *selvsensureringen* kan skape en spiral hvor stadig færre ytrer denne meningen, noe som igjen forsterker oppfatningen om at meningen er upopulær (Hampton *et al.*, 2014).

3.4.4 Kritisk medieforståelse og kommunikativ handlekraft (agency)

Kritisk medieforståelse og *kommunikativ handlingskraft* (communicative agency) er begge relevante konsepter når det kommer til å navigere kontekster i SNS – men de har ulike fokusområder og implikasjoner. Når vi representerer oss selv på SNS, er det som nevnt over, mange elementer å ta i betraktning. Det handler om å holde forestillingen av oss selv i sjakk. For å balansere spenningen og opprettholde vår egen selvrepresentasjon, kan vi ty til ulike taktikker for å kontrollere dette. Dette krever imidlertid en evne til å handle - å vite hvilke grep en skal gjøre i ulike situasjoner som kan oppstå. Det bunner ned i å *mestre* plattformene med dens tilgjengelige funksjoner og handlingsmuligheter.

Kritisk medieforståelse handler om å utruste brukerne med kunnskap og ferdigheter, for å evaluere medieinnhold kritisk. Herunder inkluderer dette å skille mellom kommersielt og redaksjonelt innhold, identifisere falsk informasjon – og forstå hvordan medieinnhold kan være formet av ulike interesser (Medietilsynet, 2021). I forhold til personvern på SNS, kan en person som har en god kritisk medieforståelse, være i bedre stand til å forstå hvordan deres personlige

informasjon blir samlet, brukt eller misbrukt. En kritisk medieforståelse sørger slikt sett for at vi har verktøyene til å bedømme det vi ser på en kritisk måte.

Dette overlapper i noen grad med det Ytre-Arne og Das (2020) omtaler som brukernes *kommunikative handlekraft* (communicative agency). I en tid med stadig økende datafisering, har individets evne til å tolke og påvirke sin egen kommunikasjon fått en større betydning. Denne handlekraften er nettopp brukernes *evne* til å påvirke, tolke og engasjere seg i hverdagslige kommunikasjonsprosesser og de strukturene som er en del av dette. Forfatterne belyser også at brukeren har et maktpotensiale, som kommer til overflaten når kommunikasjonen skal tolkes, og at dette varierer alt etter konteksten. I sammenheng med personvern på SNS, kan en høy kommunikativ handlingskraft handle om å være proaktiv i å beskytte sitt eget personvern. I praksis kan dette innebære at brukeren er i stand til å forstå og håndtere personvernsinnstillinger, velge alternative plattformer - og ta informerte valg om *hva* de deler, og med *hvem*. I stedet for å se på personvern som et valg mellom å være helt privat (gjennom å ikke dele noe) eller å være helt offentlig, så argumenteres det for at personvern er noe som kontinuerlig *forhandles* om, og blir påvirket av den kulturelle og sosiale konteksten. Brukeren foretar seg slike forhandlinger om hvordan de skal fremstå i ulike kontekster, gjennom å bruke deres handlingskraft i møte med handlingsmulighetene på SNS - noe som omtales som *networked privacy* ((Marwick og Boyd, 2014).

3.5 Teoretisk oppsummering

I dette kapitlet har vi gått igjennom en rekke studier og teorier, tilknyttet personvern og hvordan begrepet kan forstås i dagens datafiserte mediesamfunn. Denne teoretiske forankringen har hatt som formål å gi en *helhetlig* forståelse - først og fremst for hvorfor personvern er viktig, både for oss selv og for andre rundt oss. Dernest hvordan ulike overtredelser av personvernet kan tolkes. Noen tilbakevendende aspekter er at personvern må sees i *kontekst* av hvilke private *sfærer* som berøres. Vi har også sett på hvordan brukere kan anvende ulike taktikker for å opprettholde sin egen selvrepresentasjon, og et ideelt nivå av personvern. Hvordan de mestrer dette preges gjerne av deres kritiske medieforståelse og kommunikative handlekraft på plattformene. Samlet sett vil dette bidra til et teoretisk bakteppe, som vi skal vende tilbake til i analysekapitlene, og settes i kontekst i den oppsummerende diskusjonen.

KAPITTEL 4 – Metode

Denne studien er basert på semistrukturerte forskningsintervjuer og tenke høyt-protokoller med tolv informanter, tilhørende Generasjon Z og Boomers. Nå skal vi gå inn på hvordan studien har blitt planlagt, gjennomført og analysert - samt refleksjoner knyttet til denne forskningsprosessen. Herunder tar kapitlet for seg hvilke metodiske tilnærminger som ble benyttet for å undersøke holdninger til personvern på SNS, blant de to utvalgte generasjonene. En metode er i enkle trekk en systematisk fremgangsmåte for å finne svar og å lære om noe, og er selve bindeleddet mellom forskningsspørsmålene og analysen (Østbye *et al.*, 2013, 14). Formålet med kapitlet er fremfor alt å skape en transparens rundt prosessen, og således avklare og begrunne for valget av den kvalitative tilnærmingen. Dette innebærer forarbeid knyttet til intervjuguide, pilotstudie og rekruttering. Deretter går jeg inn på gjennomføring av datainnsamlingen og introduisering av utvalget - etterfulgt av selve behandlingen av datamaterialet. Kapitlet avrundes med en kritisk refleksjon av metodens styrker og svakheter.

4.1 Valg av kvalitative metoder

I dette delkapitlet skal vi se på bakgrunnen for valget av kvalitative forskningsintervjuer, kombinert med en tenke høyt-metode. Barbara Gentikow forteller at et fenomen både har kvantitative og kvalitative sider (2019, s. 35) - holdninger til personvern er intet unntak. *Kvantitative* metoder retter gjerne et fokus mot å forklare et fenomen, ofte gjennom å finne entydige svar på hypoteser (Gentikow, 2019, s. 37). Gjennom en spørreundersøkelse, kunne jeg eksempelvis samlet inn konsise svar fra mange respondenter, og dermed oppnå bredde i studiet. En slik tilnærming ville dog medført en større avstand til respondentene. Jeg ønsket derimot å oppnå en dypere forståelse av informantens erfaringer til personvern på SNS. Gjennom å ha direkte samtaler med dem, kunne jeg dermed få innsikt i deres tankemønstre rundt det intrikate temaet. Slik kan *kvalitative* metoder avdekke *ambivalenser* – slik som usikkerhet eller motstridende følelser (Gentikow, 2019). Slike metoder kan dog ikke tallfestes på samme måte som kvantitative, men bidrar med et flertydig materiale, der informantens erfaringer står i sentrum. Dette var et av resonnementene som gjorde det naturlig å gå for en kvalitativ tilnærming i denne studien. En annen begrunnelse var også at det eksisterer nyere kvantitativ forskning - slik som personvernsundersøkelsen til Datatilsynet (2020) - som gir en pekepinn på hvordan tilstanden er blant nordmenn. Men personvernsholdninger kan ikke nødvendigvis bare måles i tallverdier. Et viktig aspekt handlet dermed om å velge metoden som best kunne svare på forskningsspørsmålet.

Forskningsdesignet i denne studien er i utgangspunktet *eksplorativt*, der jeg ønsker å utforske informantenes holdninger. Samtidig befinner metoden seg i spennet mellom *induktiv* (datadrevet) og *deduktiv* (teoridrevet) tilnærming. På den ene siden, har jeg tatt utgangspunkt i de tre komponentene for holdning – kognitiv, atferd og affektiv – som jeg ønsket å utforske hos informantene. Dette har satt sitt preg på intervjuguiden og analysen. På den andre induktive siden, har jeg samtidig vært helt åpen for det som ville komme frem gjennom datamaterialet.

4.1.1 Kvalitative forskningsintervjuer

Det *kvalitative forskningsintervjuet* står sentralt i forskningsdesignet. Dette er et intervju, som kan minne om en samtale, hvor informantene kan uttrykke seg verbalt og fritt med egne formuleringer (Gentikow, 2019). Begrepet *informant* benyttes videre om personen som intervjues – siden forskeren ønsker å bli informert om refleksjoner som informanten har om fenomenet (Østbye *et al.*, 2013, s. 103). Slike intervjuer foregår en-til-en, der hensikten er å gå i dybden på tematikken.

Selv om slike intervjuer kan ligne en samtale, så er de som oftest *semistrukturerte*. Dette innebærer at tema og spørsmål er utformet på forhånd i en *intervjuguide*. Slike intervjuer er imidlertid ikke like strukturert som *respondentintervjuet* - der alle spørsmål stilles til alle i en fast rekkefølge. De er heller ikke helt åpne, slik som et *eksplorerende etnografisk* intervju (Gentikow, 2019, s. 83). Kvale og Brinkmann (2009) mener derfor at forskningsintervjuet ikke er en samtale mellom to *like* parter, da forskeren definerer og kontrollerer situasjonen. Innenfor den kvalitative metode, anerkjenner man derfor at forskeren ikke kan unngå å påvirke prosessen – noe som kalles for en *forskereffekt* (Gentikow, 2019, s. 49).

En annen utfordring er at informantene kan ha en tendens til å se forskeren som en slags ekspert, og dermed svare det de tror forskeren ønsker å høre (Tjora, 2017). Fordelene med semistrukturerte intervjuer er likevel at metoden gir forskeren stor fleksibilitet, da det er muligheter for å stille oppfølgingsspørsmål til informanten underveis, og å grave dypere dersom det dukker opp interessante innspill (Gentikow, 2019). På bakgrunn av fleksibiliteten i semistrukturerte dybdeintervju, er det også flere muligheter for å kombinere metoden sammen med andre kvalitative tilnærminger (Schröder *et al.*, 2003, s. 30). Jeg ønsket derfor å supplere forskningsintervjuet med en kvalitativ observasjonsøvelse, omtalt som en *tenke høyt-metode*.

4.1.2 Tenke høyt-metode

Med et formål om å oppnå et rikere datamateriale, komplimenterte jeg forskningsintervjuet med en avsluttende observasjonsdel, omtalt som en tenke høyt-metode (think aloud method) (Charters, 2003). Denne metoden utfordrer informanten til å *tenke høyt*, samtidig som de utfører en oppgave. Det å tenke høyt handler i praksis om å sette ord på oppfatninger og følelser underveis i øvelsen – samtidig som forskeren observerer, noterer og kan komme med oppfølgings spørsmål (Someren, Barnard og Sandberg, 1994).

I denne studien fikk informantene oppgaven *etter* forskningsintervjuet. Da ble de spurt om å gå inn på Facebook eller Instagram og finne frem til *personvernsinnstillingene*, samt se på disse. I forkant ble de oppfordret til å uttrykke seg verbalt om det som falt dem inn når de skulle utføre øvelsen. Her kunne informanten kommentere på hvordan de hadde stilt inn personvernet på profilen sin, og få frem sine tanker om dette. Beslutningen om å legge tenke høyt-metoden etter selve forskningsintervjuet, handlet om å unngå å styre informanten inn i et tematisk spor spesifikt knyttet til personvern (forskereffekt). Hadde de fått beskjed om å gå inn på innstillingene først, ville dette potensielt lagt føringer for forskningsintervjuet når de omtalte sine personvernsinnstillinger. Det handlet også om å «varme opp» informanten under intervjuet, og skape en trygg sfære for å diskutere tankene (Someren, Barnard og Sandberg, 1994, s. 43).

Poenget med øvelsen er ikke å finne frem til personvernsinnstillingene så fort som mulig - men å få en unik innsikt i informantens *kognitive* prosesser, gjennom at informantene kan vise til atferdstendenser i sanntid (Someren, Barnard og Sandberg, 1994). Gjennom forskningsintervjuet kan informanten verbalisere sine handlinger rettet mot personvernet på SNS. Det som er interessant med tenke høyt-metoden, er imidlertid at den kan si noe om informanten sin *faktiske atferd* tilknyttet personvern på SNS, og sammenligne det opp mot det de har hevdet i forkant – noe som også har vært etterspurt (Kokolakis, 2017). Hensikten er slikt sett å berike datamaterialet fra en annen vinkel - og hovedsakelig knytte resultatene til holdningskomponenten, *atferd* (Kapittel 6).

Tenke høyt-metoden kan herunder kobles til *privatlivsparadokset* presentert i teorien (3.1) - som illustrerer hvordan brukere uttrykker bekymring for privatlivet sitt, men i praksis ikke gjør tiltak for å beskytte det (Barnes, 2006). Slike tiltak innebærer blant annet å skaffe en oversikt over personvernsinnstillingene, og stille dem inn etter behov. Dette krever likevel at brukeren vet *hvor* de finner innstillingene og *hva* de ulike innstillingene har som konsekvenser. Det

bunner dermed ned i brukerens *kritiske medieforståelse* og *kommunikative handekraft*. Tenke høyt-metoden kan slikt sett bidra til å tolke informantenes forståelse, og se etter forskjeller mellom den eldre og den yngre generasjonen.

4.2 Planlegging av studien

Før den faktiske datainnsamlingen kunne iverksettes, var det en rekke elementer som måtte på plass. De neste avsnittene vil adressere denne forberedelsesfasen, som inkluderer utforming av utvalgs-kriterier, intervjuguide, samt gjennomføringen av pilotstudie.

4.2.1 Utvalgs-kriterier

Rekruttering av informanter ble planlagt med tanke på spesifikke *kriterier*. Hovedkriteriene for utvalget inkluderte *alder*, *bosted*, og at de hadde en *personlig profil* på Facebook og/eller Instagram (Se Tabell 4.1). Innenfor disse rammene var målet å samle et *heterogent* utvalg, som kunne gi innsikt fra ulike perspektiver. For å unngå skjevhet i utvalget, ble det også lagt vekt på å oppnå en balanse mellom *kjønnene* i hver generasjon.

Ettersom studien har et fokus på ulike generasjoner, var *alderskravet* av primær betydning. Selv om det ikke eksisterer fastsatte grenser for hvor en generasjon avsluttes og en annen begynner, har jeg basert meg på tidligere studier, slik som Campbell *et al.*, (2015) og Twenge (2023). De definerer *Boomers* som personer født mellom 1946-1965 (57-76 år). *Generasjon Z* tilsvarer personer født mellom 1996-2012 (10-26 år). Av praktiske årsaker tok jeg beslutning om å sette en nedre aldersgrense på 15 år. Dette ble dermed utgangspunkt for alderskravet i rekrutteringen.

Det andre utvalgs-kriteriet fokuserte på en *geografisk* begrensning, der informantene måtte ha vokst opp og være bosatt i Norge. Dette kriteriet ble satt på bakgrunn av variasjonen i personvernreguleringer mellom nasjoner – noe som antas påvirke innbyggernes holdninger til personvern. Studiens *validitet* kunne potensielt blitt svekket dersom enkelte informanter kom fra land med andre personvernlover, slik som USA. Videre hadde kriteriet et kulturelt aspekt. Nordmenn har eksempelvis blitt oppfattet som «kalde og uvelkomne» av besøkende (Fosse, 2022). Kvalnes (2010) påpeker også at intimgrenser er svært viktig for nordmenn, der de verdsetter det personlig rom. Kvalnes viser til studier som indikerer at innbyggere i Nord-Europa opprettholder en større avstand til fremmede enn hva som er tilfellet for innbyggere i Sør-Europa. Dette kan antyde at nordmenn har et større behov for privatliv, og understreker betydningen av et norsk utvalg for å samle inn et solid datagrunnlag for studien.

Det siste hovedkriteriet var at informantene måtte ha en *personlig profil* på en SNS, tilknyttet Meta – altså Facebook eller Instagram. Dette utelukket personer som kun brukte pseudonymer (falske identiteter), eller styrte profiler på vegne av andre organisasjoner. Hensikten var å koble deres bruk på plattformene til synet på personvern – noe som kunne ha blitt svekket dersom informantene kun brukte profiler uten direkte tilknytning til deres eget personlige liv. En bemerkning er at jeg i utgangspunktet ikke ønsket å begrense informantene til én bestemt plattform, men utforske deres generelle holdninger til personvern i sosiale medier. Imidlertid har mangfoldet av SNS økt betydelig - der ulike plattformer har ulike funksjoner og appellerer til forskjellige målgrupper. Dette kunne ha resultert i for stor bredde og potensielle utfordringer knyttet til analysen av materialet, dersom informantene ikke hadde noen felles plattformer å vise til. Et viktig aspekt var også at begge generasjoner hadde erfaring med Meta-plattformene over tid.

Tabell 4.1: Hovedkriterier for studien	
I.	Alder mellom 15-26 år eller 57-76 år
II.	Oppvokst og bosatt i Norge
III.	En aktiv personlig profil på Facebook og/eller Instagram

Det skal likevel bemerkes at studien kunne fokusert på andre kriterier – slik som kulturell bakgrunn, utdanningsnivå, teknologisk kompetanse, sosioøkonomiske status eller andre sosiokulturelle faktorer. Ved å inkludere flere av disse kriteriene kunne man fått et enda mer nyansert bilde av holdninger til personvern på SNS.

4.2.2 Intervjuguide

Etter å ha avklart kriteriene, utformet jeg en intervjuguide som skulle legge noen føringer i det kvalitative forskningsintervjuet. Intervjuguiden (Vedlegg 1) var *semistrukturert*, med både åpne og lukkede spørsmål for å simulere en samtale. Guiden ble utformet med utgangspunkt i det overordnede forskningsspørsmålet, og tilhørende analysespørsmål. Den er videre delt inn i seks deler med ulike formål:

I **Del 1** av intervjuguiden var hensikten å innhente grunnleggende bakgrunnsinformasjon – slik som alder, bosted og yrke. I **Del 2** var intensjonen å innhente informasjon om informantenes bruk av sosiale medier i hverdagen, og dermed få innsikt i hvor komfortable de var med å dele personlig informasjon. Videre ble deres preferanse for Meta-plattform (Facebook/Instagram) avklart - noe som påvirket resten av intervjuet, der jeg knyttet spørsmålene til den plattformen de kjente best til. Slikt sett berørte Del 2 *atferdskomponenten*, med fokus på *verbale* utsagn om bruk av handlingsmulighetene. **Del 3** fokuserte på den *affektive* holdningskomponenten, der

målet var å undersøke informantenes følelser knyttet til kontroll over egen personlig informasjon og deres opplevelse av å dele privat informasjon på SNS. **Del 4** av intervjuguiden omhandlet den *kognitive* holdningskomponenten, med spørsmål direkte relatert til personvern og kunnskap knyttet til dette. Dette ble bevisst plassert lenger ut i intervjuet, for å ikke overvelde eller styre informanten direkte inn på personvern når de snakket om de andre delene. I **Del 5** ble fokuset rettet igjen mot atferdskomponenten, men nå relatert til personvern på Meta - inkludert håndtering av informasjonskapsler og endring av personvernsinnstillinger. Dette gav en naturlig overgang til **Del 6**, hvor tenke-høyt-øvelsen ble gjennomført. Informantene ble instruert til å finne frem til personvernsinnstillingene på Facebook eller Instagram og reflektere høyt over innstillingene og deres opplevelse av plattformens personvern.

Intensjonen var å bygge opp en intervjuguide der de ulike delene fløt over i hverandre, slik at det ville oppleves mer som en samtale, fremfor et formelt intervju. På bakgrunn av dette er spørsmål knyttet til de tre holdningskomponentene også spredt litt utover, slik som spørsmål knyttet til atferd. En viktig bemerkning er at det ikke er noen eksplisitte spørsmål i intervjuguiden om hvilken *holdning* informanten har til personvern. Bakgrunnen for dette var at folk flest legger ulike betydninger i hva en holdning er. Dette kunne gi svært sprikende svar, da ulike informanter kunne ha hatt ulike oppfatninger om begrepet. Det er derfor operasjonaliseringen gjennom tre-komponentmodellen er så sentral i denne studien, fordi hver komponent – kognitiv, atferd og affektiv – skaper samlet sett selve holdningen. Spørsmålene i guiden ble også modifisert etter hvilken informant jeg henvendte meg til. Dette er en av fordelene med semistrukturerte intervjuer, men var også en nødvendighet med tanke på det store aldersspennet mellom generasjonene. Det var herunder viktig å ordlegge seg etter deres alder og erfaring. Jeg fulgte heller ikke guiden slavisk, dersom informanten svarte på et spørsmål som jeg hadde tenkt til å spørre om senere i intervjuet. Samtidig forsøkte jeg å opprettholde en viss struktur på samtalen, slik at alle del-temaene ble berørt i løpet av intervjuet.

4.2.3 Pilotstudie

Schröder *et al.* (2003, s. 163) understreker at forskningsdesignet alltid bør testes ut i forkant av datainnsamlingen – gjennom en *pilotstudie*. Dette så jeg som en nyttig øvelse for å prøve ut kombinasjonen av forskningsintervju og tenke høyt-metoden. Pilotstudien hadde stor verdi i form av at jeg fikk ett innblikk i hva som fungerte – og aspekter som kunne forbedres. Her fikk jeg også et estimat på varigheten av opplegget, som resulterte i omtrent 50 minutter. Det første intervjuet ble gjennomført fysisk på et møterom i november 2022, med en bekjent mann på 26

år. I utgangspunktet antok jeg at én gjennomgang var tilstrekkelig for pilotstudien – men innså at det ville være hensiktsmessig å teste ut intervjuguiden på en person tilhørende Boomer-generasjonen. Formålet med dette var å teste ut om spørsmålene var tydelig formulert for denne aldersgruppen, eller om det måtte gjøres tilpasninger. Det andre intervjuet var med en bekjent mann på 58 år, som ble gjennomført over den digitale kommunikasjonsplattformen, Zoom. Her var jeg noe i tvil om det ville bli utfordringer under intervjuet, spesielt med tanke på å gjennomføre tenke høyt-metoden digitalt. Faktorer slik som tekniske problemer på lyd eller andre utfordringer med kommunikasjonen mellom forsker og informant lå øverst på listen.

Gjennom å intervjuer begge generasjoner, samt i både fysisk og digitale omgivelser, viste det seg imidlertid at opplegget fungerte mye bedre enn forventet. Pilotstudien indikerte at kombinasjonen av forskningsintervjuet og tenke høyt-metoden, medførte ulike perspektiver og en dynamikk, som enkeltintervjuer alene ikke kunne oppnå. Etter pilotstudien ble mindre justeringer gjort, der jeg omformulerte noen spørsmål og fjernet enkelte som overlappet. Jeg innførte også vanen med å ta opp lyd fra to ulike opptakskilder, fremfor en – dersom den ene skulle feile. På bakgrunn av at det ikke ble utført betydelige endringer på intervjuguiden eller metoden i sin helhet ble det, i samråd med veileder, besluttet å inkludere intervjuene fra pilotstudien i datagrunnlaget.

4.3 Gjennomføring av datainnsamlingen

Dette delkapittelet tar for seg hvordan de ulike forskningsstadiene ble gjennomført. Herunder prosessen med rekruttering, og gjennomføring av intervjuene. Informasjon om studiens informanter blir også presentert. Først innledes det med etiske hensyn som ble tatt tilknyttet informantenes personvern.

4.3.1 Etiske hensyn

I en masteroppgave som handler om personvern, har det følgelig vært helt sentralt å gjennomføre forskningsprosessen i tråd med informantenes personvern. Det bunner her ned i *hva man vet* om informanten, og *hva man har lov* til å si videre. Dette kan by på etiske utfordringer, spesielt dersom datamaterialet er sensitivt. Informanten kan eksempelvis oppgi sensitive opplysninger om seg selv under intervjuet (Datatilsynet, 2019b). Selv om ikke personvern som tema nødvendigvis er sensitivt i seg selv, vil det være umulig å forutsi hvordan informantene tolker spørsmålene og hvordan de kommer til å svare. Et annet aspekt, er at barn kan samtykke til deling av personopplysninger når de først fyller 18 år (Datatilsynet, 2022). Da

jeg ønsket å rekruttere informanter ned i 15 år, var det viktig at forskningsprosessen fulgte etiske hensyn i henhold til gjeldende retningslinjer. Prosjektet ble derfor sendt inn til *Sikt* (tidligere NSD, Norsk senter for forskningsdata) og *RETTE* (system for risiko og etterlevelse ved UiB).

Sikt vurderte at prosjektet kun samler inn *alminnelige* personopplysninger (Vedlegg 2). Når det kom til informanter under 18 år, var samtykke gyldig, dersom det ble gitt av barnets foresatte. Databehandlingen i denne studien oppfyller dermed kravene om riktighet, integritet, konfidensialitet og sikkerhet. *Informert samtykke* ble innhentet ved å sende samtykkeskjema elektronisk til informantene i god tid før intervjuet (Vedlegg 3). Skjemaet informerte om studiens formål, at det var frivillig å delta og mulighet for å trekke seg. Det var kun én informant under 18 år – i dette tilfellet samtykket foreldrene på vegne av personen. I etterkant av hvert intervju ble eventuelle persondata kryptert og lagret på passordbeskyttende enheter. Konfidensialitet ble herunder opprettholdt, spesielt i utarbeidelsen av datamaterialet. Dette innebar at informantene ble anonymisert gjennom fiktive navn og identifiserende informasjon ble fjernet eller omskrevet i transkripsjonen.

4.3.2 Rekrutteringsprosess

Rekruttering av informantene viste seg å være en utfordrende prosess, og ulike metoder ble derfor benyttet for å oppnå ønsket antall deltagere. I løpet av høsten 2022 benyttet jeg meg først av *snøballmetoden* (Schröder *et al.*, 2003, s. 162). I tråd med denne rekrutteringsmetoden tok jeg kontakt med bekjente fra eget nettverk og fortalte dem om forskningsprosjektet, samt hvilke kriterier som var gjeldende. Deretter ba jeg dem kontakte sine bekjente for å finne potensielle informanter. Herunder ønsket jeg å senke terskelen for deltagelse, og det ble derfor vektlagt i kommunikasjonen at studien ikke hadde noen krav til forberedelser i forkant - samt at det kunne utføres både *fysisk* og *digitalt*. Formålet var å legge det på informantens premisser. Deltagelsen var således helt frivillig, og informantene mottok ikke økonomisk kompensasjon – da dette kunne ha påvirket besvarelsen eller motivasjonen for å delta i studien.

Snøballmetoden viste seg å være effektiv, da flere personer innen kort tid meldte sin interesse for å delta i studien. Imidlertid førte denne type rekruttering til noen utfordringer. For det første fikk mine bekjente en rolle som *meglere* – mellom meg (forskeren) og deres bekjente (potensielle deltagere). Dette resulterte i tap av tre mulige informanter, grunnet kommunikasjonssvikt. For det andre førte snøballmetoden til rekruttering av informanter som lignet noe på hverandre. Dette var gjerne et resultat av rekruttering gjennom vennskap eller

felles interesser, og kan ha hatt en innvirkning på variasjonen i utvalget. Et eksempel på dette var at tre av informantene hadde en bakgrunn fra helsesektoren, noe jeg ikke var klar over før etter intervjuene. Ellers var det generelt utfordrende å rekruttere informanter tilhørende Boomer-generasjonen – og spesielt menn. Jeg la derfor ut et innlegg på Facebook, der jeg skrev kort om tema og kriterier for studien, Her var det flere som viste interesse for prosjektet, men som dessverre lå utenfor alderskriteriet. Gjennom Facebook-innlegget ble det totalt rekruttert to informanter, utenfor eget nettverk.

Generasjon:	Informantens pseudonym	Alder	Bosted	Situasjon	Uttalt repertoar av sosiale medier	Fikk sosiale medier i år:	Aktivitet på Facebook (FB) og Instagram (IG)*
Babyboomer (f.1955-1965)	«Rita»	67	Bygd, Vestlandet	Pensjonist	Facebook og Instagram	2009 (53 år)	FB: Aktiv IG: Passiv
	«Dagny»	66	Bygd, Vestlandet	Ufør	Facebook, Instagram, Messenger, Snapchat	2012 (55 år)	FB: Aktiv IG: Aktiv
	«Åse»	62	By, Østlandet	Helsesykepleier	Facebook, Instagram, Snapchat, Messenger	2011 (50 år)	FB: Aktiv IG: Aktiv
	«Ingrid»	58	By, Innlandet	Lærer	Facebook (tidligere Instagram)	2009 (43 år)	FB: Aktiv IG: Inaktiv
	«Jan» (Pilot 2)	58	By, Vestlandet	Rådgiver	Facebook, Instagram, Twitter, LinkedIn	2007 (41 år)	FB: Passiv IG: Aktiv
	«Ove»	57	By, Vestlandet	Selvstendig næringsdrivende	Facebook, Instagram, Snapchat og Messenger	2011 (45 år)	FB: Aktiv IG: Aktiv
Generasjon Z (f.1996-2007)	«Tony» (Pilot 1)	26	By, Vestlandet	Teknisk kundebehandler	Snapchat, Instagram, Facebook, Messenger, Reddit og Discord	2009 (13 år)	FB: Passiv IG: Aktiv
	«Bertine»	25	Bygd, Østlandet	Prosjektleder	Instagram, Snapchat, TikTok, Facebook, VESCO	2011 (14 år)	FB: Passiv IG: Aktiv
	«Emilie»	23	By, Vestlandet	Frisør	Instagram, Snapchat, Facebook, TikTok	2012 (12 år)	FB: Passiv IG: Aktiv
	«Adam»	22	Bygd, Vestlandet	Fisker	TikTok, Instagram, Snapchat, Facebook, YouTube	2010 (10 år)	FB: Passiv IG: Aktiv
	«Nora»	19	By, Vestlandet	Lærling	Snapchat, Instagram, Facebook (tidligere TikTok)	2017 (13 år)	FB: Inaktiv IG: Aktiv
	«Christian»	15	By, Sørlandet	10. klasse	Instagram, Snapchat, Facebook (tidligere TikTok)	2019 (12 år)	FB: Passiv IG: Aktiv

Tabell 4.2: * Aktivitet på Facebook (FB) og Instagram (IG). Aktiv = bruker plattformen hver dag og publiserer eget innhold, Passiv = Bruker plattformen minimum ukentlig, men publiserer ikke eget innhold, Inaktiv = Har en opprettet brukerprofil, men bruker ikke plattformen jevnlig.

4.3.3 Studiens utvalg

Rekrutteringsprosessen førte til et utvalg på tolv informanter, der seks tilhørte Boomer-generasjonen (57-67 år) og seks tilhørte Generasjon Z (15-26 år). For ordens skyld er denne utvalgsstørrelsen i overensstemmelse med anbefalinger i metodelitteraturen, som oppfordrer til

en nedre grense på ti informanter (Schröder *et al.*, 2003; Gentikow, 2019). Selv om målet var å oppnå en balanse mellom kjønnene, bestod det endelige utvalget av fem menn og syv kvinner. Det er likevel verdt å merke seg at kvinner er overrepresentert blant brukere av Facebook og Instagram (Ipsos, 2023). I tillegg var det et mål å spre informantene utover generasjonens aldersspenn. Dette ble i stor grad oppnådd blant Generasjon Z (f.1996-2012), men blant Boomer-generasjonen (f.1946-1965) var det ingen informanter i alderen 68-76 år. I tabellen under er en oversikt over informantene, delt inn i de to generasjonene:

4.3.4 Datainnsamling

Selve datainnsamlingen ble iverksatt mellom desember 2022 og mars 2023. I de neste avsnittene går jeg nærmere inn på hvordan metoden ble gjennomført i praksis. Herunder ble det utført både fysiske og digitale forskningsintervjuer, der *Zoom* ble benyttet som et audiovisuelt verktøy for å samle inn kvalitative data (Archibald *et al.*, 2019a). Fire av intervjuene skulle ordinært utføres fysisk, men på grunn av utsettelse og knapphet på tid, ble disse avholdt gjennom *Zoom*. De resterende intervjuene ble gjennomført fysisk på lokasjoner med lite til ingen forstyrrelser – slik som møterom og informantens hjem. Noen dager før intervjuet mottok alle informantene et *samtykkeskjema* (Vedlegg 3) og informasjon om deltagelse. I starten av møtet med informanten ble hovedpunktene i skjemaet gjennomgått, før selve forskningsintervjuet startet. Her ble de blant annet forsikret om anonymisering. I digitale intervjuer over *Zoom*, var det også enkelte som gav samtykke *muntlig* – da enkelte informanter ikke kunne returnere dokumentet elektronisk (ifølge Sikt er muntlig samtykke også gjeldende). For å unngå personlig informasjon i datamaterialet, ble de muntlige samtykkene spilt inn på et separat lydopptak, før intervjuet startet.

Selve intervjusituasjonen var todelt, der jeg først intervjuet informanten, for så å avslutte med tenke høyt-øvelsen. Når intervjuet startet, ble lydopptakene satt i gang på min private mobil og PC. Helt overordnet var *intervjuguiden* førende i intervjuene, selv om noen temaer kom i ulik rekkefølge. Under intervjuene ble også Kvale (2001) sine *kvalifikasjonskriterier for intervjueren* tatt i betraktning. Jeg forsøkte herunder å stille klare spørsmål, unngå akademisk sjargong, samt opptre vennlig og lyttende i møte med informanten. Jeg opplevde det relativt forskjellig å intervjuer en på 15 år, i forhold til noen på 67 år. Her ble det spesielt viktig å la informantene snakke i sitt eget tempo med eget språk, samtidig som jeg var kritisk til det som ble sagt. Både under og etter intervjuet skrev jeg ned interessante refleksjoner og observasjoner, mens det fortsatt var ferskt i minnet. Under tenke høyt-øvelsen var det enkelte informanter som

hadde tidspress, og som resultat ikke fikk like mye ut av øvelsen. Ellers foregikk disse som planlagt. Opplegget hadde en total varighet på mellom 40 og 70 minutter, og varierte basert på informantenes personlighet og tilgjengelighet. Brorparten av intervjuene foregikk helt uforstyrret, men enkelte av de digitale intervjuene hadde dog noen tekniske problemer i oppstarten. Jeg opplevde likevel at informantene var vel så fokusert på samtalen - og til tider i større grad enn i de fysiske intervjuene. Spesielt under tenke høyt-metoden, fikk jeg også et bedre bilde av informantens ansiktsuttrykk når de gikk gjennom personvernsinnstillingene sine.

4.4 Analyse av datamaterialet

Når datainnsamlingen nærmet seg slutten, var det tid for å forberede datamaterialet for analysen. Selv om det er mange tilnærminger til analytiske metoder, fant jeg en inspirasjon fra artikkelen til Braun og Clarke (2006), der de forteller om *tematisk analyse*. Ifølge forskerne fanger et *tema* opp noe viktig med dataene i forhold til forskningsspørsmålet – og representerer et mønster av fellestrekk (2006, s. 82). Johannessen, Rafoss og Rasmussen (2018, s. 282) har herunder laget en trinnvis tilnærming til å analysere data på denne måten, basert på Braun og Clarke (2006). Denne analyseringsprosessen består av fire faser, som legger strukturene for dette delkapittelet: *forberedelse, koding, kategorisering og rapportering*.

Gentikow påpeker dog, at en tematisk analyse kan identifisere strukturer som går på tvers av hele tekstmengden, men kan ha en tendens til å skjule individene bak (2019, s. 134-135). Til tross for at analysen hovedsakelig er basert på en tematisk tilnærming, har jeg også benyttet meg av *personsentrert* analyse. Dette fokuserer både på *hva* informantene sier og *hvordan* de sier det - noe som gjør det enklere å identifisere selvmotsigelser. Personsentrert analyse gir muligheten til å undersøke informantens fortellinger om spesifikke erfaringer, og har gitt innsikt i hvordan personvern oppfattes i ulike kontekster (Thagaard, referert i Gentikow, 2019, s. 135).

4.4.1 Forberedelse av datamaterialet: Transkribering

I en tematisk analyse, vil det første steget være å *forberede* datamaterialet (Johannessen, Rafoss og Rasmussen, 2018, s. 283). I denne fasen fikk jeg oversikt over materialet, gjennom å *transkribere* lydfilet fra intervjuene. Mellom desember 2022 og mars 2023 ble de tolv intervjuene satt på papir – og resulterte i intet mindre enn 117 A4-sider. Etter hvert som intervjuene ble gjennomført, transkriberte jeg fortløpende. På denne måten var intervjuet fortsatt ferskt, slik at informasjon som ikke kom tydelig frem gjennom lydopptaket, også ble

dokumentert. Dette var spesielt viktig i henhold til tenke høyt-metoden - slik som informasjon om hvilken plattform de valgte og momenter de så på, men ikke verbaliserte eksplisitt.

Parallelt med transkriberingen noterte jeg i tillegg ned tanker som jeg fikk underveis om informantens besvarelse. Dette var utsagn som potensielt kunne kobles til funn, tidligere forskning eller andre teoretiske knagger. Under selve transkriberingen ønsket jeg videre å gjengi informantens uttalelser så korrekt som mulig, samtidig som det gav en god leseflyt. Herunder ble det transkribert detaljer og ordlyder slik som latter, ironiske antydninger, tenkepauser og kroppsspråk der dette var implisitt. Jeg skrev dog ikke intervjuene på informantens dialekt, da dette kunne føre til utfordringer knyttet til å forstå og tolke materialet i ettertid. Selv om det eksisterer en rekke programvarer som transkriberer lydfiler automatisk, valgte jeg å transkribere dem manuelt på PC. Til tross for at dette tok lenger tid, så jeg i ettertid at det gav stor verdi i form av å bli godt kjent med materialet alle rede fra start – noe som gav en dypere forståelse av informantens perspektiver, samt bidra til en grundigere koding og analysering av datamaterialet.

4.4.2 Koding av datamaterialet: Bearbeiding

Det andre steget i en tematisk analyse handler om *koding*. Dette innebærer å fremheve og sette ord på viktige poenger i datamaterialet (Johannessen, Rafoss og Rasmussen, 2018, s. 284). I denne fasen ble det avgjørende å skape en ny og dypere innsikt, enn det som kom frem under transkriberingsstadiet. Først finleste jeg hvert av intervjuene på papir og markerte med fargekoder over interessante utsagn – samt eventuelle koblinger til de tre holdningskomponentene (kognitiv, atferd og affektiv). Samtidig skrev jeg også ned stikkord i margen som oppsummerte andre viktige poenger. Lengre refleksjoner og innfall som jeg fikk underveis i gjennomlesingen noterte jeg i en egen notatbok. Denne prosessen førte til at en del av datamaterialet kunne lukes ut, grunnet lav relevans. Etter den fysiske kodingen overførte jeg materialet til et Excel-dokument for hver av generasjonene. Her satt jeg informantene under hverandre loddrett og aktuelle temaer vannrett. Slik kunne jeg lettere se forskjeller og sammenfall innad i og mellom generasjonene. Når alt var fylt inn digitalt, tok jeg en ny runde med koding. Dette viste seg å være nyttig, da jeg så enda flere aspekter enn i den første runden.

4.4.3 Kategorisering av datamaterialet: Analysetemaer

Etter kodingen av materialet, var det tid for den tredje fasen i den tematiske analysen – *kategorisering*. Under kodingen var formålet å dykke ned i detaljene av transkripsjonene. For å kategorisere selve materialet, måtte jeg imidlertid ta et steg tilbake for å se hvordan dataene

kunne settes sammen til en større helhet. Dette bunnet ned i å sortere dette i mer overordnede temaer (Braun og Clarke, 2006).

Et *tema* kan identifiseres gjennom en induktiv eller deduktiv tilnærming – der begge har både fordeler og ulemper. *Induktive* analyser lar dataene styre utviklingen av temaer, noe som kan lede til uventede funn. Samtidig kan forskere ha en tendens til å ikke helt fri seg fra egne teoretiske eller epistemologiske forutsetninger. *Deduktive* analyser er derimot drevet av forskerens teoretiske interesser, som kan gi en mer detaljert analyse av bestemte deler av dataene - men fort overse rikere, bredere beskrivelser av dataene (Braun og Clarke, 2006, s. 84). Som tidligere nevnt, vil denne studien dra veksel på de to tilnærmingene - da formålet er å avdekke holdninger (kunnskap, følelser og atferd). Samtidig skal det bemerkes at jeg har gått inn i datamaterialet med åpent sinn, og analysert utvalget både fra et helhetlig ståsted, på tvers av de to generasjonene og innenfor hver informant. Med utgangspunkt i forskningsspørsmålet, var det ønskelig å besvare følgende analyse spørsmål (AS) gjennom datamaterialet:

AS1 (Kognitiv): Hvordan *forstår* Boomers personvern i forhold til Generasjon Z?

AS2 (Atferd): Hvordan *handler* Boomers når det kommer til personvern på Meta, i forhold til Generasjon Z?

AS3 (Affektiv): Hva *føler* Boomers om personvernet på Meta i forhold til Generasjon Z?

Under den *kognitive* holdningskomponenten, så jeg etter hva de to generasjonene kunne om personvern, hvordan de definerte begrepet, samt om de kjente til regelverket. Det var også ønskelig å forstå deres oppfatninger om hvordan Meta samlet inn og behandlet deres personopplysninger – og hvor mye dette avvek fra realiteten. Et siste aspekt ved det kognitive, var å få innsikt i hvordan de vurderte verdien av eget privatliv. Under *atferdskomponenten*, ønsket jeg å utforske både deres verbaliserte intensjoner i møte med personvern, men også deres faktiske personvernshandlinger gjennom tenke høyt-øvelsen. Slik som deres forhold til personvernsinnstillinger og taktikker for å navigere privatliv på SNS. Under den *affektive* komponenten handlet det om å se på de emosjonelle aspektene ved Meta sin datainnsamling, om informantene stolte på selskapet og om de følte på en kontroll over egne opplysninger. Her var det også viktig å se etter emosjonelle responser på potensielle krenkelser av personvernet.

4.5 Metodiske refleksjoner

I dette avsluttende delpunktet av metodekapitlet ønsker jeg å reflektere rundt kvaliteter og mangler ved metoden. Dette uttrykkes gjennom studiens *validitet*, *reliabilitet*, samt noen ord

om *generalisering* i møte med kvalitative studier. Dette er tre verdier som er ufravikelige krav i kvantitative metoder, men som kan være utfordrende å oppnå gjennom kvalitativ tilnærming (Gentikow, 2019, s. 56-63).

Reliabilitet handler om studiens pålitelighet, der datamaterialet og resultatene av analysen må være troverdige (Østbye *et al.*, 2013, s. 29). Mine vurderinger som er blitt tatt underveis, har derfor vært sentrale for hvor pålitelig studien er. Formålet med dette metodekapittelet har nettopp vært å gjøre forskningsprosessen *transparent* - med både styrker og eventuelle svakheter. En bemerkning er at grunnet masteroppgavens formelle begrensninger på format og lengde, har det ikke vært mulig å få med alle nyansene og rikdommen i datamaterialet. Gjennom en lang analyseprosess er det kun de mest sentrale funn som er fremhevet i analysekapitlene, og som totalt sett besvarer forskningsspørsmålet. Videre må det kommenteres at selv om datamaterialet oppnådde en viss metning, hadde jeg ideelt sett ønsket å ha et større utvalg med flere informanter fra hver generasjon. Spesielt i det øvre alderssjiktet av Boomer-generasjonen. Mangel på ressurser og tid var noe av grunnen til dette. Imidlertid forsøkte jeg å sikre et heterogent utvalg basert på de ulike demografiske variablene. Angående utvalget må det også nevnes at begge informantene i pilotstudien var *bekjente* - noe som kan ha påvirket deres besvarelser, og derav reliabiliteten av selve pilotstudien. Samtidig fylte de alle kriterier og resulterte i interessante intervjuer, noe som medførte at de ble tatt med videre. Det å ha en kombinasjon av både digitale og fysiske intervjuer, kan også ha påvirket reliabiliteten. Siden Zoom viser nærbilde av ansiktet til informanten, kan jeg eksempelvis ha gått glipp av noen nyanser knyttet til kroppsspråk og andre observasjoner av ikke-verbale signaler i intervjuet. Dette kan igjen ha påvirket min tolkning av informantens svar i analysen. Archibald *et al.* (2019) mener imidlertid at de største fordelene er at det reduserer reisekostnader og tid for både forskeren og deltakerne. Dette gir fleksibilitet i planlegging av intervjuet og kan gjennomføres på tider som passer best for både forskeren og deltakerne. Etter koronapandemien kan det også antas at flere er mer komfortable med slike digitale verktøy, enn tidligere. Disse resonnementene var noe av bakgrunnen til at jeg benyttet digitale intervjuer, i tilfeller der det ikke var mulig å gjennomføre dem fysisk.

Validitet handler på sin side om studiens gyldighet og sannhet - og bunner ned i om studien faktisk svarer på forskningsspørsmålet (Gentikow, 2019, s. 59). En bemerkning som gjelder selve intervjuene og tenke høyt-øvelsen, er imidlertid at en aldri kan være helt sikker på at informantene har oppgitt ærlige svar. Herunder kan informantene ha vært preget av

forskningssituasjonen, og dermed gitt utsagn som ikke var sannferdige i forhold til deres erfaringer (Kvale, 2001). Samtidig må jeg ta utgangspunkt i at det de har fortalt, er noe som reflekterer deres oppfatninger om personvernstatistikken - og legger grunnlaget for datamaterialet.

Et viktig poeng er at det er nettopp brukerens personvernsholdninger som er temaet for masteroppgaven. Menneskers holdninger har vært under forskningslupen i over hundre år, og ulike akademia tilnærmer seg holdninger på ulik vis. Det finnes dermed en rekke holdningsteorier og modeller som kunne vært benyttet her. Det har eksempelvis vært en lang diskusjon om *atferd* er en del av holdningen, eller en virkning av den (Ajzen og Fishbein, 1977). I denne studien var det ønskelig å benytte tre-komponentmodellen for å operasjonalisere holdning, og således trekke ut flere aspekter ved holdningene til personvern. Det handler også om å kunne sammenligne generasjonene i en struktur, som er utprøvd av tidligere forskning, uten å måtte finne opp «analysehjulet» på nytt. En nyere studie av Joëlle Swart (2021) utforsker eksempelvis unge menneskers *forståelse, følelser og engasjement* i møte med nyhetsalgoritmer på sosiale medier – noe som i teorien utgjør de tre holdningskomponentene. I og med at holdning er operasjonalisert gjennom det kognitive (kunnskap og oppfatninger), affektive (følelser og preferanser) og atferd (handlinger og atferdsintensjoner) (Eiser, 1986, s. 53) – ble det naturlig å dele inn masteroppgaven i analysekapitler som dekket relevante temaer innenfor komponentene. Sammenlagt har dette vært med på å øke studiens validitet.

Å *generalisere* handler avslutningsvis om at en påstand som gjelder på ett sted eller tid – også vil gjelde et annet sted til en annen tid. Spørsmålet *om* og *hvordan* det er mulig å generalisere i kvalitativ forskning har imidlertid blitt mye debattert (Nadim, 2015). Bakgrunnen for dette er at kvalitative studier ikke er *representative*, og kan som regel ikke sette to streker under svarene. Denne studien består kun av tolv informanter, og har *ikke* som formål å generalisere funn basert på datamaterialet. Gentikow argumenterer imidlertid for å bruke *analytisk kompleksitet* som ideal fremfor generaliserbarhet. Dette viser til både kvalitative metoders fleksibilitet og forskerens selvvurderinger. Med andre ord innebærer det at konklusjoner heller gjenspeiler fenomenets kompleksitet og «understreke uferdigheten i analysen, fremfor å kamuflere den» (2019, s. 63). Hun hevder at en slik «uferdighet» ikke er overfladisk, men tvert imot et produkt av møysommelige forsøk på å utfolde fenomenets betydninger.

Vi skal nå i de resterende kapitlene utbrodere hva de to generasjonene mener, handler og føler i møte med personvern i sosiale nettverkstjenester, og således utforske deres holdninger.

KAPITTEL 5 - Den Kognitive Komponenten

– KUNNSKAP, FORSTÅELSE OG OPPFATNINGER –

Da er det straks tid for å dykke ned i materien, og besvare det empiriske forskningsspørsmålet: *hvilke holdninger har ulike generasjoner til personvern i sosiale nettverkstjenester?* For å gi en veiledende struktur over analyse og resultater, skal vi i de tre neste kapitlene (5, 6 og 7) ta for oss analyse spørsmålene som er knyttet til de tre holdningskomponentene (kognitiv, atferd og affektiv). Herunder vil ulike temaer kobles til relevant teori og illustrert gjennom eksempler fra datamaterialet. I Kapittel 8, knyttes de tre holdningskomponentene sammen - og gir en oppsummerende diskusjon av analysen, løfter tematikken og trekker noen lange linjer, før det konkluderes. Imidlertid må det understrekes at i det virkelige liv er ikke det kognitive, affektive og atferdsmessige isolerte komponenter. De kan overlape hverandre. Noen ganger kan holdninger være inkonsekvente, og fremstå som rene selvmotsigelser. Det er likevel dette som er interessant å utforske – å se hvordan dette fremtrer hos Boomer-generasjonen (57-67 år) og Generasjon Z (15-26 år). En annen bemerkning er at jeg anvender noen selvlagde begreper, for å diskutere funn i datamaterialet. Disse blir presentert underveis der de hører hjemme. De ulike temaene vil hovedsakelig bli strukturert i form av at Boomerne diskuteres først, og deretter presenteres funn knyttet mot Generasjon Z (Gen Z).

Nå skal vi ta for oss den *kognitive* komponenten, som utforsker informantenes kunnskap, forståelse og oppfatninger – og opptrer ofte i motsetning til det følelsesmessige (affektive) (Kjøll og Tranøy, 2023). Her er det sentrale analyse spørsmålet (AS1): *Hvordan forstår Boomers personvern i sosiale nettverkstjenester i forhold til Gen Z?* Dette analyseres gjennom tre deltemaer. Først skal vi se på informantenes forståelse av personvern, for så å ta for oss hvilke oppfatninger de har om Meta sin datainnsamling. Deretter går vi inn på hvordan informantene vurderer viktigheten av et privatliv og personvern på Meta, og hvordan dette har endret seg over tid. Funnene tolkes og knyttes til relevante teorier underveis, hvor informantenes *kritiske medieforståelse* vil stå sentralt.

5.1 Overordnet kunnskap om personvern

I dette delkapittelet skal vi se på hvilken kunnskap informantene har om personvern på et overordnet nivå. Dette innebærer hvordan de selv definerer begrepet og hvilke assosiasjoner de

har i forhold til personvern. Her kommenteres også deres kjennskap til Personvernforordningen (GDPR).

5.1.1 Kunnskapsnivået preges av informantenes yrkesbakgrunn

Personvern er et begrep som har blitt tillagt mange betydninger. Men er det et krav? En rettighet? En verdi? En preferanse? Personvern kan også skape assosiasjoner til både anonymitet, hemmelighetshold og ensomhet (Nissenbaum, 2010, s. 2). Selve forskningsfeltet er splittet, når begrepet skal defineres. Det er derfor ikke overraskende at informantene, på tvers av generasjonene, hadde vanskeligheter med å ordlegge seg rundt dette. Under intervjuet fikk informantene enkelte spørsmål som hadde som intensjon å avdekke deres kunnskap og forståelse av personvern. Blant **Boomerne** viste det seg ett naturlig skille mellom de som har, og de som ikke har hatt, et yrke der beskyttelse av personopplysninger har vært sentralt. Dette kom tydelig frem i måten de omtalte fenomenet. Ingrid (58) har eksempelvis jobbet både som tannlege og lærer. I spørsmålet om hva hun forbinder med personvern, knytter hun det til jobbsammenheng, og mener at personvern går på *taushetsplikt*:

«Det [personvern] går på å begrense spredning av personlige opplysninger. [...] Som helsearbeider, så har man en utvidet plikt til å ivareta folks personvern, både mitt eget og andres. At alle eier sine egne opplysninger, er personvern.»

– Ingrid, 58 år (Boomer)

Her knytter Ingrid personvern opp mot at individer *eier* sine egne personopplysninger. Selv om dette er et nobelt ideal, som kan knyttes til Westin (1967) sin personvernsforståelse om at vi skal ha kontroll over informasjonen vår – er det i dagens digitale samfunn umulig for folk flest å ta eierskap på sine personlige opplysninger som er tilgjengelig 'der ute' (Richards, 2022). Den eldste i utvalget er Rita (67), som gjennom hele sin yrkeskarriere har jobbet i eldreomsorgen. Hun er relativt kortfattet og beskriver personvern som «at jeg er beskyttet i forhold til personlige ting». Noe som i og for seg er oppsummerende. Den yngste Boomerer, Ove (57), startet på sin side opp et eget firma i ung alder, og har siden bygget opp bedriften. Han har ingen direkte kobling til behandling av andres personopplysninger (pasienter eller elever), sett bort i fra sine egne ansatte. Han så derimot ut til å kjenne på utfordringer med å forklare personvernsbegrepet, og tok heller en spisset inngang mot bruk av SNS:

«Personvern? [...] Det har jeg aldri tenkt over før [ler]. Men at jeg skal ha et privatliv, det er jo klart. [...] jeg må jo tenke. Herre min hatt. At ikke noen kan gå inn og skrive på min Instagram og Facebook? Vist noen gjør det, så kan de jo skrive hva som helst og legge ut masse drit. Så det er jo viktig at ingen kan komme inn å gjøre det.»

– Ove, 57 år (Boomer)

Ove kobler altså personvernet til noe som beskytter han mot at andre skal få tilgang til hans *private digitalsfære*, eller profil. Den yngre generasjonen, **Generasjon Z**, er i større grad ordfattige når de blir bedt om å forklare hva de tror personvern er. Utvalgets yngstemann, Christian på 15 år, går i 10. klasse og erkjenner at han ikke har hørt så mye om personvern før. Han forbinder det med «at de skal vite litt om deg...». 'De' er rettet mot teknologiselskapene. Fiskeren, Adam (23), sier at han ikke har noen tanker om det, og peker på at «det er et vanskelig ord». Det har han forså vidt også rett i, med tanke på at forskningsfeltet har forsøkt å definere begrepet de siste 100 årene. Samtidig er det viktig å spørre brukere rett ut hva de tror personvern er, eller hva de forbinder med det – slik at vi kan dekke et eventuelt kunnskapshull. Et unntak blant Gen Z, er imidlertid Tony (26), som jobber innen teknisk support. Han får daglige telefoner fra kunder som må oppgi personopplysninger for å verifisere kundeforholdet. Hans definisjon skiller seg ut i form av å være mer konkret knyttet mot en beskyttelse av privatlivet:

«Kanskje rett til privatliv [...] Jeg forbinder det [personvern] med enkelte ting som burde holdes privat i en person sitt liv. Som ikke burde bli delt i offentligheten av personlige årsaker, og for så vidt for å skape en trygghet.»

– Tony, 26 år (Gen Z)

I sitatet over knytter han personvernet til trygghet, og implisitt sikkerhet. Tony har også et yrke som krever at han må ta hensyn til personlige opplysninger. Med dette tatt i betraktning fremstår *yrkesbakgrunn* som er en sentral faktor, som ser ut til å påvirke den grunnleggende forståelsen av hva personvern er blant disse informantene. En rød tråd gjennom utvalget, på tvers av generasjonene, var likevel at de kjente på utfordringer med å forklare begrepet. Flere stod stille på spørsmålet, og heller uttalte hva de assosierte med personvern. Noe som er gikk igjen, var at de assosierte personvern med *identitetsdokumenter*, slik som pass og betalingskort. I tillegg var det flere som nevnte personnummer, og at dette var viktig å holde for seg selv.

5.1.2 Lav kjennskap til personvernsforordningen (GDPR)

For å få ett innblikk i informantenes kunnskap om personvern, var det naturlig å spørre dem om de kjente til personvernlover eller hvilke rettigheter de har i møte med brudd på personvernet. Personvernsforordningen (GDPR) ble innført i 2018 for å styrke og harmonisere personvernet for borgere i EU og EØS-landene (Datatilsynet, 2020). Personvernsundersøkelsen fra 2020 (n=1501) viste at to av tre nordmenn kjente til GDPR på dette tidspunktet.

Selv om utvalget i denne studien er liten av størrelse, er det likevel interessant å se på deres forhold til GDPR. Uten en grunnleggende kjennskap til personvernsrettigheter, så kan de heller

ikke utøve rettighetene sine i den utstrekningen som regelverket skal legge til rette for (Datatilsynet, 2020, s. 4). Under intervjuene kom det frem at hele åtte av tolv informanter verken hadde hørt om, eller kjente til, Personvernsforordningen eller andre regelverk. De resterende informantene hadde hørt om GDPR i forbindelse med jobb eller utdanning. Dette reflekterer også Personvernsundersøkelsen (2020), der tendensen var at kjennskap til personvernsrettigheter har nær sammenheng med sosioøkonomisk status. Det er i seg selv bekymringsfullt at det er større sannsynlighet for å vite om sine egne rettigheter, dersom en har en god jobb med høy inntekt.

5.2 Kunnskap om Meta sin behandling av personopplysninger

Dette delkapittelet tar for seg hvilken kunnskap informantene har om personvernet på Meta – herunder Facebook og Instagram. Dette baseres på informantenes antagelser om *hvilke* opplysninger som blir samlet inn om dem. Dette knyttes implisitt til hvilken forståelse informantene har om Meta sin *forretningsmodell* – eller hvordan selskapet tjener penger (på personopplysninger).

5.2.1 Meta sin datainnsamling: Boernerne viser til en lavere kritisk medieforståelse

Alle informantene gir uttrykk for at de er klar over at Meta samler inn opplysninger om dem. Herunder svarer flere av dem «sikkert alt», når de blir spurt om hvilke opplysninger de tror Meta samler inn. Imidlertid skiller kunnskapsnivået seg, når det kommer til *hvilke typer* opplysninger Meta samler inn – der oppfatningen av «alt» varierer mellom Boomers og Gen Z. Blant **Boomer**-generasjonen har flere en oppfatning om at det hovedsakelig er det *de selv legger ut* på sin profil, som blir samlet inn. Rita (67) lister eksempelvis opp de opplysningene som hun tror at Facebook har om henne:

«Vel, de [Facebook] vet at jeg er kvinne, at jeg har jobbet i helsevesenet og hvilken skolegang jeg har gått på ligger der også. Så kan man jo å se hvilke venner jeg har. Litt søsken og navn på dem ligger jo der. Familiemedlemmer kan du si [...] Det som jeg har lagt ut, det tenker jeg ikke kan ha noen negative konsekvenser.»

– Rita, 67 år (Boomer)

Selv om denne informasjonen er personlig, så er dette informasjon som brukeren velvillig har lagt inn på profilen på eget ansvar. Et annet eksempel som illustrerer dette, er et sitat fra Ove (57). Han forteller at han er aktiv i flere sosiale medier, og deler innhold jevnlig. På spørsmål om hva plattformene samler inn av opplysninger, svarer han følgende:

«Det jeg legger ut er jo bare familiebilder, bilder av meg selv og ting som jeg gjør... sånn som når jeg legger ut bilder av bilen eller hytta... Og hvilke opplysninger de [Meta] får ut av det? Det kan jeg ikke fatte og begripe.»
– Ove, 57 år (Boomer)

Det kan derfor se ut til at flere i den eldre generasjonen, undervurderer hvor omfattende Meta sin datainnsamling faktisk er. Eksempelene som Rita og Ove kommer med i sitatene over, er en del av den *synlige informasjonsstrømmen* - det som vises på brukerprofilene (Rasmussen, 2016). Samtidig kan den *usynlige informasjonsstrømmen*, skildre mange detaljer om brukeren. All aktivitet på Meta-plattformene *datafiseres* og sammenstilles for å lage en predikasjon, om hvem brukeren er (Mejias og Couldry, 2019). Gjennom såkalte skyggeprofiler (St. John, 2018) kan det også innhentes opplysninger fra personer som ikke har en Facebook-profil. Sitatene deres illustrerer derfor poenget godt. Det skal likevel kommenteres at informantene kan ha misoppfattet spørsmålet, eller være preget av forskningssituasjonen. Samtidig er det en tendens i Boomer-utvalget at de peker på den *synlige* informasjonsstrømmen – noe som i sin tur og kan tyde på en lavere *kritisk medieforståelse* blant denne eldre generasjonen.

Informantene tilhørende **Generasjon Z**, har derimot en antagelse om at omfanget av datainnsamling er mye større, enn det som ble formidlet blant Boomerne. Adam (22) sier eksempelvis at: «De [Meta] har kontroll på alt vi gjør og de vet hva vi søker på». Flere av disse informantene peker også på at Meta samler inn hvor de befinner seg til enhver tid, gjennom tilgang til mobilens lokasjon (stedstjenester). Tony (26) antar at *alt* han gjør på Instagram blir innsamlet:

«Absolutt alt [blir samlet inn]. Ja, jeg tror alt fra... tastetrykk til hvor lenge du ser på en video – til hvor ofte du legger ut innlegg til hva du sender til venner. Alt mulig. Selvfølgelig, kommer dette i tillegg til opplysninger som blir gitt av meg selv.»
– Tony, 26 år (Gen Z)

I sitatet løfter han frem eksempler som går på den *usynlige* informasjonsstrømmen – og hvordan all aktivitet på plattformene registreres og analyseres. Flere av de unge informantene uttrykker en høyere selvsikkerhet rundt dette temaet, enn det som kom frem under intervjuene med Boomerne. Samtidig fremstår noen av de unge som svært usikre på *hva som skjer* med informasjonen deres *etter* at Meta har samlet det inn. Emilie (22) er frisør, og bruker for det meste Instagram. Hun beskjedent at: «Jeg tror ikke det blir gjort så mye, jeg tror det bare blir samlet inn.. Vet ikke helt». Lærlingen, Nora (19) svarte også følgende: «Ingen anelse.. og det er akkurat det som er litt skummelt og». Gen Z sin *kritiske medieforståelse* knyttet til omfanget av Meta sin datainnsamling, virker å være noe høyere enn den eldre Boomer-generasjonen. Men

når det kommer til hva som skjer med den informasjonen, er det en bred usikkerhet på tvers av generasjonene.

5.3 Kognitiv vurdering av privatliv og personvern

Under teorikapittelet ble det omtalt at personvern kan ha ulike betydning i ulike kontekster (Moor, 1997). Det er ikke alltid slik at vi bryr oss om noe er offentlig eller privat. Personvern er derfor vanskelig å sette en verdi på, fordi det betyr så ulike ting for ulike mennesker (Acquisti, Taylor og Wagman, 2016, s. 443). Dette kan også endre seg over tid. For å kunne utdype informantenes kognitive holdningskomponent ønsket jeg å utforske hvordan de vurderer eget privatliv i en digital kontekst. Dette kan bidra til en viktig nyanse i deres holdning til personvern. Det skilles her mellom *privatliv* og *personvern* – der personvernet har som formål å beskytte individets privatliv fra krenkelser. Først skal vi se på hvordan denne vurderingen har endret seg over tid i lys av teori om *tidskollaps*. Deretter går vi innpå hvordan de kognitivt vurderer viktigheten av privatliv i dag, og til slutt belyse et viktig fellestrekk som trer frem i datamaterialet.

5.3.1 Blitt mer bevisst på personvern over tid

Siden sosiale nettverkstjenester (SNS) skjøt fart i Norge med Facebook, rundt år 2007, har plattformene fått flere funksjoner og stadig flere konkurrenter som slåss om brukernes oppmerksomhet. Sett bort fra de to yngste – Christian (15) og Nora (19) – startet alle informantene å bruke SNS mellom 2007-2012. Brorparten av utvalget har dermed vært vitne til plattformenes utvikling i over ti år. Det som betraktes «privat» vil også variere med tid, livssituasjon og sted – eller kontekst. På tvers av generasjonene peker informantene på at det har vært et *skifte* - der de skiller mellom «de tidlige sosiale medier» og det som eksisterer nå. At Facebook slik de kjente det i 2010 var en æra for seg selv, med et helt annet bruksmønster som ikke gav rom for personvern.

Bakgrunnen for å trekke frem denne endringen, er at datamaterialet viser at informantene har blitt mer bevisste over personvern over tid. Noe som illustrerer dette, er at flere av **Boomerne** nevner at terskelen for å legge til folk i nettverket sitt var mye mindre i starten. Målet var å ha så mange venner som mulig. Kvantitet fremfor kvalitet. Rita (67) nevner at «man la til alle før», men nå godtar hun ikke hvem som helst. Dette impliserer at terskelen for å godkjenne en Venn er høyere nå, og at hun er mer skeptisk til hvem hun tillater inn i sin digitale privatsfære. Jan (58) omtaler denne tiden som «Facebook sin barndom» og sier at «det var jo litt ville vesten periode egentlig, sånn 2007-2010». Det å legge ut noe på Facebook i 2007 med 33 stykk på

Vennelisten – kan ikke sammenlignes med å publisere noe i 2023 med 870 Facebook-venner som både omfatter familie, naboer, kolleger, ekskjæreste – og en hel del bekjente. Flere opplever som resultat at Facebook har blitt en «resteplass», med alle slags relasjoner. Slik har dermed *konteksten* for informasjonsdelingen på SNS endret seg over tid.

Selve brukerne har frem for alt blitt ti år eldre. Alle i **Generasjon Z**, startet med SNS tidlig i tenårene. I prinsippet har dagens unge hatt en overgang fra barn til ungdom, til ung voksen – og er slikt sett den første generasjonen som har opplevd disse overgangene gjennom SNS. En grunnleggende faktor i denne sammenheng er at individer også endrer *identitet* over tid (Giddens, 1991 i Aalen og Hoem Iversen, 2021). Dette kan medføre en *tidskollaps* – som refererer til hvordan konteksten i SNS kan blande tidsgrensene mellom fortid og nåtid (Brandtzaeg og Chaparro-Domínguez, 2020, s. 166). Flere av de unge informantene forteller om pinlige innlegg og poster som ble publisert i starten, samt en massiv delingsaktivitet av både personlig og upassende innhold. Enkelte erkjenner også at de ikke tenkte over konsekvensene av delingen, og peker på alder og modenhet som en faktor. Dette kommenterer både Tony (26) og Adam (22):

«Ja, vi var unge og dumme. Alle mann. Det var sånne teite bilder som ble lagt ut. Men vi tenkte jo ikke over det når vi var sånn 10 år ikke sant.. det er jo nå i ettertid at man er begynt å tenke over at 'shit, tenk at folk la ut det der før.. kanskje det ikke passer seg helt nå.'»
– Adam, 22 år (Gen Z)

«I starten av sosiale medier, så var vi ganske unge mange av oss. Vi tenkte jo ikke noen konsekvenser på hva vi la ut. Folk publiserte og la ut alt av bilder, alt av innlegg uansett hva det måtte være. De fleste som var mottaker av det, var jo også på vår alder og de fortsatte med det samme. Så det var jo litt ond sirkel. Så det var ikke fryktelig mye privatliv på Facebook på den tiden.»
– Tony, 26 år (Gen Z)

Sitatene illustrerer en tidskollaps, og hvordan oppfattelsen av personvern endrer seg med tiden. Informantene beskriver en slags *kollektiv uvitenhet* på Facebook, hvor alle deltok uten å egentlig vurdere de fremtidige konsekvensene. Dette førte til en «ond sirkel» av en ufiltrert deling av bilder og innhold i kombinasjon, med liten respekt for personvern. Det fremstår derfor som at informantene har blitt mer bevisst over personvern over tid, og innser at tidligere publisert innhold, gjerne ikke passer seg i nåværende sammenhenger.

Bertine (25) kommer også med en interessant vinkling i dilemmaet om å ta avgjørende personvernsvurderinger i ung alder:

«Det som er blitt litt ødelagt i den oppveksten der man ville være 'influencer', man ville være blogger, man ville være en offentlig person. Når vi hoppet på den bølgen – noe som jeg og som absolutt alle andre jenter også gjorde – så mister du vernet om deg som privatperson veldig tidlig og veldig fort.»

– Bertine, 25 år (Gen Z)

Fra rundt 2010 og utover - når Bertine gikk gjennom tenårene - var det en oppblomstring av «vanlige» norske jenter som startet blogger om sine private liv, der enkelte fikk stor følgeskare. Påvirkere, slik som Sophie Elise Isachsen (28) er et eksempel fra denne generasjonen, som fikk stor suksess i ung alder. Bertine sine refleksjoner illustrerer hvordan drømmen om å bli en offentlig person og oppnå berømmelse, kan føre til at unge mennesker, bevisst velger å ofre en del av sitt personvern. SNS kan bidra til både synlighet og oppmerksomhet, noe som mange kan oppleve som en stor nytteverdi. Dette kan dog ha langsiktige konsekvenser for deres oppfatning av personvern og deres evne til å beskytte seg i den digitale sfæren. Det er derfor viktig å anerkjenne og adressere slike dilemmaer, for å skape en balanse mellom personvernet og ønsket om offentlighet - spesielt blant den yngre generasjonen.

5.3.2 Privatliv betyr mer for Boomerne enn for Generasjon Z

Nå skal vi se på hva privatliv betyr for informantene. En person som mener at privatlivet er viktig, vil i en tenkt situasjon også strekke seg mot å styrke sitt eget personvern. **Boomerne**, hevder at selve privatlivet har stor betydning, og illustreres blant annet gjennom følgende sitater:

«Jeg vil beskytte privatlivet mitt, og jeg synes det er skummelt hvordan det blir brukt. Hvordan du får opp reklame... ja vist du har søkt på noe. Man legger nok igjen mange spor...»

– Åse, 62 år (Boomer)

«For meg er det viktig. Jeg har ikke noe behov for å dele livet mitt med verden. Så det er jeg veldig opptatt av.»

– Ingrid, 58 år (Boomer)

«Privatlivet, det betyr jo veldig mye. Absolutt, men jeg legger jo ikke ut alt på Facebook. Det går jo ikke an... Men ganske mye.»

– Ove, 57 år (Boomer)

Privatliv viser seg å være en viktig *individuell verdi* for den eldre generasjonen, og er en verdi de ønsker å beskytte. I sitatet over, knytter Åse dette opp mot sine digitale fotavtrykk, der hun opplever det som utfordrende å ikke vite *når* hun legger igjen spor, og *hvem* som samler de inn.

Gen Z-informantene trekker dog i motsatt retning - men er noe delt innad i generasjonen. De yngste artikulere seg i form av at privatliv ikke er så viktig, og at de bryr seg lite om det. Emilie (23) forteller herunder at; «Det [privatliv] er egentlig ikke er så nøye. Jeg legger ikke ut så mye

privat på Instagram». Dette er en vurdering som går igjen hos flere. Denne tendensen, der den eldre generasjonen anser privatliv som viktig, mens den yngre generasjonen ikke ser verdien av det, kan illustrere et viktig *generasjonsskille*. Dette understøttes også av tidligere forskning, slik som Aguirre et al. (2018) sin studie som viste at unge voksne var mindre bekymret enn eldre voksne for at selskaper hadde informasjon om dem. Samtidig kommenterer de eldste i Gen Z-informantene, at privatliv har betydd mer etter hvert som de har blitt eldre. Noe som også reflekterer effekten av *tidskollaps*, som ble drøftet i forrige punkt. Det kan derfor antas at de *ambivalente* oppfatningene hos de yngste vil endre seg over tid. I de siste avsnittene ønsker jeg å trekke frem prosjektlederen, Bertine (25), sine betraktninger på privatliv. Hun er aktiv på flere plattformer og deler mye om seg selv på Instagram:

«Egentlig så bryr jeg meg veldig lite om det [privatliv]... tror jeg. Men når man begynner å tenke over det, så betyr det jo egentlig bare mer og mer for hvert år som går. Men jeg vurderer det aldri dit hen – når jeg vil legge ut en story – har folk behov for å se hva som skjer i mitt privatliv, JA eller NEI? Det vurderer jeg ikke. Det er sånn: 'Jeg synes bildet er fint. Jeg legger det ut'.»
– Bertine, 25 år (Gen Z)

Sitatet over kan knyttes til Bertine sine kognitive *kalkuleringer* om hva hun anser som nytte og risiko ved beskyttelse av eget privatliv på SNS. Brukere utfører vanligvis en såkalt, *personvernsvurdering* når de tar en beslutning om de skal avsløre personlig informasjon i SNS. Studien til Marwick og Hargittai (2019) viser imidlertid at de fleste brukere oppfatter at fordelene veier opp for mulig risiko. Dette gjelder spesielt SNS sin nytteverdi, i form av å opprettholde vennskap og bekjentskaper. Bertine kom herunder med et svært interessant resonnement som om unges forhold til privatliv på nett:

«Jeg tror helt ærlig at det er for lite informasjon, jeg. Om hva et godt privatliv er og hva det egentlig har som effekt. For jeg synes mange av disse spørsmålene er vanskelig å svare på, fordi jeg ikke har tenkt så fryktelig mye gjennom det – mer enn at jeg har akseptert at det er sånn. Og jeg vet at det er sånn. Det er ikke noe jeg bare... det er ikke noe jeg er naiv og blind for, og bare trykker meg gjennom. Jeg vet hva det er, og jeg vet hvilke innvirkninger det har på min aktivitet. Men for å liksom kunne komme med gode svar på hva det betyr og hvor viktig det er, så tror jeg bare generelt at det er for lite informasjon om hva et privatliv egentlig er – nå som sosiale medier har tatt så mye plass som det har. Man har på en måte verken ingen oppdragelse, eller utdanning eller noe som forteller om hva det faktisk betyr da.»
– Bertine, 25 år (Gen Z)

I dette oppsummerende sitatet fremhever Bertine et sentralt aspekt med Gen Z sin personvernforståelse - nemlig at hun synes at det er *for lite kommunikasjon* om hva et privatliv faktisk innebærer. Herunder gir hun uttrykk for en frustrasjon, der hun etterlyser mer tilgjengelig informasjon om hva et «godt privatliv» er og hvilke effekter det kan ha. Samtidig

går det ikke en dag uten at det popper opp vinduer på skjermen, som ber oss om å *lese mer om personvernet* til nettsiden vi prøver å komme inn på. Så informasjon om personvern er i teorien tilgjengelig, men dersom brukeren ikke har innsikt i den verdien et (digitalt) privatliv kan gi, så vil det heller ikke være noen vilje til å prioritere å bruke tid på å opprettholde et godt personvern.

5.3.3 Mange hevder at de ikke har noe å skjule

Om man bryr seg om personvern eller ei, vil være avhengig av om man mener at personvern har en verdi, eller at man ikke har bruk for det (Datatilsynet, 2014). Et utbredt fellestrekk på tvers av generasjonene, er at det observeres et behov for en *selvrettferdiggjøring*. Dette var svært påfallende i datamaterialet, og fremtrer forbindelse med en oppfatning om at de «ikke har noe skjule». Nesten alle informantene i utvalget nevner akkurat dette i en eller annen form under sine intervjuer:

«...det jeg har lagt ut om selv, det har jeg jo lagt ut.. jeg er verken tyv eller kjeltring, så jeg har ikke noe å skjule. Vi gjør så godt som vi kan, betaler skatt og alt er bare såre vel.»

– Ove, 57 år (Boomer)

«Jeg tenker at jeg ikke har så mye å skjule.. jeg har ikke noen hemmeligheter eller driver ikke med noe snusk [...] Når du skriver noe på Facebook, så er det jo der.»

– Rita, 67 år (Boomer)

«Vist jeg søker på noe spesielt, så får de jo bare finne ut av det da. Det gjør meg ingenting. Jeg har ingen kort å skjule...»

– Adam, 22 år (Gen Z)

Gjennom å tolke sitatene over, ser de ut til at informantene har en oppfatning om at personvern er noe som beskytter de med *onde* hensikter – tyver, skattesnytere og andre uærlige kjeltringer. Siden informantene selv, ikke gjør noe 'galt' eller bevisst bryter loven - så kan de resonnerer de seg frem til at de ikke har et sterkt behov for å beskytte privatlivet sitt. Dette kan knyttes til Marwick og Hargittai (2019) sin studie som fant lignende tendenser, der de trekker paralleller til uttrykket «nothing to hide, nothing to lose». Her betraktet ikke deltagerne å dele persondata som en nytte- og risikovurdering, men heller som et uttrykk for at de ikke hadde noe å skjule. Herunder valgte de nødvendigvis ikke å gi fra seg informasjon - men unngikk i stedet den *ekstra innsatsen* som krevdes for å gjøre den privat.

Neil Richards (2022) forteller likevel at dette argumentet har en lang fartstid, og at det attribueres til Joseph Goebbels - Nazi-ministeren for offentlig opplysning og propaganda. Dette har også vært et argument for å rettferdiggjøre en rekke statlige overvåkningsprogrammer siden den tid (2022, s. 72). «Ingenting å skjule» er dermed en type holdning eller oppfatning, som

kom tydelig frem hos nesten alle informanter. Dette fellestrekket vil bli hentet opp igjen, som en del av den oppsummerende diskusjonen, som vi ser på i Kapittel 8.

5.4 Oppsummering av den kognitive holdningskomponenten

Gjennom dette kapitlet har vi sett på det kognitive aspektet ved informantenes personvernsholdninger. Dette innebar en kartlegging av informantenes forståelse av personvern, oppfatninger om Meta sin behandling av personopplysninger og vurderinger knyttet til betydningen av privatliv og personvern. Funnene avslører en interessant variasjon i kunnskap og oppfatninger mellom generasjonene.

Den *overordnede kunnskapen til personvern* viser seg dermed å være generelt lav, på tvers av generasjonene i dette utvalget. Samtidig ser det ut til at kunnskapsnivået blir positivt forsterket av informanter som har et yrke, der behandling av personopplysninger er relevant. Det var også en generelt lav kjennskap til Personvernsforordningen (GPDR).

Angående forståelsen av *Meta sin behandling av personopplysninger* viser det seg at flere av Boomerne ser ut til å undervurdere omfanget datainnsamlingen, mens Gen Z fremstiller innsamlingen som mer kompleks og omfattende. Gen Z sin kritiske medieforståelse, virker å være høyere på dette området. Ellers var det en generell oppfatning blant utvalget at Meta bruker opplysningene til å vise dem reklame og relevant innhold basert på aktivitet, men flere erkjenner at de ikke kan vite med sikkerhet hva det egentlig brukes til.

Når det kommer til informantenes *kognitive vurdering av privatliv og personvern*, fremstår det som at informantene har blitt mer bevisst over eget og andres personvern over tid. Privatliv ser videre ut til å bety mer for Boomerne, enn for Gen Z. Herunder etterlyses det mer informasjon om hvilken funksjon et godt privatliv kan ha i dagens digitale mediesamfunn. Et annet viktig fellestrekk er at nesten alle hevder at de ikke har noe å skjule, noe som kan tyde på at oppfatningen er en utbredt måte å tenke på personvern uavhengig av alder.

KAPITTEL 6 - Atferdskomponenten

– ATFERD, HANDLINGER OG INTENSJONER –

Nå skal vi ta tak i den neste holdningskomponenten, *atferd*. Atferd er det vi gjør – med andre ord våre handlinger (Kennair, 2022). Hensikten med dette kapittelet er å kunne gi innsikt i det andre analysespørsmålet (AS2): *Hvordan handler Boomers i møte eget personvern på Meta, i forhold til Gen Z?* Dette innebærer å analysere hvordan informantene bruker *handlingsmulighetene* og egen *kommunikative handlekraft (agency)* til å navigere personvernet på Facebook og Instagram. Innsamling av personopplysninger er som nevnt en del av hele brukerreisen hos Meta sine tjenester – hvor hvert steg preges av ulike personvernshandlinger. Etter å ha lest en rekke studier, opplever jeg imidlertid en mangel på ett bredere ordforråd for å snakke om atferd- og handlinger tilknyttet personvern på SNS.

I dette kapittelet kommer jeg derfor til å anvende tre selvlagde begreper for å illustrere funn tilknyttet informantenes handlinger i møte med personvern på SNS. Her skiller jeg mellom tre typer: *periodiske-, statiske- og dynamiske personvernshandlinger*. (1) Når vi laster ned applikasjonen Facebook på mobilen, må vi først velge å godkjenne en personvernserklæring og vilkår for informasjonskapsler². Dette omtales her som *periodiske personvernshandlinger*, og er handlinger som brukeren må utføre jevnlig. (2) Deretter setter vi opp en profil i vårt eget navn, og legger inn en rekke personopplysninger om oss selv. Herunder må brukeren utføre det jeg kaller for *statiske personvernshandlinger* – der de må bestemme seg for hvilken informasjon de ønsker å vise til hvem. Dette er handlinger de utfører ved behov, og som ellers står stille (statisk) dersom de ikke endrer dem. Facebook legger eksempelvis opp til at vi kan bruke personverninnstillinger for å beskytte personopplysningene våre mot andre brukere. Herunder er det mange alternativer som må evalueres. Skal vi ha en offentlig eller privat profil? Bør fødselsdato være synlig for Venner? Eller kanskje Venners Venner? (3) Når profilen er på plass, må brukeren ta kontinuerlige beslutninger om eget og andres personvern mens de *braker* plattformen. Slik som hva de legger ut av innhold og hvilke funksjoner de benytter seg av, for å skjerme seg selv på plattformen. I de kommende delkapitlene benytter jeg de tre selvlagde begrepene, for å belyse informantenes atferd i møte med personvern på Meta.

² Informasjonskapsler (cookies) er en liten datamengde som lagres som en fil på brukerens harddisk. Dette kan inneholde informasjon som brukeren har registrert på nettsiden, og som overføres til nettsiden ved neste besøk - slik at det ikke er nødvendig å registrere informasjonen hver gang (Rossen, 2021).

Delkapitlene tar for seg flere viktige temaer som har vært fremtredende i datamaterialet. Først ser vi på periodiske personvernshandlinger, og hvordan informantene trykker seg rundt i møte med informasjonskapsler. Påfølgende tar vi for oss de statiske personvernshandlingene, som går på hvordan de stiller inn sine personvernsinnstillinger. Dette sees i lys av deres *forestilte publikum* på Meta. Herunder er *tenke høyt-øvelsen* helt sentral for å belyse deres faktiske atferd. Deretter ser vi nærmere på dynamiske personvernshandlinger, i møte med deres *kommunikative handlekraft* (communicative agency) på plattformene. Dette blir skildret gjennom Erving Goffman sine teorier om *selvrepresentasjon* og *inntrykkskontroll*.

Periodiske personvernshandlinger	Statiske personvernshandlinger	Dynamiske personvernshandlinger
<ul style="list-style-type: none"> • Informasjonskapsler • Personvernserklæring • App-oppdatering 	<ul style="list-style-type: none"> • Profilinnstillinger • Stedstjenester • Mikrofon og kameratilgang 	<ul style="list-style-type: none"> • SNS repertoar • Bruk av funksjoner • Utforming av innhold

Tabell 6.1: Oversikt over ulike personvernshandlinger som utføres av brukeren. Tabellen er ikke uttømmende, og kan variere mellom ulike SNS.

6.1 Periodiske personvernshandlinger

Periodiske personvernshandlinger sikter til tilnærmet like handlinger som brukerne må ta med jevne mellomrom - slik som å godkjenne eller avvise informasjonskapsler og reviderte personvernserklæringer.

6.1.1 Boomerne trykker rett på godta – Gen Z forsøker å tilpasse personvernet

Når det kommer til informantenes periodiske personvernshandlinger, er det en klar tendens gjennom utvalget. Stort sett alle informantene hevder at de *aldri* har lest eller kikket på personvernserklæringen til Meta. Dette begrunner de i at den er for lang og omfattende, og at det å lese den vil ta for mye tid. Hovedtendensen blant **Boomer**-informantene er at de trykker rett på 'godta' – både på den grunnleggende personvernserklæringen og pop-up-vinduer om bruk av informasjonskapsler. Ove (57) sier eksempelvis at; «jeg trykker bare på at jeg har lest alt, selvfølgelig. Men ikke lest den fysisk, det er det jo ingen som gjør». Ingrid (58) sier at hun ikke nødvendigvis ønsker å godkjenne erklæringen, men føler at hun ikke har noe valg: «...så er det noe med at så lenge jeg ikke godtar den personvernserklæringen, så får jeg ikke komme inn [på Facebook] heller». Dette støttes også av tidligere statistikk, som viser til at det er kun et fåtall (19%) som leser vilkårene før de godkjenner dem (Pew Research Center, 2019).

Blant den yngre **Generasjon Z**, er det kun Nora (19) som hevder at hun har kikket på personvernserklæringen: «I begynnelsen så var jeg mer sånn, 'jeg må faktisk lese hva som er

her. Hva er det jeg faktisk var med på'. Men så datt det jo av. Nå er det; Godta, få det vekk». Det som er mer fremtredende hos denne generasjonen, er at flere hevder at de klikker seg inn og *tilpasser* alternativene og huker av enten for «Kun nødvendige» eller «Avvis alle» når det kommer til valg av informasjonskapsler. Dette var det nesten ingen av Boomerne som nevnte. Samtidig viser det seg at denne ekstra personvernshandlingen, ved å tilpasse alternativene, kan være grunnlag for frustrasjon. Noen av de unge informantene sier at de blir oppgitt over den tungvinte måten alternativene blir fremstilt. Tony (26) og Nora (19) sammenligner det med å trykke seg rundt i ring (loop), og at å tilpasse alternativene ikke egentlig utgjør en forskjell:

«Det er ufattelig mange ting du kan huke av for å gjøre det ekstra vanskelig. Så de legger jo opp til at du ikke skal gidde å ta deg bryet [...] Og det er så tungvint, og de tar deg tilbake igjen og det blir bare sånn sirkel at du slutt nesten bare gir opp. Og det synes jeg ikke er greit. For da føler man at man ikke har en frihet til å bestemme over om de samler det inn eller ikke.»

– Tony, 26 år (Gen Z)

«[...] i det siste så trykker jeg oftere på 'Tilpass', for å se hva det er. Det var en gang jeg trykket på Tilpass, men så kom egentlig akkurat det samme opp. Det var bare å trykke videre. Da er det jo ingen forskjell.. vist jeg kan tilpasse det, men så er det egentlig ikke noe der jeg kan tilpasse.»

– Nora, 19 år (Gen Z)

Slike periodiske personvernshandlinger kan oppleves som overflødige, dersom brukeren ikke føler at deres handlinger ikke har en reell effekt. Satt i perspektiv, er dette en oppfatning om at brukerne «males opp i ett hjørne», der de ikke har noe annet valg enn å godta vilkårene (Zuboff, 2019). Dette kan også være bevisste *tilsløringstaktikker* fra selskapenes side (obfuscation), for å gjøre vilkårene vanskelig å forstå, gjennom *distraheringer* fra mange alternativer og *komplisert språk* (Draper og Turow, 2019, s. 1830). Denne opplevelsen av manglende kontroll og påtvunget aksept av vilkårene, kan bidra til *digital resignasjon* (Draper og Turow, 2019, s. 1833). Når de ikke kan kontrollere datainnsamlingen, så oppleves det som enklere å bare gi opp. De resignerer slikt sett, gjennom å trykke rett på 'godta', isteden for å forsøke «ta opp kampen» gjennom å tilpasse valgmulighetene.

6.2 Statiske personvernshandlinger (tenke høyt-øvelse)

Det er først når brukeren har godkjent personvernserklæringen, at de kan sette opp en personlig profil. I dette litt lengre delkapittelet bruker jeg terminologien, *statiske personvernshandlinger*, for å illustrere hvordan brukere av SNS må gjøre en rekke beslutninger, som omhandler styrken av personvernet for sin egen profil. Med andre ord, er det her brukeren endrer *personvernsinnstillingene* for å kontrollere hvem som kan se eller samhandle med personinformasjonen. Dette er som regel fastsatte, eller statiske innstillinger, som brukeren kun

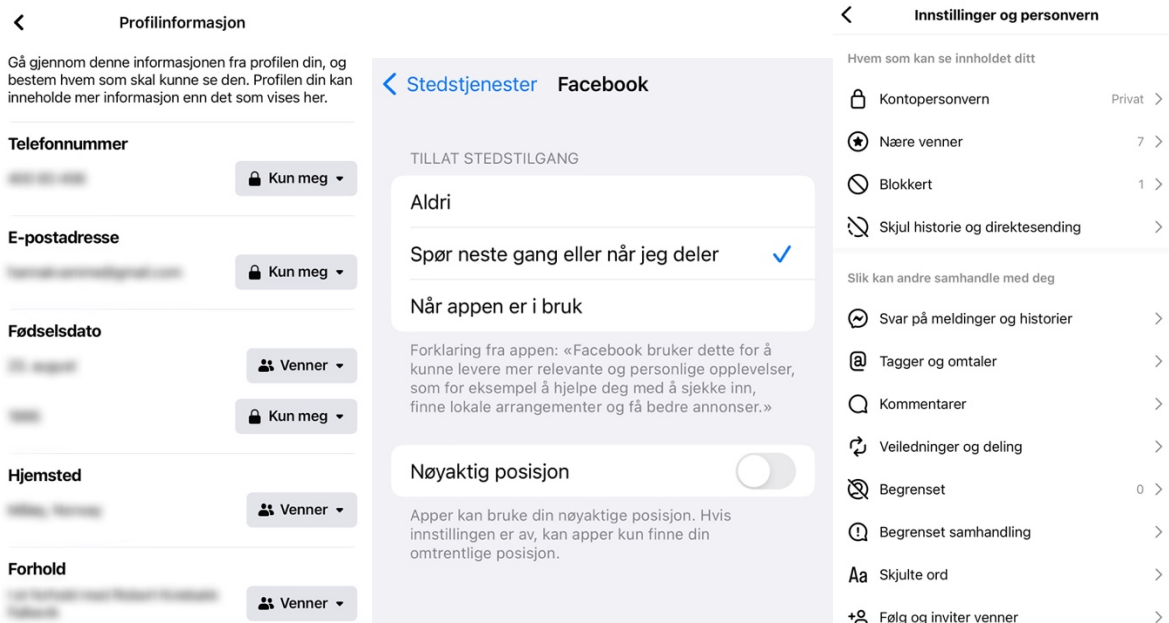
trenger å gå gjennom ved behov. *Tenke høyt-øvelsen* vil i denne forbindelse bidra til et dypere innblikk i informantenes faktiske handlinger i møte med personvernsinnstillinger på Meta.

Hvordan informantene innstiller profilene sine kan se ut til å handle om deres individuelle behov for synlighet, samt hvilken *kritisk medieforståelse* de har for mulighetene og konsekvensene ved de ulike alternativene. Utfordringen er at det er en såkalt *design bias* mot at standardinnstillingene er offentlig, og former selve brukeropplevelsen (Cho, 2018). Dette betyr at dersom brukeren ikke endrer personvernsinnstillingene gjennom eget initiativ, vil alle opplysninger være markert som «offentlig». Dersom brukeren ikke er klar over dette, kan de ende opp med å dele personlig informasjon til et vesentlig større publikum enn det de tror. Meta på sin side, tjener godt på denne illusjonen om det *forestilte publikum* (Marwick og boyd, 2011).

6.2.1 Boomerne er redde for å stille inn feil – Gen Z er skeptiske til stedstjenester

I dette delpunktet kobler jeg informantenes egne utsagn, sammen med observasjoner fra *tenke høyt-øvelsen* som ble avholdt etter forskningsintervjuet. Her fikk de beskjed om å finne frem til og kikke på personvernsinnstillingene på Facebook eller Instagram – og underveis dele sine tanker (se Skjermbilder). Informantene tilhørende **Boomer**-generasjonen knyttet sine refleksjoner rundt personvernsinnstillinger opp mot Facebook. Her har de fleste informantene en *offentlig* profil, der store deler av opplysningene ligger åpent tilgjengelig. Flere hevder at de har sett på innstillingene, men at dette er veldig lenge siden. Ove (57) antar at det er over ti år siden han så på dem sist, da han først ble medlem av Facebook. Dette ble også bekreftet under *tenke høyt-øvelsen* der han kommenterte følgende om personvernsinnstillingene: «Åh, okei... dette har jeg aldri sett før. Dette var helt nytt».

Jan (58) formidler på sin side under øvelsen at innstillingene står cirka slik han vil ha det - men påpeker at dersom han fjerner synligheten helt, «så faller noe av vitsen med sosiale medier bort». Blant Boomer-utvalget var det også flere som mente at de trengte hjelp fra andre til å stille inn profilen sin. Dagny (66) sier eksempelvis at hun kjenner på at hun trenger bistand fra barna sine for å se på innstillingene, da hun anser dem som mer teknisk anlagt enn seg selv. Åse (62) sier også at sønnen hennes hjalp henne «å ta bort fødselsdatoen» på profilen, da hun ikke kjente behovet for å få gratulasjoner av folk hun ikke hadde noe forhold til. Under øvelsen erkjenner også Åse at hun synes at personvernsinnstillinger kan være veldig «innviklet» og at grunnen til at hun ikke har stilt dem inn selv, er fordi hun er «redd for å gjøre noe feil». Dette går også igjen hos andre Boomere.



Skjermbilder: Illustrerer personverninnstillinger som informantene så på under tenke høyt-øvelsen. (t.v. og i midten) Innstillinger tilknyttet Facebook, (t.h.) Innstillinger tilknyttet Instagram.

Tenke-høyt-øvelsen viste seg å være svært nyttig for å få nyansere deres *kognitive prosesser* i møte med de statiske personvernshandlingene (Charters, 2003). Blant den eldre generasjonen var det en gjennomgående trend at flere slet med å klikke seg frem til personverninnstillingene. Flere uttrykket frustrasjon over at det var vanskelig å finne innstillingene på Facebook. Når de først kom inn på siden, hadde de flere opplysninger offentlig tilgjengelig, enn de antok under intervjuet. Ingrid (58) hevdet i intervjuet at hun vanligvis valgte «Avvis alle» informasjonskapsler; at hun hadde en helt lukket Facebook-profil; og at hun generelt aldri delte noe personlig på Facebook. Likevel fikk hun seg en liten oppvekker under tenke høyt-øvelsen:

Intervjuer: **Se om alt er som du ønsker det skal være [i forhold til innstillinger på Facebook].**

Ingrid: Profilinformasjon, telefonnummer, epost - kun meg. Fødselsdato - kun venner. Årstall er, kun meg. Nåværende bosted er offentlig. Ehm... 'hvem kan se vennelisten din' - Venner... Ja, der kan du se! 'Hvem kan se personene og sidene du følger' Det er offentlig?... Ja, nei dette var veldig morsomt faktisk [ironi].

Intervjuer: **Er det noe som overrasker deg [ved personverninnstillingene]?**

Ingrid: Ja, at 'alle venner' var synlig viste jeg ikke...

Dialogen illustrerer at det var enkelte *informasjonstyper* hun trodde var skjult, men som i realiteten var offentlig synlig. Det at Vennelisten hennes stod som offentlig, kan føre til at det kan være lett å plassere henne i forhold til andre – og i verste fall misbrukes av svindlere som kan utgi seg for å være en av vennene hennes.

Informantene blant **Generasjon Z**, knyttet sine resonneringer hovedsakelig til Instagram. Nesten alle Gen Z-informantene har *offentlige* kontoer - uten om Tony (26) og Adam (22), som har stilt inn sine som *privat* (slik at de må godkjenne alle som ønsker «å følge» dem). Uten om dette, så er det ikke mange blant de unge som har endret personverninnstillingene på Instagram. Det kan også skyldes at plattformen har andre typer innstillinger enn Facebook, noe som gir dem andre handlingsmuligheter (se Skjermbilder). De fleste hevder likevel at de er klar over at personverninnstillingene eksisterer, men at det er lett å glemme når de bruker SNS i hverdagen. Noen av dem tror også at de hadde fokusert mer på innstillingene vist de var mer aktive, i form av å legge ut mye offentlig innhold på profilen sin. På bakgrunn av det de formidler, ser det ut til at personverninnstillinger kommer litt i «bakgrunnen» av den hverdagslige bruken. Noe som gikk igjen blant Gen Z under selve intervjuene, var likevel at de viste høy skepsis til deling av sin *fysiske lokasjon* gjennom mobilen. Spesielt under tenke høyt-øvelsen var det flere som sjekket «Stedstjenester»:

[om sporing av posisjon] Da har jeg 'kun når appen er i bruk'. Det har jeg på alle appene mine. Sånn at de da ikke sporer meg forhåpentligvis når appen ikke er aktiv. [...] Men jeg er usikker på om man må lukke appen helt, eller om vist den ligger åpen i bakgrunnen at du ikke har lukket den helt da. Om den fremdeles regnes som en «app i bruk». For det står det ingenting om...

– Tony, 26 år (Gen Z)

Her uttrykker Tony sin skepsis til Meta sin sporing og illustrerer et behov for større klarhet rundt definisjonen av en «app i bruk». Han kjenner på en usikkerhet om Instagram sporer han, selv om han har endret personverninnstillingene. Bertine (25) sier i intervjuet at: «for meg så er den posisjonsgreia så stress at jeg gidder ikke å drive å trykke den av og på, så jeg lar den alltid være på». I sammenheng med dette forteller hun om en episode der hun fikk beskjed om å oppdatere Instagram. Når hun aksepterte og lastet ned den nye oppdateringen, oppdaget hun i senere tid at innstillingene hadde byttet om til å tillate bruk av stedstjenester.

Statiske personvernshandlinger, er dermed ikke alltid statiske. Men ved å utføre en *periodisk* personvernshandling, som å godkjenne en ny app-oppdatering (som ofte innebærer nye personvernsvilkår), kan innstillingene endre seg uten at brukeren er klar over det. Dette kan i enkelte tilfeller oppleves som en krenkelse av privatlivet – men dette blir gjerne ikke ett problem før brukeren *oppdager* at de deler mer om seg selv enn de trodde. Dette illustrerer potensielle utfordringer ved automatiske endringer av innstillinger i etterkant av oppdateringer - der brukerne ikke er nok informert eller har forstått konsekvensene av oppdateringen.

Frisøren, Emilie (23) hadde en generell *ubekymret tilnærming* til personvern og Meta sin datainnsamling under intervjuet (Westin, 1967). Dette kan henge sammen med at hun ikke signaliserte så stor forståelse om emnet (kognitiv komponent). Hun hevdet at hun visste hvordan innstillingene var stilt inn, og gikk god for det innholdet som lå ute. Under tenke høyt-øvelsen ble hun derimot sjokkert over at hun hadde tillat både Instagram og Facebook å spore hennes nøyaktige posisjon: «Da er det jo bare å skru av med en gang! [...] Nå føler jeg meg som Olga, 80 [år] skjønner du. Dette må jeg faktisk fikse med en gang.» Nora (19) fikk også en liten åpenbaring under øvelsen, da hun sjekket personvernsinnstillingene sine på Facebook:

Nora: Telefonnummer; kun for meg. Så står det når jeg er født og fødselsdato; det er jo vennene mine – eller Venners venner, faktisk... Så da er det jo veldig mange... [...] Det er noe jeg ikke har sett over faktisk.. Nåværende bosted - det er offentlig. Og hvem kan se Vennelisten min - Jo det kan alle se. Hvem kan se personer, sider og listene som jeg følger, er offentlig...

Intervjuer: **Er det noe du ønsker å endre på? Eller står det slik du ønsker?**

Nora: Akkurat sånne ting er jo helt greit... [Men] ting du følger på Facebook [...] kommer jeg nok til å endre. Vist jeg begynner å følge noe nå, så kommer det jo til å stå, 'Nora fulgte Pink på Facebook' [ler nervøst]».

I dialogen over, innser Nora hvor stort publikum hun egentlig har – og ligner mye på reaksjonen som Ingrid (58) hadde under hennes tenke høyt-øvelse. Det nederste sitatet illustrerer en implisitt forlegenhet overfor at hennes Venner skal få opp i sin nyhetsstrøm at hun har begynt å følge en Facebook-side. Dette kan si mye om hvem hun er, og hva hun interesserer seg for. Dette kan også knyttes til det Marwick og boyd (2011) beskriver som *imagined audience*. Dette *forestilte* publikummet kan være av helt annen størrelse fra de som faktisk kan se profilinformasjonen. Under første sitat i dialogen over, innser Nora eksempelvis at informasjon om hennes fødselsdato ikke bare er synlig for hennes *Venner* – men hennes *Venners Venner*. Dette er to vidt ulike publikummer. La oss si at Nora har 800 Venner tilknyttet sin Facebook-profil, og gjennomsnittet av hennes nettverk, har 500 Venner tilknyttet sine profiler. Dette tilsier et potensielt publikum på 400.000 personer som kan se hennes fødselsdato.

Når det kommer til de statiske personvernshandlingene fant de fleste Gen Z-informantene relativt fort frem til personvernsinnstillingene, i forhold til Boomerne, som opplevde dette som et hinder (Tabell 6.2). Forskjellen mellom de to generasjonene er dog at de unge fremstod i større grad som mer overrasket over hvordan innstillingene deres var. Spesielt med tanke på å dele sin nøyaktige posisjon.

Boomer	Generasjon Z
<ul style="list-style-type: none"> • Brukte mye tid på å finne frem til personvernsinnstillingene • Flere hadde aldri sett på innstillingene før • Fleste hadde offentlige profiler • Enkelte var redde for å stille dem inn feil • Flere hevdet at de trengte bistand fra andre for å stille dem inn 	<ul style="list-style-type: none"> • Brukte kort tid på å finne frem til personvernsinnstillingene • Flere hadde sett på dem tidligere • Fleste hadde offentlige profiler, med unntak av to som hadde privat • Flere ble overrasket over hvordan innstillingene faktisk var stilt inn, spesielt mtp stedstjenester

Tabell 6.2: Kortfattet oversikt over viktige observasjoner og hovedtrekk under tenke høyt-øvelsen.

6.3 Dynamiske personvernshandlinger

Når brukeren har godkjent personvernserklæringen og stilt inn profilen sin, kan de sette i gang med å bruke SNS. *Dynamiske personvernshandlinger* sikter til de kontinuerlige handlingene som en bruker foretar seg i forbindelse med deres aktivitet på SNS. Herunder valg om hvilke hvilke funksjoner de benytter, samt hvilket innhold og informasjon de velger å dele – for å opprettholde et ideelt nivå av personvern. Dette går på selvrepresentasjon og selvavsløring.

I delkapittelet over diskuterte vi informantenes forhold til personvernsinnstillinger. Men i mange tilfeller, så vil ikke dette være godt nok for brukeren. Å verne om eget privatliv, innebærer å avsløre ulike ting om seg selv til ulike mennesker (Moor, 1997). Det er slikt sett en kontinuerlig *forhandling* om hva brukeren ønsker å gi fra seg av informasjon, og til hvem (Palen og Dourish, 2003; Marwick og Boyd, 2014). Å kunne håndtere hvordan man avslører seg selv i SNS, er dermed sentralt for å oppnå et ideelt «opplevd» personvern, som brukeren er tilfreds med. Imidlertid vil de kunne tilskrive ulike nivåer av personvern, til ulike *typer informasjon* – avhengig av kontekst og deres preferanser (Nissenbaum, 2010; Masur og Scharkow, 2016).

Dette kan kobles til informantenes *kommunikative handlingskraft (communicative agency)* (Ytre-Arne og Das, 2020), som kan påvirke *hvordan* de benytter seg av ulike handlingsmuligheter for å navigere personvernet på SNS. Et aspekt ved å utforske ulike generasjoner, er at de har vokst opp med forskjellige mediehverdager. Mine antagelser var at informantenes kommunikative handlingskraft på SNS var farget av deres livserfaringer knyttet til medie- og teknologiutviklingen de selv hadde opplevd hittil i livet. Boomer-generasjonen har eksempelvis vært vitne til en eksepsjonell teknologisk utvikling; fra telefonkiosken, til hustelefonen til smarttelefonen. Dagens generasjon har derimot vokst opp med en *mange-til-mange-kommunikasjon* i sanntid, rett fra bukselommen (Aalen og Hoem Iversen, 2021).

6.3.1 Boomerne bruker grupper – Gen Z bruker flere kontoer

En generasjonsforskjell som går igjen i datamaterialet angående selvavsløring, er bruken av *grupper* og *ulike kontoer*. Dette er først og fremst en personvernsstrategi for å øke kontrollen over det *faktiske* publikummet, ved at de deler ulikt innhold med ulike brukere (Marwick og boyd, 2011). Herunder hevder flere av informantene blant **Boomer**-generasjonen at de sjelden publiserer offentlig innhold på sin egen Facebook-profil, men kan være svært aktive i ulike *Facebook-grupper*. Rita (67) forteller eksempelvis om at hun er medlem av en rekke *lukkede* grupper – slik som en for familien og en for utvidet slekt. Åse (62) er også medlem av flere slike grupper. I tillegg er hun også engasjert i hobby-grupper, som eksempelvis diskuterer hage og plantedyrking. Hun poengterer at det er mer behagelig å publisere innhold i slike grupper:

«Det at du snakker til alle bekjente samtidig, det er jo litt sånn tja... det jeg har likt best er egentlig de små gruppene med de du har noe felles med, annet enn at du har alle de på Vennelisten din. Det er litt annerledes med hva du legger ut.»

– Åse, 62 år (Boomer)

Her setter Åse ord på det å kunne kontrollere *hvem* som mottar innholdet (faktisk publikum) – fremfor at «alle» på Vennelisten er målgruppen. At disse gruppene utgjør en tryggere ramme for utfoldelse. I lys av Goffman (1959), kan dette sees på som en *backstage*, i forhold til den mer eksponerte profilen, som fungerer som en *frontstage*. Det er likevel ikke alle grupper på Facebook som er 'lukket'. Ingrid (58) nevner at hun var aktiv i offentlige grupper før - der hun ofte delte om samfunnsaker hun var opptatt av. Denne aktiviteten kom derimot opp i andres nyhetsstrøm, uten at hun tenkte over det. Jeg spurte henne derfor om hvorfor hun sluttet å engasjere seg i gruppene, og om det hadde noe med personvern å gjøre. Her delte hun en episode hvor hun *innså hvor mye* hun avslørte om seg selv, gjennom å bli irettesatt av datteren sin.

«Det var bare en manglende kobling. For jeg føler jeg har vært bevisst hele tiden, samtidig som jeg da la ut og re-postet innlegg som jeg synes var viktig. For eksempel, 'Nei til fyrverkeri på nyttårsaftnen'. Inntil datteren min sa, 'hvorfor poster du så mye, mamma?'. Så hun gjorde meg bevisst på at det var en mismatch der, mellom det jeg egentlig mente jeg ikke hadde lyst til å gjøre, og det jeg faktisk gjorde da. [...] Jeg la jo ikke ut personlige ting, men jeg la ut ting som engasjerte meg. Hvor hun sa at 'her forteller du mye om deg selv'.

– Ingrid, 58 år (Boomer)

Til tross for Ingrids bevissthet rundt personvern, delte hun innhold som reflekterte hennes interesser – noe som kunne avsløre betydelige personlige detaljer. Dette sitatet illustrerer *privatlivsparadokset* i praksis (Barnes, 2006). At det kan være en «manglende kobling» mellom det brukeren mener (kognitivt) og det de faktisk gjør (atferd). Det kan likevel være ubehagelig å oppleve denne *kognitive dissonansen*, der tanker og handlinger ikke stemmer overens

(Svartdal, 2023). Noe som i sin tur kan føre til atferdsendring. I Ingrid sitt tilfelle, førte det til at hun sluttet å engasjere seg i slike grupper. Dette understreker imidlertid kompleksiteten av *selvavsløring* på SNS, og at det krever en høy kommunikatív handlekraft til å navigere 'riktig'.

SNS gir oss nettopp muligheten til å avsløre oss selv på ulike måter – både bevisst og ubevisst. **Generasjon Z** benytter seg av en annen personvernstaktikk på Instagram - nemlig å opprette flere kontoer med ulike formål. Nora (19) nevner at hun har to offentlige kontoer på Instagram. Det underliggende er at hun er frisørlærling, og ønsker å vise frem sine evner til ett utvidet nettverk. Hun har derfor opprettet en konto for *personlig* innhold, og en knyttet til hår og styling. Slik kan hun vurdere innholdet til det som er passende til de ulike kontoene, som i prinsippet utgjør to ulike kontekster.

Adam (22) har på side to Instagram-profiler, der han bruker de ulikt og slik avslører ulike sider ved seg selv: «Ja, den lukkede profilen er det jo mest venner og bekjente. Litt mer drøyere bilder.. og festbilder, enn den åpne profilen, som mamma kan se for eksempel.» Her nevner han spesifikt moren sin, som han ønsker ikke skal se alt som skjer på fritiden. I et slikt tilfelle går det direkte på *selvrepresentasjon* - der Adam forsøker å *kontrollere inntrykket* av han selv, for sin mor (Goffman, 1959). Dersom alle relasjoner samles i samme digitale privatsfære, kan det nettopp føre til *kontekstkollaps* (Marwick og boyd, 2011). Konteksten hadde trolig «kollapset» dersom Adams mor hadde sett den private kontoen, med alle festbildene – og gjerne ført til forlegenhet hos Adam, som ikke ønsket at moren skulle få dette inntrykket av han.

Noe som går igjen i datamaterialet på tvers av generasjonene, er imidlertid at *ingen tenker bevisst* over at personvernet er en faktor når de bruker SNS. Ingrid (58) sier eksempelvis at: «Vel, jeg tenker ikke på det når jeg sitter på Facebook, at 'oj, nå må jeg passe på personvernet mitt'. Den er nok integrert i meg på en måte». Dette illustrerer også utfordringen om at personvernet er *usynlig*, inn til noe ubehagelig oppstår på SNS i form av kontekstkollaps.

6.3.2 Boomerne har vanskeligere for å blokkere andre brukere, enn Gen Z

En vanlig taktikk for å opprettholde et *ideelt* nivå av personvern, er å *blokkere* eller *slette* brukere man ikke ønsker å ha i eget nettverk (Marwick og Boyd, 2014). Flere **Boomere** sier at det er utfordrende å skulle blokkere andre. En ting er å blokkere en fremmed bruker fra Vennelisten - men det er en annen situasjon å velge å blokkere en langvarig venn, som man av

ulike grunner ønsker å skjermes seg selv for. Ingrid (58) forteller om at hun har en slik venn på Facebook som hun vurderer å blokkere:

«Det er særlig en som jeg synes er vanskelig [å blokkere]. Som egentlig er en veldig snill person, og som har gjort veldig mye bra for oss. Men som etter hvert begynner å få en del meninger som jeg synes er supervanskelig å svelge unna. Skal jeg fortsatt være venn med deg? Jeg kommenterer ikke noe av det vedkommende legger ut. Men som sagt så er vedkommende veldig hyggelig. Men jeg kjenner at hadde den ikke vært det, så hadde jeg blokkert med en gang.»

– Ingrid 58 år, Boomer

Dette kan være et utfordrende dilemma å havne i. Skal man blokkere en venn, fordi at de mener noe man ikke står for selv? Eller er det en *passiv* personvernsstrategi i seg selv å beholde personen i nettverket, og heller prøve å minimere all interaksjon? Sitatet illustrerer uansett den sosiale kompleksiteten ved å administrere personvern og Vennelister på SNS (Marwick og Boyd, 2014). Her opplever Ingrid en indre konflikt mellom å verdsette vennskapet, og kjenne på ubehag av hennes ytringer på Facebook. Andre Boomer-informanter hevder de har slettet flere personer som de ikke har kontakt med lenger. Rita (67) kommenterer i denne sammenheng at: «Hvorfor skal vi være venner, når vi ikke er venner i det virkelige liv?». Åse (62) reagerer også på at noen relasjoner på Facebook fremstår som «falske». Hun nevner en person som har vært nær familien, men som hun har mistet fysisk kontakt med. Denne personen engasjerte seg sterkt i kommentarfeltene på Facebook, og kommenterte alt som Åse la ut:

«Da tenker jeg nesten at også det blir sånn show-off, at vi må vise resten av verden at vi er kjempevenner, så er vi egentlig ikke det. Og det har gjort at, enten har jeg tenkt at jeg må blokkere henne eller så... Det var vel kanskje en grunn til at jeg ikke la ut noe mer faktisk. For det ble litt problematisk for meg.»

– Åse, 62 år (Boomer)

Dette sitatet henger sammen med *inntrykkskontroll* av selvrepresentasjon på Facebook (Goffman, 1959). Herunder at mange brukere kan kjenne på et behov for å vise til omverdenen (frontstage) at de har mange, gode venner. I realiteten har de ikke kontakt utenom plattformen (backstage). Åse synes dermed at dette oppleves som «kunstige vennskap», og sier i forbindelse med dette: «Hvorfor kan vi ikke snakke vanlig på telefon eller gå en tur å prate? [...] for meg så er det veldig rart, at det er der [Facebook] vi treffes». Flere har dermed en mer tradisjonell tilnærming til kommunikasjon der de kobler «ekte relasjoner» til mennesker de bruker tid på å snakke *direkte* med – ikke asynkront gjennom kommentarfeltet på Facebook.

Informantene blant **Gen Z**, virker i større grad mer impulsiv om hvem de sletter fra eget nettverk. Nora (19) har som nevnt i forrige delpunkt, to offentlige kontoer – en personlig og en

for frisørjobben. Hun er i denne forbindelse klar over at alle *kan se* den personlige kontoen - men til tross for dette, vil hun ikke at alle skal *kunne følge* henne. Hun bruker derfor en taktikk om å fortløpende slette ukjente og uønskede brukere som begynner å følge kontoen.

Generelt fremstår Gen Z sine beslutningsprosess som kortere, og tar i mindre grad hensyn til om det er en person de har hatt ett lenger forhold til eller ikke. Dersom ikke personen oppleves relevant for deres nettverk, så «kvitter» de den med seg – gjennom å slette eller blokkere – for å opprettholde deres ideelle personvern i sin egen digitale sfære. Det kan derfor antydes at det koster mer for Boomer-informantene å rense opp i nettverket, enn hos de Gen Z.

6.3.3 Boomerne «skriver dagbok» og Gen Z «skaper fotoalbum»

De to generasjonene viser også ulike tendenser for *hva* og *i hvilket omfang* de legger ut innhold om eget privatliv. Når det kommer til hvordan de representerer seg selv på Facebook og Instagram, er det noen interessante oppfatninger. I dataene kommer det frem en forestilling om at generasjonene bruker SNS på ulike måter, der det gis en analogi til *dagbøker* og *fotoalbum*. Denne generasjonsforskjellen bunner ned i brukernes ulike tilnærminger til selv-avsløring.

Oppfatningen handler om at **Boomers** har en tendens til å legge ut diverse innhold, hyppigere og i mindre grad relevant. Dette knyttes opp mot at mange eldre bruker Facebook nærmest som en «dagbok», for å legge ut oppdateringer om stort og smått:

«Helt ærlig så synes jeg at disse 70-åringene legger ut veldig mye. Jeg synes de nesten bruker det som en dagbok. De legger ut hver dag om hva de har gjort. Da tenker jeg det er en måte for å få bekreftelse, og å bli sett på. Og at de kan se tilbake på og lese hele historien sin da. At de bruker det som en dagbok omtrent. Mye er liksom fint å dele... men for min del så blir det veldig travelt.»
– Åse, 62 år (Boomer)

Her knytter Åse denne oppfatningen til hennes egen generasjon, og hvordan hun opplever at veldig mange legger ut *for mye* innhold, og at dette innholdet ofte er *for privat* – i forhold til hennes preferanser. Dette kan knyttes til hvordan *blogger* tidligere ble brukt for å fortelle om daglige hendelser – og at eldre anvender handlingsmulighetene i SNS på denne måten. **Gen Z** viser en tendens til å bruke Instagram, mer som et «fotoalbum». Der legger de ut innhold relativt sjelden, ofte i en planlagt kontekst, der de kan se tilbake på minner:

«Jeg liker å bare ha mitt eget bildegalleri. For jeg bruker mye tid på å se på min egen Instagram og gå gjennom stories og highlights. For det blir ditt eget lille digitale album, der jeg har valgt ut noen bilder som jeg synes er nice, og som andre ser på og er en del av.»
– Bertine, 26 år (Gen Z)

Flere av jentene i Gen Z-utvalget anser Instagram som et digitalt fotoalbum, der de nøye skaper og deler innhold som krever mer planlegging og redigering, med et formål for å bevare gode minner – på en estetisk måte. De fleste fotoalbum er nettopp fylt opp med utvalgte bilder av mennesker som smiler - men unnlater negative hendelser (Aalen og Hoem Iversen, 2021, s. 65). En reaksjon på dette er at Emilie (23) og Nora (19) anser mye av innhold på Instagram som «falskt» og «lite genuint». Samtidig kan denne tilnærmingen til selv-avsløring, reflektere en høyere kommunikativ handlekraft hos Gen Z – der de setter strengere krav til sin egen selvrepresentasjon, enn Boomerne.

6.3.4 Selvsensur gjennom ulike taktikker

I intervjuene ble informantene spurt om de noen gang hadde avstått fra å dele informasjon, selv om de egentlig hadde lyst. Hensikten ved dette spørsmålet var å utforske spenningen mellom deres ønske om å uttrykke eller avsløre seg, og deres behov for å verne om informasjonen. Herunder ønsket jeg å forstå hvordan informantene håndterte i denne spenningen, samt den eventuelle *selvsensureringen* de praktiserte for å finne en passende balanse.

På dette området forteller **Boomer**-generasjonen om noen interessante atferdstendenser på SNS. Åse (62) mener eksempelvis at digitale handlinger kan få fysiske konsekvenser, og unngår derfor å legge ut bilder på ferie, for å redusere risikoen for innbrudd hjemme. Dagny (66) har på sin side tidligere vært svært engasjert i politikken og lokalmiljøet – men ifølge hennes beskrivelser har hun de siste årene hatt en økning i sin egen selvsensur:

«det [å ytre meg] kunne jeg ha gjort enda mer. Men jeg blir mer og mer forsiktig. Når man etter hvert ser at denne verden ikke alltid er så grei, og har mange hatkommentarer på bagateller – så har det blitt mindre.»

– Dagny, 66 år (Boomer)

Hun sensurerer seg derfor for å unngå hat og trakassering, da dette er en stor påkjenning i seg selv. Det kan derfor antas at sitatet hennes illustrerer en pågående prosess der hun tror hun har upopulære meninger, og unngår dermed å uttrykke synspunkter åpent på Facebook, i frykt for sosial isolasjon – også omtalt som *taushetsspiralen* (Hampton *et al.*, 2014). For mange brukere handler selvsensurering gjerne om et ønske om å ikke bli mislikt av *noen*. Denne representasjonen preges dermed av det minste felles multiplum (Hogan, 2010). En vanlig taktikk for å beskytte privatlivet er nettopp en form for *selvsensur* der vi ender opp med å fremstille oss selv på en måte som vi tenker er akseptabel for flest mulig mennesker (Aalen og Hoem Iversen, 2021, s. 92). I alle fall for de *riktige* menneskene.

Jan (58) forteller eksempelvis at han tok en «oppvask» på Facebook-profilen sin, i forbindelse med et jobbskifte. Den gangen slettet han gamle innlegg, som ikke hadde stått tidens tann. Jan, som var på utkikk etter ny jobb, antok nettopp at arbeidsgivere ville søke han opp på Facebook, og valgte å sensurere eller slette, det som potensielt kunne stille han i et negativt lys. I stil med Goffman sin teori som *frontstage/backstage* (Goffman, 1959) – kan en slik «opprydding av profilen», være diktert av *inntrykkskontroll*. Å rydde eller å iscenesette egen profil - slik at det som er synlig av informasjon er anstendig og presentabelt i møte med en arbeidsgiver. Profilen måtte i dette tilfellet, være i tråd med Jan sin forestilling om frontstage. Dersom profilen inneholdt irrelevant eller i ytterste grad kompromitterende bilder - ville profilen kunne oppleves som backstage for Jan, og ikke noe han hadde ønsket at arbeidsgiveren skulle se.

Når det kommer til **Generasjon Z**, så viser de også til noen interessante tendenser. Ifølge mine analyser fra datamaterialet, ser det ut til at flere Gen Z-informanter er preget av en selvsensur, som aktiveres når de tror at de *bryter med ett mønster eller norm* i møte med egen selvrepresentasjon på plattformen. At dersom de bryter med mønsteret som karakteriserer deres «vanlige aktivitet» på plattformen – kan det få mulige konsekvenser i form av beskyldninger for at de skryter eller kjeder andre. Bertine (25) svarte eksempelvis at hun vegrer seg for å legge ut ett nytt bilde, dersom hun i en periode har lagt ut for mye i forhold til det hun bruker å gjøre. At publikummet blir «mettet» på hennes innhold. Hun unngår slikt sett å legge ut for å ikke *kjede* følgerne sine, slik at de blir lei av henne.

Tony (26) forteller om en topptur-festival, der de hadde tatt stilige bilder på fjelltoppen. Men så begynte han å reflektere over egen bruk på Instagram. Vanligvis så la han jo ikke ut så mye: «Og jeg tenkte sånn at dette er jo et veldig kult bilde, kunne jeg tenkt meg å dele det? Men så var det litt sånn, jeg tror egentlig at folk ikke bryr seg. Jeg har det for meg selv.» Her ønsket han å opprettholde representasjonen av seg selv, og ikke komme ut av det blå med *skrytebilder* på profilen sin. Christian (15) på sin side har også kjent på at det er bilder han kunne tenkt seg å legge ut – men at han synes det er for mye styr å gjøre det, og derfor unngår det.

Dette kan også kobles tilbake til Gen Z sin tendens om å skape et *fotoalbum*, der innleggene deres tilsynelatende, krever mer planlegging og bedre gjennomføring – slik som god kvalitet, redigering etc.

6.4 Oppsummering av komponenten for atferd

Når det kommer til informantenes *periodiske personvernshandlinger*, er det bemerkelsesverdig få av informantene som har tatt seg tid til å kikke på personvernserklæringen til Meta. Dette skyldes trolig at de oppfatter den som lang og tidkrevende. Når det gjelder håndtering av informasjonskapsler, viser datamaterialet at Boomers ofte trykker «godta», mens Generasjon Z ser ut til å være mer tilbøyelige til å tilpasse alternativene.

Angående deres *statistiske personvernshandlinger* ser vi at både Boomers og Gen Z, viser en mangel på bevissthet og aktiv endring av personvernsinnstillingene. Dette kan føre til utilsiktet deling av personlig informasjon og et redusert personvern. Tenke høyt-øvelsen viste seg å være nyttig for å fremme refleksjon rundt konsekvensene av å ha personopplysninger offentlig tilgjengelig.

Når det gjaldt informantenes *dynamiske personvernshandlinger*, har vi sett på hvordan de to generasjonene navigerer og håndterer selvrepresentasjon på Facebook og Instagram. Hovedtrekkene viser at Boomers foretrekker å være aktiv i Facebook-grupper; de har vanskeligheter med å blokkere bekjente; i tillegg til at det er en oppfatning om at Boomerne bruker SNS som en dagbok. På den andre siden, er Generasjon Z aktive på ulike personlige Instagram-kontoer; de er mer komfortable med å blokkere brukere; og anvender SNS mer som et fotoalbum. Begge generasjonene selvsensurerer, og ingen av den tenker bevisst over personvern når de bruker plattformen.

Informantene i denne studien bruker derfor ulike handlingsmuligheter på Facebook og Instagram for å styre personvernet sitt i gjennom en kontinuerlig forhandling preget av deres behov for synlighet og nivå av kommunikative handlingskraft. På tvers av personvernshandlingene – ser det imidlertid ut til at informantene tilhørende Generasjon Z, viser til en generelt sterkere kommunikativ handlekraft, enn Boomer-utvalget.

KAPITTEL 7 - Den Affektive Komponenten

– FØLELSER, EMOSJONER OG OPPLEVELSER –

Den *affektive* dimensjonen av tre-komponentmodellen handler om følelser og emosjoner. Dette kapitlet tar sikte på å belyse det tredje analysespørsmålet (A3): *Hva føler Boomerne om personvernet på Meta i forhold til Generasjon Z?* Her skal vi se nærmere på informantenes emosjonelle reaksjoner på egne opplevelser i møte med personvernet på Facebook og Instagram. Den kognitive komponenten som ble diskutert i Kapittel 5, er viktig å sette i sammenheng med det affektive. Våre fortolkninger av en situasjon vil være avgjørende for hvilken emosjon som utløses (Svartdal, 2020). Her kan emosjoner slik som angst, frykt, sinne og avsky oppstå i situasjoner der personvernet oppleves som krenket. Dette kapitlet deles inn i to hovedtemaer, alt etter om personvernet knyttes til Meta som *institusjon* - eller personvern knyttet til *sosiale* aspekter (Raynes-Goldie, 2010). Herunder skal vi blant annet se på hvordan informantene opplever Meta sin utbredte datainnsamling, kontokapring av profiler, opplevd overvåkning og publisering av personbiler uten samtykke.

7.1 Følelser knyttet til det institusjonelle personvernet på Meta

I Kapittel 5 så vi på hvilken *forståelse* informantene hadde om Meta sin datainnsamling og selskapets forretningsmodell – nå skal vi se på hvordan de *føler* om det. Delkapitlet tar for seg informantenes opplevelser og følelser knyttet til det *institusjonelle* personvernet. Innledningsvis ser vi om informantene føler de har kontroll over sin egen informasjon på Meta. Deretter vil fokuset rettes mot hvordan informantene føler om at de potensielt overvåkes.

7.1.1 Boomerne føler på en viss kontroll – Gen Z føler seg helt maktesløse

Personvern handler blant annet om at vi som brukere av SNS, skal kunne ha en kontroll over våre egne personopplysninger (Westin, 1967; Acquisti, Taylor og Wagman, 2016). Den massive informasjonsmengden som samles inn når vi bruker SNS, utfordrer imidlertid muligheten til å ta kontroll (Richards, 2022). Ut fra **Boomer**-informantenes beskrivelser, kjenner flertallet på en viss kontroll over deres personlige informasjon på Facebook og Instagram. Herunder er det sentralt at de hevder at de ikke har noe «nevneverdig privat» som ligger åpent på profilene deres. Flere kommenterer at dette er grunnen til at de føler på en kontroll over sine opplysninger. Denne tendensen kan være en naturlig konsekvens av at flere Boomere hadde en oppfatning om at det hovedsakelig var opplysninger og innhold tilknyttet den *synlige*

informasjonsstrømmen som ble samlet inn av Meta (se 5.2.1) – og ikke var bevisst det tekniske bak (Rasmussen, 2016). De eldre informantene fremstår heller ikke som emosjonelt engasjert når det gjelder å ha kontroll over egen informasjon.

Informantene tilhørende **Generasjon Z**, var derimot mer nyanserte i sine refleksjoner enn Boomers, når det kom til følelser av kontroll over informasjonen sin på Meta. Flere av informantene skiller mellom informasjon som andre brukere kan se, og informasjon de har gitt fra seg gjennom å godkjenne personvernsvilkårene. De har slikt sett en bedre forståelse av de to informasjonsstrømmene, enn Boomerne. Bertine (25) føler herunder at hun har god kontroll på den *synlige* informasjonen hennes, men erkjenner at hun ikke har noen kontroll på selve innholdet når det først er blitt publisert: «Det føles ukontrollerbart... og det er ikke sånn at jeg tenker over det, men jeg bare aksepterer at det er som det er». Bertine peker på at *distribusjonen* av innholdet hennes føles *ukontrollerbart*. Selv om hun har lagt ut et bilde på sin personlige Instagram, så kan dette kopieres, manipuleres og legges ut andre steder på internett – helt utenfor hennes kontroll (reproduserbarhet).

Gjennom analyse av transkripsjonene og notater fra intervjuene fremkommer det følelser av *meningsløshet* og *frykt* blant denne unge generasjonen. Adam (22) kommenterer følgende: «For alt vi vet så kan det bli brukt over alt i verden... så den har vi ikke kontroll på i det hele tatt.» Tony (26) forteller at han føler seg ofte maktesløs overfor slike situasjoner, og omtaler det som en «tapt sak som er umulig å vinne over». Han har også et interessant sitat i denne forbindelse:

«Du må enten godta det eller ikke bruke tjenesten i det hele tatt. Så jeg velger å godta det.. på bekostning av meg selv da på en måte [...] Jeg vet ikke om det er litt sånn sunk-cost-opplegg, at folk tenker sånn 'ja, men jeg har allerede gitt fra meg så mye personvern, så nå er det for sent og jeg driter i det'. Så fortsetter de bare å spy ut og dele [personopplysninger] og uten å egentlig tenke konsekvenser da. Så det blir jo ikke noe bedre...»

– Tony, 26 år (Gen Z)

Her beskriver Tony situasjonen som «sunk cost». Dette er et økonomisk begrep for å forklare at kostnader som er påløpt, ikke kan reverseres (Gårseth-Nesbakk, 2022). Tony knytter sunk cost-begrepet til en negativt ladet oppfatning om at all den informasjonen vi har gitt fra oss, kan vi aldri ta kontrollen over igjen. Innenfor medieforskning, kan dette knyttes til *digital resignasjon*, som ble nevnt i 6.1.1 angående tvungen aksept av personvernsvilkår. Dette er altså en tilstand som oppstår når en bruker ønsker å kontrollere informasjonen som organisasjoner har om dem, men føler seg maktesløs til å gjøre det (Draper og Turow, 2019). Herunder mener forskerne at denne resignasjonen er en helt rasjonell respons på forbrukerovervåking – ikke

nødvendigvis som et resultat av at de ikke bryr seg om personvernet. Dette samsvarer også med resultater fra Datatilsynets personvernsundersøkelse (2020).

Samtidig må det kommenteres at det er fullt mulig for en bruker å føle en mangel på kontroll, uten at dette oppleves som problematisk. Nytteverdien av SNS, kan oppleves så stor at brukeren godtar kontrolltapet, som en del av en byttehandel (Marwick og Hargittai, 2019; Datatilsynet, 2020, s. 12). Dette kan knyttes til Bertine sitt sitat over, der hun forteller at hun vet at det blir samlet inn mye informasjon om henne, men at hun *aksepterer* det – og som resultat, resignerer.

7.1.2 Boomerne spekulerer – Gen Z er overbevist om at de overvåkes

Det har over flere år svirret en konspirasjonsteori om at Meta avlytter private samtaler gjennom smarttelefonen, og deretter gir dem annonser på basert på hva som ble sagt (Gilbert, 2019). Meta har benektet dette gang på gang. På tvers av begge generasjonene, er det likevel en skepsis knyttet til hvordan Meta samler inn opplysninger. Nesten alle informantene nevner at å ha fått opp reklame om «noe de har snakket om, men ikke søkt på».

Flere av **Boomerne** fremstår som spekulerende når de omtaler dette. Ove (57) nevner blant annet at: «Jeg tror ikke at det er noe spionasje ute og går, men ett eller annet er der. Det er jeg helt sikker på». Her kommenterer flere at de ikke husker om de hadde søkt på ting som kom opp som annonser, og dermed ikke hadde noen spesifikke avlyttingsanklagelser - mer enn at de synes det er «veldig rart» når annonsene treffer som de gjør. Dagny (66) mener uavhengig om de lytter eller ei, at Meta kan påvirke holdningene hennes. Her forteller hun om at hun delte synspunkter om COVID19-vaksinen under pandemien, og erkjenner at hun var kritisk til den:

«Hvorfor har jeg de holdningene jeg har til det [vaksinen], og andre ikke? Men så ser jeg at det jeg googler en gang, kommer tilbake [på Facebook] og forsterker mitt syn. Så kan andre som ikke googler det jeg gjør, aldri få opp det jeg ser – og ikke kan begripe hvordan jeg har sånne holdninger. [...] Når det var det verste med det vaksinestyret, fikk jeg beskjed fra Facebook om hva som var den 'offisielle holdningen' til vaksinen, at det var ikke greit å mene det jeg gjorde. Forstår du hva jeg mener? Det kom liksom opp sånne ting hva som skulle være det rette å mene.»
– Dagny, 66 år (Boomer)

Dagny sitt sitat illustrerer effekten av Meta sine personaliserte *algoritmer*. Under koronapandemien, ble teknologiselskapene ansvarliggjort for spredning av falsk informasjon. Meta ble herunder pålagt å informere brukerne om innhold som var i strid med helsemyndighetenes anbefalinger (Smedsrud, 2020). Sitatet berører slikt sett viktigheten av å se hvordan *ytringsfrihet* og *personvern* henger sammen. Når Meta anvender algoritmer for å styre hennes informasjonsstrøm, så er dette basert på innsamling av Dagny sine personlige data,

som samlet sett gir en dyp innsikt i hennes privatliv. Utfordringen er at ingen brukere har like nyhetsstrømmer, siden de nettopp er personaliserte til hver enkelt (Kalsnes og Pettersen, 2019). Personvern er nettopp helt sentralt i dette. I Dagny sitt tilfelle, ble Facebook sin «innblanding» hvor de korrigerer hennes syn på vaksinen, ansett som et brudd på hennes *kontekstuelle integritet*. Selv om det ble gjort i offentlighetens beste, for å begrense spredning av feil informasjon - så kan slike tiltak imidlertid oppleves som en invasjon av deres personlige autonomi og ytringsfrihet – og en krenkelse av hennes private opplysningssfære (Schartum, 2020). Det er nettopp ikke sikkert at de lytter, selv om det kan oppleves slik.

I denne forbindelse, ønsker jeg å trekke frem Ingrid (58) som har noen interessante refleksjoner, der hun tror at vi lever i et mer overvåkningssamfunn enn det mange skal ha det til:

«Vi er nok naive i forhold til hva våre opplysninger kan brukes til. Nå har vi en tradisjon med demokratiske regjeringer og sånt, men om det skulle finne på å komme ett kupp en gang [...] så ligger det veldig mye opplysninger om oss rundt omkring som kan misbrukes.»
– Ingrid, 58 år (Boomer)

Hun erkjenner at hun er preget av hennes foreldregenerasjon – der hun meddeler at hennes tyske mor vokste opp under naziregimet. Som barn vokste Ingrid opp med historier om den statlige overvåkningen i Øst-Tyskland, der overvåkningen ble gjort i stor grad ved hjelp av angivere. Under krigen var det strengt forbudt å ha noen form for kontakt med Vestlig kultur. Hun nevner en anekdote om at det vestlige og østlige TV-formatet var ulikt på denne tiden – og angiverne utnyttet dette ved å spørre barn i barnehagen, om hvordan TV-bildet så ut hjemme hos dem – om hjørnene på skjermen var ovale, eller firkantet. Mange barn angav uvitende sine foreldre gjennom dette, noe som Ingrid finner dypt urovekkende, selv etter mange år:

«...og med alle historiene jeg har hørt fra mamma, så er det helt utrolig hva selv de minste opplysninger kan brukes til – for å finne deg, vist de vil det.. Men det er jo en sånn avveining også. Jeg kjenner jeg blir litt sånn paranoid av og til. Skal man gå rundt å bekymre seg eller hvor stor er sannsynligheten for at noe skjer med vårt demokratiske samfunn her i landet? Gjør det noe om folk sitter på opplysninger om meg?»
– Ingrid, 58 år (Boomer)

Sitatet illustrerer at hennes oppvekst kan ha farget hennes syn på personvern. Fremfor alt, ser hun viktigheten av at opplysningene ikke misbrukes til andre formål enn det som forventes (Nissenbaum, 2010). Dette knytter hun implisitt til digitale tjenester, og det faktum om at selv opplysninger av lav betydning for brukerne (jf. TV-format), kan misbrukes av andre. Sett fra dette perspektivet ser Ingrid noe av personvernets *kollektive* verdi, ved at det beskytter oss som

samfunn å kunne ha kontroll på egne opplysninger og vite hva de brukes til (Moor, 1997). Imidlertid kommer ikke dette frem fra noen av de andre informantene.

Blant **Generasjon Z** er det mange som er overbevist om at de overvåkes av Meta – der enkelte hevder at de opplever å få opp reklamer om ting de har snakket om, på jevnlig basis. De forteller om hendelser, og bruker adjektiv som *sjokkerende*, *skummelt* og *ekkelig* for å forklare følelser knyttet til at målrettede annonser dukker opp «uten videre». Christian (15) forteller eksempelvis at: «Jeg husker bare at jeg hadde snakket om noe, også kom det bare opp [...] Føltes litt rart egentlig. Jeg blir både litt imponert og så blir jeg litt sjokkert også». Flere av dem antar at smarttelefonen er «samkjørt» med alle apper, og på denne måten blir de overvåket hele tiden. Bertine (25) erkjenner at når hun tenker på personvern, så er det belastet med følelsene *frykt*, *sinne* og «beskyttelsesfølelsene» - men at dette ikke trer i kraft før man opplever at det går for langt. I intervjuet nevner hun et eksempel knyttet til politiets sikkerhetstjeneste (PST), der hun reflekterer over hva hun føler hun kan snakke om og ikke med mobilen i nærheten:

«Det er jo helt åpenbart at telefonen tar opp ting av det du sier [...] Det er nesten blitt noe du tuller med sånn; 'ikke snakk om ditt eller datt, ikke snakk om spesielt politikk og trusler og terror'. Det snakker du bare ikke om, for plutselig har 'de' alt du har sagt, så kommer PST og tar deg liksom. Det er jo en grunn til at det er en kødd. For det er en reell kødd.»
– Bertine, 25 år (Gen Z)

Her opplever hun at normen er at man ikke bør ytre seg om kontroversielle temaer og politiske meninger – noe som kan reflektere en *nedkjølende effekt*, der hun regulerer seg selv i frykt for å bli overvåket (Marder *et al.*, 2016). Adam (22) forteller på sin side om en episode der han og en venn faktisk *ble* ringt opp av PST, i etterkant av ett søk: «når jeg og en kompis skulle søke opp noe med fyrverkeri og pinneraketter, da ble vi ringt opp av PST, fordi de synes det var rart å søke opp. Det er jo ikke noe å legge skjul på at de følger med».

Den unge generasjonen ser ut til å ha en oppfatning om at de overvåkes på kryss og tvers av apper og institusjoner – og at mobilen er fellesnevneren for overvåkningen. Hensikten ved dette delpunktet er dog ikke å lande en konklusjon om denne konspirasjonsteorien. Uavhengig om Meta avlytter telefonen eller ikke, så kan *ideen* om at de gjør det i seg selv føles invaderende for brukeren, og oppleves som et brudd på deres *kontekstuelle integritet* (Nissenbaum, 2010). Spesielt når ord eller samtaler de har utført i en privat kontekst, ser ut til å gi utslag i annonser på Facebook kort tid etter.

7.2 Følelser knyttet til det sosiale personvernet på Meta

Dette delkapittelet fokuserer på det *sosiale personvernet* (Raynes-Goldie, 2010), der vi går inn på analysing av ulike personvernbrudd (krenkelser) på Meta, og informantenes følelser knyttet til slike opplevelser. Først ser vi på informantenes opplevelser knyttet til kontokapring (hacking) på Meta. Deretter ser vi nærmere på deres følelser, knyttet til bildedeling uten samtykke på Meta. Her vil Helen Nissenbaum sitt analytiske rammeverk om *kontekstuell integritet* stå sentralt for å analysere krenkelsene (Nissenbaum, 2010).

7.2.1 Alle kjenner noen som har blitt kontokapret den siste tiden: Frykt, Ubehag, Kynisk

SNS har gjort det enklere å nå ut til mange på kort tid. Dette går på plattformenes egenskap om *skalerbarhet* (boyd, 2010) - og er noe som svindlere vet å utnytte. Ofte innebærer dette at fysiske personer eller roboter, sender virusmeldinger der de utgir seg for å være noen andre – ofte din egen Venn. Formålet er å lure til seg personlig informasjon, gjennom å ta kontroll over private profiler. Slik kan de utnytte personlige profiler for å svindle Vennene til dens egentlige eier (Nettvett, 2016). Det å bli *kontokapret*, er en krenkelse av brukerens *opplysningsfære* (Schartum, 2020), og har blitt svært utbredt på Facebook og Instagram (Kulbrandstad, 2022).

I denne studien kjenner alle informantene noen som har opplevd kontokapring den siste tiden. Blant **Boomer**-generasjonen, sier Dagny (66) at: «Jeg føler at dette har blitt et stort problem på Facebook, at folk tar over kontoene. Men jeg prøver å passe meg for hva jeg går inn på.» Flere henviser til eksempler om «falske venneforespørsler» på Facebook. Et vanlig kjennetegn er at de får en venneforespørsel fra en person som *de vet* de er Venn med fra før av, slik som Ove (57) eksemplifiserer i følgende dialog:

Ove: Man hører jo og ser ofte det at noen har vært inne og trykket på en lenke også har man blitt hacket, også kommer det nye venneforespørsler fra noen man er venn med. Da, wow, her er det noe som er galt. For da har noen opprettet en konto i hans sitt navn. Det har jeg vært bort i flere ganger.

Intervjuer: **Vist dette hadde skjedd med din profil, hvordan hadde det føltes tror du?**

Ove: Vel da hadde jeg blitt skremt.. for da må man jo gå inn å gjøre tiltak. Slik som å gå inn å endre passordet, for da er man blitt hacket [...] det er jo tragisk og veldig dumt, men det er jo dagens virkelighet.

Ove er en av flere informanter som kobler slike hendelser til fryktfølelser. Frykt for at noen kan stjele og misbruke identiteten. Dette går både på tillit til Meta, og tillit til andre brukere av plattformen. Når en svindler kontokaprer en profil, så kan dette nettopp få store ringvirkninger, da svindleren spiller på legitimiteten og integriteten, som den ekte personen har bygget opp

gjennom sin profil. Som regel over flere år. Selv om ikke alle har opplevd slik kontokapring, er det tydelig at den eldre generasjonen er klar over at det skjer, og noen kommenterer at *naivitet* kan være en faktor. At flere som de kjenner fra eget nettverk, ikke reflekterer rundt konsekvensene – eller at de rett og slett ikke er klar over «symptomene» på at det er svindel. Slik som en luguber venneforespørsel eller en lenke. Dette viser også viktigheten av *kritisk medieforståelse* i møte med SNS.

Samtidig kan hvem som helst ha et svakt øyeblikk og å være uoppmerksom på det som skjer på skjermen. Åse (62) deler en ubehagelig hendelse som fant sted kort tid før intervjuet. Hun forteller at hun fikk en venneforespørsel fra en venninne, som hun visste var en del av Vennelisten sin på Facebook. I denne anledning forteller hun at: «Jeg vet jo at jeg ikke skal trykke på det... men så gjorde jeg det likevel». Herunder opplevde hun å bli engstelig på andres vegne, i frykt for at hennes egne venner også skulle bli hacket. Slik svindel sprer seg som ild i tørt gress, og er en stor trussel for personvernet i den digitale opplysningssfæren.

Blant **Generasjon Z** er deres opplevelser gjerne knyttet til Instagram, frem for Facebook som dominerte samtalen blant Boomerne. Utfordringen med personvern er nettopp at vernet kan oppleves usynlig inntil noe ubehagelig eller invaderende skjer. Her er det flere emosjoner i sving, men hovedsakelig følelser av frykt og ubehag:

«Jeg føler jo at jeg er redd for at alt skal bli hacket. Og da har man jo ikke helt 100% kontroll. [...] For nå om tiden, så er jo mange blitt hacket på Instagram, og da er det jo helt ute av din kontroll, men det er deg de later som de er. Og det synes jeg er litt skummelt.»
– Nora, 19 år (Gen Z)

Sitatet til Nora går mer direkte på hennes frykt om å skulle *bli* hacket. I forlengelse av dette erkjenner hun at hun er redd for å legge til folk på sine profiler, på grunn av frykten for at de kan ta over kontoen hennes. Blant Gen Z, så er det likevel et utsagn som skiller seg ut i datamaterialet. Dette gjelder Bertine (25) sin respons på spørsmål om hvordan hun tror hun hadde reagert dersom hun hadde fått kontoen sin kapret:

Nå skal jeg ikke være kynisk da, men jeg tror det handler mest om at du må lage en bruker på nytt? Nå mister jeg følgerne mine!!... Jeg tror at de som er like gamle som meg, tenker mest på det. Ut ifra hvordan jeg selv ville reagert. Jeg tror jeg hadde vært sånn 'hæ, serr? Må jeg gjøre dette på nytt? Må jeg begynne å følge folk på nytt?'. Jeg tror det hadde vært mer et ork enn en invadering av privatliv.
– Bertine, 25 år (Gen Z)

Her peker Bertine på ett interessant aspekt ved krenkelser i form av kontokapring på SNS. Med første øyekast kan sitatet oppfattes som overfladisk. Men under den personsentrerte analysen, gikk jeg nærmere inn i datamaterialet for å bedre forstå hennes *kontekst* i forhold til hvordan hun omtalte seg om personvern (kognitiv) og hvordan hun bruker SNS (atferd), samt utsagnet i seg selv. Dette ser ut til å handle om *selvrepresentasjon* (Goffman, 1959). Det at mange bruker mye tid og ressurser for å skape et bilde av seg selv for publikummet på SNS, eller deres *frontstage*.

Bertine informerer i starten av intervjuet at hun er glad i å dele bilder av egne opplevelser – spesielt på Instagram. Her kommer det også frem at hun har brukt SNS siden 2011, noe som tilsvarer over 12 år. Gjennom disse årene har hun bygget seg en følgerbase med venner, bekjente og fremmede på sin offentlige Instagram. Dersom hun skulle oppleve å bli kontokapret, vil hun kunne miste tilgangen til sin profil og sitt publikum. Selv om hun i en slik situasjon, enkelt kunne ha opprettet en ny profil på Instagram – så går hun glipp av de store nettverkseffektene, som hun hadde på sin etablerte profil med mange følgere. Hun må starte med blanke ark og bygge opp alt på nytt - med nye bilder som tar tid å planlegge, redigere, publisere og skaffe nye følgere. Hennes synspunkt om at hun ville ha opplevd en kontokapring mer som et *ork* enn en invadering av privatlivet – er egentlig helt naturlig. Men da må man se det fra hennes ståsted og fra normene som regjerer i hennes kontekst (Nissenbaum, 2010).

7.2.2 Bildedeling uten samtykke: Ubehag, Sinne, Sårbar, Vantro

I dette delpunktet løftes det frem opplevelser hvor informantenes privatliv har blitt krenket - gjennom at andre har lagt ut bilder av dem, uten deres samtykke. Ifølge Datatilsynet er et *bilde* en personopplysning - dersom personen kan *gjenkjennes* (Datatilsynet, 2019b). I teorien er det dermed ikke lovlig å publisere bilder av personer uten deres samtykke. Det er herunder helt sentralt å forstå at vårt eget personvern henger sammen med andres. Med dette i mente, hevder de fleste i **Boomer**-generasjonen at de ikke har opplevd at noen har publisert bilde av dem uten deres samtykke. Ingrid (58) og Rita (67) peker på at de ikke er med på så mye, og lar seg ikke avbilde uten videre. Ove (57) forklarer at han ikke har noen problemer med at andre legger ut bilder av han, og at han derfor ikke har reagert negativt når det først har skjedd. Dagny (66) hevder at hun ikke har opplevd det selv, men reflekterte over hennes egne vaner: «Jeg tenker jo at dersom jeg skal legge noe ut, så må det jo være et fint bilde av dem. Helst spørre. Men jeg er vel blitt flinkere til å spørre nå, uten å tenke over det.» Her begrunner hun eksempelvis med at «det må være ett fint bilde» av personen dersom hun skal legge det ut på Facebook. Det er nok

mange som kan kjenne seg igjen i dette utsagnet. Samtidig ser ikke personvern forskjell på pent eller stygt. Det er en subjektiv oppfatning. Det er *personen* som står i sentrum, og dens rett til å velge å dele (eller å ikke dele) bildet for offentligheten.

Åse (62) forteller imidlertid om en ubehagelig opplevelse, der hun hadde vært med på en klassefest. I forkant ble det opprettet en Facebook-gruppe for klassen, der det ble lagt ut flere bilder og innlegg for å mimre over tiden som var. Deriblant la en tidligere klassekamerat ut et bilde av Åse der hun lå i bikini, fra da hun var rundt 14 år gammel:

Åse: Nei, da måtte jeg sende henne en melding om at 'det må du slette, det vil jeg ikke skal ligge ute på den klassegruppa nå'. Det synes jeg ikke var ålreit. Så det var over en grense faktisk..

Intervjuer: **Hvordan følte det ut for deg når det bildet kom ut på Facebook-gruppen?**

Åse: Uff, da tenkte jeg på alle som skulle se dette og 'hva tenkte de' også, nei da følte jeg.. Jeg tenker jo at de årene er jo en veldig sånn sårbar fase i livet. Så det vil jeg ha eierskap på selv. Jeg vil jo ikke legge ut et bikinibilde fra da jeg var 14 år, og dele det med klassen når de da var blitt 60!

Denne dialogen illustrerer at grensene for privatliv, er igjen helt styrt av kontekst. For venninnen som la det ut, handlet det nok om en affeksjonsverdi – at det var hyggelig å se tilbake på gamle sommerminner. Men for Åse, ble dette å trække langt over det hun oppfattet som privatlivets grenser, og derav ble hennes kontekstuelle integritet også brutt.

Blant **Generasjon Z** har samtlige derimot opplevd at noen har lagt ut bilde uten deres samtykke – opptil flere ganger. Det vil derfor være noen flere eksempler knyttet til denne generasjonen. Herunder går det et skille mellom informantene som stiller seg positiv til det, og de informantene som har reagert negativt. Emilie (22) sier hun ikke reagerer på om andre har lagt ut uten å spørre, fordi de aktuelle bildene som oftest er koblet til en *felles forståelse* om at det 'skal skje en fotografering' – som da potensielt havner på Instagram: «Jeg har jo liksom vært med på 'nå skal vi ta bilder!' Så jeg er jo liksom klar over det». *Forventningene* for *konteksten* er derfor satt, og kjent for *aktørene*. Nissenbaums (2010) teori fremhever nettopp viktigheten av at informasjon blir delt på en måte som passer med den spesifikke konteksten.

Flere av informantene hevder at det å ta og dele bilder av andre uten å spørre først, er normen blant deres jevnaldrende. Tony (26) forteller på sin side om en ubehagelig hendelse knyttet til Instagram-historier, som kontekst for bildedelingen. Episoden hendte på en fest da han var 18

år. I løpet av kvelden ble han påvirket av alkoholen, falt om og ble liggende på bakken. Innen kort tid tok noen et bilde av Tony liggende i rusen, og la ut på sin Instagram-historie:

Tony: Ene kvelden så ble jeg kjempefull og der jeg ble liksom litt liggende da. Da var det noen som hadde lagt det ut på story, og skrevet sånn 'hahaha, han er så full og...'. Dette gikk jo selvfølgelig litt videre til andre venner og sånt da. Så når de møtte meg, gjerne en stund etterpå, så var det det de husket... og da var jeg litt sånn at – det er jo ikke så hyggelig at alle vet det!? Det skjer jo de aller fleste som drikker at de har en liten smell, men det deles nødvendigvis ikke med alle andre.

Intervjuer: **Tror du at denne episoden har bidratt til at du ikke legger ut så mye selv?**

Tony: Ja, egentlig. Visst man først har opplevd noe sånt så forhåpentligvis begynner i alle fall mange å tenke at, visst jeg gjør det samme med en annen, så da jeg vet gjerne hvordan det føles.

Dialogen illustrerer en krenkelse av Tony sin kontekstuelle integritet, som oppstod i en kontekst som han oppfattet som begrenset (privat fest). Dette var dermed en personlig og ydmykende hendelse for Tony, som ble delt på en offentlig Instagram-konto og vist til et stort publikum. Dette brøt med Tony sine forventninger om at informasjonen skulle forbli innenfor den opprinnelige konteksten (festen). Han sier selv at han opplevde denne hendelsen som svært *ubehagelig*. Selve konsekvensen av at bildet ble lagt ut, var først og fremst det *sosiale* utfallet. En følelse av at 'alle har sett meg på mitt verste eller svakeste'. En annen konsekvens, var at han begynte å *selvregulere* sin egen aktivitet i ettertid av opplevelsen. Slike brudd på den kontekstuelle integriteten, er nettopp erfaringer som kan påvirke brukernes atferd i ettertid – både på godt og vondt.

Noe som fremtrer av datamaterialet på tvers av generasjon, er at flere viser til bekymringer for barns personvern på SNS. At mange besteforeldre og foreldre legger ut bilder av barna, uten at de får kontrollere dette selv. Bertine mener at det skorter på bevissthet blant de foresatte: «foreldre som egentlig skulle hatt noe å si, har ikke innsikt i hva de gjør. Så de klarer liksom ikke å sette noen rammer for det heller.» Under intervjuet velger Nora (19) å dele en støtende opplevelse som hendte for noen år siden, der hennes mor la ut et bilde av henne på Facebook:

Nora: Jeg husker at mamma la ut ett bilde en gang. For foreldre kan jo legge ut bilder i hytt og pine, også har de den unnskyldningen om at 'du er ungen min, jeg kan gjøre det jeg vil med deg'. Så la hun ut [at] vi var på tur på fjellet, oppe på toppen. Så var jeg veldig varm, slik at håret mitt og alle babyhårene står rett ut, hestehalen henger og med en utvasket [Justin] Bieber-t-skjorte... Så da sa jeg til henne at, 'vet du, kan du slette akkurat det bilde?' Og da var det sånn, 'Nei, jeg kan jo ikke gjøre det!' Og da sa jeg at jeg kommer til å rapportere deg, vist du ikke sletter det. Men hun slettet det ikke da...

Intervjuer: **Hvordan følte du da, når hun ikke slettet bildet selv om du ønsket det?**

Nora: Jeg blir veldig sur. Jeg blir forbannet, fordi jeg er sånn; det er MEG det handler om! Du har ikke rettigheten til å fortelle om meg på denne måten, eller vise meg sånn...

Her opplever Nora et brudd på hennes kontekstuelle integritet, når moren hennes nekter å slette et upassende bilde av henne – til tross for hennes uttrykte ubehag. Dette bryter med Nora sin forventning om privatliv, og demonstrerer en *asymmetrisk maktbalanse* i foreldre-barn-relasjonen. Hennes reaksjon på situasjonen resulterte i sinne og fortvilelse. Nora (19) forteller imidlertid om ulike måter hun prøver å *respekttere andres* personvern. Herunder bruker hun først og fremst å spørre personene på bildet om lov, før hun legger ut på Instagram. Alternativt «skjuler» hun ansiktene mest mulig. Slik som å plassere et emotikon eller tegne over ansiktet, slik at personen ikke gjenkjennes. Ved selfies, tar hun heller ett nytt bilde, enn å sende ett med uvedkommende i bildet. Flere Gen Z-informanter nevner lignende taktikker for å *verne andre*.

Sammenfattet hevder nesten samtlige informanter at de spør andre om lov før de legger ut bilder - men opplever at ingen spør dem tilbake, og at dette ikke er normen blant sine sosiale kretser. Dette kan være en form for *inntrykkskontroll* i lys av forskningssituasjonen – altså å fremstå bedre enn det man er. Samtidig må jeg ta deres ord for det. Uavhengig hva de gjør, er det tydelig at de opplever at normen er å ikke spørre før publisering.

7.3 Oppsummering av den affektive komponenten

Når det gjelder det *institusjonelle* personvernet, viser det seg at Boomer-informantene gir uttrykk for en større opplevelse av kontroll over personlig informasjonen, enn Gen Z som føler seg maktesløse i møte med å ta kontroll over egen informasjon på Meta. Videre er det enkelte Boomere som er svært skeptisk til hvordan Meta potensielt påvirker og overvåker dem. Blant Generasjon Z har nesten alle informantene har opplevd å få opp annonser relatert til samtaler de har hatt, men ikke søkt opp. Noe som fører til overbevisning om at Meta overvåker dem. Når det kom til det *sosiale* personvernet så vi at ulike brudd på personvernet – eller krenkelser av den kontekstuelle integritet – fører til følelser preget av frykt, sinne, ubehag og fortvilelse. Alle informantene kjenner noen i nær krets som har blitt kontokapret den siste tiden. Her er det en gjennomgående følelse knyttet til frykt for å få kontoen sin hacket – spesielt blant de unge. Når det kommer til deling av bilder uten samtykke, oppgir et fåtall blant Boomerne at dette har hendt dem. Gen Z på andre siden, hevder at dette oppstår ofte - spesielt i sosiale lag. Samtlige mener imidlertid at normen blant deres jevnaldre er å ikke spørre før man legger ut, men at de selv hevder å gjøre dette. Det er også en økende bekymring ovenfor barn som blir lagt ut bilde av, da de ikke kan velge selv.

KAPITTEL 8 - Oppsummerende Diskusjon og Konklusjon

I dette avsluttende kapitlet ønsker jeg å løfte opp tematikken og samle trådene. Dette gjøres gjennom å forene de tre komponentene (kognitiv, atferd og affektiv), og illustrere hvordan de kan sees i sammenheng med hverandre. Analysekapitlene (5, 6 og 7) tok for øvrig for seg en rekke temaer knyttet til personvern på SNS, der de to generasjonene ble satt opp mot hverandre. For å kunne runde av og sette dette i kontekst, har jeg først og fremst sammenfattet hovedtrekkene i *Tabell 8.1* på neste side. Denne tabellen gir en oversikt over de viktigste funnene tilhørende de ulike holdningskomponentene. Dette innebærer både bemerkningsverdige generasjonsforskjeller, eventuelle kjønnsforskjeller og hvor de avviker eller sammenfaller på tvers.

Det må herunder understrekes at dette *ikke* er entydige funn, men interessante aspekter som trer fram fra datamaterialet. Hensikten med tabellen er å oppsummere analysen. Før vi konkluderer og ser på veien videre, tar jeg utgangspunkt i *Tabell 8.1*, og gir en oppsummerende diskusjon av hvordan holdningskomponentene kan henge sammen. Inkludert hvordan de kan sees i relasjon med tidligere presenterte teorier og begreper, som illustrerer dynamikkene mellom brukere og teknologiselskapene, som legger til rette personvernet. Noen sentrale begreper som vil løftes frem her er; privatlivparadokset, datafisering og panoptikon, i møte med informantenes kritiske medieforståelse og kommunikative handlekraft. Dette trekker jeg opp mot den utbredte oppfatningen om at mange hevder at de *ikke har noe å skjule*, og hvorfor dette er en problematisk holdning, som kan føre til misforståelser om hvorfor personvernet er viktig - både for individet og for samfunnet som helhet.

Holdningskomponent	Analysetemaer	Boomer (57-67 år)	Generasjon Z (15-26 år)
KOGNITIV: Kunnskap, meninger og oppfatninger	Overordnet kunnskap om personvern	<ul style="list-style-type: none"> • Lav kjennskap til personvernsbegrepet. Kunnskapsnivået preges av yrkesbakgrunn • Assosiasjoner trekkes til identitetspapir og personnummer. 	<ul style="list-style-type: none"> • Lav kjennskap til GDPR. De fleste kjenner ikke til regelverket.
	Kunnskap om Meta sin behandling av personopplysninger	<ul style="list-style-type: none"> • Det de selv legger ut av innhold og personopplysninger blir innsamlet. 	<ul style="list-style-type: none"> • Alt de gjør på plattformen blir samlet inn.
	Kognitiv vurdering av personvern og privatliv	<ul style="list-style-type: none"> • Privatliv er viktig, og bør beskyttes. 	<ul style="list-style-type: none"> • Privatliv er ikke så nøye.
		<ul style="list-style-type: none"> • Mange er blitt mer bevisst på personvern over tid • Flere er skeptiske til å legge til nye brukere i nettverket nå, enn før. • Ønsket om å bli en offentlig person, kan føre til nedprioritering av personvern • Mange hevder at de ikke har noe å skjule • Det etterlyses bedre informasjon om hva et godt privatliv har som verdi 	
ATFERD: Atferd, handlinger og intensjoner	Periodiske personvernshandlinger	<ul style="list-style-type: none"> • Kun et fåtall har kikket på personverserklæringen siden de begynte å bruke Meta 	<ul style="list-style-type: none"> • Flere tilpasser alternativene
	Statiske personvernshandlinger	<ul style="list-style-type: none"> • Fleste har offentlig Facebook-profil • Opplever innstillingene som innviklet • Tyr til hjelp hos barna for å stille inn profilen. • Øvelse: Slet med å finne frem til personvernsinnstillingene (skapte frustrasjon) 	<ul style="list-style-type: none"> • Fleste har offentlig Instagram-konto • Nedprioriterer personvernsinnstillinger • Skeptisk til å dele geografisk posisjon • Øvelse: Fant frem fort, men ble overrasket over selve innstillingene
	Dynamiske personvernshandlinger	<ul style="list-style-type: none"> • Flere undervurderer deres faktiske publikum på plattformene 	
		<ul style="list-style-type: none"> • Foretrekker Facebook • Aktiv i Facebook-grupper • Har vanskeligheter med å blokkere • Analogi til dagbok 	<ul style="list-style-type: none"> • Foretrekker Instagram • Aktiv på flere Instagram-kontoer • Blokkerer uten særlig hensyn • Analogi til fotoalbum
		<ul style="list-style-type: none"> • Ingen tenker over personvern når de bruker SNS • Alle selvsensurer i ulik grad 	
AFFEKTIV: Følelser, emosjoner og opplevelser	Følelser knyttet til det institusjonelle personvernet på Meta	<ul style="list-style-type: none"> • Føler på en viss kontroll på egne opplysninger, men få er bevisst over den usynlige informasjonsstrømmen • Lite følelsesmessig engasjert 	<ul style="list-style-type: none"> • Føler liten kontroll på egne opplysninger, • Følelser av maktesløshet og resignasjon
	Følelser knyttet til det sosiale personvernet på Meta	<ul style="list-style-type: none"> • Alle kjenner til noen i nær krets som har blitt kontokapret den siste tiden • Følelser av frykt og usikkerhet • Kan oppleves mer som et ork enn invadering av privatliv, spesielt for unge • Knytter kontokapring til falske venneforespørsler 	
		<ul style="list-style-type: none"> • Fleste har ikke opplevd å bli publisert bilde av uten samtykke • Følelser av ubehag og frustrasjon 	<ul style="list-style-type: none"> • Nesten alle har opplevd å bli publisert bilde av uten samtykke • Følelser av ubehag, sinne, angst
		<ul style="list-style-type: none"> • Mange opplever at normen blant jevnaldrende er å <i>ikke</i> spørre før man publiserer • Samtlige hevder at de er flinke til å spørre andre før de legger ut 	
		<ul style="list-style-type: none"> • Mange er bekymret for at barn ikke kan velge selv om de blir lagt ut bilde av • Noen strategier er å ta bilde av barna sitt bakhode eller å plassere et emotikon på deres ansikt for å verne om deres identitet 	

Tabell 8.1: Oversikt over hovedtrekk i de ulike holdningskomponentene, blant de to generasjonene.

8.1 Ingenting å skjule – en utfordrende holdning for personvernet

Nå ønsker jeg å løfte frem ett spesifikt trekk blant de to generasjonene, som ser ut til å overlappe og forene mange av tematikkene og teoriene, som denne studien har sett på. Dette er - som masteroppgavens retoriske tittel indikerer – en oppfatning om at *de har ingenting å skjule*. Som nevnt i punkt 5.3.3, er dette en holdning som viser seg å være utbredt blant brukerne (Datatilsynet, 2014; Marwick og Hargittai, 2019), men som slettes ikke er en ny tankegang - der det trekkes linjer helt tilbake til nazistenes propagandamaskiner (Richards, 2022, s. 72). Det at dette 'ingenting å skjule-argumentet' tilsynelatende har blitt internalisert blant brukerne, skaper imidlertid flere spørsmål enn svar - om brukerne misoppfatter *hva* personvernet egentlig er, og *hvorfor* det er viktig. I dette oppsummerende delkapittelet brukes denne oppfatningen som en overbærende paraply, der vi skal knytte sammen holdningskomponentene, trekke inn de viktigste funnene, og se på disse i lys av tidligere presenterte begreper.

(1) Først argumenterer jeg for at holdningen om at «de ikke har noe å skjule», ikke gir mening. Dette kobler jeg til informantenes *kommunikative handlekraft*, gjennom å se på *privatlivsparadokset* og frykten for *kontekstkollaps*. (2) Videre kan denne holdningen fordreie hva personvern egentlig er – herunder ser vi på *overvåkningskapitalismens datafisering* i møte med Boomernes *kritiske medieforståelse*. (3) Påfølgende ser vi på hvordan denne holdningen er til fordel for teknologiselskapene, og kobler det opp mot *panoptikon*-begrepet for å forstå Generasjon Z sin *digitale resignasjon*. (4) Avslutningsvis beskriver jeg hvordan ingenting å skjule-holdningen undervurderer personvernets betydning, gjennom å ignorere dets *instrumentelle* verdi for samfunnet som helhet.

Holdningen gir ikke mening:

Privatlivsparadokset, kontekstkollaps og kommunikativ handlekraft

For det første, så gir utsagnet – «ingenting å skjule» - egentlig ingen mening. Utsagnet kan herunder peke på en begrenset selvinnsikt. For vi har alle *noe* å skjule – i alle fall iblant. Det å kunne ha et personvern, er nettopp essensielt for å kunne separere oss selv fra andre (Véliz, 2020). På det enkleste nivået, så bruker vi klær for å *skjule kroppen* vår for andre mennesker, og opprettholde vår *kroppslige* privatsfære (Schartum, 2020). Å oppleve at noen sprer nakenbilder over digitale tjenester kan være ødeleggende for personen det gjelder. Men mange hadde nok følt en form for ubehag – eller krenkelse av privatlivet - dersom hverdagslige aktiviteter fra soverommet eller toalettet ble avbildet, og klistret ut over norske nettaviser.

Det å hevde at en ikke har noe å skjule, indikerer at informantene ikke setter pris på et privatliv. Flere av Boomerne hevdet imidlertid, at privatlivet var noe *veldig viktig* for dem - og noe som burde beskyttes (**kognitiv**). Samtidig viste de en tendens til å ikke gjøre noe bemerkningsverdig for å styrke personvernet – sett bort i fra å ikke legge ut så mye. Herunder hadde de fleste Boomerne en offentlig profil; de trykket rett på «Godta alle vilkår»; og hadde knapt sett på personverninstillingene siden de begynte med Facebook for over ti år siden (**atferd**). Generasjon Z, mente på sin side at privatliv ikke var så nøye for dem (**kognitiv**). Til tross for dette, tilpasset flere av dem alternativene, i stedet for å gå rett på «Godta alt»; de fleste var også svært skeptiske til å dele egen posisjon og benyttet seg av flere Instagram-kontoer for å bedre kunne kontrollere det forestilte publikummet (**atferd**). Med dette tatt i betraktning, ser det ut som at *privatlivsparadokset* er mye mer fremtredende hos Boomerne, enn hos Generasjon Z. Det er altså i større grad en manglende kobling mellom det de eldre sier og hva de gjør - i forhold til de yngre. Ironien i dette, er at paradokset stort sett har blitt koblet opp mot yngre brukere (Barnes, 2006; Hargittai og Marwick, 2016). Generasjon Z ser altså ut til å tenke mer på å beskytte privatlivet (**kognitiv**), enn det de selv uttrykker verbalt. Gjennom å se på komponentene i sammenheng, trer det altså frem noen motsigende holdninger, som ikke kunne blitt avdekket om vi så komponentene isolert.

En annen måte å se dette på, er at Generasjon Z sine kognitive vurderinger og taktikker er inkorporert i deres hverdagslige mediebruk (**atferd**), og utføres ikke nødvendigvis fordi personvern er en viktig faktor – men for å dempe på spenningen som kan oppstå ved potensielle *kontekstkollapser* i SNS (Marwick og boyd, 2011). Dette er ubehagelig å oppleve (**affektiv**), og unngås for enhver pris. Fra et slikt perspektiv fremstår det som at de unge navigerer skillet mellom offentlig og private sfærer, der personvern ikke er en viktig verdi for dem – men heller en utilsiktet bonus. Deres *kommunikative handlekraft* utøves slikt sett gjennom å bruke handlingsmulighetene til deres egen fordel og for å holde spenningene i sjakk. På denne måten 'sikrer' de seg for å ikke dele informasjon med folk som de ikke ønsker skal ha tilgang til den. Men de ser gjerne ikke behovet for et personvern, før kontekstene kollapser.

Uavhengig av hvor mye eller lite de to generasjonene sier at de bryr deg om privatliv - så er faktumet at dersom alt av personvern ble fjernet fra våre private sfærer, så hadde vi merket det. Et trygt digitalt miljø, er tross alt et miljø der brukerne kan *være seg selv*, uten å skulle engste seg for hvordan deres informasjon og innhold blir delt videre.

Holdningen fordreier hva personvern er (Boomers):

Datafisering, overvåkningskapitalisme og kritisk medieforståelse

Det å påstå at en ikke har noe å skjule, antyder videre at en har uklare oppfatninger om *hva* personvern egentlig innebærer. Informantene i denne studien argumenterte med at de ikke hadde noe å skjule, fordi de ikke hadde gjort noe kriminelt. Denne begrunnelsen reduserer imidlertid personvernet til noe som kun skal dekke over mørke hemmeligheter og kriminelle handlinger fra å bli avslørt (Richards, 2022). Denne oppfatningen vil implisitt si at dersom du er en ordinær, pliktoppfyllende og lovlydig borger – så trenger du egentlig ikke personvern. Dette overser i tillegg selve grunnlaget for *overvåkningskapitalismen* og hvorfor teknologiselskapene samler inn personopplysninger – nemlig for å kunne påvirke, manipulere eller utnytte brukerne (Zuboff, 2019).

Analysen viste at Boomer-informantene så ut til å undervurdere Meta sin datainnsamling, der flere hadde en oppfatning om at det var det de selv la ut av informasjon og innhold, som ble samlet inn (**kognitiv**). Deres *kritiske medieforståelse*, så dermed ut til å være noe lavere, enn det som kreves for å kunne navigere personvernet til et optimalt nivå. Dette kan i så fall forklare hvorfor de ikke utførte særlige tiltak for å styrke personvernet (**atferd**), og at de følte at de hadde en viss kontroll på informasjonen sin på Facebook (**affektiv**). Ikke nødvendigvis bare på grunnlag av de hadde lite informasjon tilgjengelig på profilen sin, men fordi at de ikke hadde forståelsen om hvordan den *usynlige informasjonsstrømmen* – med dens algoritmer og kunstige intelligens – samler inn personlig informasjon om *alt* de gjør på plattformene (Rasmussen, 2016; Kalsnes og Pettersen, 2019).

Våre liv er gjerne preget mer av *datafiseringen* enn vi muligens erkjenner. I teorikapittelet så vi at det var viktig for en borger i et demokratisk samfunn, å kunne tenke *selv* (Véliz, 2020; NOU 2022: 11; Richards, 2022). Dette innebar å kunne trekke seg tilbake med sine egne tanker. Å kunne lese, lære og planlegge det man ønsket - og å dele disse nye tankene med dem en ville (autonomi, integritet og ytringsfrihet). Et tankekors i denne sammenheng er at når vi lurert på noe – så *søker* vi det opp for å finne ut av det. Om det så gjelder nyheter, pavlova-opskrifter eller hva gamle ekskjærester holder på med. Når vi først leser eller lærer oss noe, så er dette som oftest på en smarttelefon, PC eller nettbrett. Siste del i denne tankerekken er at når vi først ønsker å dele ideene vi har lært om, så gjør vi det som regel over en telefonsamtale, på en melding eller i en statusoppdatering på SNS. Datafiseringen gjennomtrenger slikt sett mange sider ved våre hverdagslige vaner, og sier noe om viktigheten av å ha en kritisk medieforståelse

for å kunne trives og ferdes trygt i den digitale sfæren (Mejias og Couldry, 2019; Medietilsynet, 2021).

Holdningen er i institusjonenes favør (Generasjon Z):

Panoptikon, asymmetrisk makt og digital resignasjon

Tanken om at en ikke har noe å skjule, fordi en ikke er kriminell, vil også kunne overse *hvorfor* personvernet er viktig. Bakgrunnen for dette er at til tross for at medieteknologiene bringer med seg mye positivt, så er de imidlertid laget for å loggføre. Disse aktivitetsloggene består av persondata, som kan bli delt med andre (Mejias og Couldry, 2019). Problemet at brukerne sjelden vet *hvem* disse 'andre' er (selskaper, datameglere eller andre personer), *hvilken* informasjon de har, og *når* de samler det inn (NOU 2022: 11).

Mange av de unge informantene i studien uttrykket sine bekymringer og usikkerhet knyttet til dette. Flere blant Generasjon Z hevdet at hele situasjonen føltes ukontrollerbar, der de bar preg av maktesløshet (**affektiv**). Dette kan være en naturlig konsekvens av at de uttrykket en høyere kritisk medieforståelse – der de var klar over at mye informasjon ble samlet inn om dem (**kognitiv**). Samtidig var de ikke sikre på hva som egentlig skjedde med denne informasjonen. Flere av dem var derfor redde for å bli hacket og overvåket – der enkelte var skråsikre på at de ble avlyttet av mobilen. Dette kan enten bevisst eller ubevisst ført til en endring eller selvregulering av deres egen atferd. Sett i sammenheng med Foucault (1977) sine tanker om *panoptikon*, kan denne følelsen av at noen følger med på dem - uten at de vet helt *hvem* de er eller *når* de ser - være ubehagelig. Enkelte hevdet eksempelvis at de ikke turte å snakke om kontroversielle temaer med mobilen i nærheten, i frykt for at PST kom på døren (**atferd**). De unge informantenes bevissthet og maktesløshet knyttet til *datafiseringen*, kan nettopp gi en motivasjon i seg selv for å gjøre tiltak for å styrke personvernet. Slik som å ha en privat konto for de nærmeste vennene, blokkere uvedkommende og generelt utøve en selvregulering av hvilket innhold de legger ut.

Slik jeg tolker det, kan holdningen om at «jeg ikke har noe å skjule» nettopp eksemplifisere effekten den *asymmetriske makten* mellom brukeren og teknologiselskapene - i tråd med betydningen av panoptikon (Foucault, 1977; Zuboff, 2019). Meta bryr seg nødvendigvis ikke om *hvor* mørke eller banale våre hemmeligheter er – de ønsker 'bare' å vite om dem. Denne asymmetriske, eller skjevt fordelte makten, om at de store selskapene og institusjonene vet alt om oss, men vi vet lite til ingenting om dem – kan igjen forsterke følelsen av maktesløshet og

digital resignasjon (Draper og Turow, 2019). Alt henger slik sett sammen. Det at brukerne tenker at de ikke har noe å skjule, har selskapene derfor alt å vinne på - da de trolig ikke kommer til å møte på motstand for å utvinne mer persondata med en slik holdning. For de har jo nettopp ingenting å skjule. Klisjéen viser seg i at kunnskap (om menneskers liv) er *makt* (Richards, 2022, s. 8). Personvern er en måte å balansere ut dette maktforholdet.

Se bare for deg en digital sfære der det ikke er nødvendig med verken en høy kritisk medieforståelse eller en høy kommunikativ handlekraft for å kunne oppnå et ideelt personvern – men at dette var *bygget inn* i plattformene. Der brukere på tvers av alle generasjoner, evner og kompetanse kunne ha en trygg tilstedeværelse. At brukeren, trengte bare å *bruke*. Ikke bekymre seg, for om denne bruken førte til noe annet lugubert. Dette er noe av hensikten med å regulere teknologiselskapene, slik at de ikke utnytter sin posisjon, men 'tvinger dem' til å tilrettelegge for fellesskapet.

Holdningen undervurderer personvernets betydning:

Instrumentell verdi, individuelle- og kollektive goder

Holdningen om at «*jeg ikke har noe å skjule*», kan indikere at personvernet kun er verdifullt for enkeltpersoner - og at dette blir helt vilkårlig styrt av individuelle preferanser. Dersom man ikke bryr seg, så har det ingenting å si. Selv om personvern har en viktig *individuell* verdi, som gir en beskyttelse av våre private sfærer – så vi imidlertid i teorien at Moor (1997) knytter flere typer verdier til personvernet, i form av at det fører til andre *kollektive* goder for samfunnet. Slik som å beskytte oss fra maktmisbruk og diskriminering (Véliz, 2020). Personvern er slikt sett en viktig brikke i det demokratiske systemet. Edward Snowden (2020) har hevdet at «hvis du sier at du ikke bryr deg om privatlivet fordi du ikke har noe å skjule, så tilsvarer det at jeg ikke bryr meg om ytringsfrihet, fordi jeg ikke har noe å si».

I introduksjonen ble det for øvrig nevnt at Personvernkommisjonens nye utredning (NOU 2022: 11, s. 9) ønsket at diskusjoner om personvern burde gjøres relevant for det norske samfunnet som helhet – ikke bare et tema som noen få eksperter kan forstå. Noe av grunnen til dette er at personvern berører oss *alle*. Vi er alle sammenkoblet (Véliz, 2020). Samtidig kan det se ut til at mange brukere resignerer, og tenker at personvernet er en tapt sak (Draper og Turow, 2019; Datatilsynet, 2020). Det kan derfor virke håpløst å skulle innføre personvern som en *kjerneverdi* i samfunnet vårt. Noe som innebærer at personvern blir noe som grunnleggende og verdsatt i seg selv (Moor, 1997).

Samtidig utvikles vår identitet og holdninger gjennom livet, ved at vi tilegner oss nye erfaringer (Pickens, 2005). For å endre brukernes holdninger til personvern, må vi se på *hvor* endringen trenger å oppstå – i det *kognitive, atferdsmessige* eller *affektive*. Gjennom å utforske personvernsholdningene gjennom tre-komponentmodellen, har det vært viktig å se de to ulike generasjonene i deres *kontekst* med den kunnskapen, atferd og følelser som de besitter. Dette innebar å ta i betraktning at de ulike generasjonene har vært preget av ulike samfunnsverdier, normer og tilgang på medieteknologi (Twenge, 2023). Boomerne vokste opp i en tid før internett og sosiale nettverkstjenester. De har dermed *opplevd* en tid der det var et tydeligere skille mellom offentlig og privat. En tid der medier, teknologi og identitet i større grad var adskilt.

Generasjon Z har på sin side vokst opp i et digitalisert samfunn, hvor disse skillene har vært overlappende, uklare – og til tider ikke-eksisterende. De kjenner ikke til noe annet. I analysen, så vi at enkelte etterspurte mer informasjon om hva et godt privatliv er, og hva det har som effekt. Dette er helt grunnleggende. For hvorfor prioritere personvern, dersom de ikke har forståelse for *hva* det beskytter? Med andre ord kan selskaper slik som Meta, fylle nettsidene til randen med informasjon om personvern. Men dersom mottakerne av denne informasjonen (brukerne) ikke forstår verdien av det som skal beskyttes (privat informasjon), så vil personvernskalkuleringene kunne helle mot at SNS ikke er så inngripende, som det i realiteten kan være.

Verdien i seg selv, av å *erfare* hva et privatliv er, kan dermed ha gått tapt i den altomfattende datafiseringsen av våre liv. Grunnen til at personvern har vært utfordrende å innarbeide som en viktig verdi i samfunnet, kan være så enkelt som at kunnskapen om hva et *godt privatliv* er – har gått tapt – og de som har denne kunnskapen, tar den for gitt. Men det de ikke vet, kan de ikke gjøre noe med. Det blir derfor avgjørende å koble sammen kunnskap om personvern med forståelsen av et godt privatliv, for å dekke igjen dette gapet. Slikt sett er det ikke rart, at mange hevder at de ikke har noe å skjule. Samtidig så bør vi mulig snu det om på hodet, og spørre – hva trenger vi å verne?

8.2 Konklusjon

Nå er det tid for å samle trådene, og oppsummere det viktigste. Denne kvalitative studien har utforsket *hvilke holdninger som ulike generasjoner har til personvern i sosiale nettverkstjenester*. Det empiriske datamaterialet er basert på tolv forskningsintervjuer, inkludert en tenke høyt-øvelse, med informanter tilhørende det vi her omtaler som, Boomer-generasjonen (57-67 år) og Generasjon Z (15-25 år). For å kunne besvare forskningsspørsmålet, ble det tatt utgangspunkt i tre analyse spørsmål (AS), inspirert av *tre-komponentmodellen*, for å operasjonalisere holdningsbegrepet i mer håndfaste dimensjoner: kognitiv, atferd og affektiv (Rosenberg og Hovland, 1960; Pickens, 2005). I korte trekk innebar dette å utforske og sammenligne hvordan de to generasjonene tenker, handler og føler som sitt personvern på Facebook og Instagram (Meta).

De lange linjene kan tyde på at det rører seg en del misforståelser om hva personvern er og hvorfor det er viktig. Informantene i denne studien overser i større grad at personvernet er noe som kan bidra til kollektive gevinster for samfunnet. Det første analyse spørsmålet (AS1) berørte imidlertid den *kognitive* holdningskomponenten, og ønsket å besvare hvordan Boomers *forstår* personvern i forhold til Generasjon Z. Her så vi at den overordnede kunnskapen om personvern viste seg å være lav – både med tanke på hvordan de forstod personvernsbegrepet og om de hadde kjennskap til GDPR. Samtidig mente nesten samtlige Boomere at privatlivet er viktig og noe som burde beskyttes. Flere hadde også en oppfatning om at det var det de selv la ut av informasjon, som ble innsamlet av Meta. Generasjon Z mente derimot at privatliv ikke var så nøye, men uttrykket imidlertid en høyere kritisk medieforståelse for omfanget av Meta sin datainnsamling. Privatlivsparadokset ser dermed ut til å sprike mer blant de eldre, enn de yngre informantene. Ellers fremstår det som at informantene, uavhengig av generasjon, har blitt mer bevisst på personvern på SNS over tid. Flere er eksempelvis mer skeptisk til å legge folk til i nettverket sitt nå, enn før. Informantene viste også en fremtredende tendens til selvrettferdiggjøring om bruk av SNS, der nesten samtlige hevder at de ikke har noe å skjule.

Det andre analyse spørsmålet (AS2) dreide seg om atferdskomponenten, og belyste hvordan Boomere *handler* når det kommer til personvernet på Meta, i forhold til Generasjon Z. Her ble det introdusert tre selvlagde begreper. Når det kom til *periodiske personvernshandlinger*, var det kun et fåtall som har sett på personvernserklæringen siden de begynte å bruke SNS. Ellers viste det seg at de fleste Boomere trykker direkte på «Godta», når de blir bedt om å velge informasjonskapsler. Blant Generasjon Z, var det flere som hevdet at de tilpasset

alternativene, men kunne i noen tilfeller føle på at det ikke hadde en reell effekt. Angående informantenes *statiske personvernshandlinger*, så opplever mange av Boomerne at personvernsinnstillingene er innviklet, og flere tyr til hjelp fra andre for å stille dem inn. Under tenke høyt-øvelsen slet også flere med å finne frem til innstillingene, noe skapte frustrasjon hos enkelte. Generasjon Z fant derimot fort frem til personvernsinnstillingene under øvelsen, men flere ble overasket over hvordan innstillingene deres var. Generelt undervurderte de fleste informantene sitt faktiske publikum på Meta. I forbindelse med *dynamiske personvernshandlinger*, nevnte flere av Boomerne at de var mest aktive i private Facebook-grupper og Generasjon Z hadde de fleste flere Instagram-kontoer for ulike formål. Alle informantene uttrykte at de selvsensurerte seg i ulik grad, for å opprettholde ønsket selvrepresentasjon. Det var også en oppfatning om at den eldre generasjonen delte mye og til tider irrelevant innhold, mens den yngre generasjonen publiserte sjeldnere, men i mer planlagte kontekster. Dette ble illustrert gjennom en analogi til dagbok og fotoalbum. Generasjon Z viste til en generelt høyere kommunikativ handlingskraft, enn Boomer-generasjonen.

Det tredje og siste analysespørsmålet (AS3) tok for seg den *affektive* komponenten, og utforsket hvordan Boomerne følte om personvernet på Meta, i forhold til Generasjon Z. Her ble det løftet frem ulike aspekter knyttet til det *institusjonelle*- og det *sosiale* personvernet på Meta (Raynes-Goldie, 2010). Når det kom til det institusjonelle personvernet, var det flere Boomere som følte på en viss kontroll over egen informasjon på Meta - men få så imidlertid ut til å være bevisst over den *usynlige informasjonsstrømmen* (Rasmussen, 2016). Nesten alle i Generasjon Z følte at de ikke hadde kontroll over egen informasjon, der flere uttrykte maktesløshet, og derav *digital resignasjon*. Angående følelser knyttet til det sosiale personvernet, løftes det frem en rekke hendelser som analyseres i tråd med Nissenbaum (2010) sitt rammeverk for *kontekstuell integritet*. Herunder kjenner alle noen som har blitt kontokapret den siste tiden, og bidrar til følelser av frykt og usikkerhet. Når det kommer til publisering av bilder uten samtykke, har de færreste av Boomers opplevde dette. Generasjon Z, hevder imidlertid at dette oppstår på jevnlig basis, spesielt i sosiale lag. Det er også en utbredt bekymring knyttet til barns personvern. Følelser av ubehag, sinne, frustrasjon og angst knyttes til slike kontekstuelle personvernbrudd. Alle opplever at normen er å ikke spørre før man publiserer, samtidig hevder samtlige at de spør andre.

Om det er noe som kan konkluderes i denne studien, så er det at personvern er et komplekst fenomen. Det brer seg over en rekke fagfelt, der det regjerer uenigheter om hvordan begrepet

skal forstås, tolkes og anvendes. Samtidig er det også et fenomen som berører så mange deler av vår egen hverdag. Denne studien har dermed identifisert noen kunnskapshull. For å tette disse igjen, kreves det en bedre forståelse for hva et personvern er og hvilken funksjon det har. Som vi så i delkapittelet over, kan holdningen om at «vi ikke har noe å skjule» sette noen kjepper i hjulet for denne utviklingen. Hvordan vi definerer personvern og privatliv vil derfor ha noe å si - fordi det kan påvirke hvordan vi snakker om det og er med på å farge våre holdninger til det. Det er kanskje der vi må starte. Her stiller jeg meg dermed bak Personvernkommissjonens ønske om at personvern bør anerkjennes og vurderes positivt for sin grunnleggende verdi (NOU 2022: 11). Personvern må altså betraktes både som et *individuell* gode og noe som *kollektivt* tjener hele samfunnet. På denne måten kan personvern få den statusen den fortjener og behøver.

8.3 Veien videre

Det er ikke til å komme unna at personvern vil bli et viktig grep for den fremtidige utviklingen av medieteknologi. Dette innebærer også at det er mange felt som bør kartlegges i forhold til personvernsholdninger. Nå er det slik at denne studien er liten av størrelse, og fokuserer kun på to generasjoner. Det kan derfor være interessant å gjennomføre dette forskningsdesignet med et større utvalg, som også inkluderer andre plattformer og generasjoner – spesielt Generasjon Alfa (-2010), som nå vokser frem med sine egne preferanser til digital kommunikasjon og selvavsløring. Det bør også vurderes å benyttes etnografiske metoder, som kan bidra til større innsikt i brukerens kognitive prosesser, når det kommer til hvordan de vurderer personvernet på digitale tjenester. Personvernsinnstillingenes grensesnitt vil herunder være viktig å utvikle på brukernes vilkår. At det er lett for dem å finne frem og å stille inn, når de kjenner behov for det. Spesielt med tanke på eldre brukere.

Det er imidlertid flere faktorer som ikke har blitt fokusert på i denne studien, men som i ettertid virker interessant å gå i dybden på. Dette er gjelder først og fremst utvalgsfaktorer knyttet til sosiale ulikheter, slik som klasse og kulturell bakgrunn. I større grad sårbare eller marginaliserte grupper, slik som LGBTQ+-samfunnet vil også være interessant å se på – da de kan ha mer å tape på et dårlig personvern. Sosioøkonomiske faktorer var også noe jeg med ettertanke, ville ha inkorporert i større grad. Det å se på familier - gjerne i foreldre-barn-relasjon - vil i tillegg kunne bidra til en bedre forståelse av eksisterende holdninger knyttet til personvern og tingenes internett. Vi trenger å vite mer om hvordan barn opplever at foreldrene sporer dem, eksempelvis

gjennom smartklokker eller Snapmap. Bare de siste månedene har det også blitt en massiv utbredelse av kunstig intelligens (KI), som har blitt tilgjengeliggjort for brukermarkedet. Tjenester slik som ChatGPT og Bing vil kunne skape store debatter rundt personvern og hvordan personvernet skal håndteres i praksis. Det samme gjelder produsering og spredning av deepfakes, som krenker både personvern og opphavsretten. Hvordan brukerne opplever dette, bør settes på dagsorden i forskningssammenheng.

Veien videre på personvernsfeltet vil være vanskelig å forutse – men det er mye å ta av. Det vil imidlertid være sentralt å finne gode rammeverk for å studere brukeres personvernsholdninger, og at det må jobbes med defineringsen av hva personvern egentlig er. Så lenge vi snakker om ulike meningsinnhold på tvers av hverandre, vil forskningsfeltet fortsette å sprike.

Referanser

- Aalen, I. og Hoem Iversen, M. (2021) *Sosiale Medier*. 2. utg. Bergen: Fagbokforlaget.
- Acquisti, A., Taylor, C. og Wagman, L. (2016) The Economics of Privacy, *Journal of Economic Literature*, 54(2), s. 442–492.
- Aguirre, X., Woodward, B. og Martin, N. (2018) Perception of Privacy Through Generations, *Issues In Information Systems*, 19(1), s. 83–90.
- Ajzen, I. og Fishbein, M. (1977) Attitude-behavior relations: A theoretical analysis and review of empirical research, *Psychological Bulletin*, 84(5), s. 888.
- Allport, G.W. (1935) Attitudes, i C. Murchison (red.) *Handbook of social psychology*. Worcester: Clark University Press, s. 798–844.
- Altman, I. (1975) *The Environment and Social behaviour: Privacy, Personal Space, Territory Crowding*. California: Brooks/Cole Publishing Company.
- Archibald, M.M. *et al.* (2019) Using Zoom Videoconferencing for Qualitative Data Collection: Perceptions and Experiences of Researchers and Participants, *International Journal of Qualitative Methods*, 18, s. 1-8. Hentet fra: <https://doi.org/10.1177/1609406919874596>.
- Arendt, H. (1958) *The Human Condition*. Chicago: University of Chicago Press.
- Arnett, J.J. (2000) Emerging adulthood: A theory of development from the late teens through the twenties., *American Psychologist*, 55(5), s. 469–480. Available at: <https://doi.org/10.1037/0003-066X.55.5.469>.
- Barnes, S.B. (2006) A privacy paradox: social networking in the United States, *First Monday*, 11(9). Hentet fra: <http://firstmonday.org/article/view/1394/1312>.
- Barth, S. og de Jong, M.D.T. (2017) The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, 34(7), s. 1038–1058.
- Bodoni, S. (2023) Meta Fined €390 Million, Ordered to Change Way It Processes Ads, *Bloomberg.com*, 04.01.2023. Hentet fra: <https://www.bloomberg.com/news/articles/2023-01-04/meta-fined-390-million-ordered-to-change-way-it-processes-ads> (Accessed: 1 May 2023).
- boyd, d. (2010) Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications, i Z. Papacharissi (red.) *A Networked Self*. Routledge, s. 39–57. Hentet fra: <https://doi.org/10.4324/9780203876527-8>.
- Brandeis, L.D. og Warren, S.D. (1890) The right to privacy, *Harvard Law Review*, 4(5), s. 193–220.
- Brandtzaeg, P.B. og Chaparro-Domínguez, M.-Á. (2020) From Youthful Experimentation to Professional Identity: Understanding Identity Transitions in Social Media, *YOUNG*, 28(2), s. 157–174. Hentet fra: <https://doi.org/10.1177/1103308819834386>.
- Braun, V. og Clarke, V. (2006) Using thematic analysis in psychology, *Qualitative Research in Psychology*, 3(2), s. 77–101. Hentet fra: <https://doi.org/10.1191/1478088706qp063oa>.
- Breckler, S.J. (1984) Empirical Validation of Affect, Behavior, and Cognition as Distinct Components of Attitude, *Journal of Personality and Social Psychology*, 47(6), s. 1191–1205.
- Bucher, T. (2012) ‘Want to be on the top? Algorithmic power and the threat of invisibility on Facebook’, *New Media & Society*, 14(7), s. 1164–1180. Hentet fra: <https://doi.org/10.1177/1461444812440159>.
- Bucher, T. (2021) *Facebook*. Medford: Polity Press. Hentet fra: <https://www.google.no/books/edition/Facebook/10QsEAAAQBAJ?hl=no&gbpv=1&dq=bucher+Facebook&printsec=frontcover>.
- Buckingham, D. og Willett, R. (2013) *Digital Generations: Children, Young People, and the New Media*. Routledge.
- Cadwalladr, C. og Graham-Harrison, E. (2018) Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, *The Guardian*, 17.03. Hentet fra: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.
- Campbell, W.K. *et al.* (2015) Generational Differences Are Real and Useful, *Industrial and Organizational Psychology*, 8(3), pp. 324–331. Hentet fra: <https://doi.org/10.1017/iop.2015.43>.
- Charters, E. (2003) ‘The Use of Think-aloud Methods in Qualitative Research An Introduction to Think-aloud

- Methods', *Brock Education Journal*, 12(2). Hentet fra: <https://doi.org/10.26522/brocked.v12i2.38>.
- Cho, A. (2018) 'Default publicness: Queer youth of color, social media, and being outed by the machine', *New Media & Society*, 20(9), pp. 3183–3200. Hentet fra: <https://doi.org/10.1177/1461444817744784>.
- Datatilsynet (2014) *Personvern - Tilstand og Trender*. Oslo: Datatilsynet.
- Datatilsynet (2019a) *Hva er personvern?* Hentet fra: <https://www.datatilsynet.no/rettigheter-og-plikter/hva-er-personvern/>.
- Datatilsynet (2019b) *Personopplysninger*, *Datatilsynet*. Hentet fra: <https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/>
- Datatilsynet (2020) *Personvernundersøkelsen 2019/2020 - Om befolkningens holdninger til personvern og kjennskap til det nye personvernregelverket*. Oslo: Datatilsynet.
- Datatilsynet (2022) *Samtykke fra mindreårige*, *Datatilsynet*. Hentet fra: <https://www.datatilsynet.no/personvern-pa-ulike-omrader/skole-barn-unge/samtykkje-fra-mindreareige/>
- Dhir, A. et al. (2017) Do Online Privacy Concerns Predict Selfie Behavior among Adolescents, Young Adults and Adults?, *Frontiers in Psychology*, 8, s. 815. Available at: <https://doi.org/10.3389/fpsyg.2017.00815>.
- Dienlin, T. og Metzger, M.J. (2016) An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample: The Extended Privacy Calculus Model For SNSs', *Journal of Computer-Mediated Communication*, 21(5), s. 368–383. Hentet fra: <https://doi.org/10.1111/jcc4.12163>.
- Dinev, T. og Hart, P. (2006) An Extended Privacy Calculus Model for E-Commerce Transactions, *Information Systems Research* [Preprint]. Hentet fra: <https://doi.org/10.1287/isre.1060.0080>.
- Draper, N.A. (2017) From Privacy Pragmatist to Privacy Resigned: Challenging Narratives of Rational Choice in Digital Privacy Debates: Challenging Rational Choice in Digital Privacy Debates, *Policy & Internet*, 9(2), s. 232–251. Hentet fra: <https://doi.org/10.1002/poi3.142>.
- Draper, N.A. og Turow, J. (2019) The corporate cultivation of digital resignation, *New Media & Society*, 21(8), s. 1824–1839. Hentet fra: <https://doi.org/10.1177/1461444819833331>.
- Eiser, J.R. (1986) *Social Psychology: Attitudes, Cognition and Social Behaviour*. Cambridge University Press.
- Ellison, N.B. og Boyd, D.M. (2013) *Sociality Through Social Network Sites*, i W.H. Dutton (red.). Oxford University Press. Hentet fra: <https://doi.org/10.1093/oxfordhb/9780199589074.013.0008>.
- Elueze, I. og Quan-Haase, A. (2018) Privacy Attitudes and Concerns in the Digital Lives of Older Adults: Westin's Privacy Attitude Typology Revisited, *American Behavioral Scientist*, 62(10), s. 1372–1391. Hentet fra: <https://doi.org/10.1177/0002764218787026>.
- Evans, D.S. og Schmalensee, R. (2016) *Matchmakers: the new economics of multisided platforms*. Boston: Harvard Business Review Press.
- Fosse, A.L. (2022) *Norge på verstingliste: Bare Kuwait er verre*, *Nettavisen*. Hentet 22.04.23 fra: <https://www.nettavisen.no/5-95-572294>
- Foucault, M. (1977) *Discipline & Punish*. New York: Knopf Doubleday Publishing Group.
- Gårseth-Nesbakk, L. (2022) 'sunk cost', *Store norske leksikon*. Hentet 03.05.2023 fra: https://snl.no/sunk_cost
- Gentikow, B. (2019) *Hvordan utforsker man medieerfaringer? - Kvalitativ Metode*. Oslo: Cappelen Damm Akademisk.
- Gentikow, B. og Østbye, H. (2009) Kartlegging av et felt, i B. Gentikow (red.) *Medievitenskap - Mediebruk*. 2. Utg. Bergen: Fagbokforlaget, s. 13–28.
- Giddens, A. (1991) *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Stanford University Press.
- Gilbert, B. (2019) *There's a wildly popular conspiracy theory that Facebook listens to your private phone calls, and no matter what the tech giant says, people just aren't convinced it's not true*, *Business Insider*. Tilgjengelig fra: <https://www.businessinsider.com/facebook-ads-listening-to-you-2019-5> (Hentet: 03.05.2023).
- Goffman, E. (1959) *The Presentation of Self in Everyday Life*. Garden City, NY: Doubleday.
- Gripsrud, J. (2017) Idealer, realiteter og tilfellet Norge, i Gripsrud, J. (red.) *Allmenningen - Historien om norsk offentlighet*. Oslo: Universitetsforlaget, s. 15–51.
- Grunnloven. *Lov 17.05.1814 nr. 102 om Menneskeretter*
- Habermas, J. (1991) *Borgerlig offentlighet*. Oslo: Gyldendal.
- Hampton, K. et al. (2014) *Social Media and the Spiral of Silence*. Pew Research Center.

- Hareide, D. (2021) *Mennesket og Teknomaktene*. Oslo: Aschehaug.
- Hargittai, E. og Marwick, A. (2016) “What Can I Really Do?” Explaining the Privacy Paradox with Online Apathy, *International Journal of Communication*, 10, s. 3737-3757
- Hogan, B. (2010) The Presentation of Self in the Age of Social Media: Distinguishing Performances and Exhibitions Online, *Bulletin of Science, Technology & Society*, 30(6), s. 377–386. Hentet fra: <https://doi.org/10.1177/0270467610385893>.
- Igo, S.E. (2018) *The Known Citizen : a history of privacy in modern America*. Cambridge, Massachusetts: Harvard Unieversity Press.
- Ipsos (2023) *Ipsos SoMe-tracker Q1 '23*. Hentet 12.05.23 fra: <https://www.ipsos.com/nb-no/ipsos-some-tracker-q123>.
- Johannessen, L.E., Rafoss, T.W. og Rasmussen, E.B. (2018) *Hvordan bruke teori? Nyttige verktøy i kvalitativ analyse*. Oslo: Universitetsforlaget.
- Kalsnes, B. og Pettersen, L. (2019) Algoritmer, analysedata og automatisering i det digitale medielandskapet – en avkledningsmanøver, *Norsk medietidsskrift*, 26(1), s. 1–10. Hentet fra: : <https://doi.org/10.18261/ISSN.0805-9535-2019-01-01>.
- Kalsnes, B. (2019) *Falske Nyheter - Løgn, desinformasjon og propaganda i den digitale offentligheten*. Oslo: Cappelen Damm Akademisk.
- Kennair, L.E.O. (2022) atferd, *Store norske leksikon*. Hentet 05.05.2023 fra: <https://snl.no/atferd>.
- Kjøll, G. og Tranøy, K.E. (2023) kognitiv, *Store norske leksikon*. Hentet 02.05.23 fra: <https://snl.no/kognitiv>
- Kokolakis, S. (2017) Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon, *Computers & Security*, 64, pp. 122–134. Hentet fra: <https://doi.org/10.1016/j.cose.2015.07.002>.
- KR&I (2022) *Global Perceptions of Privacy Research Report - Global KR&I study commissioned by Snap Inc.* Kresnicka Research & Insights. Hentet fra: https://assets.ctfassets.net/inb32lme5009/6rLa031mhNu3SOxCz4nQn8/272a8f9b92b9f979d18f2a370e28623/Snap_Inc_Privacy_Research_2022.pdf.
- Kulbrandstad, I. (2022) *Mange opplever å miste kontroll over sin Facebook eller Instagram-konto: Slik sikrer du deg*, NRK. Hentet 04.05.2023 fra: https://www.nrk.no/tromsogfinnmark/mange-opplever-a-miste-kontroll-over-sin-facebook-eller-instagram-konto_-slik-sikrer-du-deg-1.16235557
- Kvale, S. (2001) *Det kvalitative forskningsintervju*. Oslo: ad Notam, Gyldendal.
- Kvale, S. og Brinkmann, S. (2009) *InterViews: Learning the Craft of Qualitative Research Interviewing*. SAGE.
- Kvalnes, Ø. (2010) *Det personlige rom*, *Aftenposten*. Hentet 22.04.23 fra: <https://www.aftenposten.no/meninger/kronikk/i/oAlg7/det-personlige-rom>.
- Lervik, F. (2018) *Eldre-boom på sosiale medier*, *adressa.no*. Tilgjengelig fra: <https://www.adressa.no/nyheter/i/V1vA2V/eldre-boom-pa-sosiale-medier> (Hentet: 17.04.2023).
- Lomborg, S. og Mortensen, M. (2017) Users across media: An introduction, *Convergence: The International Journal of Research into New Media Technologies*, 23(4), s. 343–351. Hentet fra: <https://doi.org/10.1177/1354856517700555>.
- Madden, M. og Smith, A. (2010) *Reputation Management and Social Media - How people monitor their identity and search for others online*. Washington: Pew Internet & American Life Project.
- Marder, B. et al. (2016) ‘The extended “chilling” effect of Facebook: The cold reality of ubiquitous social networking’, *Computers in Human Behavior*, 60, s. 582–592. Hentet fra: <https://doi.org/10.1016/j.chb.2016.02.097>.
- Marwick, A. og Hargittai, E. (2019) Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online, *Information, Communication & Society*, 22(12), s. 1697–1713. Available at: <https://doi.org/10.1080/1369118X.2018.1450432>.
- Marwick, A.E. og boyd, d. (2011) ‘I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience’, *New Media & Society*, 13(1), s. 114–133. Hentet fra: <https://doi.org/10.1177/1461444810365313>.
- Marwick, A.E. og boyd, d. (2014) ‘Networked privacy: How teenagers negotiate context in social media’, *New Media & Society*, 16(7), s. 1051–1067. Hentet fra: <https://doi.org/10.1177/1461444814543995>.
- Masur, P.K. og Scharrow, M. (2016) Disclosure Management on Social Network Sites: Individual Privacy

- Perceptions and User-Directed Privacy Strategies, *Social Media + Society*, 2(1), s. 1-13. Hentet fra: <https://doi.org/10.1177/2056305116634368>.
- Mathieu, D. og Vengerfeldt, P.P. (2020) The data loop of media and audience, *Mediekultur*, 36(69), s. 116–138.
- Medietilsynet (2021) *Kritisk medieforståing i den norske befolkninga - 2021*. Hovudrapport. Fredrikstad: Medietilsynet.
- Mejias, U.A. og Couldry, N. (2019) Datafication, *Internet Policy Review*, 8(4).
- Menneskerettsloven. *Lov 21.05.1999 art. 8* om Retten til privatliv og familieliv.
- Moor, J.H. (1997) Towards a theory of privacy in the information age, *ACM SIGCAS Computers and Society*, 27(3), s. 27–32. Hentet fra: <https://doi.org/10.1145/270858.270866>.
- Nagell, H. (2020) *Digital Revolusjon - Hvordan ta makten og friheten tilbake*. Oslo: Res Republica.
- Nettvett (2016) Sikkerhet i sosiale medier, *Nettvett.no*, Tilgjengelig fra: <https://nettvett.no/sikkerhet-i-sosiale-medier/> (Hentet: 04.05 2023).
- Nissenbaum, H. (1998) 'Protecting Privacy in an Information Age: The Problem of Privacy in Publici', *Law and Philosophy*, (17), s. 559–596.
- Nissenbaum, H. (2010) *Privacy in context - Technology, Policy, and the Integrity of Social Life*. Stanford, California: Stanford University Press.
- NOU 2009: 1. *Individ og integritet: personvern i det digitale samfunnet*.
- NOU 2022: 9. *En åpen og opplyst offentlig samtale*.
- NOU 2022: 11. *Ditt personvern - vårt felles ansvar. Tid for en personvernspolitikk*.
- Palen, L. og Dourish, P. (2003) Unpacking "Privacy" for a Networked World, *New Horizons*, (5).
- Park, Y.J. (2013) Digital Literacy and Privacy Behavior Online, *Communication Research*, 40(2), s. 215–236. Hentet fra: <https://doi.org/10.1177/0093650211418338>.
- Pew Research Center (2019) *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*.
- Pickens, J. (2005) Attitudes and Perceptions, i *Organizational behavior in health care*, s. 43–76.
- Quan-Haase, A. et al. (2018) Dividing the Grey Divide: Deconstructing Myths About Older Adults' Online Activities, Skills, and Attitudes, *American Behavioral Scientist*, 62(9), s. 1207–1228. Tilgjengelig fra: <https://doi.org/10.1177/0002764218777572>.
- Rasmussen, T. (2016) *Hva skjer med internett og web?* Oslo: Cappelen Damm Akademisk.
- Raynes-Goldie, K. (2010) Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook, *First Monday* [Preprint]. Tilgjengelig fra: <https://doi.org/10.5210/fm.v15i1.2775>.
- Resvoll, A. (2023) *Meta jekker opp forventningene – bykser i etterhandelen, E24*. Tilgjengelig fra: <https://e24.no/i/P4emq5> (Hentet: 01.05.2023).
- Richards, N. (2022) *Why Privacy Matters*. New York: Oxford University Press.
- Ritvo, E. (2012) *Facebook and Your Brain - The inside dope on Facebook, Psychology Today*. Tilgjengelig fra: <https://www.psychologytoday.com/intl/blog/vitality/201205/facebook-and-your-brain> (Hentet: 12.05.2023)
- Rosenberg, M.J. og Hovland, C.I. (1960) Cognitive, affective, and behavioral components of attitude, i McGuire, W.J. (red) *Attitude Organization and Change: An Analysis of Consistency among Attitude Components*. Yale University Press, s. 1–14.
- Rossen, E. (2021) Informasjonskapsel, *Store norske leksikon*. Tilgjengelig fra: <https://snl.no/informasjonskapsel> (Hentet: 03.05.2023).
- Schartum, D.W. (2020) *Personvernforordningen - En lærebok*. Bergen: Fagbokforlaget.
- Schröder, K. et al. (2003) *Researching Audiences*. London: Hodder Arnold.
- Snowden, E. (2020) *Systemfeil*. Oversatt av Stokseth, L. Oslo: Aschehaug & Co.
- Solvang, T.M. (2018) *Kina med kontroversiell masseovervåking: – Kan påvirke andre lands suverenitet, NRK*. Tilgjengelig fra: https://www.nrk.no/urix/kina-med-kontroversiell-masseovervaking_-_kan-pavirke-andre-lands-suverenitet-1.14103605 (Hentet: 14.05.2023).
- Someren, M., Barnard, Y. og Sandberg, J. (1994) *The think aloud method: A practical guide to modelling cognitive processes*. London: Academic Press. Tilgjengelig fra: <https://linkinghub.elsevier.com/retrieve/pii/0306457395900314>.
- St. John, A. (2018) *How Facebook Tracks You, Even When You're Not on Facebook, Consumer Reports*.

- Tilgjengelig fra: <https://www.consumerreports.org/privacy/how-facebook-tracks-you-even-when-youre-not-on-facebook-a7977954071/> (Hentet: 06.05.2023).
- Svartdal, F. (2020) emosjon, *Store norske leksikon*. Tilgjengelig fra: <https://snl.no/emosjon> (Hentet: 02.05.2023).
- Svartdal, F. (2023) kognitiv dissonans, *Store norske leksikon*. Tilgjengelig fra: https://snl.no/kognitiv_dissonans (Hentet: 13.05.2023).
- Svendsen, L. (2014) *Hvorfor personvern?*, *Civita - Den Liberale Tankesmien*. Tilgjengelig fra: <https://civita.no/politisk-filosofi-og-idedebatt/hvorfor-personvern-2/>.
- Swart, J. (2021) Experiencing Algorithms: How Young People Understand, Feel About, and Engage With Algorithmic News Selection on Social Media, *Social Media + Society*, 7(2), s.1-11. Tilgjengelig fra: <https://doi.org/10.1177/20563051211008828>.
- Tjora, A. (2017) *Kvalitative forskningsmetoder i praksis*. 3. Utg. Oslo: Gyldendal Akademisk.
- Twenge, J.M. (2023) *Generations: The Real Differences Between Gen Z, Millennials, Gen X, Boomers, and Silents—and What They Mean for America’s Future*. Simon and Schuster. Hentet fra: https://books.google.no/books?id=UCS2EAAAQBAJ&printsec=frontcover&hl=no&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
- Véliz, C. (2020) *Privacy Is Power - Why and how you should take back control of your data*. London: Penguin Random House.
- Vitak, J. og Kim, J. (2014) “‘You can’t block people offline’: examining how facebook’s affordances shape the disclosure process”, in *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing. CSCW’14: Computer Supported Cooperative Work*, Baltimore Maryland USA: ACM, s. 461–474. Tilgjengelig fra: <https://doi.org/10.1145/2531602.2531672>.
- Wessel-Aas, J. og Ødegaard, M. (2018) *Personvern - Publisering og Behandling av personopplysninger*. Oslo: Gyldendal.
- Westin, A. (1967) *Privacy and Freedom*. New York: Atheneum Publishers.
- Ytre-Arne, B. og Das, R. (2020) Audiences’ Communicative Agency in a Datafied Age: Interpretative, Relational and Increasingly Prospective, *Communication Theory*, 31(4), s. 779–797. Tilgjengelig fra: <https://doi.org/10.1093/ct/qtaa018>.
- Zuboff, S. (2019) *The Age of Surveillance Capitalism - The fight for a human future at the new frontier of power*. London: Profile Books Ltd.
- Østbye, H. et al. (2013) *Metodebok for Mediefag*. 4. Utg. Bergen: Fagbokforlaget.

Vedlegg 1 – Intervjuguide

Gå gjennom samtykkeskjema og sikre at informanten vet at den anonymiseres i masteroppgaven. Informanten gir sitt samtykke. Start lydopptak.

Del 1: Generell bakgrunn	Alder, bosted, jobb/studier, utdanning, fritid, forhold til teknologi.
Del 2: Bruk av sosiale medier (Affordances/Agency)	<ol style="list-style-type: none">1) Kan du fortelle hvilke sosiale medier du bruker til vanlig? <i>Eksempelvis i løpet av en uke.</i> (Hvor ofte bruker du Instagram og Facebook)2) Husker du når du begynte å bruke sosiale medier? (Hvordan synes du dette har endret seg siden du begynte?)3) Fordeler: Hva liker du best med sosiale medier?4) Ulemper: Hva synes du er de største ulempene med sosiale medier?5) Kan du fortelle litt om hvordan du bruker funksjonene på Instagram/Facebook?
Del 3: Affektiv (følelser) a) Dele innhold/ opplysninger b) Annonser og adferdsbasert markedsføring	<ol style="list-style-type: none">6) Hva betyr privatliv for deg? <i>Hvor mye betyr det for deg å beskytte privatlivet ditt på SoMe?</i>7) Hvilken informasjon/innhold synes du er greit å legge ut på Instagram/Facebook, og hva føler du er for privat for din del å legge ut? <i>Gjerne kom med eksempler.</i>8) Unngår du noen ganger å legge ut innhold selv om du egentlig har lyst til det? <i>Har du noen tanker om hvorfor?</i>9) Har du opplevd at noen la ut et bilde av deg på Instagram/Facebook, som du ikke synes var greit? <i>(ikke gitt samtykke til) Hvordan følte dette?</i>10) Føler du at du har kontroll over din personlige informasjon på Instagram/Facebook? (Hva som står der, hvem som kan se det etc)11) Har du opplevd, eller kjenner noen som har fått kontoen sin hacket? <i>Hva føler du om det?</i>12) Tror du at Facebook/Instagram samler inn annen/mer informasjon om deg, enn det du har lagt til selv? <i>Hva tror du skjer med den informasjonen som blir samlet inn? Etter din mening, hvor mye av det du gjør i sosiale medier tror du blir sporet?</i> (Av annonsører, teknologibedrifter eller andre selskaper)13) Hva synes du om innhold/annonsene som dukker opp i nyhetsstrømmen på sosiale medier?14) Tror du det er mulig å leve i dagens samfunn uten at selskaper samler inn informasjon om deg? <i>Hvorfor/Hvorfor ikke.</i>
Del 5: Kognitiv (Kunnskap og meninger) Om personvern	<ol style="list-style-type: none">15) Hva legger du i ordet, personvern? Hva forbinder du det med?16) Hvor viktig vil du si at personvern er for deg? <i>Er det noe du tenker over når du er på nett eller bruker sosiale medier? Kan du huske når du ble oppmerksom på at personvernet ditt ble påvirket i sosiale medier?</i>

	<p>17) Hva tenker du er fordelene med å ha en god beskyttelse av privat informasjon på sosiale medier?</p> <p>18) Hvilken type informasjon/opplysninger anser du som sensitive? <i>Opplysninger som ikke er ment for å offentliggjøres: helseopplysninger etc.</i></p> <p>19) Har du hørt om Personvernsforordningen (GDPR) eller andre personvernlover/regler? <i>Hvor har du eventuelt hørt om dette?</i></p> <p>20) Hvor mye stoler du på at Instagram/Facebook tar vare på personvernet ditt og din informasjon?</p>
<p>Del 6: Atferd (Handlinger) Personvernshandlinger</p>	<p>21) Har du lest eller kikket på personvernserklæringen til Instagram/Facebook? <i>Hvorfor/Hvorfor ikke?</i></p> <p>22) Hvordan forholder du deg til såkalte informasjonskapsler? (cookies) <i>Hva bruker du å klikke på? (Tillate/Godkjenne/ikke tillate)</i></p> <p>23) Hva tenker du om personvernsinnstillingene på Instagram/Facebook? <i>Har du endret dem?</i></p> <p>24) Hvilke andre tiltak vet du om for å beskytte privatlivet ditt på sosiale medier? <i>Har du gjort noen av disse selv? Hvorfor/Hvorfor ikke?</i></p>
<p>Del 7: Tenke høyt øvelse Personvernsinnstillinger</p>	<p>Be informanten om hen kan se på sine personvernsinnstillinger på Instagram eller Facebook på sin mobil/PC. Gå gjennom disse, og diskuter.</p> <p><i>Vet de hvor de finner personvernsinnstillingene? Hvor lang tid bruker de? Vet de hvordan profilene er innstilt? Blir de overasket over innstillingene eller har de kontroll?</i></p>

Vedlegg 2 – Vurdering fra Sikt



[Meldeskjema](#) / [Personvernsholdninger i sosiale medier - hvor dyp er generasjonskløften](#) / Vurdering

Vurdering av behandling av personopplysninger

Referansenummer
608479

Vurderingstype
Standard

Dato
13.01.2023

Prosjekttittel

Personvernsholdninger i sosiale medier - hvor dyp er generasjonskløften?

Behandlingsansvarlig institusjon

Universitetet i Bergen / Det samfunnsvitenskapelige fakultet / Institutt for informasjons- og medievitenskap

Prosjektansvarlig

Torgeir Uberg Nærland

Student

Hanna Kvamme

Prosjektperiode

01.09.2022 - 01.06.2023

Kategorier personopplysninger

Alminnelige

Lovlig grunnlag

Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 01.06.2023.

[Meldeskjema](#)

Kommentar

OM VURDERINGEN

Sikt har en avtale med institusjonen du forsker eller studerer ved. Denne avtalen innebærer at vi skal gi deg råd slik at behandlingen av personopplysninger i prosjektet ditt er lovlig etter personvernregelverket.

FØLG DIN INSTITUSJONS RETNINGSLINJER

Vi har vurdert at du har lovlig grunnlag til å behandle personopplysningene, men husk at det er institusjonen du er ansatt/student ved som avgjør hvilke databehandlere du kan bruke og hvordan du må lagre og sikre data i ditt prosjekt. Husk å bruke leverandere som din institusjon har avtale med (f.eks. ved skylagring, nettspørreskjema, videosamtale el.)

Personverntjenester legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1 f) og sikkerhet (art. 32).

Du må dele meldeskjemaet ditt med prosjektansvarlig. Det gjør du ved å velge «Del prosjekt» øverst til venstre i meldeskjemaet. Deretter velger du «Inviter bruker», og skriver inn e-postadressen. Prosjektansvarlig vil bli bedt om å akseptere invitasjonen innen en uke, ellers må du invitere på ny.

MELD VESENTLIGE ENDRINGER

Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til oss ved å oppdatere meldeskjemaet. Se våre nettsider om hvilke endringer du må melde: <https://sikt.no/melde-endringer-i-meldeskjema>

OPPFØLGING AV PROSJEKTET

Vi vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!

Vedlegg 3 - Samtykkeskjema

Vil du delta i forskningsprosjektet «Holdninger til personvern i sosiale medier»?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt, hvor intensjonen er å finne ut av hvordan folk forholder seg til personvern i sosiale medier. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Dette prosjektet utgjør min masteroppgave i Medier og Kommunikasjon ved Universitet i Bergen. Formålet er å se nærmere på brukeres holdning til personvern i sosiale medier, med utgangspunkt i Instagram og Facebook. Herunder skal det undersøkes to kulturelle generasjoner; Generasjon Z (f.1997-2007) og Baby boomers (f.1946-1964), og slik sammenligne disse opp mot hverandre.

For å finne ut av hvilken holdning de ulike generasjonene har, skal det intervjues en rekke informanter fra hver generasjon. Disse intervjuene foregår en-til-en, enten fysisk eller digitalt, og handler om å gå i dybden på temaet.

Hvem er ansvarlig for forskningsprosjektet?

Universitetet i Bergen er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?

Det er minimum 12 informanter som deltar i studien.

Utvalget baserer seg på kriterier slik som:

- Hvilken generasjon du tilhører; Baby Boomer (55-75 år) eller Generasjon Z (15-25 år)
- At du har en personlig profil på Instagram og/eller Facebook
- At du bor og er oppvokst i Norge

Hva innebærer det for deg å delta?

Denne studien har en såkalt kvalitativ metode, der vi ønsker å gå i dybden og spørre deg om hva du tenker, synes og handler om ulike ting. I denne anledning gjennomføres det et intervju som vil ta deg omtrent 45 minutter. Det trengs ingen forberedelser fra din side. Intervjuet inneholder spørsmål om hvordan du bruker sosiale medier og hvordan du forholder deg til personvern.

Andre personopplysninger som samles inn under intervjuet er: alder, yrke/studie og hvilken landsdel du kommer fra. Jeg tar lydopptak og notater fra intervjuet.

I selve masteroppgaven vil du bli anonymisert. Dette innebærer at det ikke skal være mulig å spore dine opplysninger tilbake til deg.

Dersom du er under 18 år, kan dine foreldre få se på intervjuguiden på forhånd ved å ta kontakt.

Det er frivillig å delta

Det er helt frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrevet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- *Den behandlingsansvarlige institusjonen er Universitetet i Bergen. Herunder er det kun jeg, Hanna Kvamme (masterstudent) og min veileder, Torgeir Uberg Nærland, som har tilgang til dine opplysninger.*
- *Ditt navn og kontaktopplysninger vil erstattes med en kode som lagres på egen navneliste adskilt fra øvrige data. Datamaterialet vil også lagres i en digital innelåst mappe.*

I publikasjonen vil du bli anonymisert. Herunder vil du som person ikke kunne bli identifisert.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?

Prosjektet vil avsluttes 01.07.2023. Etter prosjektslutt vil datamaterialet med dine personopplysninger slettes.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Universitet i Bergen har Personverntjenester vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- Universitet i Bergen ved student, Hanna Kvamme (h.kvamme@student.uib.no) og veileder og førsteamanuensis, Torgeir Uberg Nærland (torgeir.narland@uib.no)
- Vårt personvernombud: Janecke Helene Veim (personvernombud@uib.no)

Hvis du har spørsmål knyttet til Personverntjenester sin vurdering av prosjektet, kan du ta kontakt med:

- Personverntjenester på epost (personverntjenester@sikt.no) eller på telefon: 53 21 15 00.

Med vennlig hilsen

Prosjektansvarlig
(Forsker/Veileder)

Masterstudent

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *Holdninger til Personvern i sosiale medier*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å delta i intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

(Signert av prosjektdeltaker, dato)