Masteroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for samfunns- og utdanningsvitenskap
Institutt for sosiologi og statsvitenskap

Kristian August Røstad-Tollefsen

Mellom deling og beskyttelse av personopplysninger

En kvalitativ studie av nordmenns beskrivelser av personvern

Masteroppgave i Medier, kommunikasjon og informasjonsteknologi
Veileder: Melanie Magin
Juni 2023

NTNU
Kunnskap for en bedre verden

Kristian August Røstad-Tollefsen

Mellom deling og beskyttelse av personopplysninger

En kvalitativ studie av nordmenns beskrivelser av personvern

Masteroppgave i Medier, kommunikasjon og informasjonsteknologi
Veileder: Melanie Magin
Juni 2023

Norges teknisk-naturvitenskapelige universitet
Fakultet for samfunns- og utdanningsvitenskap
Institutt for sosiologi og statsvitenskap

NTNU
Kunnskap for en bedre verden

Sammendrag

Personvern er et aktuelt tema i dagens datadrevne samfunn, der omfattende digitaliseringsprosesser og teknologisk utvikling ofte går på bekostning av individets personvern. Flere forskningsstudier viser at individer verdsetter personvern høyt, men likevel er villige til å gi fra seg personopplysninger for små fordeler. Denne masteroppgaven baserer seg på 11 kvalitative dybdeintervjuer med eksperter på personvern og brukere i ulike aldersgrupper (21-30, 31-49 og over 50 år) for å besvare problemstillingen: «*Hvordan beskriver nordmenn sine holdninger til personvern når det gjelder innsamling, behandling og bruk av personopplysninger, og hvordan er disse beskrivelsene knyttet til deres atferd og beslutninger om beskyttelse og deling av personopplysninger på nett*?».

Analysen er delt inn i tre deler som dekker informantenes beskrivelser av deres forhold til behandlingsansvarliges praksiser, villighet til å avsløre og deres behov for beskyttelse. Dette understreker betydningen av innebygd personvern som en standard og tilliten brukerne har til behandlingsansvarlige når det gjelder opplevd grad av kontroll og risikobevissthet. Videre utforskes det hvordan brukernes digitale kompetanse kan være en forutsetning og personvernhensyn kan være en hindring for deling eller beskyttelse av personopplysninger på nett. Disse hovedfunnene knyttes til personvernparadokset som en forklaringsmodell og til personvernfremmende teknologier som tiltak for å belyse aldersforskjeller blant informantene. Det ble observert at eldre informanter beskrev at opplevde et mindre behov for beskyttelse og hadde begrenset digital kompetanse når det gjaldt bruk av personvernfremmende beskyttelsestiltak, i motsetning til yngre informanter i utvalget. Denne innsikten er med på å fremheve behovet for å utforske forholdet mellom nordmenns holdninger, atferd og beslutningstaking i dybden.

Abstract

Privacy is a relevant topic in today's data-driven society, where extensive digitization processes and technological advancements often come at the expense of individuals' privacy. Several research studies show that individuals highly value privacy but are still willing to give up personal information for small benefits. This master's thesis is based on 11 qualitative in-depth interviews with privacy experts and users in different age groups (21-30, 31-49, and over 50 years old) to address the research question: "*How do Norwegians describe their attitudes towards privacy regarding the collection, processing, and use of personal information, and how are these descriptions linked to their behaviour and decisions regarding the protection and sharing of personal information online*?"

The analysis is divided into three parts, covering the informants' descriptions of their relationship with data controllers' practices, their willingness to disclose information, and their need for protection. This emphasizes the importance of privacy by design as a standard and the trust users have in data controllers regarding perceived control and risk awareness. Furthermore, the study explores how users' digital competence can be a prerequisite and privacy considerations can be a barrier to sharing or protecting personal information online. These main findings are linked to the privacy paradox as an explanatory model and privacy-enhancing technologies as measures to shed light on age differences among the informants. It was observed that older informants described perceiving a lesser need for protection and had limited digital competence when it came to using privacy-enhancing protective measures, in contrast to younger informants in the sample. This insight helps highlight the need to explore the relationship between Norwegians' attitudes, behaviour and decision making in depth.

Forord

Denne oppgaven markerer slutten på en lang og innholdsrik reise i min mangeårige studentkarriere. Det er med stor glede at jeg endelig kan presentere denne masteroppgaven som et endelig sluttresultat etter flere måneders intensivt arbeid og dedikasjon.

Jeg vil takke veilederen min Melanie for uvurderlig støttet og veiledning gjennom hele prosessen. Dine konstruktive tilbakemeldinger og tilgjengelighet var til stor hjelp for meg. Det samme gjelder i forhold til de andre studentene som var en del av gruppeveiledningene våre. Tusen takk for alle tilbakemeldinger, uvurderlige støtte og tips som bidro til å hjelpe meg gjennom denne prosessen. Jeg vil også takke mine medstudenter som har gått gjennom dette sammen med meg. Nå er vi endelig ferdige og jeg gleder meg til å se hva fremtiden vil bringe for alle.

Jeg vil også rette en spesiell takk til mine nærmeste familiemedlemmer, som har vært en kilde til uendelig støtte, oppmuntring og kjærlighet gjennom hele studietiden. Tusen takk for at dere tok dere tid til å lese over og gi verdifulle tilbakemeldinger på denne oppgaven.

Til min kjære samboer som har vært der for meg gjennom hele denne perioden og bidratt med alt fra å lese gjennom til å støtte meg når jeg lå langt nede. Tusen takk til deg og nå er jeg endelig ferdig!

Til slutt vil jeg takke alle informantene som tok seg tid til å bli med i denne studien. Dere har vært helt avgjørende og en uvurderlig del av hele prosessen fra A til Å. Uten deres engasjement, bidragsytende perspektiver og refleksjoner hadde ikke denne oppgaven vært mulig å gjennomføre.

Takk for at du tar deg tid til å lese denne masteroppgaven og god fornøyelse.

Kristian August Røstad-Tollefsen

Trondheim, juni 2023

Innholdsfortegnelse

1. Innledning

I dagens digitale samfunn er personvern og håndtering av personopplysninger blitt et stadig viktigere tema. Den økende digitaliseringen har gjort det mulig å samle inn og behandle enorme mengder data om Internett-brukere, og dette har ført til at datainnsamling er svært utbredt i dagens informasjonssamfunn (Acquisti et al., 2015). Brukere blir stadig bedt om å akseptere informasjonskapsler (cookies) og andre teknologier som samler inn opplysninger om dem (Dabrowski, 2019; Kretschmer et al., 2021). Norge, som et av verdens mest digitaliserte land, har integrert digitalisering i nesten alle aspekter av samfunnet (NOU 2022: 11). Med økende bruk av digitale tjenester, sosiale medieplattformer og ny teknologi, har spørsmål om personvern og bruk av personopplysninger fått økt relevans og betydning.

I norsk kontekst har Datatilsynet (2020) gjennomført en omfattende spørreundersøkelse som en del av Personvernundersøkelsen 2019/20 (Datatilsynet, 2020). Undersøkelsen hadde som formål å kartlegge nordmenns holdninger til personvern og deres kunnskap om personvernrettigheter og -regelverk. Resultatene av undersøkelsen avdekket flere bekymringsfulle trender blant den norske befolkningen. Det ble konstatert at kunnskapen om personvernforordningen (GDPR), personopplysningsloven og grunnleggende personvernrettigheter var sterkt knyttet til sosioøkonomisk status (Datatilsynet, 2020). Dette kan føre til ulikheter i evnen til å utøve personvernrettigheter og ta informerte valg, Det er derfor viktig å forstå hva som påvirker befolkningens kunnskap og kompetanse knyttet til hva, hvordan og hvorfor personopplysningene brukes (Dienlin & Trepte, 2015).

Undersøkelsen viste også at mange nordmenn opplevde en følelse av maktesløshet, manglende kontroll og usikkerhet når det gjaldt innsamling, behandling og bruk av personopplysninger (Datatilsynet, 2020). Dette kan skyldes frykt for sporing og overvåking. Videre ble det avdekket at nordmenn generelt hadde høyere tillit til offentlige virksomheter, mens tilliten til private teknologiselskaper bak sosiale medieplattformer og søkemotorer var svært lav (Datatilsynet, 2020). Dette kan sees i lys av hendelser som Cambridge Analytica-skandalen i 2018 (Carlsen, 2018) og den nylige rekordstore boten på 1,2 milliarder euro pålagt Meta av det irske datatilsynet og europeiske tilsynsmyndigheter i mai 2023 (Resvoll, 2023). Disse hendelsene understreker betydningen av tillit i personverndebatten og behovet for åpenhet rundt innsamling, behandling og bruk av personopplysninger. I tillegg til Datatilsynets undersøkelse har Personvernkommisjonen (2022) på oppdrag fra Kommunal- og distriktsdepartementet gjennomført en grundig utredning og kartlegging av

personvernsituasjonen i Norge (NOU 2022: 11). Her ble det fremhevet hvordan personvern både er en grunnleggende individuell menneskerettighet og en viktig forutsetning for et velfungerende demokratisk samfunn (NOU 2022: 11). Rapporten pekte på flere drivkrefter, bekymringsverdige trender og utfordringer knyttet til personvern i Norge, inkludert begrensede muligheter for nordmenn til å ivareta sitt personvern, kontrollere og beskytte personopplysningene sine. Dette ved understreke behovet for en nasjonal personvernpolitikk og tiltak for å begrense innsamlingen av personopplysninger av kommersielle aktører og gi brukerne bedre muligheter til å kontrollere deres personopplysninger og ivareta sitt personvern på en effektiv måte (NOU 2022: 11). Til tross for disse bekymringsverdige utviklingstrekkene knyttet til personvern og virksomheters praksiser for innsamling, behandling og bruk av personopplysninger er enkeltpersoner fortsatt villige til å gi fra seg personopplysninger mot relativt små fordeler (Kokolakis, 2017; van Ooijen et al., 2022).

1.1 Problemstillingen

Med utgangspunkt i både Datatilsynets (2020) personvernundersøkelse og Personvernkommisjonens (2022) rapport, tar denne oppgaven masteroppgaven utgangspunkt i å belyse ulike aspekter av nordmenns meningsdannelse rundt deres holdninger til personvern og atferd. I denne sammenhengen vil jeg ikke undersøke hva som påvirker forholdet mellom nordmenns holdninger og faktiske atferd. Til forskjell vil jeg vektlegge en kvalitativ tilnærming som gjør det mulig å utforske nordmenns indre tanker, opplevelser og refleksjoner rundt deres holdninger til personvern knyttet til deres atferd og beslutninger. På bakgrunn av dette har jeg valgt å formulere følgendeproblemstilling:

> «*Hvordan beskriver nordmenn sine holdninger til personvern når det gjelder innsamling, behandling og bruk av personopplysninger, og hvordan er disse beskrivelsene knyttet til deres atferd og beslutninger om beskyttelse og deling av personopplysninger på nett*?»

Her har jeg valgt å avgrense oppgaven til å omhandle nordmenns meningsdannelse og beskrivelser av personvern i kontekst av deres personopplysninger For å kunne besvare dette vil jeg i tillegg belyse hvordan nordmenn opplever hvem og hvordan personopplysningene deres samles inn, behandles og brukes på nett. I tillegg vil jeg undersøke dette i forhold til nordmenns bruk av personvernfremmende teknologier for å beskytte deres personopplysninger på nett.

1.2 Oppgavens struktur

For å kunne besvare denne problemstillingen er jeg valgt å strukturere oppgaven etter 5 deler. Først vil jeg redegjøre for sentrale begreper, tidligere forskningslitteratur og teoretiske perspektiver på personvern knyttet til personvernparadokset, personvernkynisme, digital kompetanse og eksempler på personvernfremmende teknologier. Deretter vil jeg diskutere valget av intervju som metode og gi et overblikk over forskningsprosessen som en helhet. Her vil jeg redegjøre for alle valgene som ble tatt i forhold til utvalget, innsamlings- og behandlingsprosessen av empirien (data), samt vurdere dette opp mot ulike kvalitetskriterier. Videre vil jeg systematisk gjennomgå og analysere utvalgte sitater fra intervjuene med utgangspunkt i tre hovedtemaer. I diskusjonsdelen vil jeg presentere og drøfte de viktigste hovedmomentene fra analysen opp mot oppgavens problemstilling. Her vil jeg sette disse hovedmomentene i en større sammenheng og diskutere det opp mot oppgavens teoretiske rammeverk og tidligere forskningslitteratur på feltet. Avslutningsvis vil jeg fremheve oppgavens bidrag, begrensninger og forslag til videre forskning.

2. Teoretisk rammeverk og sentrale begreper

I denne delen vil jeg redegjøre for sentrale begreper, teoretiske perspektiver og tilhørende forskningslitteratur rundt personvern. Formålet med delen er å belyse og synliggjøre det teoretiske rammeverket som er benyttet i denne masteroppgaven. Først vil jeg redegjøre for ulike perspektiver som tar for seg hva personvern er, og avgrense dette til «information privacy». Deretter vil jeg trekke fram personvernparadokset som en mulig måte å forklare forholdet mellom individers holdninger til personvern og atferd. Personvernkynisme og digital kompetanse vil trekkes fram som konsepter innenfor personvernparadokset. Videre vil jeg redegjøre for hva personvernfremmende teknologier er, samt ta for meg tidligere forskning på slike teknologier. Avslutningsvis vil jeg fremheve og beskrive noen eksempler på ulike personvernfremmende teknologier.

2.1 Perspektiver på personvern

Det finnes ingen entydig definisjon eller beskrivelse på hva er personvern, og det kan betraktes som et komplekst og flerdimensjonalt fenomen (Kokolakis, 2017; Solove, 2021; Westin, 2003). Utviklingen av konseptet rundt personvern kan trekkes tilbake Warren og Barndeis (1890) tradisjonelle oppfatning av personvern som «*the right to be left alone*» (Warren & Barndeis, 1890). Forståelsen av personvernsbegrepet har senere utviklet seg til å inkludere og belyse en mer kompleks og sammensatt oppfatning, som er tilpasset dagens digitale informasjonssamfunn. Personvern kan i dag omfatte en rekke forskjellige personvernhensyn knyttet til personlig autonomi, tanke- og ytringsfrihet, samt sikkerhet og beskyttelse (Bélanger & Crossler, 2011; Solove, 2002; Westin, 2003).

Dette kan ses i sammenheng med den stadig mer omfattende digitaliseringen og teknologiske utviklingen i samfunnet som har medført at mennesker i dag etterlater store mengder digitale spor og opplysninger. Disse opplysningene deles både bevisst og uvitende til offentlige og kommersielle aktører gjennom deres dagligdagse nettaktiviteter (Acquisti et al., 2015; NOU 2022: 11). Dette har vært med på å skape et økende behov for å samle inn opplysninger gjennom automatiserte prosesser som brukes til å effektivisere og utvikle alt fra tjenester til produkter (Acquisti et al., 2015; NOU 2022: 11). Begrepet personopplysninger fungere som en samlebetegnelse for mangfoldet av opplysninger som kan brukes til å identifisere enkeltindivider. Videre er det mulig å skille mellom direkte eller indirekte opplysninger (Datatilsynet, 2019b). Direkte opplysninger kan for eksempel være navn, kjønn, adresse, e-

postadresse, telefonnummer, personnummer eller andre personlige kjennetegn (Sikt, 2023). Det kan også omfatte sensitive opplysninger som alder, kjønn, sivilstatus, geografisk tilhørighet, nasjonalitet, ideologi eller politisk tilhørighet. Indirekte opplysninger refererer til bakgrunnsinformasjon som kan bidra til å identifisere enkeltpersoner, og ofte kan disse opplysningene kombineres (Datatilsynet, 2019b).

Dette kan for eksempel være bostedskommune, og tilknytning til institusjoner i kombinasjon med andre identifiserende opplysninger. I konteksten av det moderne digitale informasjonssamfunnet kan personvern på denne måten avgrenses til begrepet «information privacy». Dette innebærer individets rett og behov for å kontrollere og ha en viss innflytelse over hvordan deres opplysninger samles inn, behandles og brukes i ulike kontekster (Bélanger & Crossler, 2011; Smith et al., 2011; Solove, 2006). Videre er «information privacy» knyttet opp mot spørsmål om hvem som har eierskap over disse opplysningene, samt hvordan omfattende personvernregelverk og retningslinjer skal implementeres for å beskytte individers rettigheter og personopplysninger mot misbruk og uautorisert tilgang (Bélanger & Crossler, 2011; Smith et al., 2011).

2.1.1 Informasjonskapsler

Det kan være hensiktsmessig å trekke inn informasjonskapsler for å beskrive og forklare hvordan brukerens personopplysninger samles inn, behandles og distribueres gjennom Internett og digitale teknologier. Informasjonskapsler, også kjent som «cookies», er små tekstfiler med informasjon som lagres i brukerens nettleser eller digitale enhet når de besøker en nettside eller bruker en tjeneste (Dabrowski, 2019; Nasjonal Kommunikasjonsmyndighet, 2020). Informasjonskapslene kan avdekke personopplysninger gjennom ulike former for elektroniske spor. Bruken av informasjonskapsler er motivert av formål som effektivisering, personalisering, målrettet annonsering, identifisering/sporing og forbedring av brukeropplevelsen (Dabrowski, 2019).

Informasjonskapsler gjør det mulig for nettsiden lagre informasjon om brukerens preferanser, bruksmønstre eller annen identifiserende informasjon. De samler kontinuerlig inn informasjon (data) hver gang brukeren besøker nettsider og/eller digitale tjenester (Dabrowski, 2019; Kretschmer et al., 2021). Det er mulig å diskriminere mellom funksjonelle og ikke-funksjonelle informasjonskapsler (Kretschmer et al., 2021). Funksjonelle informasjonskapsler er strengt nødvendige for å opprettholde nettsidens eller tjenestens funksjonalitet og brukeropplevelse. Ikke-funksjonelle informasjonskapsler brukes til formål som ikke er direkte

knyttet til nettsidens funksjonalitet, men som bidrar til å effektivisere og tilpasse brukeropplevelsen. Et eksempel på dette kan være tredjeparts informasjonskapsler, som brukes til personlig tilpasset markedsføring eller innhold (Kretschmer et al., 2021).

2.1.2 Personopplysningsloven og GDPR

Det finnes en rekke personvernlover og -forskrifter som har blitt implementert for å beskytte enkeltindividers personvernrettigheter, slik som General Data Protection Regulation (GDPR). GDPR, eller den europeiske personvernforordningen, er et regelverk for personvern som omfatter en rekke regler og plikter som gjelder innenfor EU og det europeiske økonomiske samarbeidsområdet (Datatilsynet, 2021). I norsk kontekst er den europeiske personvernforordningen en del av loven om behandling av personopplysninger, eller personopplysningsloven, som ble vedtatt og trådte i kraft som norsk lov i 2018. Dette lovverket omfatter en rekke plikter for virksomheter som er etablert og behandler personopplysninger i Norge (Personopplysningsloven, 2018).

Behandlingen av personvernopplysninger må være i samsvar med tilhørende personvernsprinsipper. Personvernsprinsippene handler blant annet om (1) lov, rettferdighet og åpenhet/gjennomsiktighet, (2) formåls- og lagringsbegrensning, (3) dataminimering, (4) riktighet, (5) integritet og konfidensialitet, og (6) ansvarlighet (Datatilsynet, 2019c; Personopplysningsloven, 2018, artikkel 5). Samlet har disse prinsippene som formål å sikre forutsigbarhet og trygghet gjennom at enkeltindividers personvern blir ivaretatt. Formålet med dette er å gi individet en økende grad av kontroll over deres personopplysninger basert på et krav om et gyldig samtykke, samt ved å pålegge strenge regler for virksomheter som samler inn, behandler eller lagrer personopplysninger i Norge (Kommunal- og distriktsdepartementet, 2019).

2.1.3 Den behandlingsansvarlige og innebygd personvern

Begrepet «behandlingsansvarlig» kan i denne sammenhengen brukes til å beskrive virksomheten, selskapet eller organisasjonen som behandler brukerens personopplysninger. Den behandlingsansvarlige kan være en juridisk person i form av en offentlig myndighet, institusjon eller privat virksomhet, som enten alene eller sammen med andre behandler personopplysninger til spesifikke formål (Datatilsynet, 2019a). Det finnes flere eksempler på virksomheter som kan opptre i rollen som behandlingsansvarlig og som har det overordnede ansvaret for å behandle personopplysninger i tråd med personopplysningsloven og andre gjeldende regelverk. Dette inkluderer alt fra en kommune, arbeidsgiver eller offentlig organ til

private selskaper som Meta, Google, Schibsted og Aller Media. Det er også rom for en ansvarsfordeling med en databehandler som kan behandler personopplysninger på vegne av den behandlingsansvarlige (Datatilsynet, 2019a). Denne fordelingen kan ha ulike former, og bidrar til å danne grunnlaget for hvordan brukerens personopplysninger samles inn, behandles og brukes.

Det som kan betegnes som «Privacy by Design», eller innebygd personvern, er knyttet til den behandlingsansvarliges personvernpraksiser for innsamling og behandling av personopplysninger. Ifølge Cavoukian (2009) er det mulig å identifisere syv grunnleggende prinsipper som inngår i den behandlingsansvarliges innebygde personvern. Disse prinsippene inkluderer (1) proaktivitet og forebygging, (2) personvern som standardinnstilling, (3) personvern innebygd i design, (4) full funksjonalitet, (5) ende-til-ende sikkerhet (ivareta informasjonssikkerhet), (6) synlighet og åpenhet, og (7) respekt for brukerens personvern (Cavoukian, 2009, 2020; Datatilsynet, 2022). Disse grunnleggende prinsippene er tett knyttet til personvernprinsippene som vektlegges i personopplysningsloven. De vil derfor være avgjørende for å behandle personopplysninger på en lovlig, rettmessig og formålsspesifikk måte (Datatilsynet, 2019a). Formålet med å fremheve disse ulike grunnleggende personvernprinsippene i denne oppgaven er å belyse hvordan innebygd personvern vil kunne påvirke hvordan brukerens personopplysninger samles inn, behandles, lagres og brukes på ulike måter av den behandlingsansvarlige. Videre vil det derfor være interessant å undersøke hvordan nordmenn forholder seg til og opplever hvordan den behandlingsansvarlige vektlegger innebygd personvern i sin praksis.

2.2 Et personvernparadoks?

Flere studier har utforsket individers holdninger til personvern og atferd i ulike kontekster, med forskjellige metodiske tilnærminger og teoretiske perspektiver (Barth & de Jong, 2017; Gerber et al., 2018; Kokolakis, 2017). På den ene siden har forskningslitteraturen fremhevet at individer uttrykker bekymringsverdige holdninger til personvern og det som en primær bekymring i når det gjelder hvordan personopplysningene deres samles inn, behandles og brukes (Acquisti et al., 2015; Kokolakis, 2017). På den andre siden er individer fortsatt villige til å gi fra seg eller avsløre personopplysninger på nettet for å få tilgang til sosiale medier, digitale tjenester, innhold eller andre fordeler (Acquisti & Grossklags, 2005; Norberg et al., 2007). Dette fenomenet som omhandler gapet mellom individers uttrykte holdninger og

motstridende atferd har resultert i en forklaringsmåte som har blitt betegnet som «personvernparadokset» (Barnes, 2006; Kokolakis, 2017; Norberg et al., 2007).I den tidlige etableringsfasen av personvernparadokset har flere studier argumentert for en foreslått dikotomi eller et motstridende forhold mellom individers holdninger og atferd (Acquisti, 2004; Acquisti & Grossklags, 2005; Brown, 2001; Cohen, 2000). Tidligere forskning har også undersøkt hvordan individers beslutningstaking kan påvirkes av manglende eller ufullstendig informasjon, begrensninger i individets rasjonalitet og psykologiske skjevheter (Acquisti, 2004; Acquisti & Grossklags, 2005). Videre hvordan dette vil kunne oppstå når den opplevde nytteverdien ved å avsløre eller gi fra seg personopplysninger og andre relative fordeler veier tyngre enn deres uttrykte bekymringer (Acquisti & Grossklags, 2005; Brown, 2001).

Barnes (2006) argumenterer også for en uoverensstemmelse i personvernparadokset, spesielt når det gjelder unge folk sin bruk av sosiale medier som kjennetegnes av manglende risikobevissthet og økende villighet til å dele personopplysninger på nettet.Norberg et al. (2007) har spilt en sentral rolle i etableringen av personvernparadokset som en forklaringsmodell. Dette gjennom deres studier av individenes villighet og intensjon til å avsløre personopplysninger. Funnene fra Norberg et al. (2007) indikerer et gap eller personvernparadoks mellom individers intensjoner (uttrykte holdninger) og faktiske villighet til å gi fra seg eller avsløre personopplysninger. Dette ved på å peke at funnene antydet at deltakerne i studien var mer villige til å dele og avsløre en betydelig større mengde personopplysninger enn det de tidligere hadde uttalt (Norberg et al., 2007).

2.2.1 Kritikken av personvernparadokset

En rekke studier har argumentert for personvernparadokset på bakgrunn av sine funn. Det har likevel oppstått en debatt omkring motstridende forskningsresultater, uenigheter og misvisende eller ufullstendige forklaringsmåter i forskningslitteraturen (Kokolakis, 2017). Dette ble blant annet demonstrert av Dienlin og Trepte (2015), som brukte to ulike metodiske tilnærminger for å teste personvernparadokset, og fant motstridende resultater. Begge tilnærmingene baserte seg på det samme utvalget og datamaterialet fra en spørreundersøkelse. I den første tilnærmingen tok de utgangspunkt i en regresjonsanalyse for å teste forholdet mellom respondentenes personvernhensyn og spesifikk atferd på sosiale mediesider (Dienlin & Trepte, 2015). Funnene fra denne tilnærmingen indikerte at det ikke var en statistisk signifikant sammenheng mellom respondentenes bekymringsverdige personvernhensyn og avsløringsatferd på nett. Ved hjelp av den første metodiske tilnærmingen kunne personvernparadokset benyttes som forklaringsmåte, men kun når det ble analysert i likhet

med tidligere forskning på fenomenet (Dienlin & Trepte, 2015). Den andre alternative tilnærmingen baserte seg på et flerdimensjonalt perspektiv på personvern. Dette ved å differensiere mellom tre typer personvern, som informasjonsmessig, sosialt eller psykologisk (Dienlin & Trepte, 2015).

Resultatene fra den andre tilnærmingen antydet både en direkte og indikerte sammenheng mellom respondentenes holdninger og atferd knyttet til brukeres uttrykte personvernhensyn og intensjoner om å avsløre opplysninger. I denne sammenhengen Dienlin og Trepte (2015) argumenterer for at forholdet mellom brukeres holdninger og atferd ikke kunne oppfattes som paradoksalt, men heller var basert på distinkte holdninger I likhet med Dienlin og Trepte (2015) argumenterer Martin (2020) for å avvise personvernparadokset, og peker på flere bekymringsverdige aspekter ved denne forklaringsmåten. Martin (2020) påpeker hvordan argumentet for at personvern er en kjerneverdi undergraver tidligere forskning og argumentene som har blitt benyttet til støtte for personvernparadokset. Funnene til Martin (2020) antyder at forbrukere beholder sine bekymringsverdige holdninger og rimelige forventninger i kontekst av virksomheters assosierte plikter og praksiser, selv etter at de avslører eller deler personopplysninger. Martin (2020) sine funn bidrar også til å undergrave personvernparadokset ved å fremheve hvordan brukerens villighet til å gi fra seg personopplysninger er basert på spesifikke forventninger til hvordan opplysningene deres skal behandles, lagres og brukes. I denne sammenhengen vil behandlingsansvarlige som ikke overholder eller bryter med disse forventningene oppleves som lite troverdige av brukeren (Martin, 2020).

Solove (2021) bygger videre på Martin (2020) ved å argumentere for at personvernparadokset er basert på en feilaktig logikk og misforståelser. Videre hvordan det foreslåtte motstridende forholdet kan anses som misvisende etter som individers holdninger og atferd ikke nødvendigvis trenger å være i samsvar. På bakgrunn av dette konkluderer Solove (2021) med at personvernparadokset kan betraktes som en myte. Solove (2021) sin kritikk bidrar til å understreke at personvernsfenomenets komplekse natur, og at det kan forklares og beskrives på ulike måter. For å forstå personvern kan det derfor være viktig å spesifisere konteksten og sammenhengen det forklares i (Kokolakis, 2017; Solove, 2021). At kontekst og sammenheng ikke tidligere har blitt spesifisert, kan mulig bidra til å forklare de motstridende resultatene i forskningslitteraturen og den påfølgende debatten. Noe som er med på å fremme et behov for å utvikle en nyansert forståelse av forholdet mellom individers holdninger til personvern og atferd. På bakgrunn av dette vil det i denne oppgaven være interessant å utforske hvorvidt

personvernparadokset fortsatt vil kunne anses som gjeldende i kontekst av nordmenns beskrivelser av deres holdninger til personvern. For å undersøke dette kan forskningslitteraturen på personvernparadokset være viktig for å belyse hva som påvirker individers holdninger og atferd. Datatilsynets (2020) spørreundersøkelse og personvernkommisjonens (2022) rapport har fremhevet en rekke aspekter som påvirker nordmenns holdninger til personvern. Denne oppgaven vil imidlertid gå i dybden på nordmenns beskrivelser av holdninger, atferd og beslutninger. Oppgaven vil forsøke å dekke behovet i forskningslitteraturen når det gjelder å undersøke hvordan brukere beskriver deres holdninger til personvern, samt hvordan dette er tilknyttet forståelse av atferd og beslutninger om personopplysninger på nett.

2.2.2 Personvernkynisme

I Hoffman et al. (2016) fokusgruppestudie av brukeres generelle atferd på Internett i forhold til personvernparadokset blir konseptet personvernkynisme foreslått som en alternativ tilnærming til å forklare personvernparadokset. Personvernkynisme er en form for kognitiv forsvarsmekanisme, som kan brukes til å forklare brukeres villighet til å avsløre personopplysninger (Hoffmann et al., 2016). Konseptet inkluderer aspekter som en utbredt følelse av maktesløshet, usikkerhet og mistillit til bedrifters eller tjenestetilbyderes innsamling og behandling av personopplysninger. Dette kan bidra til å belyse sentrale aspekter ved personvernparadokset ved å forklare hvordan individer oppfatter sine personvernbekymringer, tilhørende risikobevissthet og behov for beskyttelse som subjektivt meningsløst (Hoffmann et al., 2016).

Lutz et al. (2020) beskriver personvernkynisme som et flerdimensjonalt konsept bestående av fire faktorer eller dimensjoner. Disse er usikkerhet, resignasjon eller aksept, mistillit og maktesløshet (Lutz et al., 2020). Maktesløshet kan fremheves som den mest utbredte og fremtredende dimensjonen, i tillegg til brukerens grad av tillit som kan føre til en form for aksept eller resignasjon (Hoffmann et al., 2016; Lutz et al., 2020). Brukeren vil på denne måten kunne rettferdiggjøre sin beslutning om å avsløre personopplysninger på sin manglende evne til å kontrollere slike opplysninger. Personvernkynisme kan derfor være et resultat av manglende bevissthet, kunnskap og kompetanse knyttet til personvern, eller en oppfatning av at personvern ikke er viktig nok til å bekymre seg for. I noen tilfeller kan personvernkynisme anses som et uttrykk for at personvern ikke prioriteres når individer vurderer nettsider eller digitale tjenesters relative fordeler (Hoffmann et al., 2016; Lutz et al., 2020).

Dette er noe van Ooijen et al. (2022) bygger videre på sin studie av personvernkynismens rolle i enkeltpersoners beslutningstaking basert på et amerikansk utvalg og tversnittdata fra en nasjonal spørreundersøkelse i USA. Med utgangspunkt i «Protection Motivation Theory» (PMT) argumenterer van Ooijen et al. (2022) for at resultatene fra studien antyder at personvernkynisme kan anses å fungere som en moderator med en betydelig dempende effekt på forholdet mellom individers vurderinger av personverntrusler og mestringsatferd. Videre hvordan dette knyttet til individers beskyttelsesatferd når det gjelder deres opplevde sårbarhet alvorlighetsgrad og avsløringsfordeler, samt individers selv- og responseffektivitet (van Ooijen et al., 2022). På bakgrunn av dette argumenterer van Ooijen et al. (2022) for at personvernkynisme som de karakteriserer som en holdning av frustrasjon, håpløshet og desillusjon, at funnene fra studien i samsvar med Lutz et al. (2020) antyder at personvernkynisme har en negativ effekt på individers beskyttelsesatferd. Disse funnene er med på å fremheve hvordan individer som utvikler en form for personvernkynisme vil kunne dempe eller forhindre dem fra å beskytte personopplysningen deres på nett.

Videre har Khan et al. (2023) undersøkt forholdet mellom personvernkynisme, tilfredshet og tillit basert på en spørreundersøkelse og utvalg av sosiale mediebrukere. Funnene fra denne studien var med på å indikere at personvernkynisme kan ha en betydelig negativ innvirkning på brukerens tilfredshet. Til forskjell fant de ingen signifikant effekt på tilliten deres til sosiale medier (Khan et al., 2023). Videre var funnene med på å fremheve et gap mellom brukerens ønske om å beskytte personopplysninger og deres selv-rapporterte avsløringsatferd som samsvarer med den tidlige litteraturen på personvernparadokset (Norberg et al., 2007). Khan et al. (2023) undersøkte også om demografiske faktorer som alder, kjønn og erfaring hadde en modererende eller dempende effekt, men fant ingen konsekvente signifikante funn. Demografiske faktorer kan likevel anses som relevante for å utforske variasjoner i brukerens holdninger og intensjoner (Khan et al., 2023). Personvernkynisme vil på denne måten kunne anses som et relevant konsept etter som Datatilsynets (2020) personvernundersøkelse fremhever flere av dimensjonene som er knyttet til personvernkynisme. Videre vil det i denne oppgave være interessant å undersøke hvorvidt nordmenns beskrivelser er knyttet til en form for personvernkynisme.

2.2.3 Digital kompetanse

Begrepet digital kompetanse kan benyttes for å forklare forholdet mellom brukernes bekymringer om personvern og deres faktiske atferd, når det gjelder beskyttelse av personopplysninger på nettet. Brukerens digitale kompetanse handler om deres kunnskap,

ferdigheter og holdninger som gjør dem i stand til å bruke Internett og digitale teknologier på en effektiv, sikker og ansvarlig måte (Bartsch & Dienlin, 2016; Büchi et al., 2017; Trepte et al., 2015). Det er ikke alle brukere som har tilstrekkelig kompetanse for å beskytte personopplysningene sine på nettet, på grunn av manglende kunnskap eller tekniske ferdigheter som er nødvendige for å imøtekomme personvernrelaterte bekymringer (Park, 2013; Trepte et al., 2015).

Forskjeller i kompetanse kan bidra å skape digitale skiller, da enkelte brukere eller brukergruppers digitale kompetanse kan hindre dem fra å engasjere seg i å beskytte og ivareta deres personopplysninger på nett (Hargittai, 2002; Lythreatis et al., 2022). Trepte et al. (2015) deler brukeres digitale kompetanse inn i faktabasert og prosesskunnskap. Faktabasert kunnskap omfatter brukerens kunnskap om tekniske aspekter ved behandling av personopplysninger, grunnleggende personvernprinsipper, personvernrettigheter og relevante lover som GDPR eller personopplysningsloven (Bartsch & Dienlin, 2016; Trepte et al., 2015). Prosessuell kunnskap omfatter brukerens grunnleggende tekniske ferdigheter som gjør dem i stand til å bruke strategier for å ivareta og beskytte personopplysningene sine på nettet (Kezer et al., 2016; Trepte et al., 2015)

Park (2013) understreker betydningen av tre dimensjoner av brukerens digitale kompetanse i sin studie om digital kompetanse og beslutninger knyttet til personvern på internett. Dette gjelder kunnskap om tekniske aspekter ved internett, bevissthet om vanlige institusjonelle personvernpraksiser, og forståelse av gjeldende retningslinjer og personvernpolitikk. Resultatene til Park (2013) er basert på en kvantitativ spørreundersøkelse og en regresjonsanalyse, og ga varierende funn. Funnene indikerte likevel at personer med høyere nivå av generell digital kompetanse innen kunnskapsdimensjonen var mer engasjert i å ta kontroll over og beskytte personopplysningene sine på nettet (Park, 2013). Dette funnet stemmer overens med funn fra Bartsch og Dienlin (2016) sin studie om Facebook-brukeres digitale kompetanse. Bartsch og Dienlin (2016) hevder at brukerens erfaringer og bruk av internett bidrar til økt digital kompetanse, samtidig som de påpeker at det ikke ble funnet en direkte sammenheng mellom tidsbruk på Facebook, kjennskap til gjeldende personvernregler og brukerens oppfattede sikkerhet og faktiske atferd (Bartsch & Dienlin, 2016).

Büchi et al. (2017) argumenterer for den sentrale betydningen av brukerens digitale kompetanse for deres beskyttelsesatferd i sin studie. Studien omfattet sveitsiske internettbrukeres digitale kompetanse, og baserte seg på en kvantitativ spørreundersøkelse.

Funnene fra studien indikerer at brukerne generelt forsøkte eller ønsket å beskytte personopplysningene sine på nettet, men mange gjorde ikke nok eller manglet tilstrekkelig digital kompetanse for å gjøre dette (Büchi et al., 2017). Büchi et al. (2017) argumenterer blant annet for at brukerens tidligere erfaringer med personvernbrudd kan påvirke deres nåværende beskyttelsesatferd.

Dette var med på å antyde en positiv sammenheng mellom brukerens digitale kompetanse og behovet for å beskytte personopplysninger på nettet, i tråd med funnene til Park (2013). Brukerens generelle digitale kompetanse på denne måten sentral og avgjørende for å forklare brukernes personvernadferd. Dette fordi brukerens digitale kompetanse kan bidra til å redusere opplevde risikoer ved deling av personopplysninger, samt dra nytte av fordelene det gir (Büchi et al., 2017). På bakgrunn av dette vil det i denne oppgaven være interessant å utforske hvordan nordmenns beskrivelser av deres atferd og beslutninger om å dele eller beskytte personopplysninger på nett er knyttet til deres digitale kompetanse. Videre om det er mulig å antyde noen skiller eller forskjeller i ulike bruker- eller aldersgruppers meningsdannelse og refleksjoner rundt deres digitale kompetanse som muliggjør eller hindrer dem for å ta beslutninger som imøtekommer deres personvernhensyn og bekymringsverdige holdninger.

2.3 Personvernfremmende teknologier

Personvernfremmende teknologier(er en samlebetegnelse for et sett digitale metoder, teknikker eller verktøy som er utviklet for å beskytte, sikre og bevare personvernet til enkeltpersoner eller brukergrupper (Heurix et al., 2015). Disse teknologiene muliggjør personvernfremmende tjenester, eller alternativer som fokuserer på informasjonssikkerhet, bevissthet og anonymisering av personopplysninger. Hovedformålet med personvernfremmende teknologier er å tillate og hjelpe brukere med deres daglige bruk av nettsider og digitale tjenester, ved å beskytte og begrense innsamling, behandling og bruk av deres personopplysninger (Heurix et al., 2015; Kaaniche et al., 2020). Videre kan dette ses i forhold til behovet for å styrke individets personvern og muliggjøre deling av personopplysninger som er til fordel for brukeren og som kan forbedre, effektivisere og tilpasse deres brukeropplevelse (Kaaniche et al., 2020). Fischer-Hbner og Berthold (2017) også argumenterer for at personvernfremmende teknologier dekker flere

personvernprinsipper. Dette er prinsipper som legitimitet, formålsspesifisering, dataminimering, sikkerhet, gjennomsiktighet og individers rettigheter (Fischer-Hbner, 2017).

2.3.1 Personvernfremmende nettlesere, verktøy (programutvidelser) og moduser

Når det kommer til bruken av personvernfremmende teknologier, vil det også være interessant og hensiktsmessig å fremheve hvordan disse teknologiens og funksjonalitet vil kunne anses som personvernfremmende. Harborth og Pape (2020) har utforsket hvordan forholdet mellom personvernbekymringer, tillit og risikooppfatninger kan påvirke brukernes atferd og intensjoner om å bruke personvernfremmende nettlesere med utgangspunkt i «The Onion Router» eller «Tor». Resultatene fra studien til Harborth og Pape (2020) indikerte at brukere med høyere nivå av personvernbekymringer har en tendens til å ha tillit til personvernfremmende teknologier. Harborth et al. (2020) argumenterer for at resultatene indikerte hvordan variabler som oppfattet anonymitet, opplevd nytteverdi, brukervennlighet og tillit kan påvirke brukerens atferd. Brukervennlighet, opplevd nytteverdi og tillit ble fremhevet som sentrale aspekter ved brukerens intensjon og bruk av personvernfremmende teknologier (Harborth et al., 2020). Det er mulig å se dette i forhold til Skalkos et al. (2020) som argumenterer for at brukerens intensjon eller motivasjon til å bruke personvernfremmende anonymiseringsverktøy er tilknyttet oppnåelse av kjerneverdier som frihet, økonomisk velstand, faglig utvikling og en fryktløs livsstil.

DuckDuckGo er også en et personvernfremmende søkemotor eller nettleserutvidelse, som ble lansert som et alternativ til de etablerte søkemotorene som Google, Microsoft Bing og Yahoo!, på grunn av økende personvernbekymringer (DuckDuckGo, 2023b). I motsetning til mange andre søkemotorer, sporer eller lagrer ikke DuckDuckGo personopplysninger eller søkehistorikk (DuckDuckGo, 2023a). Tjenesten har som mål å tilby brukerne et personvernfremmende alternativ som legger vekt på informasjonssikkerhet, anonymitet og brukerens kontroll over informasjonen de søker etter. DuckDuckGo har flere funksjoner som er designet for å forbedre personvernet, som muligheten til å utføre anonyme søk, bruk av krypterte tilkoblinger (HTTPS) og blokkering av reklamesporingsverktøy (DuckDuckGo (2023a). Det kan være verdt å bemerke at det eksisterer lite forskning på DuckDuckGo som en personvernfremmende søkemotor noe som denne oppgaven vil kunne bidra til å dekke.

Det finnes også personvernfremmende annonseblokkeringsverktøy som AdBlock, som kan blokkere annonser på nettsteder (AdBlock, 2023). Tjenesteleverandører som AdBlock, eller konkurrenten Adblock Plus, tilbyr nettleserutvidelser eller nedlastbare apper for nettlesere

som Chrome, Firefox, Safari og Edge (Adblock Plus, 2023). Formålet med slike annonseblokkeringsverktøy er å gi brukere en opplevelse med begrenset annonsering og/eller sporing, og dermed fjerne distraherende, påtrengende eller skadelig innhold på nettsider (Traverso et al., 2017). Disse verktøyene kan betraktes som en form for anti-informasjonskapsler eller blokkeringsmetoder (Kaaniche et al., 2020). Videre kan det omfatte blokkering av ulike typer annonser som bannere, popup-annonser og videoannonser, avhengig av det spesifikke annonseblokkeringsverktøyet som brukes.

Annonseblokkeringsverktøy kan også bidra til å beskytte brukerens personvern ved å forhindre at annonsører sporer deres aktivitet, selger deres data eller tilpasser innholdet til annonseringsformål (Kaaniche et al., 2020; Traverso et al., 2017). Traverso et al. (2017) fant i sin studie av forskjellige annonse- og sporingsblokkere, at nettleserutvidelsen Ghostery hadde den beste dekningsgraden (91,3 %) for å blokkere sporingsverktøy på et utvalg av nettsider. Dette resultatet ble funnet gjennom systematisk sammenligning av resultatene fra ulike sporingsblokkere, inkludert Adblock Plus (Traverso et al., 2017). Det kan være viktig å merke seg at denne typen personvernfremmende teknologier kan påvirke funksjonaliteten til nettsider eller tjenester. De kan blant annet påvirke audiovisuelt innhold som ikke er relatert til annonser. De kan også begrense inntektene fra annonsering for tjenesteleverandøren eller bedriften som eier nettsiden (Traverso et al., 2017).

2.3.2 Inkognitomodus og virtuelle private nettverk (VPN)

I tillegg til personvernfremmende verktøy og programutvidelser, finnes det også innebygde alternativer i form av private moduser i de fleste nettlesere, som Chrome, Safari, Edge og Firefox (Apple, 2023; Google, 2023a; Microsoft, 2023; Mozilla, 2023). Disse modusene, som inkognitomodus eller privatmodus, kan betraktes som personvernfremmende siden de oppretter et midlertidig «inkognito» eller privat nettlesingsvindu som fungerer separat fra nettleserens normale funksjoner (Apple, 2023; Google, 2023a; Microsoft, 2023; Mozilla, 2023). I denne modusen blir ikke brukerens nettleserhistorikk, informasjonskapsler, nettstedsdata eller identifiserende brukerdata lagret (Kaaniche et al., 2020). Private modus har også muligheten til å blokkere informasjonskapsler fra tredjeparter, men denne beskyttelsen er ikke like omfattende som dedikerte personvernfremmende verktøy (Kaaniche et al., 2020). Inkognitomodusen fungerer derfor som en nyttig tilleggsfunksjon for brukere som ønsker en privat nettlesingsøkt der de kan kontrollere, begrense og forhindre at personopplysningene deres lagres, behandles og deles.

En IP-adresse (Internet Protocol address) er et unikt nummer som tildeles enheter som er koblet til et datanettverk, for eksempel datamaskiner eller telefoner (Gueye et al., 2006; Mishra et al., 2020). IP-adressen fungerer som enhetens unike identifikasjon og brukes til å identifisere brukeren eller nettverksområdet, samt angi plasseringen til brukeren gjennom geolokalisering (Gueye et al., 2006; Mishra et al., 2020). I forbindelse med IP-adresser er virtuelle private nettverk (VPN) et eksempel på personvernfremmende teknologi. En VPN oppretter en sikker og kryptert "tunnel" mellom brukerens enhet og nettverket. Den beskytter dermed brukerens personopplysninger som IP-adresse, nettrafikkdata og bidrar til å omgå geografiske begrensninger (Alshalan et al., 2016). Det finnes flere selskaper som tilbyr VPN-tjenester, som for eksempel NordVPN, ExpressVPN, Surfshark, Google One og Cisco AnyConnect.

Namara et al. (2020) argumenterer for at brukernes motivasjoner og bruksmønstre kan deles inn i praktiske og emosjonelle hensyn i sin studie om VPN-bruk. Emosjonelle hensyn identifiseres som den primære motivasjonen for å benytte en VPN som personvernfremmende teknologi, og er knyttet til økende personvernbekymringer, frykt for digital overvåking, medieoppmerksomhet og manglende tillit til personvernregulering (Namara et al., 2020). Praktiske hensyn påvirker også brukerens anvendelse av VPN, og handler behovet for anonymitet, tilgang til bestemte nettverk og andre spesifikke personverntiltak (Namara et al., 2020). På bakgrunn av dette vil det i denne oppgaven være i interessant å ta utgangspunkt i personvernfremmende teknologier som beskyttelsestiltak. Dette for å kunne undersøke nordmenns beskrivelser av hvilke situasjoner eller tilfeller som de opplever et behov for å beskytte personopplysningene deres. Det kan i tillegg være av interesse å se nærmere på om beskrivelser av deres holdninger til personvern er knyttet til deres bruk og meningsdannelse rundt personvernfremmende teknologier.

3. Metode

I denne delen vil jeg presentere metoden som ble benyttet i denne oppgaven. Det ble klart i løpet av arbeidet at valget av metode var en kompleks og ikke-lineær prosess. Dette innebærer flere kritiske vurderinger og beslutninger som måtte tas for å velge en hensiktsmessig og fordelaktig tilnærming som passet oppgavens formål og problemstilling. Metodedelen har som mål å gi en grundig forståelse av den metodiske tilnærmingen som ble brukt i oppgaven, samt å begrunne de valgene og tiltakene som ble gjort. Formålet med dette er å gi et overblikk over forskningsprosessen som en helhet. I denne delen vil jeg diskutere valget av intervju som metode, utvalgsprosessen, bruk av måleinstrumentet (intervjuguider), behandlingen av datamaterialet og vurderingen av oppgavens kvalitet.

3.1 Valg av metode

Valget av metode er sentralt for å kunne besvare oppgavens problemstilling og belyse temaet personvern fra nordmenns perspektiv. Det ble derfor ansett som hensiktsmessig å vurdere hvorvidt det kunne anvendes en kvalitativ eller kvantitativ tilnærming til å besvare oppgavens problemstilling. I denne sammenhengen har eksperimenter og kvantitative spørreundersøkelser vært blant de mest utbredte metodiske tilnærmingene som har blitt brukt til å undersøke forholdet mellom individers holdninger til personvern og atferd (Barth & de Jong, 2017; Gerber et al., 2018; Kokolakis, 2017). Her ble det viktig å vurdere hvorvidt metoden var tilpasset oppgavens formål og behov før jeg satt i gang med neste steg av forskningsprosessen. For å kunne besvare problemstillingen ble det vurdert som nødvendig og hensiktsmessig å vektlegge et forskningsdesign som gjorde det mulig å utforske og få dypere innsikt i nordmenns meningsdannelse, perspektiv og refleksjoner rundt personvern og deres personopplysninger. Videre har et mindretall av studiene innenfor forskningslitteraturen tatt i bruk kvalitative metoder i form av dybde- og fokusgruppeintervju (Kokolakis, 2017). Til tross for at kvalitative metoder er mindre utbredt i forskningslitteraturen ble denne metodiske tilnærmingen oppfattet som relevant og fordelaktig for å besvare oppgavens problemstilling. På bakgrunn av dette har jeg valgt kvalitative dybdeintervju som oppgavens metodiske tilnærming.

3.1.1 Semistrukturerte dybdeintervju

I kvalitative forskningsstudier kan intervjuer struktureres på tre vanlige måter: strukturerte, semistrukturerte og ustrukturerte (Kvale & Brinkmann, 2015). Disse formene skiller seg fra

hverandre med hensyn til intervjusituasjonens struktur, maktbalansen mellom intervjuer og informant, samt andre aspekter som tid, nærhet og åpenhet. I denne oppgaven vil jeg fokusere på en semistrukturert tilnærming. Målet med dette er å forbedre og utvikle en intervjuguide med forhåndsdefinerte spørsmål basert på temaer og fokusområder knyttet til personvern, innsamling, behandling og bruk av personopplysninger. Dette vil bidra til refleksjon, flyt og diskusjon gjennom oppfølgingsspørsmål, relasjonsbygging og utforskning av temaer under intervjuet (Tjora, 2021). Intervjuet er en interaktiv prosess der forskeren og informanten diskuterer individuelle synspunkter, forståelser og perspektiver på et aktuelt fenomen. Deltakerne som tar del i denne intervjuprosessen, blir satt i fokus og får en aktiv og bidragsytende rolle som informanter.

Denne strukturen gir meg fleksibilitet til å tilpasse spørsmålene basert på informantenes uttrykksmåter og andre temaer som kan oppstå. Dette øker graden av fleksibilitet og tilpasningsevne i intervjuet som bidrar til at jeg kan utforske og avdekke betydningen av individets meningsdannelse, indre tankeprosesser og erfaringer med personvern og personopplysninger (Kvale & Brinkmann, 2015). Ved å velge intervjuer som metode for oppgaven, får jeg muligheten til å komme i direkte kontakt med et utvalg norske informanter, noe som legger til rette for refleksjon, erfaringsdeling og tolkning. Dette bidrar til å maksimere og effektivisere datainnsamlingsprosessen (Bryman, 2016; Tjora, 2021).

Personvern er et komplekst tema, og det var derfor viktig å sette av nok tid til at informantene kunne uttrykke seg fritt og føle seg komfortable i intervjusituasjonen. Dybdeintervju ble derfor valgt som metode for oppgaven, da det gir et tilstrekkelig og tilpasset grunnlag for å diskutere komplekse problemstillinger og temaer (Tjora, 2021). Varigheten på intervjuene ble satt til 45-60 minutter, slik at det var tilstrekkelig med tid til å diskutere komplekse problemstillinger og temaer knyttet til informantenes holdninger til personvern og deres forståelse av atferd og beslutninger. Imidlertid varierte lengden på intervjuene mellom informantene, noe som er forventet, da enkeltmennesker er forskjellige og tilpasser seg intervjusituasjonen på ulike måter basert på deres villighet, engasjement og mulighet til å uttrykke sine indre tanker, erfaringer og opplevelser.

3.2 Utvalg og rekrutteringsprosessen

Utvalget er avgjørende i kvalitative intervjustudier, da det utgjør kilden til den datamaterialet og fenomenet som skal undersøkes Tjora (2021). Rekrutteringsprosessen spiller dermed en

viktig rolle i å svare på oppgavens problemstilling. I denne oppgaven har jeg rekruttert 11 informanter som kunne bidra med interessante og nyanserte perspektiver på personvern. Videre har jeg valgt å dele disse 11 dybdeintervjuene inn i to utvalg av eksperter og brukere (se Tabell 1). Alle informantene er anonymisert med tilfeldig valgte navn, slik at sitater fra de ulike informantene som fremheves i analysedelen ikke kan identifiseres. I denne sammenhengen er det verdt å bemerke at oppgavens problemstilling fokuserer på brukerdelen av utvalgets meningsdannelse og beskrivelser. Videre vil utdrag fra ekspertenes intervjuer kun trekkes inn for å diskutere og belyse et annet perspektiv på den behandlingsansvarliges rolle sammenlignet med brukerdelen av utvalgets beskrivelser.

Tabell 1. Oversikt over informanter

Navn (annonymisert)	Gruppe	Fagfelt/Aldersgruppe
Eva	Ekspert 1	Rettsikkerhet (jurist)
Emma	Ekspert 2	Informasjonssikkerhet
Aksel	Bruker 1	21-30
Andrea	Bruker 2	21-30
Adam	Bruker 3	21-30
Bente	Bruker 4	31-49
Berit	Bruker 5	31-49
Bjørn	Bruker 6	31-49
Casper	Bruker 7	Over 50
Cathrine	Bruker 8	Over 50
Christoffer	Bruker 9	Over 50

3.2.1 Presentasjon av utvalget

Den første delen av utvalget består det jeg har valgt å omtale som eksperter. Innledningsvis i forskningsprosessen og utviklingen av oppgavens problemstilling opplevde jeg det som nødvendig å få bedre oversikt og innhente tilstrekkelig kunnskap om personvernsituasjonen i Norge. Personvernkommisjonens (2022) rapport gå et godt utgangspunkt for dette, men samtidig opplevde jeg personvernregelverket og prosessen rundt hvordan brukerens personopplysninger blir samlet inn, behandlet og brukt som kompleks og omfattende. Dette var med på å skape et behov for å komme i kontakt med noen som hadde grunnleggende kompetanse innen personvern. Formålet med dette var å innhente nødvendig

bakgrunnsinformasjon som kunne belyse behandlingsansvarliges perspektiv og rolle når det gjelder brukerens personvern og personopplysninger. For å kunne rekruttere denne delen av utvalget tok jeg først kontakt med en bekjent med kompetanse innenfor rettsvitenskap som til daglig jobber med personvern for en behandlingsansvarlig i Norge. Videre ønsket jeg å ha med en enda en ekspert i utvalget og tok kontakt med aktuelle informanter via e-post i mitt allerede eksisterende nettverk. Den andre informanten i utvalget har kompetanse innen informasjonssikkerhet og tidligere jobbet som personvernombud i en offentlig virksomhet. Når det gjelder ekspertdelen av utvalget, ble deres fulle navn, arbeidssted og -tittel anonymisert etter deres ønske. Det ble ikke ansett som nødvendig å inkludere disse opplysningene, men det kan potensielt svekke deres troverdighet som eksperter i noen grad.

Den andre delen av utvalget består av ni intervjuer med brukere. Under rekrutteringsprosessen ble det tydelig at det ville være interessant å sette alderskriterier for denne delen av utvalget ved å dele brukerne inn i tre aldersgrupper: 21-30 år, 31-49 år og over 50 år. Formålet med dette var å undersøke om det var mulig å identifisere noen aldersforskjeller når det gjelder brukerens beskrivelser og meningsdannelse. Kokolakis (2017) fremhever blant annet at personvernparadokset ikke bare kan anses å gjelde i forhold til det Barnes (2006) argumenterer for som et symptom blant unge menneskers manglende behov for beskyttelse og villighet til å dele personopplysninger. Noe av formålet med å sette disse kriteriene for utvalget i form av aldersgrupper var å forsøke å skille informantene fra hverandre ved at de ikke tilhørte samme sosiale nettverk, eller var i samme livssituasjon. Videre ble ikke kjønnsforskjeller vektlagt i oppgaven, men det er verdt å merke seg at Gerber et al. (2018) i sin litteraturgjennomgang fremhever at kvinner til en viss grad er mer villige til å dele personopplysninger enn menn i kontekst av sosiale medier.

3.2.2 Utvalgsproblemer i rekrutteringsprosessen

Rekrutteringsprosessen er en vesentlig del av den metodiske tilnærmingen i denne studien. Til tross for fordelene med fleksibilitet og åpenhet i intervjusituasjonen, er det viktig å erkjenne begrensningene og problemene knyttet til utvalget. I denne sammenhengen vil jeg fremheve nærhet, tid og tilgjengelighet som faktorer som har påvirket rekrutteringsprosessen. Nærhet refererer til min relasjon og kjennskap til informantene i utvalget (Tjora, 2021). Jeg benyttet mitt eksisterende nettverk av bekjente for å rekruttere en del av utvalget, noe som gjorde det enklere å komme i kontakt med relevante informanter i begynnelsen. Tid spilte også en avgjørende rolle i rekrutteringsprosessen. Dette omfattet varigheten av dybdeintervjuene og forskningsperioden, samt planlegging av kontakter, avtaler og reisevei for gjennomføringen

av intervjuene. Informantene måtte sette av tid i sin hverdag for å delta i dybdeintervjuene. Tilgjengelighet var derfor en sentral utfordring for forskeren i forhold til tilgangen på aktuelle informanter. Når det gjelder brukerdelen av utvalget, var det ingen krav til forkunnskaper, men alderskriteriet begrenset tilgjengeligheten av informanter. Det oppsto problemer med å komme i kontakt med aktuelle informanter i aldersgruppen 31-49.

For å imøtekomme og håndtere disse utfordringene, ble snøballmetoden brukt som en utvalgsmetodikk. Snøballmetoden involverer å starte med mitt etablerte nettverk av «nøkkelinformanter» og deretter systematisk innhente nye potensielle informanter gjennom anbefalinger fra det eksisterende utvalget (Andrews & Vassenden, 2007). Det var også viktig å reflektere over hvorfor og hvordan informantene valgte å delta i dybdeintervjuene (Tjora, 2021). Her ønsket jeg å skille mine personlige relasjoner og forskerrollen fra hverandre under intervjuene. Det var også fordeler med å gjennomføre de fleste intervjuene ansikt-til-ansikt, der både jeg og informantene var fysisk til stede. Formålet med dette var å skape nærhet i intervjusituasjonen som var sammenlignbar på tvers av utvalget (Kvale & Brinkmann, 2015; Tjora, 2021). Informantene i dette utvalget ble rekruttert fra Trondheim og Oslo, noe som medførte at jeg som intervjuer måtte reise for å møte dem. Dette førte til begrensninger knyttet til informantenes tilgjengelighet og geografiske lokalisering. Derfor ble fire av intervjuene gjennomført digitalt ved hjelp av videokonferanseverktøy som Zoom og Teams. Dette bidro til en dypere forståelse av utvalgsprosessen, noe som ofte blir oversett eller undervurdert i kvalitative intervjustudier (Andrews & Vassenden, 2007).

3.2.3 Metningspunkt

En relevant problemstilling som kvalitative intervjustudier står ovenfor, er spørsmålet om når datagenereringen skal avsluttes og det ikke skal rekrutteres eller gjennomføres flere intervjuer. I denne sammenhengen er det mulig betegne dette som et metningspunkt som innebærer et punkt der den nye empirien (dataene) som genereres i intervjusituasjonen ikke lenger anses til å avdekke nye aspekter eller momenter ved det aktuelle fenomenet (Tjora, 2021). Den opplevde metningen vil på denne måten kunne brukes som et utgangspunkt for å avslutte intervjuprosessen og gå dermed gå over til neste fase i forskningsprosessen (behandling og analyse). Det er verdt å bemerke at det kan være vanskelig å definere eller komme med påstander om at det er oppnådd et metningspunkt (Bryman, 2016; Tjora, 2021). Videre valgte jeg å avslutte rekrutteringsprosessen etter at jeg opplevde flere gjentakende beskrivelser i informantenes uttrykksmåter. Det samme gjaldt i forhold til inndelingen av aldersgrupper der jeg ikke ønsket en overvekt av informanter i av aldersgruppene. Her er det

verdt å bemerke at flere intervjuer kunne bidra til å tilføye andre nyanserte beskrivelser og perspektiver På denne måten er det viktig at jeg selv tok kritiske vurderinger i utvalgsprosessen som ikke kun var basert på antall intervjuer, men som er tilpasset og kunne begrunnes basert på oppgavens formål og behov.

3.3 Måleinstrument og intervjuprosessen

For å gjennomføre dybdeintervjuene ble det nødvendig å utarbeide en intervjuguide bestående av spørsmål og fokusområder. Intervjuguiden fungerte som et utgangspunkt og bidro til semistrukturen i intervjusituasjonen. Ifølge Tjora (2021) er det tre faser som er sentrale i dybdeintervjuet: oppvarmingsspørsmål (introduksjon), refleksjonsspørsmål (hoveddel) og avrundingsspørsmål (avslutning). Denne strukturen bidrar til å gi et overblikk over intervjusituasjonen i forskjellige faser. Tidlig i forberedelsene og utarbeidelsen av intervjuguiden vurderte jeg det som hensiktsmessig å bruke visuelle hjelpemidler under intervjuene. Personvern er et komplekst tema, spesielt knyttet til tekniske aspekter og lovverket rundt innsamling, behandling og bruk av personopplysninger. Dette gjelder også i forhold til mengden av informasjonskapsler som brukere møter på og må ta stilling til.

I denne sammenhengen ble det vurdert som fordelaktig og hensiktsmessig å bruke min egen datamaskin for å illustrere ulike typer informasjonskapsler på forskjellige nettsider. Her opprettet en ny brukerkonto og nettleserøkt som kunne vise informantene deres første møte med den aktuelle nettsiden. Dette gjorde det mulig for informanten å dele sine opplevelser, tanker og erfaringer med informasjonskapslene på nettsider de selv hadde kjennskap til. Denne visuelle eller stimulerende tilnærmingen bidro til at informantene kunne reflektere og beskrive hva de gjorde når de møtte informasjonskapsler på nettsider de var kjent med, innenfor rammen av intervjuet (Bryman, 2016; Tjora, 2021). Før jeg startet intervjuprosessen, var det viktig og nødvendig å teste intervjuguidene. Formålet var å kunne gjøre justeringer i innholdet, formuleringene av spørsmålene og varigheten av intervjuene (Tjora, 2021). Intervjuguiden kan forbedres og tilpasses både før og underveis i prosessen, men pilotintervjuene ga et nyttig utgangspunkt og oversikt for å tilpasse verktøyet tidlig i prosessen. Jeg gjennomførte to pilotintervjuer med bekjente for hver av intervjuguidene. Dette gjorde det mulig å tilpasse varigheten, spørsmålsformuleringene og antall spørsmål.

3.3.1 Strukturen på intervjuguiden

For ekspertdelen av utvalget ble det utarbeidet en intervjuguide med fem deler (se Vedlegg 1). Første del omhandlet generelle spørsmål om informantenes bakgrunn og deres arbeid med personvern. Andre del inneholdt spørsmål om informantenes perspektiv og forståelse av personvern i forbindelse med personvernsituasjonen i Norge, samt definisjonen av personopplysninger. Den tredje delen fokuserte på personvernregelverket i Norge og brukerrettigheter. Her kunne spørsmål bidra til en dypere forståelse av personvernforordningen (GDPR) og personopplysningsloven i Norge, samt beskrive virksomheters eller behandlingsansvarliges plikter knyttet til innsamling, behandling og bruk av personopplysninger. Deretter ble den fjerde delen viet informantenes kunnskap om bruk av informasjonskapsler og personvernfremmende teknologier. Avslutningsvis ble det stilt spørsmål om informantene hadde noen råd eller tips til brukere.

Intervjuguiden for ekspertdelen ble utformet med vekt på veiledende og åpne spørsmål som ga informantene mulighet til å utdype sin kunnskap, kompetanse og erfaringer. Disse dybdeintervjuene dannet grunnlaget for utviklingen av intervjuguiden for brukerdelen. Spørsmålene ble utledet fra forskningslitteraturen for å identifisere relevante fokusområder. Dette var nyttig for å forklare ulike begreper, spesielt knyttet til perspektiver på personvern, brukerrettigheter, GDPR, personvernforordningen, bruk av informasjonskapsler, personvernfremmende teknologier og tilhørende eksempler.

Til forskjell var intervjuguiden for brukerdelen ble delt inn i seks deler (se Vedlegg 2). Første del inneholdt oppvarmingsspørsmål om informantenes bakgrunn, bruk av digitale enheter og Internett. Neste del omhandlet informantenes forståelse og perspektiv på personvern, samt definisjonen av personopplysninger. Deretter fulgte spørsmål om informantenes rettigheter, GDPR og det norske regelverket. Den fjerde delen omhandlet bruk av informasjonskapsler, der visuelle hjelpemidler som delt skjerm ble brukt for at informantene selv kunne undersøke hvordan informasjonskapsler ble brukt på relevante nettsider. Dette bidro til at informantene kunne reflektere over og beskrive hvordan den behandlingsansvarlige samlet inn, behandlet og brukte deres personopplysninger til ulike formål. Den neste delen handlet om informantenes kjennskap til og bruk av personvernfremmende teknologier. Til slutt ble det stilt avrundingsspørsmål om informantenes egne erfaringer, opplevelser og tips til andre. Disse spørsmålene ble også utledet fra forskningslitteraturen for å identifisere relevante fokusområder knyttet til personvern, brukerrettigheter, GDPR, personvernforordningen, bruk av informasjonskapsler, personvernfremmende teknologier og tilhørende eksempler.

3.4 Datainnsamlingsprosessen og analyseprosedyre

Databehandlingsprosessen omfatter en analyseprosedyre eller strategi for videre behandling av dataene (empirien). Formålet med å beskrive denne prosessen er å gi innsikt i hvordan og hvorfor datamaterialet (empirien) ble behandlet, samt de forutsetningene og strategiene som ble brukt i den videre analysen (Bryman, 2016; Tjora, 2021). Videre ble det gjennomført lydopptak av alle intervjuene ved hjelp av en båndopptaker og diktafonappen til nettskjema. Intervjuene ble deretter fullstendig transkribert både underveis og etter intervjuprosessen. I ettertid ble det utført nødvendige kontrollere av de transkriberte tekstdokumentene for å forsikre at de samsvarte med lydopptakene. I tillegg ble det skrevet et sammendrag på 3-4 sider som oppsummerte intervjuene for å gi bedre oversikt og fungerte som et første steg i behandlingsprosessen. Disse 11 transkripsjonene utgjør datamaterialet eller empirien i form av tekstdata. Det er viktig å merke seg at transkripsjoner ikke kan anses som fullstendig objektive eller nøytrale. Videre var det det viktig å inkludere momenter fra intervjusituasjonen der informantene stoppet opp, søkte etter ord eller hadde problemer med å formulere seg (Kvale & Brinkmann, 2015; Tjora, 2021).

3.4.1 SDI-metoden som analyseprosedyre

Det neste delen i databehandlingsprosessen var å starte bearbeidingen eller behandlingen av tekstdataene (transkripsjonene). Her var viktig å velge en analysestrategi som tillot en systematisk og strategisk tilnærming til dataene. Formålet var å gi leseren et helhetlig inntrykk av forskningsprosessen (Bryman, 2016). Det finnes ulike tilnærminger til behandling eller analyse av kvalitative intervjudata. I dette tilfellet valgte jeg å bruke det Tjora (2021) beskriver som den stegvis-deduktive induktive metode (SDI-metoden). Denne metoden gir en strukturert tilnærming til behandlingen av datamaterialet som ble generert fra dybdeintervjuene i en trinnvis prosess. Ved første øyekast kan SDI-metoden, i likhet med mye annen kvalitativ forskning virke induktiv (fra data til teori), men den tar også hensyn til deduktive tilbakekoblinger og vektlegger en teoretisk motivasjon i forskningsprosessen (Tjora, 2021). Metoden inkluderer seks forskjellige «tester» eller tilbakevendende kritiske spørsmål som bidrar til kvalitetssikring mellom de ulike induktive stegene i modellen

Det første trinnet omhandler generering av empiriske data, samt en utvalgs- og datatest (Tjora, 2021). Dette er noe jeg allerede har vært inne på i diskusjonen rundt utvalget og rekrutteringsprosessen. Videre var utvalgstesten fordelaktig for å undersøke om at jeg hadde en passende utvalgsstørrelse eller trengte å rekruttere flere informanter. Formålet med dette er å forsikre meg om at jeg hadde nådd et metningspunkt. Den andre delen av metoden dreier

seg om dataforberedelse (Tjora, 2021). Dette er noe jeg allerede har diskutert i forhold til transkriberingen av lydopptakene (rå empiriske data) og anonymisering. Videre involverer datatesten kritiske spørsmål om hvorvidt intervjuguiden kan forbedres eller tilpasses, og om tekstdataene er tilstrekkelige og detaljerte nok (Tjora, 2021). Etter at disse testene var bestått kunne jeg gå over til neste steg i SDI-metoden som omhandler koding og systematisering av datamaterialet.

3.4.2 Koding og gruppering

Her ble analyseprogrammet NVivo brukt for å få oversikt og systematisere tekstdataene fra intervjuene. Videre gikk det over til koding av tekstdataene gjennom en induktiv empirisk kodetilnærming (Tjora, 2021). Formålet med denne kodestrategien er å forsøke å hente ut essensen i tekstdataene ved redusere påvirkningen av mine forutinntatte antagelser, forventinger, tidligere forskningslitteratur på fenomenet eller teoretiske perspektiver. Dette vil kunne bidra idégenering som er forankret i informantenes uttrykksmåter, perspektiver og utsagn (Tjora, 2021). Her startet jeg med å gå over den første intervjutranskripsjonen for å opprette og utvikle koder av alt av tekstdataene som ble brukt til å identifisere og fremheve informantenes utsagn i form av fraser og setninger. Videre ble de resterende intervjutranskripsjonene gjennomgått med utgangspunkt i de allerede opprettede kodene, samt nye koder som ble identifisert og opprettet. Formålet med dette er å skape en bevisst kobling mellom kodene og empirien noe som vil kunne bidra til idégenering og belyse interessante aspekter ved informantenes tolkninger og beskrivelser.

Det ble hvert tydelig at dette var en tidskrevende og utfordrende prosess som resulterte i et 167 empirinære koder. Her var kodetesten nødvendig for å undersøke hvorvidt kodene kunne anses å representere empirinær koding eller kun bidro til å sortere empirien (Tjora, 2021). I denne sammenhengen var det hensiktsmessig å undersøke om kodene faktisk belyste i detalj hva informantene sa, og ikke bare beskrev eller sortere generelle temaer gjennomgående temaer. Videre var det viktig å gå gjennom alle kodene igjen systematisk for å se om disse kunne omkodes og dermed forsikre meg om at ingen koder ble fjernet uten grunn. Etter å ha gjennomført kodetesten ble et antall på 25 koder fjernet. Dette resulterte i en kodestruktur bestående av 142 empirinære koder. Videre går vi over til å gruppere kodene tematisk sammen gjennom en form for kodegruppering (Tjora, 2021). Dette vil danne utgangspunktet for strukturen i den videre analysen. Videre var det mulig å gjennomføre en pågående kodegrupperingstest for å teste hvorvidt disse gruppene kunne anses å være hensiktsmessige og relevante for å kunne besvare oppgavens problemstilling (Tjora, 2021). Dette var en

krevende prosess som krevde en del prøving og feiling når det kom til å samle alle kodene innenfor relevante og konkret kodegrupper.

For å kunne gjøre dette valgte jeg innledningsvis å kategorisere de ulike kodene som hadde innbyrdes tematisk sammenheng eller likheter i ulike kategorier. Videre opplevde jeg at disse som gruppene som relativt smale og bestemte meg for derfor for å opprette et nytt overordnet nivå av kodegrupper (Tjora, 2021). Det første steget i kodegrupperingsprosessen resulterte i det jeg har valgt å betegne som 10 undergrupper, som senere ble plassert under tre overordnede tematiske kodegrupper. Formålet med dette var å utarbeide kodegrupper som var forskningsmessig interessante, bidro til en empirinær kodestruktur og skilte seg tematisk fra hverandre (se Vedlegg 3). Disse kodegruppene representere på denne måten strukturen til den senere analysen, og blir beskrevet som følgende (1) *forhold til behandlingsansvarliges praksiser, (2) villighet til å avsløre*, og (3) *behov for beskyttelse.* Videre er det mulig å se hvordan de ulike kodegruppene representerer tre hovedtemaer som går i dybden og belyser flere relevante aspekter av informantenes beskrivelser av deres holdninger til personvern, atferd og beslutninger når det gjelder deres personopplysninger.

3.4.2 Utvikling av konsepter og teori

Det neste steget i SDI-metoden omhandler utviklingen av konsepter (Tjora, 2021). Noe som er med på å fremheve den teoretiske ambisjonen og motivasjonen som ligger bak databehandlingsprosessen. Til forskjell fra de tidlige stegene innebære å løfte blikket gjennom et teoretisk dypdykk for undersøke sammenheng mellom de foreslåtte kundegruppene i lys av oppgavens teoretiske rammeverk og tidligere forskningslitteratur (Tjora, 2021).Videre var det mulig å se hvordan kodegruppene (2) villighet til å avsløre og (3) behov for beskyttelse var nært knyttet til forskningslitteraturen som individers avslørings- og beskyttelsesatferd (Boerman et al., 2021; Knijnenburg et al., 2013; Meier et al., 2021; Taddei & Contena, 2013). Det samme vil kunne anses å gjelde for den første kodegruppen (1) forhold til behandlingsansvarliges praksiser, som omhandler grunnleggende personvernprinsipper, -praksiser eller en form for innebygd personvern (Cavoukian, 2009, 2020). I denne sammenhengen vil jeg ikke presentere noen nye konsepter eller teorier som er en del av det siste steget i SDI-metoden (Tjora, 2021). Til forskjell vil jeg diskutere hvordan forholdet mellom disse tre kodegruppene er med på å belyse sentrale aspekter av nordmenns beskrivelser av deres holdninger til personvern knyttet til deres atferd og beslutninger om å dele eller beskytte personopplysninger på nett. Dette med utgangspunkt relevante teoretiske perspektiver og tidligere forskning på personvernparadokset som forklaringsmåte,

personvernkynisme som en forsvarsmekanisme, digital kompetanse som en forutsetning, samt bruken og behovet for beskyttelsestiltak gjennom personvernfremmende teknologier. Videre vil jeg diskutere hvorvidt dette samsvarer, motstrider eller har noen praktiske og teoretiske implikasjoner. I denne sammenhengen vil dette kunne tolkes som å bidra til en form for teoriutvikling (Tjora, 2021). I sin helhet kan SDI-metoden på denne måten brukes hensiktsmessig for å få et overordnet perspektiv, fungere som et utgangspunkt for å forstå og et dypere innblikk i alle valgene og vurderingene som er tatt i forskningsprosessen fra start til slutt på en systematisk, stegvis og tilbakevendende måte.

3.5 Kvalitetskriterier

For å vurdere kvaliteten av denne masteroppgaven har jeg valgt å fokusere på tre formelle kvalitetskriterier: pålitelighet, gyldighet og generaliserbarhet (Tjora, 2021). Ved å vektlegge disse kvalitetskriteriene bidrar jeg til å legge viktige forutsetninger for en god forskningsprosess. Det innebærer ikke bare å være kritisk og reflektere over hvilke valg som har blitt tatt i løpet av denne prosessen. I denne sammenhengen er det viktig å se på forskningsprosessen i et helhetlig, overordnet og kritisk perspektiv. Videre vil diskusjonen av disse kvalitetskriteriene kunne bidra til å belyse oppgavens kvalitet og framstilling ved å knytte dette til presentasjonen av empirien.

3.5.1 Pålitelighet

Ifølge Tjora (2021) innebærer pålitelighet om oppgavens indre logikk og systematikken i forskningsprosessen. Utfordringen i kvalitative intervjustudier er å velge ut og presentere empirien på en god måte. Dette gjøres ved å inkludere utvalgte sitater som gir leseren et inntrykk av hvilke deler av empirien som blir brukt, og hvor store disse delene er. Det er viktig å merke seg at denne oppgaven er basert på to ulike utvalg av eksperter og brukere. Ekspertene blir i denne sammenhengen sitert for å belyse rollen og beskrivelsene knyttet til den behandlingsansvarliges perspektiv. Disse sitatene utgjør en mindre del av analysen, men formålet er å representere beskrivelser fra behandlingsansvarliges perspektiv i forhold til brukerne i utvalget. Dette gjelder spesielt for den første delen av analysen som omhandler behandlingsansvarliges praksiser. Videre vil jeg presentere utvalgte sitater fra informanter i brukerdelen av utvalget, som utgjør den største delen av analysen og er sentrale for å besvare oppgavens problemstilling. Jeg vil bruke anonymiserte navn basert på relevante karakteristikker som kjønn og alder for å differensiere mellom informanter (Tjora, 2021).

Målet er å belyse sentrale aspekter av empirien, samtidig som jeg forsøker å representere hele utvalget. For å styrke påliteligheten i oppgaven har jeg beskrevet relevante koblinger mellom empirien (sitater) og oppgavens teoretiske rammeverk. Dette viser hvordan relevante perspektiver og teorier har formet og inspirert analysen (Tjora, 2021) Pålitelighet omhandler også relasjonen mellom forskeren og informantene. Noen av informantene ble rekruttert fra mitt eget sosiale nettverk, og jeg kjente flere av dem personlig. Det er viktig å merke seg at mine personlige relasjoner kan påvirke intervjusituasjonen eller informantenes uttrykk, men uansett vil informantene tilpasse seg intervjusituasjonen uavhengig av om de kjenner forskeren fra før av. Jeg har forsøkt å rekruttere informanter som ikke var i samme livssituasjon, ved å inkludere ulike aldersgrupper.

3.5.2 Gyldighet og generaliserbarhet

Det neste kvalitetskriteriet handler om gyldighet, som handler om sammenhengen mellom oppgavens struktur og funn eller hovedmomenter (Tjora, 2021). Det handler om å besvare og belyse oppgavens problemstilling gjennom analyse og diskusjon. Bruken av utvalgte sitater fra intervjuene bidrar til å styrke oppgavens gyldighet ved å belyse sentrale aspekter av informantenes beskrivelser. Utdragene fra intervjuene gir innsikt i hvordan informantene tenker, reflekterer og erfarer sin forståelse av sin atferd og beslutninger i intervjusituasjonen (Tjora, 2021). Jeg har bevisst valgt å belyse relevante koblinger mellom oppgavens teoretiske rammeverk og empirien (sitater) ved å inkludere teoretiske innspill i analysen. Formålet med dette er å sikre at analysens presentasjon er forankret i relevant forskningslitteratur og innenfor rammene av samfunnsvitenskapelig forskning.

Videre ble det tatt en rekke pragmatiske valg i forskningsprosessen som førte til nødvendige justeringer og endringer av oppgavens problemstilling. Jeg vil imidlertid ikke trekke noen antagelser eller konklusjoner om hva som påvirker nordmenns holdninger til personvern eller deres faktiske atferd. Dette kan ses i lys av det neste kvalitetskriteriet, som er generaliserbarhet. Oppgavens relevans går utover den spesifikke sammenhengen og konteksten den er gjennomført i, og kan bidra til ny innsikt knyttet til fenomenet. Ifølge Tjora (2021) kan dette beskrives som en form for konseptuell generalisering. I denne oppgaven utvikler jeg ikke et nytt konsept, men presenterer og diskuterer hvordan hovedmomentene fra analysen bidrar til teoriutvikling. Det er verdt å merke seg at studiet av personvern er et kontekstavhengig, flerdimensjonalt og komplekst fenomen (Kokolakis, 2017; Solove, 2021). Denne masteroppgaven er gjennomført i en norsk kontekst med et utvalg av nordmenn, og

utvalgsstørrelsen begrenser på denne måten generaliserbarheten av denne nye innsikten til andre tilfeller eller situasjoner.

3.5.3 Etiske prinsipper og helheten

I tillegg til disse kriteriene er det flere forskningsetiske prinsipper som oppgaven er basert på, inkludert forskerens integritet, informantenes rettigheter og personvern, informert samtykke, konfidensialitet, behandling av personopplysninger, ærlighet og gjensidighet (Tjora, 2021). Anonymitet og sikker behandling av informantenes personopplysninger ble ivaretatt for å møte deres behov og redusere risikoen for å skape lojalitetsproblemer eller at informantenes opplysninger kom på avveie. Det er også viktig å reflektere over min rolle som forsker, inkludert mine styrker, svakheter og erfaringer, og hvordan de kan påvirke forskningsprosessen. Disse etiske prinsippene understreker behovet for å tilnærme seg og synliggjøre forskningsprosessen som helhet, og vurdere metodens formål, fordeler, verdi og innhold. Det er flere etiske problemstillinger og vurderinger som tas hensyn til, spesielt knyttet til informantenes personvern og andre forskningsetiske hensyn. Jeg utarbeidet et informasjonsskriv og et samtykkeskjema som ble sendt til informantene før intervjuet for å imøtekomme dette (se Vedlegg 4). Dette ga informantene en oversikt over oppgavens innhold og formål, samt nødvendig informasjon om deres rettigheter. Jeg sendte også inn en søknad om behandling av personopplysninger til Sikt, hvor oppgavens formål, innhold og prosedyre for behandling av personopplysninger i forskningsprosjektet ble beskrevet detaljert. I sin helhet belyser disse de grunnleggende etiske prinsippene og kvalitetskriteriene behovet for å tilnærme seg og synliggjøre forskningsprosessen på en systematisk og helhetlig måte.

4. Analyse

For å kunne besvare oppgavens problemstilling ar jeg valgt å dele analysen inn i tre deler for å forsøke å belyse nordmenns beskrivelser av deres holdninger til personvern er knyttet til deres forståelse av, atferd og beslutninger om deres personopplysninger. Denne inndelingen er et resultat av tre overordene kodegrupperinger eller relevante hovedtemaer som danner strukturen til hvert delkapittel: (4.1) forhold til behandlingsansvarliges praksiser, (4.2) villighet til å avsløre og (4.3) behov for beskyttelse. Her vil jeg presentere utvalgte sitater fra informantene som belyser disse hovedtemaene.

4.1 Forhold til behandlingsansvarliges praksiser

Den første delen tar for seg det som blir betegnet som behandlingsansvarliges praksiser. Videre vil en rekke forskjellige aktører kunne opptre i rollen som behandlingsansvarlig. Formålet med denne delen er å belyse informantenes beskrivelser av deres forhold til, meningsdannelse rundt og perspektiv på den behandlingsansvarlige som samler inn, behandler og bruker personopplysningene deres. Her er det verdt å bemerke at sitater fra ekspertdelen av utvalget vil brukes til å representere den behandlingsansvarlige perspektiv og rolle. Videre vil hovedvekten av analysen basere seg på et utdrag av sitater fra informantene i brukerdelen av utvalget. Denne inndelingen gjør det mulig å sammenligne ulike beskrivelser og perspektiver på den behandlingsansvarliges praksiser. Først vil jeg fremheve innebygd personvern som en standard med utgangspunkt i informantenes beskrivelser og opplevelser av ulike personvernprinsipper og -rettigheter. Deretter vil jeg belyse hvordan informantenes meningsdannelse og perspektiv på den behandlingsansvarlige er knyttet til beskrivelser av deres opplevde grad av kontroll. Avslutningsvis vil jeg fremheve en todelt ansvarsfordeling mellom den behandlingsansvarlige og brukeren.

4.1.1 Innebygd personvern som en standard

I diskusjonen med informantene ble det etter hvert tydelig hvordan et flertall av informantene kom med beskrivelser av deres forhold til og opplevelse av offentlige eller private virksomheters innsamling, behandling og bruk av deres personopplysninger. I denne sammenhengen vil den behandlingsansvarlige innebære virksomheter eller aktører som Google, Meta, LinkedIn Schibsted, Aller Media eller NRK. Her ble det i hovedsak vektlagt beskrivelser av private aktører som informantene fremhevet. Eksperten Eva trekker blant annet frem begrepet innebygd personvern (Privacy By Design) for å forklare og beskrive

hvordan den behandlingsansvarlige forholder seg til ulike personvernprinsipper gjennom sine praksiser og behandlingsgrunnlag:

> «*Et av prinsippene til personvern er at man skal ha noe som kalles Privacy By Design, og det er jo det at man skal ha personvern som en del av arbeidsmetodikken. Det er jo det vi jobber med i bedriften min når vi jobber med mengder av data og mengde av statusobjekter. Så det er veldig viktig at vi fra A til Å tenker på hvordan vi kan bevare personvernet, og det er jo primært det jeg jobber med ved å sørge for at alt går rettmessig og at vi har alt på plass*.» (Eva)

Denne formen for innebygd personvern som informanten beskriver kunne bidra til dekke sentrale krav for å kunne behandle og samle inn personopplysninger. Den behandlingsansvarlige må på denne måten ta hensyn til en rekke grunnleggende personvernprinsipper ved å implementere og vektlegge ulike personverntiltak i sin arbeidsmetodikk (Cavoukian, 2009, 2020; Datatilsynet, 2022). Videre vil denne formen for innebygd personvern kunne tilpasses til behandlingsansvarliges grunnlag for å samle inn, behandle og bruke personopplysninger til ulike formål. Innebygd personvern fungerer på denne måten som en standard og garanti for at brukerens rettigheter og personopplysninger blir ivaretatt i alle faser av innsamlings- og behandlingsprosessen (Datatilsynet, 2022). Når det gjelder brukerens perspektiv og opplevelse av behandlingsansvarliges praksiser nevner informantene flere aspekter av deres personvernrettigheter og hvordan de mener behandlingsansvarlige burde vektlegge, muliggjøre og håndheve dette. Informanten Bente fremhever blant annet behovet for innsyn:

> «*Mest sentralt for meg er det faktum at jeg bestemmer hvem som har innsyn. Det gjelder både for personer, men det gjelder og for større firmaer. Jeg ønsker ikke at Meta skal ha innsyn i mine personlige opplysninger som jeg legger igjen. Jeg ønsker heller ikke at andre skal finne meg på Google, på LinkedIn, finne ut hvor jeg bor eller hvem jeg er.»* (Bente, 33)

Retten til innsyn er sikrer på denne måten brukerens mulighet til å oversikt og informasjon om hvordan personopplysningene deres samles inn, behandles og lagres (Datatilsynet, 2018a; Personopplysningsloven, 2018, artikkel 15). Dette når det gjelder behandlingsansvarliges formål og behov for å samle inn personopplysninger på en effektiv og rettmessig måte. Noe som vil kunne bidra til å opplyse og bevisstgjøre brukeren. Videre vil dette bidra til å gi brukeren et dypere innblikk i hvordan personopplysningene deres lagres, hvem de deles med,

samt tilhørende sikkerhets- og beskyttelsestiltak (Datatilsynet, 2022). På denne måten kan behandlingsansvarlige tilrettelegge for at brukeren kan varsles om eventuelle endringer i deres praksiser eller personvernbrudd der personopplysninger kommer på avveie. Retten til innsyn er av flere rettigheter som er informantene fremhever, men Adam trekker også frem behovet for å slette personopplysninger:

> «*Å få muligheten til å slette noe som jeg synes er sensitivt. Det er viktig, eller det er kanskje det viktigste, og få innsyn da i dataene mine da. Hvis du trenger det da. Det er jo ikke alltid man føler at man trenger det, men hvis man føler for eksempel at man har blitt fremsatt feil eller utnyttet på noe måte.*» (Adam, 26)

På denne måten vil brukerens mulighet til å kunne slette eller fullstendig fjerne personopplysninger støtte opp under retten til sletting eller å bli glemt (Datatilsynet, 2018b; Personopplysningsloven, 2018, artikkel 17). Noe som gjør det mulig for brukeren begrense eller minimalisere innsamlings- og behandlingsprosessen. Dette ved å vurdere og ta beslutninger slette unødvendige eller sensitive personopplysninger. På denne måten vil det kunne medføre at mengden av personopplysninger som behandlingsansvarlige samler inn begrenses til et minimum som er tilpasses brukerens villighet til å dele personopplysninger og som respekterer deres personvernrettigheter (Colesky et al., 2016). Den behandlingsansvarlige er i denne sammenhengen pliktig til å slette brukeres personopplysninger etter forespørsel, men samtidig er dette avhengig av en sammensatt vurdering av andre forhold med hensyn til formålet med behandlingen (Datatilsynet, 2018b; Personopplysningsloven, 2018, artikkel 17). Til forskjell var det ikke alle informantene som hadde kjennskap til hvilke personvernrettigheter de hadde eller reflekterte kritisk rundt hvordan disse rettighetene var viktige når det kom til den behandlingsansvarliges praksiser.

4.1.2 Opplevd grad av kontroll

I denne sammenhengen er det mulig å se hvordan brukerens rett til innsyn og sletting vil kunne bidra til å gi brukeren kontroll over deres personopplysninger. Kontroll vil på denne måten innebære en strategi eller personvernprinsipp som tilrettelegger for brukerens evne til å kontrollere og påvirke innsamlings- og behandlingsprosessen (Cavoukian, 2009, 2020). Begge parter vil på denne måten kunne tildeles en viss grad av kontroll over brukerens personopplysninger. Muligheten for å avvise alle informasjonskapsler eller å trekke tilbake samtykke er noe som eksperten Eva trekker frem som en begrensning i sammenhengen med innebygd personvern:

> «*Det som er skummelt med at vi bruker samtykke, så er det jo selvfølgelig det at man kan trekke det tilbake, og det er det sånn at man må overholde det på en god måte. Da er det ekstra viktig med privacy by design*.» (Eva)

I denne sammenhengen er den behandlingsansvarlige på denne måten pliktig til å slette brukerens personopplysninger om samtykke trekkes tilbake (Personopplysningsloven, 2018, artikkel 17). Dette gjelder i forhold i tilfeller der behandlingen av brukerens personopplysninger er basert på et gyldig samtykke. Noe som gir et rettslig behandlingsgrunnlag for å behandle enkelte personopplysninger til forhåndsdefinerte og spesifikke formål. (Personopplysningsloven, 2018, artikkel 6). Det informanten beskriver som skummelt er på denne måten knyttet til usikkerheten rundt om brukeren opplever den behandlingsansvarlige formål og behov for deres personopplysninger som fordelaktig og er i trådd med deres forventninger. Til forskjell vil ikke dette oppleves som skummelt for brukeren som har rett til å avvise samtykke, men samtidig vil denne usikkerheten kunne påvirke brukerens beslutningstaking når det gjelder hvordan den behandlingsansvarlige tilrettelegger for muligheten til å avvise eller godta samtykke. Dette er noe informanten Cathrine trekker frem i diskusjonen rundt å avvise eller godta alle informasjonskapsler på nettsider og tjeneste der Google er behandlingsansvarlig:

> «*Hvis jeg ikke da blir stoppet videre i prosessen så ville jeg ha avvist alle, men jeg må jo innrømme at jeg ha tenkt at hvis jeg avviser alle så blir jeg stoppet på veien og at jeg skaper problemer meg da*.» (Cathrine, 59)

Her er det verdt å bemerke at rekke behandlingsansvarlige som Google ikke anbefaler og informerer sine brukere om at informasjonskapsler i noen tilfeller er nødvendige for å opprettholde funksjonaliteten eller gi adgang til enkelte nettsider (Google, 2023b). Videre er det mulig å se dette i forhold til behandlingsansvarliges manglende grunnlag for å behandle brukerens personopplysninger uten et gyldig samtykke. Noe som vil kunne påvirke deres mulighet til å tilby effektive tjenester og produkter til brukeren. Denne usikkerheten som informanten beskriver, er på denne måten knyttet til en manglende digital kompetanse eller uvitenhet rundt risikoen og konsekvensene ved å avvise samtykke (Büchi et al., 2017; Kehr et al., 2015; Lutz et al., 2020). Dette er noe som informanten Bente diskuterer videre ved å reflektere over brukerens evne til å kontrollere deres personopplysninger når behandlingsansvarlige som Meta (Facebook) ikke gir muligheter for å avvise bruk av informasjonskapsler:

> «*Samtidig problemet er at det ikke gir muligheten for å si nei. Den gir deg kun muligheten for å innhente aksept. Det er jo et genuint problem over alt, samtidig så er det ganske viktig. For Facebook har ikke lov til å gå videre med mindre de henter inn aksept, så de har jo valgt en metode, som betyr at de trenger disse informasjonskapslene for å fungere som et firma.»* (Bente, 33)

Videre stiller informanten på måten denne spørsmålstegn ved hva brukeren faktisk kan gjøre for å beskytte sine personopplysninger (Hargittai & Marwick, 2016). Det er mulig å se dette i forhold til behandlingsansvarliges manglende evne til å presentere og informere brukeren om samtykke på en forståelig måte. Dette inkluderer brukerens tilgang på relevant og aktuell informasjon om formålet bak samtykke i den gitte konteksten, samt behandlingsansvarliges håndhevelse av trygge og sikre behandlingspraksiser (Schaub et al., 2017). I denne sammenhengen har ikke den behandlingsansvarlige mulighet til å gå videre i behandlingsprosessen uten et gyldig samtykke. Noe som er med på å skape et økende behov for å engasjere brukeren til å akseptere og samtykke til bruken informasjonskapsler. Brukerens oppleve grad av kontroll vil på denne måten være avhengige av de spesifikke eller eksplisitte valgmulighetene de står ovenfor, men i noen tilfeller er det nødvendig at brukeren samtykker til bruken av funksjonelle informasjonskapsler (Schaub et al., 2017; Solove, 2013). Dette er noe informanten Andrea bygger videre på ved å forklare hvordan de bekymringsverdige aspektet ved behandlingsansvarliges bruk av informasjonskapsler. Videre hvordan tilgangen på og behandlingen av brukerens personopplysninger kan oppleves som tapt:

> «*At noen har så mye informasjon om deg liksom, men helt ærlig så føler jeg at kampen er litt lost. Fordi jeg har vært på sosiale medier hele ungdommstiden og mitt liksom relativt korte voksne liv. Ja, det er ikke noe som bekymrer meg i hverdagen. Selv om det kanskje sikkert burde vært en bekymring, så er det ikke det*.» (Andrea, 21)

Ifølge Solove (2013) står individer ovenfor komplekse problemstillinger og overveldende utfordringer for å ivareta sitt eget personvern og opplysninger på en fordelaktig måte. Dette vil kunne bidra til en opplevd følelse maktesløshet eller det informanten beskriver som en tapt kamp mot den behandlingsansvarlige. Videre vil dette også kunne gjelder i forhold til den behandlingsansvarlige som vil kunne bruke samtykkeforespørsler for å legitimere deres bruk av bruk av informasjonskapsler, samt innsamlings- og behandlingspraksiser (Solove, 2013). Kontrollen som brukeren tildeles av den behandlingsansvarlige vil på denne måten kunne

oppleves som subjektivt meningsløst (Hoffmann et al., 2016; Lutz et al., 2020). Det er mulig å se dette i forhold til at informanten beskriver en form for personvernkynisme som en forsvarsmekanisme som lar informanten rasjonalisere og rettferdiggjøre sine manglende bekymringer og behov for å beskytte personopplysningene på nett. Videre vil dette kunne bidra til det Hoffmann et al. (2016) beskriver som en form for resignasjon ved at brukeren velger å gi opp.

4.1.3 Hvem har ansvaret for personopplysningene mine?

Videre går dette inn på et spørsmål om ansvar eller ansvarsfordelingen mellom brukeren og den behandlingsansvarlige (Hargittai & Marwick, 2016). I denne sammenhengen vil dette innebære hvem som har ansvaret for å sikre at brukerens personopplysninger blir ivaretatt og beskyttet i alle deler av innsamling- og behandlingsprosessen. Det samme gjelder i forhold til mengden av opplysninger som blir samlet inn, samt vurderinger av formålet og grunnlaget for behandlingen. Dette ansvaret er noe eksperten Emma trekker frem, men forsøker samtidig å tydeliggjøre at brukeren har en sentral rolle i denne ansvarsfordelingen:

> «*Altså bedriften har jo et veldig stort ansvar for det er de som skal være de som behandle en stor mengde data og personopplysninger om deg, men du som individ har også et ansvar for å kunne sørge for at du har inngått et samarbeid eller levert fra deg personopplysninger på forsvarlig måte. Ved at du er skeptisk til at du ikke gir fra deg mer enn nødvendig, men definitivt så er det bedriften som har det største ansvar her.*» (Emma)

Dette er med på å belyse en delt ansvarsfordeling der behandlingsansvarlige har det overordnede ansvaret for behandlingen brukerens personopplysninger. Det er mulig å se dette i forhold til ansvarlighetsprinsippet som plikter den behandlingsansvarlige til å overholde personvernprinsippene og regelverket i personopplysningsloven på en forsvarlig, rettferdig og proaktiv måte (Datatilsynet, 2019a, 2019c; Personopplysningsloven, 2018, artikkel 5). Videre hvordan brukeren med fordel kan minimalisere eller begrense hva de samtykker til og ta beslutninger om hvilke personopplysninger de er villige til å gi fra seg. I denne sammenhengen vil ikke alle ha de samme forutsetningene for å ta fordelaktige beslutninger om deres personopplysninger (Bartsch & Dienlin, 2016; Büchi et al., 2017). Noe som forutsetter at bruken selv forstår og er klar over de mulighetene de har noe som er knyttet til deres digitale kompetanse. Dette er noe som informanten Cathrine bygger videre på ved å vektlegge det personlige ansvaret som brukeren selv har, men også hvordan regelverket og

lovgivningen som omfatter personopplysningsloven bidrar til å regulere denne ansvarsfordelingen:

> «*I utgangspunktet så tenker jeg på at jeg må passe på det selv. At det er et personlig ansvar, men jeg tenker jo også som det ligger et overordnet ansvar, regler og sånn sett normer i samfunnet vårt som gjør at vi skal være vernet. At det ligger nok lover og regler som gjør at de blir stoppet da, eller andre instanser som stopper de fra å samle inn opplysninger med mindre jeg har godtatt det da*.» (Cathrine, 59)

På denne måten vil brukeren selv har et personlig ansvar for å forsikre seg om at de selv er klar over hvilke personopplysninger avslører eller villig til å gi fra seg til den behandlingsansvarlige. Dette ved å beskrive hvordan brukeren selv burde være ansvarlig for å ta beslutninger om sine personopplysninger, men samtidig hvordan dette er avhengig av personvernregelverket som er satt på å plass for å regulere og sikre brukerens personvernrettigheter. Videre er dette knyttet til en forventning om at den behandlingsansvarlige innhenter og overholder brukerens samtykke på en forsvarlig og rettferdig måte. Det er mulig å se dette i forhold til Martin (2020) argument for at personvern er en kjerneverdi og knyttet til informantenes rimelige og spesifikke forventninger om hvordan personopplysningene deres samles inn, behandles og brukes. Dette er med på å tydeliggjøre hvordan behandlingsansvarlige til syvende og siste er den som er ansvarlig for å håndheve og demonstrere ovenfor brukeren at deres innsamlings- og behandlingspraksiser er i henhold til personvernregelverket og gjeldende juridiske krav. Dette går inn på det informanten Bjørn fremhever som en todeling av ansvarsforholdet:

> «*Nei, jeg tenker jeg det er et delt svar på. For det første så synes jeg jo at man har et ansvar selv selvfølgelig for det man på en måte sier ja til, men jeg synes det er dumt at det skal være en forbrukergreie. At vi skal legge all skylden eller alt ansvaret over på forbruken*.» (Bjørn, 42)

Denne todelingen beskriver på denne måten hvordan ansvaret mellom brukeren og en behandlingsansvarlige ikke vil være fordelt likt. Videre var det mest utbredte synpunktet blant informantene at brukeren selv hadde et personlig ansvar for hvilke personopplysninger de selv valgte å dele, men at den behandlingsansvarlige hadde ansvaret for at de ble behandlet på en forsvarlig og sikker måte. Dette ved å fremheve beskrivelser av behovet for at brukeren selv skal kunne ta pragmatiske eller kritiske beslutninger ved å ved vurdere fordelene og ulempene ved å dele personopplysninger som et personlig ansvar (Hargittai & Marwick, 2016). Den

behandlingsansvarlige står på denne måten ovenfor en rekke utfordringer for å kunne ivareta og bevare brukerens personvernrettigheter og personopplysninger på gjennom ulike personverntiltak og evalueringer en effektiv, formålsspesifikk og sikker måte (Datatilsynet, 2022).

4.2 Villighet til å avsløre

Den neste delen tar for som informantenes beskrivelser av deres villighet til å dele eller avsløre personopplysninger gjennom det som vil betegnes som villighet til å avsløre. Dette er knyttet til brukerens villighet og motivasjon til å avsløre eller gi fra seg personopplysninger til den behandlingsansvarlige. Videre vil dette kunne beskrive som en form for selvavsløring ved at brukeren bevisst eller ubevisst tar en beslutning om å avsløre deres personopplysninger (Joinson et al., 2010; Knijnenburg et al., 2013; Taddei & Contena, 2013). Først vil jeg belyse hvordan informantenes beskrivelser av deres villighet til å avsløre er knyttet til deres grad av tillit. Videre hvordan dette er knyttet til beskrivelser av informantenes risikobevissthet og digitale kompetanse. Avslutningsvis vil jeg fremheve informantenes beskrivelser av brukerens kritiske vurderingsevne og hindringer som tid. Formålet med dette er å belyse informantenes beskrivelser av deres motivasjon og hva som gjør de mer eller mindre villige til å dele personopplysninger.

4.2.1 Ulike former for tillit

Innledningsvis har vi sett hvordan behandlingsansvarliges praksiser er pålagt og med fordel kan vektlegge en rekke personvernprinsipper for å i imøtekomme brukerens rettigheter, behov eller ønsker. I denne sammenhengen fremhever et flertall av informantene hvordan deres villighet og beslutning om å avsløre eller dele personopplysninger var basert på deres tillit til den behandlingsansvarlige. Tillit er et komplekst fenomen, men vil i denne konteksten kunne omhandle hvordan brukeren forstår og oppfatter at deres personopplysninger blir samlet inn og behandles på en forsvarlig, kompetent og nødvendig måte (Bansal et al., 2016; Joinson et al., 2010; Kehr et al., 2015). Taddei og Contena (2013) har blant annet fremhevet den fremtredende rollen som tillit har for individers selvavslørende atferd. Informanten Christoffer fremhever blant hvordan denne tilliten kan være knyttet til hvordan den behandlingsansvarlige forholder seg til og formidler sine innsamlings- og behandlingspraksiser:

«*Ja, de sier jo at de ikke skal dele informasjonen om mine personopplysninger, og at de forholder seg til lovgivninger om GDPR og det nye som kommer nå fra EU. Så jeg tror det er trust based. Jeg stoler på dem*.» (Christoffer, 63)

Behandlingsansvarliges lovnader om at deres praksiser er basert på innebygd personvern vil på denne måten kunne bidra til å styrke den behandlingsansvarliges troverdighet og pålitelighet. Videre beskriver informanten det som kan betegnes som en form for generell, eller institusjonell tillit (Hoffmann et al., 2016; Kehr et al., 2015). På denne måten vil den behandlingsansvarlige kunne bygge tillit og oppmuntre brukeren til å dele sine personopplysninger ved å respektere brukerens rettighet og gjeldende personvernregelverk gjennom åpenhet og synlighet (Cavoukian, 2009, 2020). Dette ved å vektlegge sin evne til å håndheve og demonstrere deres behandlingspraksiser i samsvar med personopplysningsloven og gjeldende juridiske krav. Dette er noe informanten Casper bygger videre på ved å fremheve nettavisen Aftenposten som et eksempel:

«*Nei, jeg ville jo ut ifra at det er Aftenposten og jeg tenker at det er en seriøs avis, og jeg har jo tillit til innholdet de skriver. Da er jeg mer positiv til denne nettdelen da. Så vil jeg av den grunn også være mye lettere til å skrive eller trykke jeg forstår enn å gå til personverninnstillinger, som jeg kanskje i større grad hadde gjort om jeg hadde vært inne på en annen side.*» (Casper, 56)

Brukerens meningsdannelse rundt nettsidens integritet og omdømme vil på denne måten kunne påvirke deres grad av tillit. Her er det verdt å bemerke at det er mediekonsernet Schibsted, som vil være den behandlingsansvarlige for brukerens personopplysninger når de besøker Aftenpostens nettside (Schibsted, 2023). På denne måten vil brukeren vektlegge opplevde relative fordeler som behovet for tilgang på innhold, effektive og forbedrede tjenester når de tar beslutninger om å dele personopplysningene deres. Dette ved å rasjonalisere sin beslutning og villighet til å akseptere eller samtykke når brukeren allerede har en personlig relasjon og opplever den behandlingsansvarlige som troverdig og pålitelig. Videre er det mulig å se dette i forhold til hvordan informanten skiller mellom ulike behandlingsansvarlige gjennom en form for kildekritikk som er knyttet til deres digitale kompetanse (Bartsch & Dienlin, 2016; Trepte et al., 2015). I denne sammenhengen ble også Norges rikskringkaster (NRK) trukket frem av informanten Andrea som et eksempel på en troverdig behandlingsansvarlig sammenlignet med andre kommersielle nyhetsmedier som Verdens Gang (VG) og Dagbladet:

> «*NRK gjør jo alt veldig ordentlig. Fordi de kan jo også gjøre det veldig ordentlig da. Jeg tviler på at VG eller Dagbladet har det samme da*.» (Andrea, 21)

Brukerens grad av tillit vil på denne måten kunne avhenge av deres meningsdannelse rundt behandlingsansvarliges formål bak innsamlings- og behandlingsprosessen. I likhet med Aftenposten er VG underlagt Schibsted, og Dagbladet en del av Aller Media med en lignende mediekonsernstruktur (Aller Media, 2023; Schibsted, 2023). Disse behandlingsansvarlige representerer på denne måten kommersielle aktører, som er avhengig av reklame- og annonseinntekter for å finansiere og opprettholde sine tjenester. Videre er det interessant hvordan de ulike informantene beskriver at de forholder seg ulikt og skiller mellom forskjellige behandlingsansvarlige. Brukerens villighet og motivasjon er på måten avhengig av kontekst og deres relasjon til den behandlingsansvarlige (Bansal et al., 2016). Denne personlige relasjonen som de ulike informantene beskriver vil på denne måten kunne fungere og brukes som en forsvarsmekanisme som styrker brukerens villighet til å avsløre eller dele personopplysninger (Hoffmann et al., 2016; Khan et al., 2023).

4.2.2 Mistillit

I denne sammenhengen er det verdt å trekke inn det komplekse forholdet eller samspillet mellom brukerens personvernbekymringer (hensyn), tillit og grad av kontroll (Taddei & Contena, 2013). Dette vil kunne innebære brukerens vurderinger av fordelene og ulempene ved å dele personopplysninger med den behandlingsansvarlige. Noe som kan betegnes som en form for mistillit knyttet til den behandlingsansvarliges troverdighet, omdømme eller praksiser. Til forskjell fra de andre informantene var det kun informanten Aksel som fremhevet det som kan betegnes som en form for utbredt mistillit:

> «*For jeg stoler jo ikke på selskapene. Først så ser jeg jo, jeg trykker ned på hvert punkt. For å se hva som ligger der, og at det ikke er noe annet lureri. Før jeg da til slutt tillater kun de nødvendigste. For at nettsiden skal fungere*.» (Aksel, 25)

Her beskriver informanten sin fremgangsmåte for å gjøre seg kjent med og få oversikt over behandlingsansvarliges formål med deres personopplysninger. Noe som vil kunne innebære en form for usikkerhet eller bekymringsverdige spekulasjoner rundt behandlingsansvarliges egoistiske eller lite fordelaktige hensikt med brukerens personopplysninger (Lutz et al., 2020; Martin, 2020; Solove, 2021). Informanten Adam fremhever blant annet Kvinneguiden.no som et eksempel på en bekymringsverdig og mindre troverdig behandlingsansvarlig:

O: «*Nei, men når jeg har gått inn på noen sånne litt mer shady nettsider for å være en litt sånn besserwisser. Så har jeg gått inn på noen shady sider som Kvinneguiden eller noe sånne ting. Da har jeg vært litt sånn her vil jeg ikke gi fra meg dataene mine. Jeg vil ikke få noen anbefalinger til Kvinneguiden*.» (Adam, 26)

Her er det mulig å se hvordan informantens grad av tillit vil kunne variere i forhold til brukerens tidligere erfaringer og meningsdannelse. Brukerens lave tillit eller mistillit kan på denne måten være basert på skeptisisme eller misnøye med den behandlingsansvarlige (Hoffmann et al., 2016; Lutz et al., 2020). Denne svekkende tilliten vil kunne oppstå ved at brukeren opplever at personopplysningene deres brukes til formål som ikke er fordelaktige for dem. Det er mulig å se dette i forhold til informantens beskrivelse av sin digitale kompetanse som avgjørende for å ta beslutninger som reduserer risikoen for å avsløre personopplysninger på nett. Videre vil denne kompetanse kunne medføre et økende behov for beskyttelse mot den behandlingsansvarlige, samtidig som det gir brukeren handlingsfrihet til å oppnå de samme fordelene fra nettaktiviteter som i økende grad avhenger av å personopplysninger (Büchi et al., 2017). Videre er det mulig å se dette i forhold til et konsept som personvernkynisme der brukeren som har en høy grad av digital kompetanse føler seg mindre maktesløse når gjelder deres villighet til å avsløre personopplysninger (Lutz et al., 2020). I denne sammenhengen vil den behandlingsansvarlige kunne sikre brukerens evne eller deres grad av kontroll ved å tilby full funksjonalitet i sine personverninnstillinger. Dette ved å bidra til synlighet og åpenhet rundt hvilke personopplysninger som samles inn, behandles og brukes til ulike formål som reklame eller personlig tilpassing av innhold.

4.2.3 Risikobevissthet og tid som en hindring

Dette går inn på den neste delen av brukerens villighet til å avsløre som omhandler informantenes beskrivelser av deres risikobevissthet. Dette innebærer hvordan brukerens kunnskap, oppmerksomhet og personvernhensyn vil kunne påvirke deres evne til å forstå, vurdere og gjøre seg klar over potensielle risikoer og konsekvenser ved å avsløre deres personopplysninger. Informanten Andrea trekker i denne sammenhengen sin egen manglende oppmerksomhet rundt nettsiders bruk av informasjonskapsler:

«*Det kan godt være at det kunne vært nødvendig, men jeg kjenner meg selv godt for å vite at jeg ikke tenker på det. Når du viser meg disse nettsidene her. Jeg tenker faktisk aldri på at det kommer opp sånne cookies. Det er ikke noe jeg i det hele tatt tenker på*

til vanlig. Så jeg ble nesten litt sjokkert nå på at det faktisk kommer opp hele tiden.» (Andrea, 21)

På denne måten vil brukerens manglende bevissthet medføre at de ignorer eller glemmer at personopplysningene deres blir samlet inn og behandlet. Videre beskriver informanten på denne måten en manglende digital kompetanse når det gjelder hens bevissthet rundt behandlingsansvarliges bruk av informasjonskapsler der disse har blitt en integrert og naturlig del av brukerens dagligdagse nettaktiviteter. Her kan det hende at brukeren tidligere har samtykket til informasjonskapslene eller oppfatter behandlingsansvarliges forespørsel som subjektivt meningsløst og dermed overser den (Cha et al., 2018; Hoffmann et al., 2016). Videre er det mulig å se dette i forhold til at brukeren utvikler en form for personvernkynisme, som en mer eller mindre bevisst forsvarsmekanisme. Dette ved å rasjonalisere deres manglende oppmerksomhet eller lykkelige uvitenhet som fordelaktig og nødvendig for å bruke en nettside eller digital tjeneste (Hoffmann et al., 2016; Kehr et al., 2015; Lutz et al., 2020). Noe som vil kunne hindre brukeren i å iverksette eller se behov for beskyttelsestiltak. I likhet med et flertall av informantene på tvers av de ulike aldersgruppene fremhever Berit brukerens kritiske vurderingsevne og digitale kompetanse som et godt råd for å øke brukerens bevissthet rundt hvilke personopplysninger de valgte å avsløre:

«*Ja, jeg tenker at det er viktig å være kritisk, og tenke at det er en bevisst grunn til at andre ønsker å bruke disse opplysningene. Det er jo for å bruke det til noe og det kan at det til slutt blir veldig mye informasjon som du har utlevert da, som andre vil komme til å bruke mot deg. Eller samle i en total som ikke nødvendigvis er så heldig for deg*.» (Berit, 46)

Her beskriver informanten sitt perspektiv på brukerens evne til å ta kritiske beslutning være basert på en risikovurdering av potensielle fordeler og ulemper ved å dele opplysninger med den behandlingsansvarlige. Videre er dette knyttet til brukerens bevissthet rundt hva opplysningen deres brukes til (behandlingsansvarliges formål), mengden og konteksten som opplysningene blir samlet inn og delt i. På denne måten vil brukerens kritiske vurderingsevne være knyttet til deres risikobevissthet og digitale kompetanse (Bartsch & Dienlin, 2016; Dienlin & Trepte, 2015). Informanten Cathrine beskriver blant annet hvordan en faktor som tid ville kunne oppleves for en hindring:

«*Egentlig så tenker jeg at det ikke er det, men så tenker jeg de gjør jo det her fordi man går inn her for å lese noe og har ikke all evighet på seg eller tid. Så derfor må det være*

komprimert informasjon, men jeg tenker jo også at jeg vet jo egentlig ikke hva dette innebærer. Men jeg godtar det ganske kjapt fordi jeg er ganske keen på å komme meg inn og lese på det som jeg vil få med meg.» (Cathrine, 59)

På denne måten vil brukeren kunne forsvare eller rasjonalisere sin beslutning å samtykke eller ignorere behandlingsansvarliges nødvendige informasjon basert på deres behov for tilgang og opplevde tidsbegrensninger. Tid vil på denne måten kunne anses som en hindring for at brukeren selv kan ta kritiske personvernbeslutninger. Noe som vil kunne gå utover brukerens kontroll når det gjelder å begrense eller minimalisere hvilke personopplysninger de ønsker å dele (Boerman et al., 2021). Dette vil kunne oppstå når brukere står overfor et nivå av informasjon som de ikke har tilstrekkelig kapasitet eller en grunnleggende digital kompetanse til å ta kritiske beslutninger om deres personopplysninger (Acquisti et al., 2015).

4.3 Behov for beskyttelse

Den siste delen omhandler informantenes beskrivelser av deres behov for å beskytte deres personopplysninger. Dette innebære brukerens motivasjon og villighet til å beskytte deres personopplysninger i ulike situasjoner og kontekster. Videre vil jeg belyse hvordan dette vil kunne basere seg på informantenes beskrivelser av deres personvernhensyn og spesifikke beskyttelsestiltak (Boerman et al., 2021; Meier et al., 2021). Brukeren vil kunne beskytte deres personopplysninger på ulike måter, men jeg har valgt å belyse dette med utgangspunkt i fire personvernfremmende teknologier. Først vil jeg diskutere ulike praktiske og emosjonelle personvernhensyn som er knyttet til bruken av VPN-er. Deretter vil jeg trekke inn AdBlock og DuckDuckGo som ulike beskyttelsestiltak for annonseblokkering, anonymisering av brukerens personopplysninger og påvirkninger på brukeropplevelsen. Avslutningsvis vil jeg belyse potensielle fordeler og ulemper når det gjelder informantenes meningsdannelse rundt anonymiseringsgraden og nytteverdien som inkognitomodus gir.

4.3.1 VPN: anonymisering og sikker Internett-tilkobling

Den første personvernfremmende teknologien som ble trukket frem i diskusjonen rundt informantenes beskyttelsesatferd var deres bruk, meningsdannelse rundt hva en VPN var. Et flertall av informantene uttrykte kjennskap til hva en IP-adresse var og hvordan dette kunne anses som en personopplysning, men fremhevet en manglende teknisk kompetanse og opplevde bekymringsverdige aspekter ved denne typen personopplysninger. I denne sammenhengen er det mulig å se hvordan et flertall av informantene beskriver at de mangler

en form for digital kompetanse. Her var det 6 informantene som hadde både kjennskap til og brukt en VPN på tvers av de ulike aldersgruppene med en overvekt av alle informantene yngste aldergruppen (20-31). Informanten Aksel var den eneste av informantene som aktivt brukte en VPN som følge personvernhensyn i privat kontekst, og fremhever hvordan denne personvernfremmende teknologien vil kunne bidra til å anonymisere og sikre brukerens Internett-tilgang:

> «*Jeg bruker det jo overalt, men jo selvfølgelig noen situasjoner når det er helt elementært da, som når du bruker åpne eller offentlige nettverk. Det er jo kanskje den fremste, og som deler av befolkningen nå begynner å bli klar over. Sitter du på en cafe eller et hotell da, som er åpent er du utsatt. Det er jo noe du kan forhindre gjennom å bruke VPN, men det er jo og litt det som går på sporing. Det er jo noe som du unngår gjennom til en viss grad gjennom VPN»* (Aksel, 25)

Her trekker informanten inn en rekke situasjoner der brukerens personopplysninger (IP-adresse og nettaktivitet) vil være særlig utsatt eller sårbare. Brukeren av en VPN vil på denne måten kunne anses å være situasjonsspesifikk og kontekstavhengig basert på praktiske personvernhensyn (Namara et al., 2020). Videre var interessant å se hvordan denne informanten som tilhørte den yngste aldersgruppen (21-31) beskrev at hen bruk flere typer personvernfremmende teknologi til ulike formål og uttrykte en bred eller høy digital kompetanse (Büchi et al., 2017). Denne opplevde alvorlighetsgraden eller risikobevisstheten som informanten fremmer gjelder i forhold til mangelen på en sikker Internett-tilkobling og brukerens sårbare posisjon for uvedkommende sporings- eller tilgangsforsøk (Adhikari & Panda, 2018). Videre er det også mulig å se hvordan det ligger emosjonelle personvernhensyn bak brukerens villighet, motivasjon og behov for å bruke en VPN (Namara et al., 2020). Dette gjelder i forhold til brukerens risikobevissthet rundt bekymringsverdige aspekter knyttet til identifisering, sporing, misbruk eller manglende kontollevne. Videre fremhevet informantene også emosjonelle hensyn som de opplevde som hindringer. Dette er noe som informanten Adam diskuterer i sin begrunnelse for å ikke bruke en VPN:

> «*Jeg skjønner ikke helt vitsen med VPN egentlig så nei. Hvis du skal gjøre noe shady greier da kanskje. Så er jo VPN gull da. For du kan jo få det til å se ut som om du er en annen plass da. Du kan jo ha en VPN, på en VPN, på en VPN. Så da kan du sitte på en plass og re-route det hele tiden igjennom det da. Du kan gjøre ganske mye ulovlige*

greier med VPN da egentlig når jeg tenker meg om, selvfølgelig i teorien da.» (Adam, 26)

Det er mulig å se hvordan dette er knyttet til en oppfatning av at en VPN primære bruksområdet som en anonymiseringsteknikk til en viss grad er forbeholdt ulovlig nettaktivitet eller andre former for cyberkriminalitet. Denne manglende motivasjonen og behovet for å ikke ta i bruk en VPN er på denne måten ikke knyttet til brukerens mangel på risikobevissthet, men heller basert på en antagelse eller oppfatning om at de selv ikke har noe å skjule eller behov for å anonymiseres. Dette bygger på det som betegnes som «ingenting å skjule, ingenting å tape» argumentet (Marwick & Hargittai, 2019; Solove, 2007, 2011). I denne sammenhengen vil brukere som ikke forstår formålet eller opplever at den personvernfremmende teknologien samsvarer med deres behov avstå fra å bruke disse teknologiene. Videre vil være knyttet til brukerens manglende digitale kompetanse når det gjelder å forstå hva en VPN kan brukes til og hvordan dette kan bidra til å beskytte brukerens personopplysninger. Til forskjell beskriver informanten Ole hvordan brukere som har mer normale eller sosialt aksepterte nettlesingsaktiviteter ikke opplever noe behov for å sikre Internett-tilkoblingen deres (Marwick & Hargittai, 2019). Det er mulig å se dette i forhold til et konsept som personvernkynisme der ingenting å skule argumentet i likhet vil kunne fungere som en avlastingsfunksjon som lar brukeren rasjonalisere og rettferdiggjøre sin beslutning om å ikke bruke en personvernfremmende teknologi (Hoffmann et al., 2016); Marwick og Hargittai (2019).

4.3.2 AdBlock og DuckDuckGo: blokkering, anonymisering og brukeropplevelsen

Den neste personvernfremmende teknologien som ble trukket frem som en del av informantenes beskyttelsestiltak var blokkeringsverktøyet AdBlock. Her var det 4 av informantene likt fordelt mellom aldersgruppene 20-31 og 31-49, som selv hadde kjennskap til og brukte AdBlock. I hovedsak var det AdBlocks annonseblokkeringsfunksjon som ble fremhevet som det primære bruksområdet for denne personvernfremmende. Det er noe informanten Bjørn trekker frem ved å fremheve hvordan AdBlock bidrar til å gi en tilfredsstillende brukeropplevelse, men også hvordan det ville kunne ha økonomiske konsekvenser for tjenestetilbyderen av nettsider eller den behandlingsansvarlige:

«*Du får jo en mer behagelig opplevelse mener jeg da når du surfer på nett. Ved at du slipper å bli proppet full av reklame uansett hvor du går. Det er jo sånn at det klart har jo noen negative innvirkninger også. Ved at annonseinntekter, skal du drive en*

> *avis da, så er du gjerne avhengig av disse inntektene. Så jeg ser jo den og, men for min egen del så er det jo at du slipper å bli sporet og du slipper å se reklame som du ikke har lyst på*.» (Bjørn, 42)

På denne måten vil et blokkeringsverktøy som AdBlock kunne bidra til å beskytte brukeren mot distraherende, påtrengende eller personlig tilpasset innhold eller annonser (Kaaniche et al., 2020; Traverso et al., 2017). Videre hvordan dette vil kunne bidra til en mer tilfredsstillende brukeropplevelse og dekke brukerens beskyttelsesbehov ved å blokkere annonser, informasjonskapsler og sporingsforsøk. Samtidig fremhever også informanten hvordan en faktor som økonomi vil kunne ha konsekvenser for den behandlingsansvarlige og som dermed blir en del av brukerens vurderingsprosess. Et mindretall av informantene hadde kjennskap til hva DuckDuck var, spesielt knyttet til den eldste aldersgruppen (50+). Kun 1 av informantene brukte det aktivt, 3 hadde teste det, men ikke valgte å bruke det videre. Informanten Aksel som selv aktivt bruker DuckDuckGo, som en del av nettleseren Brave Browser, fremhever blant annet en oppfatning om at teknologiens anonymiserings- og søkefunksjon er fordelaktig og tilrettelagt for brukerens personvernhensyn:

> «*DuckDuckGo samler ikke inn i nærheten like mye data om brukerne. Det går mer på hva det søkes på da. Så det er ikke på en måte hva du som bruker spesifikt gjør, men mer på det allmennheten søker etter da*.» (Aksel, 25)

Til forskjell fra andre søkemotorer opplyser DuckDuckGo i sin personvernerklæring at de som en del av deres behandlingspraksiser ikke lagrer eller deler brukerens personopplysninger (DuckDuckGo, 2023a). Dette vil kunne bidra til å anonymisere og begrense mengden av personopplysninger som blir samlet inn om brukeren. Anonymisering er på denne måten også en del av søkefunksjonen ved å tillate brukeren å gjennomføre anonyme søk som vil kunne gi treffsikre og mindre personaliserte søkeresultater. Informanten Bente fremhever blant annet hvordan sin motivasjon til å bruke DuckDuckGo var basert på praktiske hensyn i jobbsammenheng, men at dette behovet og personvernhensynet ikke lenger eksisterte:

> «*Ja, jeg har brukt det. Når jeg jobbet med automasjon før. Så da fikk jeg bare lov til å bruke DuckDuckGo. Eneste grunnen til at jeg ikke bruker det lenger er fordi jeg synes det er en dårlig søkemotor. Så er jeg litt villig til å gi opp mine private greier for Google, rett og slett.».* (Bente, 33)

I denne sammenhengen vil brukeropplevelsen som søkemotoren til eksempelvis Google gir kunne overveie og anses som mer fordelaktig enn det beskyttelsesgraden og praktiske personvernhensynet som DuckDuckGo gir. Brukeren vil på denne måten kunne utvikle en form for personvernkynisme (Hoffmann et al., 2016; Lutz et al., 2020). Hvorav deres tidligere erfaringer og behov for en tilfredsstillende eller personlig tilpasset brukeropplevelse rasjonaliseres som viktigere enn beskyttelsesgraden som DuckDuckGo gir. Dette vil kunne medføre at denne personvernfremmende søkemotoren oppleves som lite kompatibel eller subjektivt meningsløst når det gjelder brukerens vurderinger av søkemotorens nytteverdi, relative fordeler og brukeropplevelsen (Harborth et al., 2020).

4.3.3 Inkognitomodus og den opplevde nytteverdien

I forlengelse av informantenes behov for beskyttelse og bruk av personvernfremmende teknologier blir også inkognitomodus trukket frem av informantene som et eksempel på en personvernfremmende teknologi. Dette gjennom måten denne private modusen bidro til å anonymisere brukerens nettaktivitet og fungerte som en blokkeringsteknikk mot informasjonskapsler og reklame/annonser (Kaaniche et al., 2020). I denne sammenhengen var det 4 av informantene som opplyste at de brukte inkognitomodus eller en annen form for privatmodus i deres nettleser. Informanten Adam trekker blant annet frem hvordan hen bruker inkognitomodus til situasjonsspesifikke anonymiseringsformål:

> «*Når jeg går på Hotells.com, så går jeg alltid inn på inkognitomodus. Fordi jeg har inntrykk av at desto mer jeg trykker inne på hotell, som er i samme område så blir det dyrere. Men når jeg går inn i inkognito modus så har det ingenting å si eller da husker den ikke på at jeg har søkt på det før. Også får de ikke hypet opp tilbudene eller tilpasset prisen på grunn av dataene dine, men jeg har ikke noe bevis.»* (Adam. 26)

Her er det mulig å se hvordan en faktor som økonomi og behovet for tilgang på de beste tilbudene ville kunne motivere brukeren til å ta i bruk inkognitomodus. Modusens anonymiseringsfunksjon bidrar på denne måten til at bruken ikke blir utnyttet eller at den behandlingsansvarlige har lite fordelaktige hensikter med å samle inn brukerens personopplysninger. I likhet med en VPN vil dette kunne være basert på brukerens praktiske og emosjonelle personvernhensyn (Namara et al., 2020). Denne beskrivelsen skiller seg fra informanten Christoffer i den eldste aldersgruppen som i likhet er kritisk til en nettside som Hotells.com, men som fremdeles velger å samtykke til informasjonskapslene:

> «*Jeg må si når jeg går inn på Hotells.com så tvier jeg meg litt til å trykke yes på den. For da aner jeg ikke hva som kommer. Sannsynligvis kommer det en haug med reklamer som kommer.»* (Christoffer, 63)

Dette er med på å fremheve hvordan brukerens bevissthet rundt og kjennskap til personvernfremmende teknologier vil kunne påvirke deres behov for beskyttelse. Her fremhever begge informantene en form for usikkerhet eller bekymringsverdige aspekter behandlingsansvarliges (Hotels.com) lite fordelaktige eller forstyrrende bruk av deres personopplysninger og annonser. Der Adam beskriver hvordan hens bruk av inkognitomodus bidrar til å bruke Hotells.com på en måte som reduserer risikoen for å gi fra seg personopplysninger som går utover tilbudene som nettsiden gir eller mengden av personalisert reklame som kommer i etterkant. Brukerens digitale kompetanse vil på denne måten bidra til å dekke deres beskyttelsesbehov, samtidig som de får tilgang til fordelene som nettsiden gir (Büchi et al., 2017). I forhold til utvalget fremhever dette en aldersforskjell mellom de ulike de ulike informantene. Der kun én av informantene i den eldste aldersgruppen (over 50) som hadde kjennskap til, men ingen hadde brukt inkognitomodus. I likhet beskriver informanten Cathrine at hen ikke så noen nytteverdi i nettleserens personvernfremmende modus:

> *Jeg ser vel egentlig ikke at jeg får noe nytteverdi av det egentlig da. Når det står sånn begge deler. For det er jo ikke det at jeg inne på så mange interessante sider, men det er jo det med at det lagres mye informasjon om meg som jeg ikke liker.»* (Cathrine, 59)

Dette går igjen inn på ingenting å skjule argumentet som en begrunnelse for at informanten ikke så behovet eller ønsket å ta i bruk inkognitomodus som et beskyttelsestiltak (Marwick & Hargittai, 2019; Solove, 2007, 2011). Det at informanten ikke opplever sin egen nettaktivitet som problematisk eller bekymringsverdig, og dermed ikke ser det som nødvendig og subjektivt meningsløst å bruke en personvernfremmende modus (Hoffmann et al., 2016; Lutz et al., 2020). Det er mulig å se dette i forhold til at informantene beskriver en manglende risikobevissthet eller digital kompetanse når det gjelder bruken av inkognitomodus. Her er det verdt å bemerke at informanten Cathrine aldri hadde brukt inkognitomodus før og ble introdusert for det for første gang under intervjuet. I denne sammenhengen er det mulig å se hvordan beskrivelser av de personvernfremmende teknologienes nytteverdi og tilhørende praktiske hensyn vil kunne medføre at de undervurder eller mangler en tilstrekkelig digital kompetanse for å vurdere den faktiske graden av personvernbeskyttelse som oppnås ved å bruke en personvernfremmende modusen (Büchi et al., 2017; Harborth et al., 2020).

5. Diskusjon

I denne delen av oppgaven vil jeg diskutere og drøfte hovedmomentene fra analysen av svarene som kom fram under intervjuene med informantene for å besvare oppgavens problemstilling:

> «*Hvordan beskriver nordmenn sine holdninger til personvern når det gjelder innsamling, behandling og bruk av personopplysninger, og hvordan er disse beskrivelsene knyttet til deres atferd og beslutninger om beskyttelse og deling av personopplysninger på nett*?»

Jeg har valgt å fremheve tre sentrale aspekter som er knyttet til nordmenns meningsdannelse og beskrivelser av deres holdninger til personvern, atferd og beslutninger til å beskytte eller dele deres personopplysninger. Først vil jeg oppsummere hovedmomentene fra analysen. Deretter vil jeg drøfte disse hovedmomentene i forhold til relevante teoretiske perspektiver og i sammenheng med tidligere forskningslitteratur. Dette på personvernparadokset som forklaringsmåte, personvernfremmende teknologier som beskyttelsestiltak, personvernkynisme og digitale kompetanse som en forutsetning. Avslutningsvis vil jeg diskutere oppgavens bidrag, begrensninger og muligheter for videre forskning på området.

5.1 Oppsummering av hovedmomentene fra analysen

Når det gjelder informantenes beskrivelser av deres forhold til behandlingsansvarliges praksiser, blir betydningen av innebygd personvern som standard tydeliggjort. Dette uttrykkes gjennom behandlingsansvarliges fokus på brukernes rettigheter til innsyn og sletting av personopplysninger. Dette har igjen innvirkning på brukerens evne til å handle og opplevelsen av å ha kontroll over egne personopplysninger. Ansvarsfordelingen er todelt. Der behandlingsansvarlige har et overordnet ansvar, samtidig som brukerne har et individuelt ansvar for å begrense og være bevisste på hvilke opplysninger de deler. Informantenes beskrivelser av deres villighet til å gi ut personopplysninger var i denne konteksten knyttet til tilliten de har til en eller flere behandlingsansvarlige. Hvis de har en høy grad av tillit øker informantenes villighet til å utgi informasjon, mens ved en lav grad av tillit medfører et behov hos informantene til å beskytte sine personopplysninger. Brukernes bevissthet om risiko, digitale ferdigheter, personvernbekymringer og oppmerksomhet rundt behandlingsansvarliges bruk av informasjonskapsler påvirker graden av hva de gir av personopplysninger. Videre

knyttes dette til brukernes evne til kritisk vurderingsevne, samt hindringer som liten tid eller manglende kapasitet. Avslutningsvis blir informantenes behov for beskyttelse undersøkt i sammenheng med personvernfremmende teknologier, inkludert ulike anonymiserings- og blokkeringsteknikker. Betydningen av praktiske og emosjonelle personvernhensyn, samt informantenes oppfatning av nytteverdi, blir fremhevet som avgjørende faktorer for motivasjon og villighet til å bruke slike teknologier. Brukeropplevelsen kan både motivere, men også utgjøre en potensiell hindring. Argumentet om «ingenting å skjule, ingenting å tape» blir derimot brukt av informantene s for å forklare deres motstand mot bruk av personvernteknologier. Det er viktig å merke seg at disse hovedmomentene ikke er separate aspekter, men at de påvirker hverandre. Dette blir spesielt tydelig når det gjelder hvordan brukernes atferd med hensyn til å avsløre og beskytte personopplysninger påvirkes av deres oppfatning av behandlingsansvarliges praksiser. Videre vil jeg diskutere disse hovedmomentene i sammenheng med oppgavens teoretiske rammeverk.

5.2 Personvernparadokset og villigheten til å avsløre personopplysninger

Innenfor forskningslitteraturen på personvernparadokset er det foreslått en motsetning mellom menneskers bekymringer rundt personvern og deres atferd når det gjelder håndtering av personopplysninger (Acquisti, 2004; Acquisti & Grossklags, 2005; Barnes, 2006; Norberg et al., 2007). I denne sammenhengen ble det variasjoner og forskjeller i informantenes beskrivelser av holdninger, atferd og beslutninger. Disse er knyttet til deres forhold til behandlingsansvarlige, og dermed deres villighet til å dele personopplysninger eller beskytte personopplysningene sine. Dette samsvarer med funnene til Acquisti og Grossklags (2005) som i likhet med funnene i oppgaven viser at informantenes beskrivelser av hvordan de vurderer forventede eller relative fordeler ved å dele personopplysninger kan påvirke deres villighet til å dele denne informasjonen Spesielt er dette knyttet til behovet for tilgang og usikkerheten knyttet til tilgangen på nettsidene. På den andre side indikerer ikke disse funnene noen motsetning mellom informantenes beskrivelser av deres holdninger og reelle atferd.

Disse funnene samsvarer med Kokolakis (2017) som i sin litteraturgjennomgang argumenterer for at personvernparadokset ikke bør betraktes som en dikotomi mellom brukerens holdninger og atferd. Til tross for at denne forklarningsmåten bidrar til å belyse et forestilt gap mellom brukeres holdninger og atferd var ikke dette nødvendigvis er motstridende, men basert på deres rasjonelle vurderinger og beslutningstaking (Kokolakis,

2017; Solove, 2021). Videre er det verdt å bemerke at informantenes subjektivitet og uttrykksmåter kan være påvirket av konteksten og interaksjonen mellom partene i intervjusituasjonen. Informantene kan på denne måten ha tilpasset svarene sine for å virke mer sosialt akseptable eller for å svare «riktig» på spørsmålene i intervjusituasjonen (Tjora, 2021). Dette kan ses i sammenheng med Dienlin et al. (2023) som argumenterer for at enkeltpersoners midlertidige atferd knyttet til deres motivasjon og villighet til å dele personopplysninger kan endres over tid. Imidlertid fant de ingen langsiktige effekter på personvernholdninger eller bekymringer etter 6 måneder (Dienlin et al., 2023).

Informantenes beskrivelser av hvor villige de var til å dele personopplysninger var i denne sammenhengen basert på deres oppfatninger av hvor ansvarlige de var, graden av kontroll de hadde og tilliten til den behandlingsansvarlige. Dette samsvarer med funnene til Taddei og Contena (2013) som fremhever betydningen av tillit og troverdighet til behandlingsansvarlige i forhold til brukerens villighet i å dele informasjon. Lav tillit kan føre til et behov for å beskytte sine personopplysninger. Dette kan også ses i sammenheng med Dienlin og Trepte (2015) som argumenterer for at brukerens personvernholdninger er basert på distinkte holdninger og perspektiver på personvern. Dette understreker behovet for at behandlingsansvarlige legger vekt på åpenhet og synlighet som viktige forutsetninger for brukerens personvernbeslutninger og oppfatninger om innsamling, behandling og bruk av personopplysninger. Dette kan oppnås gjennom håndhevelse og ved å demonstrere at de etterlever gjeldende personvernlover, GDPR eller andre relevante juridiske krav (Cavoukian, 2009, 2020). Informantenes beskrivelser av deres beslutninger om å dele eller beskytte personopplysninger var på denne måten ikke paradoksal eller motstridende, men basert på deres meningsdannelse og refleksjoner under intervjuene. Det er mulig å se dette i forhold til Martin (2020) som også argumenterer for at brukere som velger å dele personopplysninger opprettholder rimelige forventninger om at behandlingsansvarlige vil ivareta personvernrettighetene deres og ikke bare samle inn personopplysningene deres uten et tilstrekkelig og legitimt behandlingsgrunnlag.

5.2.1 Aldersforskjeller og digital kompetanse

Det ble tatt et bevisst valg om å ha et utvalg fra tre aldersgrupper. Dette for å undersøke likhet eller forskjeller mellom informantenes alder og deres beskrivelser av å dele eller beskytte personopplysninger. Dette er i tråd med tidligere forskning som har knyttet personvernparadokset til manglende bevissthet og dermed risiko for å utgi for mye personopplysninger blant unge mennesker i forbindelse i bruk av sosiale medier (Barnes,

2006; Kokolakis, 2017). Informantenes beskrivelser av deres digitale kompetanse spilte i denne sammenhengen en viktig rolle i deres beslutninger om å dele eller beskytte personopplysninger på nettet. Dette kan forstås som at brukerens digitale kompetanse kan påvirke deres evne til å ta beslutninger om deres personopplysninger på en informert og effektiv måte (Bartsch & Dienlin, 2016; Büchi et al., 2017). I denne undersøkelsen vardet indikasjoner for forskjeller i beskrivelser av digital kompetanse mellom aldersgruppene i utvalget. Noen eldre informanter (over 50 år) beskrev at de manglet tilstrekkelig kunnskap eller hadde en begrenset grunnleggende digital kompetanse knyttet til deres prosesskunnskap.

Yngre informanter (21-30 år) beskrev en dypere forståelse og refleksjon rundt strategier for å beskytte sine personopplysninger på nettet. Tabata et al. (2021) argumenterer i denne konteksten for at yngre mennesker generelt er mer kunnskapsrike og føler seg mer i stand til å beskytte personvernet sitt enn eldre mennesker. Dette når det gjelder navigering og endring av personverninnstillinger på nettsider (Tabata et al., 2021). Det er viktig å merke seg at de eldre informantene ikke nødvendigvis beskrev at de var mer villige til å avsløre personopplysninger på nettet, men de opplevde mindre behov for, eller hadde begrenset digital kompetanse til å ta i bruk personvernbeskyttende tiltak. Det er mulig å se dette i forhold til Kezer et al. (2016) studie av aldersforskjeller på Facebook. Resultatene fra denne studien viste at sannsynligheten var mindre for at eldre brukere ville dele personopplysningene sine, men heller ikke utnyttet eller opplevde et behov for å beskytte personopplysningene sine. Dette understøttes av Khan et al. (2023) som i likhet med disse resultatene fant at eldre brukere hadde en tendens til å være mer kyniske når det kom til personvernspørsmål. Til tross for at van Ooijen et al. (2022) og Boerman et al. (2021) argumenterer for at variabler som kjønn og alder ikke nødvendigvis direkte påvirker brukernes motivasjon eller grad av personvernbeskyttelse.

Videre kan dette ses forhold til at disse aldersforskjellene knyttet til informantenes beskrivelser av deres uttrykte bekymringsverdige holdninger til personvern ikke nødvendigvis er nok eller medfører at brukere endrer atferd eller tar beslutninger som imøtekommer deres personvernhensyn og behov (Büchi et al., 2017). Kokolakis (2017) har blant annet påpekt at aldersforskjeller ikke bare gjelder for yngre generasjoners motstridende atferd og manglende risikobevissthet, men at det også er et fenomen som gjelder for brukere i alle aldre. Dette understreker behovet for å forstå hvordan digitale kompetanser blant forskjellige brukergrupper kan bidra til å skape digitale skiller. Brukere med begrensede kunnskaper, ferdigheter og erfaringer står i en sårbar posisjon overfor personverntrusler og

behandlingsansvarlige som ønsker å samle inn og bruke deres personopplysninger (Hargittai, 2002; Lythreatis et al., 2022).

5.3 Personvernfremmende teknologier og behovet for beskyttelse

Informantenes behov for beskyttelse når det gjelder personvernfremmende teknologier kan ses fra ulike perspektiver. Informantene var forskjellige når det gjaldt holdninger, motivasjon og villighet til å bruke slike teknologier for anonymisering og blokkering. Noen personvernfremmende teknologier hadde flere praktiske bruksområder som kunne imøtekomme og tilfredsstilte brukernes generelle eller spesifikke personvernhensyn (Boerman et al., 2021; Harborth & Pape, 2020; Namara et al., 2020). I likhet med Harborth og Pape (2020) var det mulig å se hvordan beskrivelser av behovet for anonymitet eller anonymisering var viktige forutsetninger for deres motivasjon og beslutning om å bruke personvernfremmende teknologier. For eksempel kan bruken av DuckDuckGo, AdBlock og inkognitomodus oppleves i å gi økonomiske fordeler eller gi trygghet, og bruken av VPN kan knyttes til ønsket om frihet og en fryktløs livsstil (Skalkos et al., 2020). Dette er med på å tydeliggjøre hvordan disse ulike personvernfremmende teknologiene fungerer som beskyttelsestiltak som kan være fordelaktige i ulike situasjoner og tilfeller der brukeren opplever et behov for å beskytte personopplysningene deres. Slike teknologier er gunstige for brukerne, da de setter brukerens rettigheter, personopplysninger og sikkerhet i fokus ved å vektlegge kontroll, håndhevelse av lovverk, begrense av personopplysninger og beskytte disse opplysningene (Cha et al., 2018).

Det ble det også påpekt at manglende motivasjon og villighet blant brukerne til å dele personopplysninger kunne være relatert til opplevd nytteverdi og brukeropplevelse. Brukerens tillit og ivaretagelse av anonymitet spilte en viktig rolle for deres motivasjon og villighet til å bruke personvernfremmende teknologier (Harborth & Pape, 2020). Informanter som beskrev at de opplevde en lav anonymiseringsgrad, misvisende informasjon eller manglende troverdighet, var i mindre grad villige til å bruke slike teknologier. Den opplevde nytteverdien av beskyttelsen og konsekvensene for brukeropplevelsen var også viktige faktorer (Harborth & Pape, 2020). I tillegg var det også forskjeller i oppfatninger av anonymitet og behovet for å skjule sin identitet, noe som kunne påvirke brukerens motivasjon og villighet til å bruke personvernfremmende teknologier knyttet til informantenes beskrivelser av deres praktiske og emosjonelle personvernhensyn (Namara et al., 2020).

«Ingenting å skjule»-argumentet ble nevnt som en måte brukerne kunne rasjonalisere sitt manglende behov for å beskytte seg og liten motivasjon for å bruke personvernfremmende teknologier. Dette ved å undervurdere potensielle beskyttelsesfordeler som de ikke anså som relevante for deres emosjonelle personvernhensyn eller behov (Marwick & Hargittai, 2019; Solove, 2007, 2011). Informantene i aldersgruppene 21-30 og 31-49 beskrev i større grad hvordan de brukte ulike personvernfremmende teknologier i ulike situasjoner der de opplevde et behov for beskyttelse. Bare én informant i den eldste aldersgruppen (over 50 år) hadde erfaring med å bruke slike teknologier. Det er verdt å merke seg at aldersforskjellen i bruk av personvernfremmende teknologier ikke nødvendigvis forklarer forskjeller i brukerens motivasjon og behov for beskyttelse (Kokolakis, 2017; Marwick & Hargittai, 2019). Det bidrar imidlertid til å understreke betydningen av brukerens digitale kompetanse for å forklare hvorfor noen brukere er mer villige til å beskytte personopplysningene sine på nett enn andre. Videre er dette med på å fremheve hvordan brukerens villighet til å avsløre personopplysninger og behov for å beskytte disse vil kunne anses å være kontekstavhengig og situasjonsspesifikk (Bansal et al., 2016; Kehr et al., 2015).

5.4 Personvernkynisme og digital kompetanse som en forutsetning

I undersøkelsen ble det utforsket om konseptet personvernkynisme kunne benyttes for å analysere informantenes beskrivelser av deres holdninger til personvern i forhold til deres atferd og beslutninger ved deling eller beskyttelse av personopplysninger Funnene indikerte at personvernkynisme hadde en mindre betydningsfull rolle enn forventet. Dette til tross for at Datatilsynets (2020) personvernundersøkelse har identifisert en rekke av de mest utbredte dimensjonene av personvernkynisme knyttet til mistillit, maktesløshet, usikkerhet og resignasjon (Lutz et al., 2020). Dette til tross for at Datatilsynets (2020) personvernundersøkelse har identifisert en rekke av de mest utbredte dimensjonene av personvernkynisme knyttet til mistillit, maktesløshet, usikkerhet og resignasjon (Lutz et al., 2020). Det ble samtidig observert likheter med Hoffmann et al. (2016) sin konseptualisering av personvernkynisme som en forsvarsmekanisme, men til forskjell hvordan dette kunne fungere som en avlastingsfunksjon knyttet til informantenes manglende digitale kompetanse.

Videre ble det observert en sammenheng mellom informantenes beskrivelser av en følelse av maktesløshet, usikkerhet og manglende påvirkningsmuligheter eller kontroll (Lutz et al., 2020). Noe som vil kunne medføre at brukeren oppfatter beskyttelsestiltak som subjektivt

meningsløse og deling av personopplysninger som uunngåelig i deres nettlesingsaktiviteter. Dette stemmer overens med van Ooijen et al. (2022) som argumenterer for at personvernkynisme er preget å av frustrasjon, håpløshet og være desillusjonert. Det kan bidra til en form for lært hjelpeløshet eller lykkelige uvitenhet som er relatert til informantenes beskrivelser av deres opplevde grad av maktesløshet og begrensede påvirkningsmuligheter (Bandara et al., 2020; Kehr et al., 2015). Videre ble det observert hindringer som tid og en manglende kapasitet for å ta kritiske beslutninger.

På denne måten vil brukeren kunne oppleve å bli utmattet av mengden med informasjon som de må ta stilling til for å imøtekomme utfordringen med å håndtere og skaffe tilstrekkelig kunnskap om deres rettigheter og gjeldende personvernregelverk. Det vil kunne medføre at brukeren opplever frustrasjon over sin manglende digitale kompetanse knyttet til deres kapasitet og evne til å forstå, kontrollere og ta fordelaktige personvernbeslutninger (Büchi et al., 2017; Choi et al., 2018; Trepte et al., 2015). Videre der det mulig å se dette i forhold til Solove (2021) som argumenterer for at personvernkynisme kan betraktes som et reelt fenomen som påvirker individets personvernbeslutninger, men at det går utover å være en forsvarsmekanisme. Brukere som utvikler en form personvernkynisme, ser det som den eneste rasjonelle reaksjonen på de overveldende personvernutfordringene de møter i hverdagen (Solove, 2021).

5.4.1 Teoriutvikling og praktiske implikasjoner

Denne masteroppgaven har noen teoretiske og praktiske implikasjoner for studie av konseptet personvernkynisme i sammenheng med brukerens digitale kompetanse. Når det gjelder brukerens tillit stemte ikke denne overens med den tidligere forskningslitteraturen som har sett på sammenhengen mellom personvernkynisme og mistillit (Hoffmann et al., 2016; Khan et al., 2023; Lutz et al., 2020; van Ooijen et al., 2022). Flertallet av informantene i denne studien uttrykte en opplevelse av behandlingsansvarlige som pålitelige og troverdige. Dette var basert på deres tidligere positive erfaringer eller personlige relasjoner med nettsidene eller spesifikke behandlingsansvarlige. Disse funnene antyder at brukere som har høy tillit til en eller flere behandlingsansvarlige, rettferdiggjør sin beslutning om å bruke en nettside eller tjeneste på grunnlag av dette, til tross for at de avslører sine personopplysninger. Det er imidlertid viktig å merke seg at mistilliten som Hoffmann et al. (2016) argumenterer for, er knyttet til en risikokontekst der personvernbrudd og skandaler har svekket brukerens tillit. Imidlertid indikerte funnene at informantene i denne studien, som uttrykte lavere tillit eller mistillit, begrunnet dette med et økende behov for å beskytte sine personopplysninger.

Dette fenomenet kan observeres i Acikgoz og Vega (2022) sin studie av digitale stemmeassistenter, som også fant at personvernkynisme tilsynelatende hadde en positiv innvirkning på brukernes tillit. Dette er overraskende funn, da tidligere studier primært har hevdet at kynisme fører til mistillit (Acikgoz & Vega, 2022; Hoffmann et al., 2016; Lutz et al., 2020). Til tross for dette uventede funnet, gir det verdifull innsikt i betydningen av tillit i brukernes beslutninger om deres personopplysninger. I denne sammenhengen fungerer brukernes tillit til behandlingsansvarlige i mindre grad som en forsvarsmekanisme, men heller som en avlastingsfunksjon som tillater dem å ignorere deres emosjonelle personvernhensyn. Informantenes beskrivelser av deres digitale kompetanse fungerte på denne måten som en forutsetning for at de kunne beskytte personopplysningen sine på nett.

Dette ved å redusere risikoen for å avsløre eller gi fra seg personopplysninger til lite troverdige behandlingsansvarlig uten at dette gikk utover deres mulighet til å dra nytte av fordelene som tilgangen til ulike nettsider eller digitale tjenester gir (Büchi et al., 2017). Videre samsvarer dette med Büchi et al. (2017) og Park (2013) som antyder at det er en positiv sammenheng mellom brukerens digitale kompetanse og beslutninger om å beskytte personopplysningene deres på nett. Her vil brukerens digitale kompetanse kunne bidra til at de ikke utvikler personvernkyniske holdninger og dermed føler seg mindre maktesløse ovenfor den behandlingsansvarlige (Lutz et al., 2020). Det er verdt å merke seg at personvernkynisme skiller seg fra den tradisjonelle definisjonen av kynisme ved at den baserer seg på brukernes uttalte holdninger til personvernbeskyttelse og andre bekymringsverdige hensyn (Hoffmann et al., 2016).

Basert på funnene om informantenes behov for å bruke av personvernfremmende teknologier i visse situasjoner og tilfeller, kan det antas at brukerens manglende digitale kompetanse gjøre at de opplever omfattende beskyttelsestiltak som en hindring og dermed subjektivt meningsløst. Samlet sett understreker dette behovet for at brukerne selv er bevisste på hvordan deres personvernkyniske holdninger og digitale kompetanse kan påvirke deres vilje og motivasjon til å dele personopplysninger (Boerman et al., 2021; Khan et al., 2023; van Ooijen et al., 2022). Dette ved å fungere som en forsvarsmekanisme og avlastingsfunksjon som lar brukeren ignorere bekymringsfulle aspekter ved sine beslutninger og fremkaller risikofylt atferd (Hoffmann et al., 2016). Videre er dette med på å understreke behovet for å undersøke personvernkynisme som et reelt fenomen i sammenheng med brukernes digitale kompetanse og i konteksten av personvernfremmende teknologier

5.5 Konklusjon og bidrag

Denne studien bidrar til en mer nyansert forståelse av nordmenns holdninger til personvern ved innsamling, behandling og bruk av personopplysninger. Beskrivelsene er basert på deres forhold til behandlingsansvarlige og dannelsen av meninger rundt deres praksiser. Informantene beskriver også sin atferd og beslutninger angående graden av deling og beskyttelse av personopplysninger på nettet. Sammenhengen mellom dette og informantenes beskrivelser av deres digitale kompetanse, risikobevissthet, bruk av personvernfremmende teknologier og personvernkynisme ble også observert.

Funnene understreker behovet for økt bevissthet blant den norske befolkning om deling og beskyttelse av personopplysninger på nettet. Omfattende personvernlovgivning og retningslinjer er nødvendige for å regulere praksisene til behandlingsansvarlige og for å sikre beskyttelse av brukernes personvernrettigheter. Det er også av avgjørende betydning å legge til rette for en kontinuerlig utvikling og vedlikehold av brukernes digitale kompetanse i en tid der personverntrusler stadig blir mer utbredt. Brukere kan beskytte personopplysningene sine gjennom en bevisst omgang og tilgang til personvernfremmende teknologier. Samtidig er det viktig å ta hensyn til hvilken rolle personvernkynisme kan spille og hvordan brukernes digitale kompetanse er en viktig faktor som påvirker enkeltpersonens evne til å handle i tråd med personvernhensyn og egne bekymringer. Behandlingsansvarlige spiller en viktig rolle i å fremme og forsikre om innebygd personvern blir en standard, i å informere brukerne og gjøre det enklere for dem å ivareta personopplysningene sine på en effektiv, fordelaktig og lovlig måte.

5.5.1 Begrensninger i oppgaven og anbefalinger for videre forskning

Tross de bidragene denne masteroppgaven har den sammen med andre forskningsstudier visse begrensninger som identifiserer viktige områder for videre forskning i det moderne digitale informasjonssamfunnet. Jeg vil derfor fremheve noen av begrensningen i oppgaven og hvordan disse tydeliggjør behovet for videre forskning. Den første begrensningen gjelder i forhold til utvalget. På grunn av studiets korte varighet og intensive datainnsamlingsperiode, gjorde at utvalget ble relativt lite og basert på et ikke-representativt utvalg av nordmenn. Utvalgsmetoden og størrelsen på utvalget gjør at funnene ikke kan generaliseres til hele den norske befolkningen eller andre befolkningsgrupper. En større informantgruppe ville kunne ha bidratt til flere nyanser og ha gitt mulighet til å i å utforske flere sammenhenger mellom de viktigste temaene. Det ville økt muligheter til å få frem flere forskjeller og likheter i informantenes meningsdannelse, beskrivelser og uttrykksmåter. Videre forskning kan med

fordel undersøke variasjonen i brukernes beskrivelser av holdninger, atferd og beslutninger på tvers av ulike kulturelle kontekster og befolkningsgrupper.

Den andre begrensningen omhandler valget av kvalitative intervjuer som metode. Selv om intervjuer gir verdifull innsikt i informantenes beskrivelser, og er hypotesegenererende, gir ikke denne kvalitative tilnærmingen svar på hva som påvirker forholdet mellom holdninger og atferd. Videre forskning kan dra nytte av kvantitative tilnærminger som spørreundersøkelser med lukkede svaralternativer eller eksperimentelle studier som randomiserte kontrollerte studier (RCT) for å utforske nordmenns faktiske adferd og faktorer som påvirker deres beslutninger om å dele eller beskytte personopplysninger. Hovedfunnene fra denne oppgaven kan danne et grunnlag for utvikling av en intervjuguide for å få en mer nyansert forståelse av forholdet mellom nordmenns holdninger, atferd og beslutninger.

Den siste begrensningen er knyttet til kompleksiteten i temaet personvern og behovet for en mer nyansert forståelse av personvernparadokset som en forklaringsmodell. Det er viktig å erkjenne at brukernes uttalte holdninger og intensjoner ikke alltid samsvarer med faktisk atferd. Dette understreker behovet for at fremtidig forskning tar hensyn til at personvern er kontekstavhengig og situasjonsbestemt. For å møte disse utfordringene og undersøke nordmenns holdninger og atferd når det gjelder personvern i spesifikke kontekster, som sosiale medieplattformer som TikTok, SnapChat eller Instagram, kan fremtidig forskning benytte seg av tilnærminger som longitudinelle studier eller observasjonsstudier.

Når det gjelder avgrensningen av oppgaven, har fokuset vært på informantenes beskrivelser av deres forhold til behandlingsansvarliges vilje til å avsløre og behovet for beskyttelse gjennom personvernfremmende teknologier. Fremtidig forskning kan velge å fokusere på ett av disse hovedmomentene. Videre er det viktig å merke seg at det er lite empirisk forskning som undersøker konseptet rundt personvernkynisme og brukerens digitale kompetanse i kontekst av personvernfremmende teknologier. Fremtidig forskning kan utforske denne sammenhengen grundigere. Det ville også være interessant å undersøke ikke-brukernes meningsdannelse og beskrivelser av personvernfremmende teknologier, og sammenligne dette med faktiske brukeres perspektiver. Videre forskning kan dra nytte av denne studiens innsikt ved å bruke et større og mer representativt utvalg, samt kombinere ulike forskningsmetoder for å utforske forholdet mellom nordmenns holdninger til personvern og deres atferd når det gjelder beslutninger om å dele eller beskytte personopplysninger på nettet.

Referanseliste

Acikgoz, F. & Vega, R. P. (2022). The Role of Privacy Cynicism in Consumer Habits with Voice Assistants: A Technology Acceptance Model Perspective. *International journal of human-computer interaction*, *38*(12), 1138-1152. https://doi.org/10.1080/10447318.2021.1987677

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. Proceedings of the 5th ACM conference on Electronic commerce,

Acquisti, A., Brandimarte, L. & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science (American Association for the Advancement of Science)*, *347*(6221), 509-514. https://doi.org/10.1126/science.aaa1465

Acquisti, A. & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE security & privacy*, *3*(1), 26-33. https://doi.org/10.1109/MSP.2005.22

AdBlock. (2023). *About AdBlock*. Hentet 01. mars fra https://getadblock.com/en/

Adblock Plus. (2023). *Surf the web with no annoying ads*. Hentet 01. mars fra https://adblockplus.org/

Adhikari, K. & Panda, R. K. (2018). Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks. *Journal of global marketing*, *31*(2), 96-110. https://doi.org/10.1080/08911762.2017.1412552

Aller Media. (2023). *Våre merkevarer* Hentet 2. mai fra https://www.aller.no/vare-merkevarer

Alshalan, A., Pisharody, S. & Dijiang, H. (2016). A Survey of Mobile VPN Technologies. *IEEE Communications Surveys & Tutorials*, *18*(2), 1177-1196. https://doi.org/10.1109/COMST.2015.2496624

Andrews, T. & Vassenden, A. (2007). Snøballen som ikke ruller. Utvalgsproblemer i kvalitativ forskning. *Sosiologisk tidsskrift*, *15*(2), 151-162. https://doi.org/10.18261/ISSN1504-2928-2007-02-02

Apple. (2023). *Privat nettlesing i Safari på Mac*. Hentet 4. april fra https://support.apple.com/no-no/guide/safari/ibrw1069/mac

Bandara, R., Fernando, M. & Akter, S. (2020). Explicating the privacy paradox: A qualitative inquiry of online shopping consumers. *Journal of Retailing and Consumer Services*, *52*. https://doi.org/10.1016/j.jretconser.2019.101947

Bansal, G., Zahedi, F. M. & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & management*, *53*(1), 1-21. https://doi.org/10.1016/j.im.2015.08.001

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). https://doi.org/10.5210/fm.v11i9.1394

Barth, S. & de Jong, M. D. T. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and informatics*, *34*(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

Bartsch, M. & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147-154. https://doi.org/10.1016/j.chb.2015.11.022

Bélanger, F. & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly*, *35*(4), 1017-1041. https://doi.org/10.2307/41409971

Boerman, S. C., Kruikemeier, S. & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication research*, *48*(7), 953-977. https://doi.org/10.1177/0093650218800915

Brown, B. (2001). Studying the internet experience. *HP laboratories technical report HPL*, *49*.
Bryman, A. (2016). *Social research methods* (5. utg.). Oxford University Press.
Büchi, M., Just, N. & Latzer, M. (2017). Caring is not enough: the importance of Internet skills for online privacy protection. *Information, communication & society*, *20*(8), 1261-1278. https://doi.org/10.1080/1369118X.2016.1229001
Carlsen, H. (2018, 4. april). *Cambridge Analytica-skandalen vokser i omfang*. NRK. Hentet 4. mai fra https://www.nrk.no/urix/cambridge-analytica-skandalen-vokser-i-omfang-1.13992414
Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada*, *5*, 12.
Cavoukian, A. (2020). Understanding How to Implement Privacy by Design, One Step at a Time. *IEEE consumer electronics magazine*, *9*(2), 78-82. https://doi.org/10.1109/MCE.2019.2953739
Cha, S.-C., Hsu, T.-Y., Xiang, Y. & Yeh, K.-H. (2018). Privacy enhancing technologies in the Internet of Things: Perspectives and challenges. *IEEE Internet of Things Journal*, *6*(2), 2159-2187. https://doi.org/10.1109/JIOT.2018.2878658
Choi, H., Park, J. & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42-51. https://doi.org/10.1016/j.chb.2017.12.001
Cohen, J. E. (2000). Examined Lives: Informational Privacy and the Subject as Object. *Stanford Law Review*, *52*(5), 1373-1438. https://doi.org/10.2307/1229517
Colesky, M., Hoepman, J.-H. & Hillen, C. (2016). A Critical Analysis of Privacy Design Strategies. IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA.
Dabrowski, A., Merzdovnik, G., Ullrich, J., Sendera, G., Weippl, E. . (2019). Measuring Cookies and Web Privacy in a Post-GDPR World. I D. Choffnes, Barcellos, M. (Red.), *Passive and Active Measurement* (s. 258-270) (Lecture Notes in Computer Science). Switzerland: Springer International Publishing AG. https://doi.org/10.1007/978-3-030-15986-3_17
Datatilsynet. (2018a, 17. juli). *Rett til innsyn*. Hentet 1. mai fra https://www.datatilsynet.no/rettigheter-og-plikter/den-registrertes-rettigheter/rett-til-innsyn/
Datatilsynet. (2018b, 18. juni). *Rett til sletting*. Hentet 05. april fra https://www.datatilsynet.no/rettigheter-og-plikter/den-registrertes-rettigheter/rett-til-sletting/
Datatilsynet. (2019a, 07. juli). *Behandlingsansvarlig og databehandler*. Hentet 05. april fra https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/behandlingsansvarlig-og-databehandler/
Datatilsynet. (2019b, 19. juli). *Hva er en personopplysning* Hentet 18. januar fra https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/
Datatilsynet. (2019c, 16. juli). *Personvernprinsippene*. Hentet 18. januar fra https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/
Datatilsynet. (2020). *Personvernundersøkelsen 2019/2020*. Hentet 1. mai fra https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/personvernundersokelser/personvernundersokelsen-20192020/
Datatilsynet. (2021, 12. oktober). *Om personopplysningsloven med forordning og når den gjelder*. Hentet 18. jaunar fra https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/om-personopplysningsloven-og-nar-den-gjelder/
Datatilsynet. (2022, 24. mars). *Innebygd personvern og personvern som standard*. Hentet 03. april fra https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern-og-personvern-som-standard/

Dienlin, T., Masur, P. K. & Trepte, S. (2023). A longitudinal analysis of the privacy paradox. *new media & society*, *25*(5), 1043-1064. https://doi.org/10.1177/14614448211016316
Dienlin, T. & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European journal of social psychology*, *45*(3), 285-297. https://doi.org/10.1002/ejsp.2049
DuckDuckGo. (2023a, 11. mai). *We don't collect or share personal information*. Hentet 1. april fra https://duckduckgo.com/privacy#s4
DuckDuckGo. (2023b). *Your personal data is nobody's business.* Hentet 25. januar fra https://duckduckgo.com/about
Fischer-Hbner, S. B., S. (2017). Privacy-Enhancing Technologies. I J. Vacca (Red.), *Computer and Information Security Handbook* (3. utg., s. 759-778). Morgan Kaufmann. https://doi.org/10.1016/B978-0-12-803843-7.00053-3
Gerber, N., Gerber, P. & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security*, *77*, 226-261. https://doi.org/10.1016/j.cose.2018.04.002
Google. (2023a). *How private browsing works in Chrome*. Hentet 4. april fra https://support.google.com/chrome/answer/7440301?sjid=2174762868167160456-EU
Google. (2023b). *Slett, slå på og administrer informasjonskapsler i Chrome*. Hentet 16. januar fra
Gueye, B., Ziviani, A., Crovella, M. & Fdida, S. (2006). Constraint-Based Geolocation of Internet Hosts. *IEEE/ACM transactions on networking*, *14*(6), 1219-1232. https://doi.org/10.1109/TNET.2006.886332
Harborth, D. & Pape, S. (2020). How privacy concerns, trust and risk beliefs, and privacy literacy influence users' intentions to use privacy-enhancing technologies - The case of Tor. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *51*(1), 51-69. https://doi.org/10.1145/3380799.3380805
Harborth, D., Pape, S. & Rannenberg, K. (2020). Explaining the Technology Use Behavior of Privacy-Enhancing Technologies: The Case of Tor and JonDonym. *Proceedings on Privacy Enhancing Technologies*, *2020*(2), 111-128. https://doi.org/10.2478/popets-2020-0020
Hargittai, E. (2002). Second-level digital divide: Differences in people's online skills. *First Monday*, *7*(4). https://doi.org/10.5210/fm.v7i4.942
Hargittai, E. & Marwick, A. (2016). "What can i really do?" Explaining the privacy paradox with online apathy. *International journal of communication*, *10*, 3737-3757. https://doi.org/10.5167/uzh-148157
Heurix, J., Zimmermann, P., Neubauer, T. & Fenz, S. (2015). A taxonomy for privacy enhancing technologies. *Computers & security*, *53*, 1-17. https://doi.org/10.1016/j.cose.2015.05.002
Hoffmann, C. P., Lutz, C. & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4). https://doi.org/10.5817/CP2016-4-7
Joinson, A. N., Reips, U.-D., Buchanan, T. & Schofield, C. B. P. (2010). Privacy, Trust, and Self-Disclosure Online. *Human-computer interaction*, *25*(1), 1-24. https://doi.org/10.1080/07370020903586662
Kehr, F., Kowatsch, T., Wentzel, D. & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607-635. https://doi.org/10.1111/isj.12062
Kezer, M., Sevi, B., Cemalcilar, Z. & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology*, *10*(1). https://doi.org/10.5817/CP2016-1-2

Khan, M. I., Loh, J., Hossain, A. & Hasan Talukder, M. J. (2023). Cynicism as strength: Privacy cynicism, satisfaction and trust among social media users. *Computers in Human Behavior*, *142*. https://doi.org/10.1016/j.chb.2022.107638
Knijnenburg, B. P., Kobsa, A. & Jin, H. (2013). Dimensionality of information disclosure behavior. *International journal of human-computer studies*, *71*(12), 1144-1162. https://doi.org/10.1016/j.ijhcs.2013.06.003
Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, *64*, 122-134. https://doi.org/10.1016/j.cose.2015.07.002
Kommunal- og distriktsdepartementet. (2019, 30. oktober). *Ny personopplysningslov* Regjeringen. Hentet 18. januar fra https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/ny-personopplysningslov/id2340094/
Kretschmer, M., Pennekamp, J. & Wehrle, K. (2021). Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web. *ACM transactions on the web*, *15*(4), 1-42. https://doi.org/10.1145/3466722
Kvale, S. & Brinkmann, S. (2015). *Det kvalitative forskningsintervju*. Gyldendal akademisk
Kaaniche, N., Laurent, M. & Belguith, S. (2020). Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey. *Journal of network and computer applications*, *171*, 102807-102807:102885. https://doi.org/10.1016/j.jnca.2020.102807
Lutz, C., Hoffmann, C. P. & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. *new media & society*, *22*(7), 1168-1187. https://doi.org/10.1177/1461444820912544
Lythreatis, S., Singh, S. K. & El-Kassar, A.-N. (2022). The digital divide: A review and future research agenda. *Technological forecasting & social change*, *175*, 121359. https://doi.org/10.1016/j.techfore.2021.121359
Martin, K. (2020). Breaking the privacy paradox: the value of privacy and associated duty of firms. *Business Ethics Quarterly*, *30*(1), 65-96. https://doi.org/10.1017/beq.2019.24
Marwick, A. & Hargittai, E. (2019). Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, communication & society*, *22*(12), 1697-1713. https://doi.org/10.1080/1369118X.2018.1450432
Meier, Y., Schäwel, J. & Krämer, N. C. (2021). Between protection and disclosure: Applying the privacy calculus to investigate the intended use of privacy-protecting tools and self-disclosure on different websites. *Studies in Communication and Media*, *10*(3), 283-306. https://doi.org/10.5771/2192-4007-2021-3-283
Microsoft. (2023). *InPrivate-visning i Microsoft Edge*. Hentet 4. april fra https://support.microsoft.com/nb-no/microsoft-edge/inprivate-visning-i-microsoft-edge-cd2c9a48-0bc4-b98e-5e46-ac40c84e27e2
Mishra, V., Laperdrix, P., Vastel, A., Rudametkin, W., Rouvoy, R. & Lopatka, M. (2020). Don't Count Me Out: On the Relevance of IP Address in the Tracking Ecosystem.*WWW '20*
Mozilla. (2023). *Private Browsing - Use Firefox without saving history*. Hentet 4. april fra https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history
Namara, M., Wilkinson, D., Caine, K. & Knijnenburg, B. P. (2020). Emotional and Practical Considerations Towards the Adoption and Abandonment of VPNs as a Privacy-Enhancing Technology. *Proceedings on Privacy Enhancing Technologies*, *2020*(1), 83-102. https://doi.org/10.2478/popets-2020-0006
Nasjonal Kommunikasjonsmyndighet. (2020, 06. mars). *Informasjonskapsler/cookies*. Hentet 16. januar fra https://www.nkom.no/internett/informasjonskapsler-cookies

Norberg, P. A., Horne, D. R. & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs*, *41*(1), 100-126. https://doi.org/10.1111/j.1745-6606.2006.00070.x
NOU 2022: 11. (2022). *Ditt personvern – vårt felles ansvar — Tid for en personvernpolitikk*. Kommunal- og distriktsdepartementet. https://www.regjeringen.no/no/dokumenter/nou-2022-11/id2928543/
Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. *Communication research*, *40*(2), 215-236. https://doi.org/10.1177/0093650211418338
Personopplysningsloven. (2018). *Lov om behandling av personopplysninger* (LOV-2018-06-15-38). Lovdata. https://lovdata.no/dokument/NL/lov/2018-06-15-38
Resvoll, A. (2023, 23. mai). *Meta ilagt rekordbot på 14 milliarder kroner*. E24. Hentet 24. mai fra https://e24.no/boers-og-finans/i/5BMEe1/meta-ilagt-rekordbot-paa-14-milliarder-kroner
Schaub, F., Balebako, R. & Cranor, L. F. (2017). Designing Effective Privacy Notices and Controls. *IEEE internet computing*, *21*(3), 70-77. https://doi.org/10.1109/MIC.2017.75
Schibsted. (2023). *News Media*. https://schibsted.com/about/we-are-schibsted/news-media/
Sikt. (2023). *Hva er en personopplysning?* Hentet 18. januar fra https://sikt.no/hva-er-personopplysninger
Skalkos, A., Tsohou, A., Karyda, M. & Kokolakis, S. (2020). Identifying the values associated with users' behavior towards anonymity tools through means-end analysis. *Computers in human behavior reports*, *2*, 100034. https://doi.org/10.1016/j.chbr.2020.100034
Smith, H. J., Dinev, T. & Xu, H. (2011). Information privacy research: An Interdisciplinary Review. *MIS quarterly*, *35*(4), 989-1015. https://doi.org/10.2307/41409970
Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, *90*(4), 1087-1155. https://doi.org/10.2307/3481326
Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania law review*, *154*(3), 477-564. https://doi.org/10.2307/40041279
Solove, D. J. (2007). "I've got nothing to hide" and other misunderstandings of privacy. *The San Diego law review*, *44*(4), 745.
Solove, D. J. (2011). *Nothing to hide : the false tradeoff between privacy and security*. Yale University Press.
Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, *126*(7), 1880-1903. https://www.jstor.org/stable/23415060
Solove, D. J. (2021). The myth of the privacy paradox. *George Washington Law Review*, *89*(1). https://doi.org/10.2139/ssrn.3536265
Tabata, N., Sato, H. & Ninomiya, K. (2021). Comparison of Privacy Consciousness Between Younger and Older Adults. *Japanese psychological research*, *63*(2), 104-110. https://doi.org/10.1111/jpr.12284
Taddei, S. & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, *29*(3), 821-826. https://doi.org/10.1016/j.chb.2012.11.022
Tjora, A. (2021). *Kvalitative forskningsmetoder i praksis* (4. utg.). Gyldendal Akademisk.
Traverso, S., Trevisan, M., Giannantoni, L., Mellia, M. & Metwalley, H. (2017). Benchmark and comparison of tracker-blockers: Should you trust them? 2017 Network Traffic Measurement and Analysis Conference (TMA),
Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A. & Lind, F. (2015). Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). I S. Gutwirth, R. Leenes & P. de Hert (Red.), *Reforming European data protection law* (s. 333-365) (Law, Governance and

Technology Series). Springer Netherlands. https://doi.org/10.1007/978-94-017-9385-8_14
van Ooijen, I., Segijn, C. M. & Opree, S. J. (2022). Privacy cynicism and its role in privacy decision-making. *Communication research*. https://doi.org/10.1177/00936502211060984
Warren, S. D. & Barndeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193-220. https://doi.org/10.2307/1321160
Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of social issues*, *59*(2), 431-453. https://doi.org/10.1111/1540-4560.00072

Vedlegg

Vedlegg 1: Intervjuguide eksperter

Vedlegg 2: Intervjuguide brukere

Vedlegg 3: Kodestruktur og grupperinger

Vedlegg 4: Informasjonsskriv og samtykkeskjema

Vedlegg 1: Intervjuguide eksperter

Denne intervjuguiden fungerer som et utgangspunkt og en veiledning intervjusituasjonen. Formålet med intervjuguiden er å utarbeide spørsmål som kan brukes til videre utarbeiding og spesifisering av spørsmål til den resterende delen av utvalget. Spørsmålene som blir stilt til informantene (deltakerne) er knyttet til temaet personvern. Alle informantene vil anonymiseres. Varigheten på intervjuene estimeres til ca. 40-60 minutter.

Introduksjon: Generell bakgrunnsinformasjon

1. Hva fikk deg til å bli interessert i personvern?
2. Hva er ditt forhold til personvern?
    a. Er det noe du er opptatt av i ditt private liv?
    b. Er det noe spesielt du gjør for å beskytte dine personopplysninger på Internett?
3. Hva er din arbeidstittel?
4. Hva er din utdanningsbakgrunn?
5. Hvordan jobber du med personvern i det daglige?
    a. Hva jobber du med?
    b. Hvorfor valgte du dette feltet?

Om personvern

1. Hva innebærer personvern for deg?
    a. Er det noe brukere burde være bevisste om når de bruker Internett eller andre digitale enheter?
2. Hva er det som gjør personvern til et aktuelt tema i dag?
    a. Hva er det som eventuelt gjør det komplekst?
3. Om informanten har kjennskap til eller lest personvernkommisjonens rapport:
    a. Vil du si deg enig i påstanden om at personvern kan anses å ha bekymrende utviklingstrekk i dagens samfunn?
    b. Hva og hvordan har det endret seg?
    c. Hvordan synes du personvern i Norge utviklet seg de siste tiårene?
4. Hva er egentlig personopplysninger?
    a. Hvilke personopplysninger kan anses som sensitive?

    b. Er personopplysninger det samme som brukerdata?
    c. Hvilke opplysninger bør folk ikke oppgi eller dele med andre virksomheter?
5. Hvilke organisasjoner eller offentlige virksomheter jobber med personvern i Norge?

Regelverk og personvernrettigheter

1. Hva er GDPR eller personvernforordningen?
    - Hvilke positive og negative konsekvenser kan GDPR ha for individer, organisasjoner/bedrifter og samfunnet?
2. Hva er et personvernombud og hva er hens oppgaver?
    - Hvorfor er det viktig med et personvernombud?
3. Hvilke rettigheter har individer etter personvernregelverket når personopplysninger eller informasjon samles inn og brukes?
    - Gjelder de samme reglene for alle eller gjør det en forskjell om det dreier seg f.eks. om kommersielle selskaper/bedrifter vs vitenskapelige forskning?
4. Hvilke plikter har virksomheter/selskaper til å oppfylle eller tilpasse individers rettigheter etter personvernregelverket?
5. Hvor kan man henvende seg om man har spørsmål om behandling av personopplysninger og de rettighetene du har etter personopplysningsregelverket?
6. Hvor kan man gjøre for å forsikre seg om eller beskytte sine egne personopplysninger?
7. Har du noen eksempler på selskaper som har brutt personvernforordningen i form av et personvernbrudd?
8. Hva skjer hvis personopplysninger overføres ut av EØS/EU?
    a. Er dette en problemstilling som brukere må ta stilling til?
    b. Er det noen forskjeller i hvordan personopplysninger blir samlet inn og behandlet utenfor EU/EØS?

Bruk av informasjonskapsler og personvernfremmende teknologier

1. Hva er informasjonskapsler?
    a. Hvordan bruker virksomheter informasjonskapsler?
    b. Opplever du at virksomheter gjør det enklere eller vanskelig å navigere seg gjennom innstillinger for informasjonskapsler eller personvern på nettsteder?

2. I denne masteroppgaven vil fokuset rettes mot det som kan betegnes som personvernfremmende teknologier. Med dette mener jeg teknologier, verktøy, digitale teknikker eller programutvidelser som tilbyr personvernfremmende alternativer til eksempelvis nettsurfing.
    a. Har du hørt om dette begrepet før eller har kjennskap til hva det innebærer?
    b. Kan du tenke deg hvorfor dette kan være et passende alternativ for brukere?
3. Er det hensiktsmessig å bruke Virutal Privacy Networks = VPN?
    a. Hvordan hjelper dette?
    b. Hva er en IP-adresse? Og hvordan kan dette brukes?
4. Har det noe å si hvilke nettlesere man bruker?
    a. Har du noen eksempler på nettlesere som tilbyr bedre eller dårligere databeskyttelse/sikkerhet?
5. Er det hensiktsmessig å bruke inkognitomodus i nettleseren?
    a. Vil det kunne bidra til å beskytte enkeltpersoners personopplysninger?
6. Er det hensiktsmessig for brukere å benytte seg av AdBlock eller andre blokkeringsverktøy?

Tips og råd til brukere

1. Er det noe brukere burde være kjente med når det gjelder personvern?
2. Hva kan brukere gjøre beskytte sine personopplysninger? Nå rer det spesielt viktig å gjøre det?
3. Har du noen tips til brukere som ønsker å lære mer om hvordan deres personopplysninger behandles, brukes og distribueres?
    a. Har du noen andre anbefalinger om personvernfremmende alternativer som enkeltpersoner kan ta i bruk for å beskytte sine personopplysninger?
4. Mener du norske brukere er bevisste nok rundt personvern?
    a. Er det noe som bør gjøres i så fall hva?
    b. Hvordan bør ansvaret fordeles mellom enkeltpersoner og private/offentlige virksomheter(selskap)?

Vedlegg 2: Intervjuguide brukere

Denne intervjuguiden fungerer som et utgangspunkt og en veiledning intervjusituasjonen. Spørsmålene som blir stilt til informantene (deltakerne) er knyttet til temaet personvern. Alle informantene vil anonymiseres. Varigheten på intervjuene estimeres til ca. 40-60 minutter.

Kort introduksjon (Bakgrunnsinformasjon):

1. Hvor gammel er du?
2. Hvor mange års utdanning har du?
    - Hva er din utdanningsbakgrunn?
    - Er du student, arbeidsledig eller ute i arbeidslivet?
3. Hvor ofte bruker du Internett eller andre digitale enheter (f.eks telefon, PC, osv.)?
    - Bruker du noen sosiale medier?
    - Er du medlem av noen kundeklubber?
        - Hva tenker du om den informasjonen som ligger tilgjengelig der?

Om personvern

1. Forklare litt om hva personvern er og litt ulike perspektiver på dette.
    a. Hva er ditt forhold til personvern?
2. Hva er viktig for deg når det gjelder personvern?
    a. Hvilken betydning har personvern for deg i det daglige?
3. Har personvern noen konsekvenser for måten du bruker Internett eller digitale enheter på?
    a. Er det noen grunn til dette?
    b. Hvor går grensen?
4. Hva betyr personopplysninger for deg?
    a. Er du opptatt av hvordan personopplysningene dine behandles, samles inn og brukes?
    b. Hvem har eller burde ha tilgang til personopplysningene dine?
        i. Begrenser du hvem som har tilgang?
        ii. Har dette noen påvirkning for deg?
        iii. Har du hatt noen gode eller dårlige opplevelser knyttet til bruken eller behandlingen av personopplysningene dine?

5. Minus: Hva tenker du om at dine personopplysninger selges, distribueres og brukes av tredjeparter?
    a. Er det noen som ikke bør ha tilgang til dine personopplysninger?
    b. Har det noe å si for deg at du deler personopplysningene dine?
6. Har personvern noe å si for deg når du skal bruke en digital tjeneste, kjøpe noe eller søke etter informasjon på nettet?
    a. Hvorfor?
    b. Er det noe spesielt du gjør for å sikre personopplysningene dine?
7. Hvem har ansvaret for dine personopplysninger?
    a. Hva tenker du om at disse kan misbrukes eller er tilgjengelig for bedrifter/selskaper som du ikke kjenner til?

Kjennskap til rettigheter og regelverk rundt personvern

1. Har du kjennskap til hvilke personvernrettigheter du har?
    a. Er dette noe som er viktig for deg?
2. Vet du hva GDPR eller personvernforordningen er?
    a. Eventuelt forklare hva det er.
    b. Har dette regelverket påvirket deg på noen måte? Er det noe spesielt du har lagt merke til?
3. Hvor ville du har henvendt deg eller undersøkt for å finne informasjon om personvern eller rettighetene dine?
    a. Tenker du det er enkelt å finne fram til nødvendig informasjon om dette?
    b. Om de har kjennskap:
        i. Hvor fant du informasjon om dette eller hørte om det?

Forhold til behandlingsansvarliges bruk av informasjonskapsler og personopplysninger

1. Forklare litt rundt informasjonskapsler (Cookies).
    a. Vet du hva dette er eller er det noe du merke til?
    b. Hvorfor tenker du det er nødvendig at nettsider bruker eller ber deg om å samtykke til bruken av informasjonskapsler (cookies)?

Her vil jeg ta i bruk visuelle hjelpemidler for å gå gjennom ulike nettsider og ulike typer informasjonskapsler med intervjuobjekt. Det vil ikke lagres noe opptak av denne gjennomgangen dette vil kun forekomme gjennom lydopptaket. Nettsidene vil bli valgt ut basert på intervjuobjektets kjennskap og ønske. Dette vil gjennomføres på intervjuerens PC på en nyopprettet konto uten innlogging eller tidligere nettlesingshistorikk. Informantene vil selv kunne velge nettsider som de selv bruker, har kjennskap til eller vil se nærmere på.

2. Hva tenker du når du ser dette?
    a. Hva ville du har gjort her?
    b. Hvorfor ville du valgt dette?
    c. Er dette noe du vanligvis legger merke til eller tenker over?
        i. Kommer dette opp hver gang du besøker nettsiden?
3. Godkjenner du eller ikke vanligvis informasjonskapsler på nettsider?
    a. Hvorfor gjør du det?
    b. Tenker du dette er frivillig?
4. Leser du gjennom den informasjonen som er tilgjengelig?
    a. Endrer du tillatelser?
    b. Har du noen gang valgt å ikke godkjenne informasjonskapsler?
        i. Hvorfor og hva skjedde?
5. Tenker du at informasjonskapsler (cookies) påvirker brukeropplevelsen din av en nettside?
    a. Hvorfor tenker du det?

Bruk av personvernfremmende teknologier

1. Forklare kort hva personvernfremmende teknologier (PETs) er og hva det brukes til.
    a. Er de kjent med det? Eller tenker hvorfor dette kan være nødvendig i forhold til personvernet ditt?
    b. Er dette funksjoner/verktøy som du tenker burde vært tilgjengelig kostnadsfritt eller som en normal del av de digitale tjeneste/nettsidene du bruker til daglig?
2. Er det viktig at du har alternativer som gjør det mulig for deg å beskytte eller begrense hvordan dine personopplysninger samles inn, behandles og brukes?
    a. Hvorfor?
3. Hvilken nettleser bruker du?

    a. Kjenner du til eller bruker:
        i. Brave Browser
        ii. Tor
        iii. Mozilla FireFox
    b. DuckDuckGo hva er det?
4. Har valget ditt av nettleser noe å si for ditt personvern?
    a. Kan nettleseren din har noe å si for personvernet ditt?
5. Har du kjennskap til eller bruker inkognito modus?
    a. Hvorfor bruker du dette?
    b. Hva skjer når du bruker denne funksjonen?
    c. Hva tenker du om at når du bruker inkognito modus så:
        i. Vil aktiviteten din kan fortsatt være synlig for:
            1. nettsteder du besøker
            2. arbeidsgiveren eller skolen din
            3. Internett-leverandøren din
6. Hva er det som kan identifisere deg på Internett?
    a. Vet du hva en IP-adresse er?
        i. Hva brukes det til?
7. Er du kjent med hva en VPN eller virtuelt privat nettverk er?
    a. Bruker du det selv?
    b. Hvis ja, fortell litt om det.
        i. Hvorfor bruker du det?
        ii. Er det noen spesielle situasjoner som gjør det nødvendig?
            1. Hvis ja/nei, hvorfor?
            2. Kunne du tenkt deg hvorfor dette kan være nødvendig?
8. Kjenner du til hva AdBlock er eller bruker det selv?
    a. Hvorfor bruker du(ikke) dette?
    b. Hva skjer når du bruker AdBlock
9. Hvordan ble det kjent med noen av disse (ovenfor)?
    a. Hvorfor tenker du det eventuelt ikke er nødvendig?
10. Har du noen andre eksempler på personvernfremmende teknologi, verktøy, utvidelser eller annet som bidrar til å styrke personvernet ditt?
    a. Hvorfor?

Informantenes opplevelser, erfaringer og tips til andre

1. Har du noen gang valgt å gå bort fra en tjeneste på grunn av personvern?
    a. Hvorfor, og hva skjedde?
2. Tenker du det bør gjøres endring som gjør det lettere for deg å ivareta personvernet ditt eller er dette bedrifter/selskaper/offentlighetens oppgave?
    a. Hvorfor det?
3. Har du noen erfaringer eller tips som du vil dele med andre som ønsker å bli mer opptatt av eller er bekymret over sitt eget personvern?
4. Er det noe annet du vil ta opp før vi avslutter?

Vedlegg 3: Kodestruktur og grupperinger

Kodegruppe 1: Forhold til behandlingsansvarliges praksiser

- Undergruppe 1: Innebygd personvern
- Undergruppe 2: Kontroll over personopplysninger
- Undergruppe 3: Ansvarsfordeling

Kodegruppe 2: Villighet til å avsløre

- Undergruppe 1: Ulike former for tillit
- Undergruppe 2: Bevissthet rundt risiko og konsekvenser
- Undergruppe 3: Opplevde hindringer

Kodegruppe 3: Behov for beskyttelse

- Undergruppe 1: Anonymisering
- Undergruppe 2: Blokkering og begrensning
- Undergruppe 3: Opplevd nytteverdi
- Undergruppe 4: Påvirkning på brukeropplevelsen

Vedlegg 4: Samtykkeskjema og informasjonsskriv

Vil du delta i et forskningsprosjekt?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å undersøke nordmenn holdninger til personvern knyttet til deres atferd og beslutninger når det gjelder deres personopplysninger. Dette skrivet gir deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Formålet med dette forskningsprosjektet er å undersøke temaet personvern i forhold til det som kan betegnes som personvernparadokset. I denne sammenhengen har en rekke tidligere studier fremhevet hvordan menneskers holdninger til personvern nødvendigvis ikke stemmer overens med deres faktiske atferd og brukerpraksiser. På bakgrunn av dette har denne masteroppgaven som formål å utforske teknologibrukeres holdninger og praksiser som er knyttet til personvern. Videre hvordan dette forholdet mellom mennesket og teknologi er med på å skape nye, forventede og uforventede måter å forstå og bruke teknologi på.

Dette prosjektet er en del en masteroppgave i Medier, kommunikasjon og informasjonsteknologi ved Norges teknisk-naturvitenskapelige universitet i Trondheim. Alle dataene i prosjektet vil bli anonymisert, slik at ingen avgitte svar, utsagn eller sitater kan knyttes opp mot eller gjør det mulig å identifisere enkeltindivider.

Hvem er ansvarlig for forskningsprosjektet?

NTNU, fakultet for samfunns- og utdanningsvitenskap (SU) og Institutt for sosiologi og statsvitenskap, er ansvarlig for prosjektet. Det samme gjelder for studenten, Kristian August Røstad-Tollefsen, som gjennomfører prosjektet som en del av sitt masterprogram.

Hvorfor får du spørsmål om å delta?

Du får spørsmål om å delta ettersom dette prosjektet har som formål å komme i kontakt med teknologibrukere som ønsker å dele deres erfaringer og opplevelser med personvern i deres hverdagslige bruk av digitale teknologier.

For å kunne besvare prosjektets problemstilling er det ansett som hensiktsmessig og nødvendig å rekruttere en ekspert på personvern dette i form av en jurist. Formålet med dette er å kunne belyse relevant informasjon og bidra med verdifull innsikt, kunnskap og kompetanse rundt personvernets betydning regelverk (GDPR) og teknologibrukeres personvernrettigheter. Den andre delen av utvalget vil videre bestå av utvalgte enkeltindivider

som har vist interesse for å delta i dette prosjektet. For å kunne rekruttere disse vil jeg benytte mitt eksisterende nettverk av bekjente, samt forsøke å rekruttere andre tilfeldige aktuelle kandidater. Det er ikke satt noen krav om forkunnskaper eller nødvendige kriterier for dette utvalget med tanke på kunnskap, kompetanse og ferdigheter.

Hva innebærer det for deg å delta?

Deltakere som ønsker å være med i dette forskningsprosjektet vil bli invitert til å ta del i et personlig semi-strukturert intervju på om lag 40-50 minutter. Disse intervjuene vil gjennomføres fysisk eller digitalt. Spørsmålene vil i hovedsak omhandle dine erfaringer, opplevelser og forståelse av personvern knyttet til bruk av digitale teknologier. Videre vil spørsmålene være rettet mot dine hverdagslige brukerpraksiser, samt hvordan disse påvirkes av, formes eller kan sees i sammenheng med personvern. Dette gjelder i forhold til hvordan forsikrer seg om eller er oppmerksomme om at deres rettigheter og personopplysninger ivaretas, samt hvilken rolle personvern spiller i deres digitale hverdagslige praksiser.

Det vil ikke stilles spørsmål om andre personopplysninger enn alder, kjønn, og bruk av spesifikke digitale tjenester, preferanser og/eller verktøy. For å kunne gjøre opptak av intervjuene vil det brukes en separat lydopptaker som gjør det mulig å lagre samtalen i form av et lydopptak fra intervjusituasjonen. Formålet med detter å gjøre det mulig å transkribere intervjuet til tekst som vil kunne brukes i masteroppgavens analysedel. Alt av datamaterialet (tekst og tale) vil bli transkribert på NTNUs eget nettverksområde. Videre vil datamaterialet anonymiseres og slettes ved prosjektets sluttdato, som er 06.06.2023.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke deg som deltakere i dette forskningsprosjektet ved å 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 skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket. Det er kun jeg, Kristian August Røstad-Tollefsen, som ønsker og vil ha tilgang til dine personopplysninger og datamaterialet. For å sikre at dine personopplysninger blir ivaretatt vil det kun benyttes utstyr som er lånt fra NTNU (lydopptaker) dette gjelder også for behandling av lydopptakene. Alt av datamaterialet vil lagres og overføres på NTNUs hjemmeområde (egne servere) ved hjelp av en kryptert minnepenn som er beskyttet med passord. Et utvalg av sitater fra intervjuene vil publiseres som en del av det ferdigstilte forskningsprosjektet. Alt av datamaterialet vil anonymiseres og unødvendig personopplysninger vil bli fjernet, noe som

tilsier at det ikke vil kunne være mulig å gjenkjenne eller identifisere enkeltindivider i det transkriberte materialet.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er 06.06.2023. Alle data i form av lydopptak og transkriberinger vil slettes ved prosjektets slutt.

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

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke. På oppdrag fra NTNU, fakultet for samfunns- og utdanningsvitenskap (SU) og Institutt for sosiologi og statsvitenskap, har Sikt – Kunnskapssektorens tjenesteleverandørs personverntjenester vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- Kristian August Røstad-Tollefsen: kristaro@ntnu.no.
- NTNU, fakultet for samfunns- og utdanningsvitenskap (SU) og Institutt for sosiologi og statsvitenskap ved Melanie Magin. Kontaktopplysninger er tlf: 73413277 og mail: melanie.magin@ntnu.no.
- Vårt personvernombud: Thomas Helgesen, personvernombud ved NTNU. Kontaktopplysninger er tlf: 93079038 og e-post: thomas.helgesen@ntnu.no

Hvis du har spørsmål knyttet til vurderingen av prosjektet som er gjort av Sikts personverntjenester ta kontakt på:

- Epost: personverntjenester@sikt.no, eller telefon: 53 21 15 00.

Med vennlig hilsen

Melanie Magin
(Forsker/veileder)

Kristian August Røstad-Tollefsen
(student)

Samtykkeerklæring

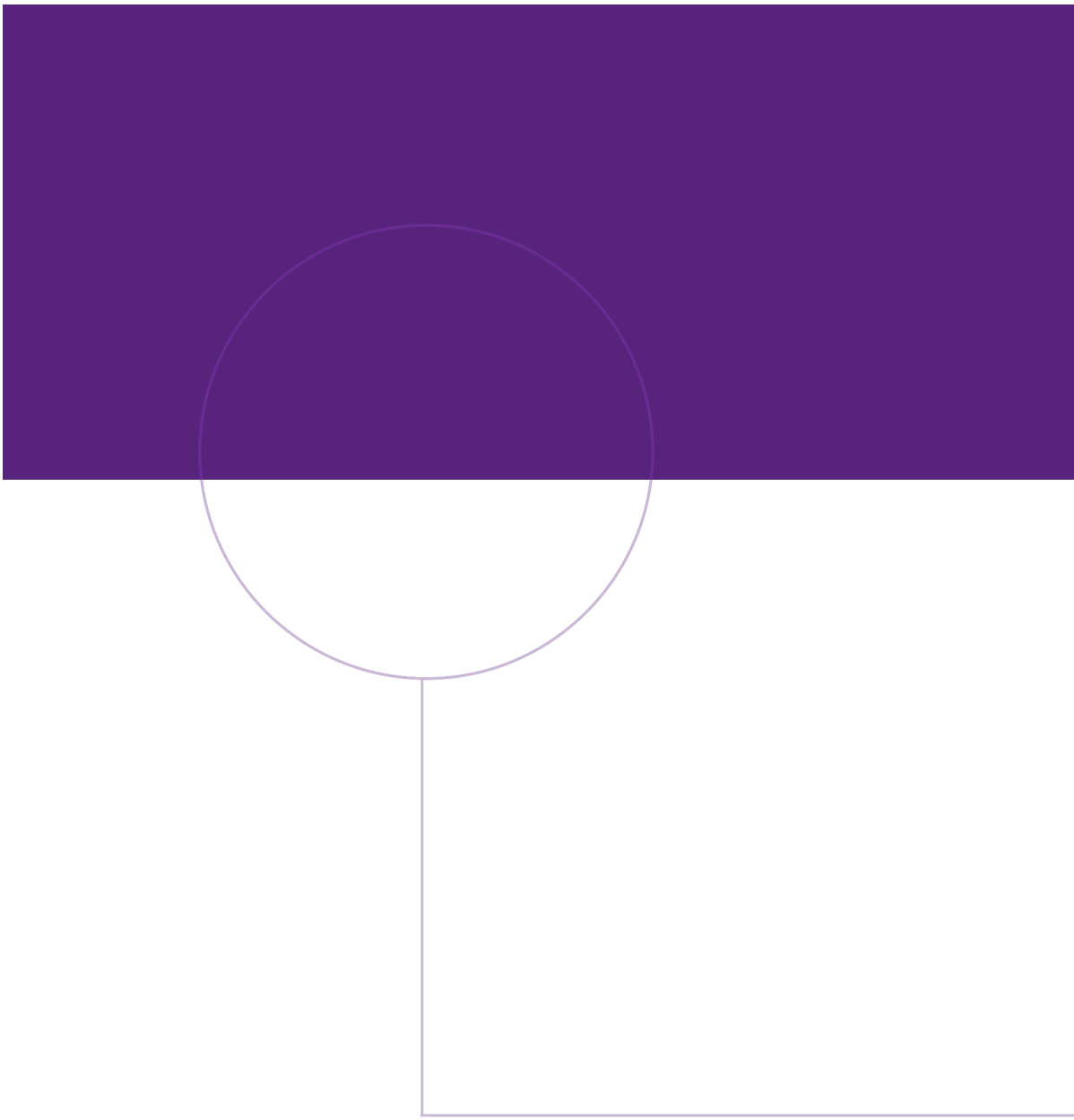
Jeg har mottatt og forstått informasjon om prosjektet «Personvern og bruker praksis», og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i intervju
- ☐ at det gjennomføres lydopptak av intervjuet, som slettes ved prosjektets sluttdato
- ☐ at dataene anonymiseres og benyttes i den endelige rapporten

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

---

(Signert av prosjektdeltaker, dato)



NTNU

Kunnskap for en bedre verden