Masteroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for økonomi
NTNU Handelshøyskolen

Sondre Garli

Individers villighet til å dele personlige data i banknæringen

Masteroppgave i ledelse av teknologi
Veileder: Jon Martin Denstadli
Juni 2020

NTNU
Kunnskap for en bedre verden

Sondre Garli

Individers villighet til å dele personlige data i banknæringen

Masteroppgave i ledelse av teknologi
Veileder: Jon Martin Denstadli
Juni 2020

Norges teknisk-naturvitenskapelige universitet
Fakultet for økonomi
NTNU Handelshøyskolen

NTNU
Kunnskap for en bedre verden

Forord

Som summer intern i SpareBank 1 SMN sommeren 2019, fikk jeg et innblikk i bankens satsningsområder og utfordringer, hvor vi fokuserte på kundesegmentet «Ung». Denne kundegruppen består av kundene mellom 18–34 år, hvor kundene gjerne sparer i BSU, starter i sin første jobb og etter hvert kjøper sin første eiendom.

I den forbindelse presenterte SpareBank 1 SMN en utfordring med å innhente samtykker for å samle, behandle og analysere kunde- og persondata. Jeg har derfor valgt å se på denne utfordringen i masteroppgaven, hvor jeg ønsker å hjelpe SpareBank 1 SMN med å belyse denne problematikken. Det faktum at jeg vil forske på en reell utfordring skaper en økt motivasjon for arbeidet. Jeg skal også starte arbeidskarrieren som konsulent innenfor digitalisering og prosjektledelse, og jeg håper denne oppgaven gir meg kunnskaper jeg har nytte av i fremtiden.

Coronaviruset har utfordret hele verden denne våren, og skapt en annen studiehverdag enn den jeg er vant med. Det har resultert i en mindre sosial skolehverdag, som har gjort det utfordrende å holde motivasjonen oppe. En viktig årsak i denne skriveprosessen kan tilskrives veilederen min, professor ved NTNU, Jon Martin Denstadli. Du har vært min viktigste støttespiller, og hjulpet meg med å opprettholde motivasjonen og ved å sikre fremdriften gjennom digitale veiledningsmøter. Tusen takk for samarbeidet!

Innholdet i denne oppgaven står for forfatterens regning, og jeg vil takke SpareBank 1 SMN for at de ønsket å stille med en problemstilling til masteroppgaven min.

Trondheim, 24. Juni 2020

Sondre Garli

Sammendrag

Denne studien har sett på problemstillingen: *«Hvilke faktorer kan forklare kundens villighet til å dele personlige data med banken?»* For å belyse problemstillingen har studien benyttet en privacy calculus modell basert på etablerte studier fra Dinev & Hart (2006) og Kim & Kim (2018). Privacy calculus modellen bygger på elementene *oppfattede fordeler, oppfattet risiko* og *håndteringsevnen*, som underliggende faktorer for å anslå kundens villighet til å dele data. Om de *oppfattede fordelene* overstiger den *oppfattede risikoen* ved å dele data, hevder teorien at kundene ville være villige til å dele personopplysninger. *Håndteringsevnen* viser til individets evne til å beskytte sine personopplysninger, og opprettholde kontrollen over personvernet.

Banksektoren preges også av en rekke drivere for en digital transformasjon, hvor kundene forventer at bankene skal kunne levere digitale tjenester som hjelper med å holde økonomisk oversikt. Konsulentrapporten for bankbransjen (Cicero, 2019) peker derimot på at det er store hull i tjenestespekteret hos bankene, hvor kundene i liten grad har tilgang til persontilpassede tjenester.

Empirien til denne studien er samlet inn ved bruk av en spørreundersøkelse, og resultatene indikerer at de *oppfattede fordelene* er den viktigste faktoren for individers villighet til å dele data. *Oppfattet risiko* ble målt ved hjelp av de latente variablene *tillit* og *sensitivitet på dataopplysningene*, og indikerte at den *opplevde risikoen* hadde en negativ relevans for villigheten til å dele data. Funnet var relatert til de sensitive *kunde- og personopplysningene*, men viste seg å ikke være signifikant for *kontaktopplysningene*. *Håndteringsevnen* er sammensatt av *mestringsevnen* og *effektiviteten av tiltakene*, og etablert teori argumenterer for at disse faktorene er positivt relatert til villigheten om å dele personopplysninger. Resultatene fra denne studien indikerer derimot at *mestringsevnen* er signifikant negativt relatert til å dele både kontaktopplysninger og sensitive kunde- og personopplysninger. Funnet kan muligens forklares med at de individene som scorer høye verdier av *mestringsevne* også kjenner til konsekvensene ved et brudd på personvernet, og dermed har en tilbakeholden holdning til å dele personopplysninger. *Effektiviteten på tiltakene* er kun signifikant positivt relatert til de sensitive kunde- og personopplysningene i denne studien, og er ikke å regne som signifikant for kontaktopplysningene.

Abstract

This master thesis has researched the following problem statement; *"Which factors could explain users' willingness to provide personal information to banks?"* I've used the privacy calculus model of Dinev & Hart (2006) and Kim & Kim (2018) to investigate the problem statement. The model is constructed by elements of *perceived benefits, perceived risk* and *coping appraisal*, and is viewed as explanatory factors for individual's willingness to provide personal information. If the *perceived benefits* are of greater value than the *perceived risk*, the model argues that users would be more likely to disclose their personal information. *Coping appraisal* is linked to individual's ability to control the *perceived risk* and protect their personal information.

The banking industry is affected by several factors that accelerates digital transformation, that results in higher expectations from their customers. The customers want personalized services that could help them keep control of their economy, but a report from Cicero (2019) implies that the Norwegian banking industry isn't utilizing the potential of offering value-adding services to their customers.

I've collected the empirical data through a survey, and the results indicates that the *perceived benefits* are the most important factor for customers willingness to provide personal data. *Perceived risk* was measured with help of variables of *organizational trust* and *sensitivity data information* and indicated that the *perceived risk* was negative related to the willingness to provide personal information. The correlation significant for the *sensitive financial data* but proved to be insignificant for *contact information*. *Coping appraisal* is combined of user's *self-efficacy* and the *effectiveness of protective actions,* and previous studies stated that these factors was positive correlated to the willingness to disclose personal information. Instead, this study indicated that *self-efficacy* was significant negative related to provide both *contact information* and *sensitive financial data*. It could be argued that high levels of *self-efficacy* imply that a person is well-known with the consequences of a privacy breach, and therefore would be reluctant to disclose personal data. The *effectiveness of protective actions* was significant for the *sensitive financial data* in this study but proved to be insignificant for the *contact information.*

Innholdsfortegnelse

1. Innledning

1.1 Viktigheten av data

Data er blitt en nøkkelressurs for alle digitale organisasjoner, noe man ser verdien av hos globale organisasjoner som Amazon og Facebook. Forbes (2018) anslår at Big Data markedet ville øke med over 10% i året frem til 2027, og omsette for mer enn 100 milliarder dollar i året. Viktigheten av ressursen underbygges også av en studie fra Accenture, hvor 79 prosent av de spurte lederne var enig om at bedriftene som ikke var villige til å bruke Big Data ville miste konkurransekraften sin. I motsatt ende hadde 83 prosent av lederne satset på Big Data prosjekter for å oppnå en konkurransefordel i markedet (Forbes, 2018). I takt med at mengden ustrukturerte data har økt, har analyseteknikkene også utviklet seg. Det har ført til at bedriftene er i stand til å bruke data til å skape verdi, enten i form av innsikt å ta bedre strategiske avgjørelser eller ved å utvikle CRM systemer til å øke kundetilfredsheten (Forbes, 2019).

Viktigheten av ustrukturerte data vil også gjelde for SpareBank 1 SMN og resten av bankbransjen, da kundene stort sett kommuniserer med banken via digitale flater. I en markedsrapport fra konsulentbyrået Cicero (2019) hevder man at data kan være nøkkelen til å utvikle tjenestespektret og tilby verdiøkende tjenester til bankkundene. Samtidig avdekte rapporten store hull i tjenestespekteret til bankene, og konkluderte med at bankene hadde brukt for lang tid på å legge strategiske planer i stedet for å utvikle verdiøkende tjenester som utnytter mulighetene i PSD2-direktivet. **(**Kapittel 2.1.2**)**

Data blir dratt frem som tungen på vektskålen i kampen om kundene, og rapporten til Cicero poengterer at bankene sitter på enorme mengder kundedata. Selv om bankene i dag sitter på store mengder kundedata, må de fortsatt ha kundens samtykke for å behandle, sammenstille og behandle informasjonen. Samtykkene er derfor et viktig ledd for å ha mulighet til å realisere potensialet som finnes i bankbransjen, slik at bankene kan tilby verdiøkende tjenester for kundene. På en side er dataopplysninger en viktig ressurs for organisasjonene, men på en annen side har bekymringene relatert til personvern økt i tråd med økt bevisstgjøring hos kundene. Det har ført til at færre og færre velger å dele data, og SpareBank 1 SMN har i dag mulighet til å innhente data for rundt 35% av kundene sine.

Formålet med denne oppgaven er å avdekke forhold som er med på å påvirke individers villighet til å dele data med banken sin, som igjen kan hjelpe SpareBank 1 SMN med å realisere potensialet som ligger i å innhente, behandle og analysere store datamengder. Det leder dermed til følgende problemstilling:

«Hvilke faktorer kan forklare kundens villighet til å dele personlige data med banken?»

Studien har grunnlag i forskningslitteraturen innenfor fagfeltene digitalisering, personalisering og personvern. Ved hjelp av privacy calculus teorien (Dinev & Hart, 2006), vil denne studien teste empirien mot tidligere studier. Privacy calculus modellen benytter motivasjonsteori og beskyttelsesmotivasjonsteori for å anslå individers adferd i en gitt kontekst. Modellen er også benyttet flere ganger innenfor de nevnte fagfeltene, og denne studien kan derfor være med på å styrke forskningslitteraturen gjennom å teste modellen i en ny kontekst. Det betyr at denne studien kan bidra til å teste privacy calculus modellens relevans for finansielle organisasjoner, og belyse hvilke holdninger bankkundene har til å dele finansielle data for å oppnå økt personalisering. Der hvor tidligere forskning gjerne har målt villigheten til å dele dataopplysninger knyttet til netthandel, Internet of Things tjenester eller helseopplysninger, vil denne studien måle villigheten til å dele finansiell informasjon med banken. Dermed håper jeg å avdekke hvilke holdninger og oppfattelser bankkundene har til å dele sin finansielle informasjon, og eventuelt hvilke faktorer som påvirker villigheten til å dele denne informasjonen.

1.2 Presentasjon av samtykkene til Sparebank 1 SMN:

Per dags dato opererer SpareBank 1 SMN med to samtykker, hvor man henholdsvis spør om retten til å drive elektronisk markedsføring av bankens produkter (1) og retten til å dele, benytte og sammenstille kundeopplysningene mellom SpareBank 1 selskapene (2).

Samtykke 1 omhandlet elektronisk markedsføring av bankens produkter, hvor man aksepterer å motta «gode råd og tilbud digitalt». Eksempler på disse digitale kanalene vil være e-post, bankens digitale plattformer og tekstmeldinger, noe som fører til at kontaktopplysninger som telefonnummer og e-postadresse er relevante for samtykke 1. I tillegg påpeker SpareBank 1 SMN at dette samtykket ikke nødvendigvis vil føre til at man kontaktes oftere av banken, men at de henvendelsene man gjennomfører skal oppleves mer relevant.

Samtykke 2 omhandlet som nevnt retten til å dele, benytte og sammenstille kundeopplysninger mellom SpareBank 1 selskapene, slik at SpareBank 1 «skal forstå hva jeg trenger». Dette innebærer at banken vil kunne tilpasse sine råd og tilbud på tvers av deres produktkategorier, som for eksempel innebærer sparing, lån, betaling og forsikring. Jeg anser videre deling av data som et nøkkelelement i samtykke 2, hvor SpareBank 1 SMN deler, sammenstiller og analyserer kundeopplysningene for å oppnå formålet med å forbedre sine råd og tilbud. Disse personopplysningene klassifiseres i to grupper, henholdsvis sensitive dybdeopplysninger og opplysninger tilknyttet kundeadferd. Dybdeopplysninger eksemplifiseres med finansiell informasjon som kunde- og produktavtaler, kredittkorthistorikk, inntektsopplysninger, betalingskortnummer og transaksjonshistorikk som sammenstilles og analyseres for å kunne gi tilpassede råd eller relevante tilbud til kunden. Opplysningene tilknyttet kundeadferden omhandler derimot informasjon om hvordan kunden benytter seg av bankens nettside, plattformer og digitale apper, hvor trafikkdata, stedsdata og andre kommunikasjonsdata hentes inn.

2. Bakgrunn

2.1 Digitalisering av banksektoren

Fjørtoft, Presttun og Tvedt (2019) beskriver banken som en etablert og tillitsfull aktør i samfunnet som forvalter av penger, hvor forretningsmodellen er bygd på å ta seg betalt for prising av risiko ved utlån. Forenklet, kan kjernevirksomheten knyttes til å flytte penger (1), plassere penger (2) og utlån av penger (3).

Den forenklede beskrivelsen av kjernevirksomheten i bankene utfordres i dag som et resultat av økt digitalisering, hvor Cortet, Rijks og Nijland (2016) hevder flere drivere er med på å endre bankbransjen. Digitaliseringen betraktes som bakgrunnen for denne transformasjonen, og er dermed med på å danne underlaget for denne oppgaven, hvor innsamling, behandling og analyse av person- og kundeopplysninger er nøkkelelementer i verdiskapingen hos bankene. Digitalisering defineres som kjent ved å anvende teknologi til å fornye, forenkle og forbedre produkter og tjenester som er enkle å bruke, effektive og pålitelige (Regjeringen, 2014) På den måten legger digitalisering til rette for økt verdiskaping og innovasjon, og kan være med på å øke produktiviteten i både privat og offentlig sektor (Regjeringen, 2014).

Cortet, Rijks og Nijland (2016) hevder digitaliseringen i bankbransjen drives av tre drivere; Endring i kundeadferd, politiske regulativ og teknologisk innovasjon. Jeg anser også disse elementene som sentrale drivere for utviklingen av bankbransjen, og vil dermed presentere driverne for å gi et innblikk i bankenes utfordring.

2.1.1 Driver 1: Endring i kundeadferd

Denne delen er relevant for å kunne forstå digitaliseringens rolle i bankens kundedialog, og hvordan digitale kanaler har endret måten man kommuniserer og samarbeider med kundene på. Bankene er avhengige av å innhente digitale samtykker for å bruke kundedata til å effektivisere kundedialogen på nett, så jeg vil argumentere for at denne driveren er sentral for å kunne forstå oppgavens problemstilling.

"Digitaliseringen i banksektoren har ført til at kundeatferden har endret seg, og åpnet opp for at utradisjonelle aktører kan entre markedet med nye, innovative løsninger. For bankene er det ikke nok å tilby tjenester som er tilfredsstillende for kundene, de må i tillegg være innovative og utvikle nye tjenestetilbud" (Kvistad, 2016, s. iii). EY (2011, s. 6) hevder at digitaliseringen medfører organisatoriske utfordringer, siden kundene kan bruke digitale kanaler til å tilegne seg mer informasjon og øke sin kundemakt. Flere bedrifter kan derfor oppleve å miste

kontrollen over kunderelasjonen, og de digitale flatene har endret måten man må kommunisere og samarbeider med kundene på (EY, 2011, s. 6).

Spesielt bruken av mobile løsninger har vært med på å akselerere endringen i kundeadferden, og tall fra Finans Norge (2018) viser at nordmenn i økende grad bruker mobile enheter for å utføre banktjenester. Undersøkelsen viser at 67 prosent av befolkningen benytter seg av mobilbank, og at de aller fleste er innom mobilbanken enten daglig eller minst ukentlig (Finans Norge, 2018). Om lag 90 prosent av brukerne er også fornøyde med mobilbanken, noe som tyder på at bankene har lyktes med å tilpasse seg endringen i kundeadferden.

Digitalisering fører også med seg analoge konsekvenser for kundeadferden, hvor forbruker. og finanstrender undersøkelsen (Finans Norge, 2018) viser en tydelig nedgang i bankens filialbesøk. Endringen i kundeadferd har dermed utfordret den etablerte forretningsmodellen i bankene, som historisk er preget av kontorlandskaper og møtelokaler. Bankene har derfor tatt grep for å være i stand til å møte kundene i den nye digitale hverdagen, hvor bankene i tur og orden kuttet årsverk og lagt ned kontorer. «The physical world is being replicated in the digital world through digital communities, businesses and assets, fundamentally changing the way consumers engage with businesses and each other» (EY, 2011, s. 6). Rapporten fra EY harmonerer godt med nedleggelsen av bankkontorer, hvor man ser at den fysiske verdenen vi kjenner blir erstattet av et digitalt univers. DNB beskriver sin transformasjon med at de målrettet jobber med å omdanne banken til en teknologibedrift med banklisens (DNB, 2018).

Ciceros bankundersøkelse (2019) påpeker at den norske banksektoren ligger langt fremme i den digitale transformasjonen, hvor man nyter godt av høy teknologisk adopsjon og en sterk digital infrastruktur. Allikevel poengterer man i rapporten at det tross alt er sluttbrukerne som sitter med makten, da de står fritt til å velge sin bankforbindelse. Det er dermed viktig for bankene å tilegne seg en sterk posisjon innenfor det digitale segmentet, der man er i stand til å levere verdiøkende tjenester gjennom bankens digitale flater.

Utfordringen er å gjøre fremtidens kundedialog både digital og personlig, uten at det føles som at man blir overvåket av banken. I den balansegangen blir derfor at kunde- og persondata blir sentralt for å levere verdiøkende tjenester på digitale plattformer. EY (2011) mener også at bankene må skape nye forretningsmodeller, hvor man kommuniserer med kundene på nye måter for å skaffe inntektsstrømmer på finansielle produkter.

Cortet, Rijks og Nijland (2016) viser eksempelvis til en disruptiv endring, hvor de hevder bankene er i ferd med å miste kontrollen over betalingene. Trådløse betalingsløsninger på

mobilen, hvor store globale organisasjoner som Apple og Google sikter seg inn på verdikjeden til bankene. Her i Norge kan man argumentere for at Vipps er et resultat av denne eksterne trusselen, hvor bankene nå samarbeider for å drifte og utvikle tjenesten. Fjørtoft, Presttun og Tvedt (2019) argumenterer for at betalingsfunksjonen er strategisk viktig for bankene, for at de skal klare å holde på dialogen mellom banken og kundene. Med andre ord hevder de at betalingsfunksjonen fungerer som en viktig nøkkel for å bedrive kryss-salg av andre bankprodukter.

Cicero (2019) avdekker at nordmenn bruker veldig liten tid på å organisere sin egen økonomi. I snitt bruker kundene mindre enn en time i uken på å organisere deres egen økonomi. Rapporten argumenterer derfor for at kundene ønsker verktøy og tjenester som vil være med på å effektivisere hverdagen, og gi økt kunnskap om deres økonomiske situasjon. Data og digitalisering vil dermed kunne spille en viktig rolle for å lykkes med å effektivisere hverdagen til kundene, siden digitalisering som nevnt betegnes ved å benytte teknologi til å fornye, forenkle og forbedre produkter og tjenester. Dessuten har den digitale forbrukeren også en forventning om at bankene skal kunne klare å levere verktøy og tjenester som er på høyde med teknologiselskapene når det kommer til brukeropplevelse, tilgjengelighet og sikkerhet (Cicero, 2019).

2.1.2 Driver 2: EU regulativ – GDPR & PSD2

GDPR

General Data Protection Regulation, GDPR, er et lovverk som har til formål å gi forbrukerne økt personvern og eierskap over egne data. GDPR har dermed vært en driver for endring i alle teknologiske virksomheter, siden man trues med betydelige bøter for å ikke etterkomme regelverket.

Den teknologiske utviklingen har ført til at mengden data man produserer som kunde har økt betraktelig. Dette volumet av data har en høy verdi for organisasjonene, ved at man kan kartlegge kundeadferden til forskjellige segmenter, samt bidra til å utvikle nye tjenester. Man ser at denne ressursen står sentralt i store globale organisasjoner som Facebook og Amazon. Den teknologiske utviklingen i disse selskapene gikk raskere enn det gjeldende lovverket. Det utfordret personvernet til brukerne, hvor forbrukerne mistet makten og kontrollen over sine data. For eksempel innrømmet Facebook at de hadde gjort en feil ved å utgi data til Cambridge Analytica i 2018, hvor Cambridge Analytica hadde samlet inn personlig

informasjon fra mange millioner Facebook kontoer uten direkte samtykke. Cambridge Analytica brukte informasjonen til å skape psykologiske profiler av brukerne, som de igjen solgte til politiske aktører for å drive valgkamp.

Selv om eksempelet fra Facebook isolert sett er en enkelthendelse, så man de samme utfordringene i andre digitale forretningsmodeller. Dette avdekte et behov for å regulere metodene man innhentet og behandlet personlige data på, som resulterte i at Europeiske myndigheter presenterte GDPR i 2018.

Payment Service Directive 2

I 2019 ble PSD2 regulativet implementert for alle europeiske banker, og regulativet har til hensikt å fremme konkurranse og innovasjon fra «ikke-bank» aktører (Cortet, Rijks & Nijland, 2016, s. 17). PSD2 direktivet består av *payment information service provider* (PISP) og *account information service provider* (AISP) (Cicero, 2019). Disse elementene vil gi lisensregistrerte tredjeparter tilgang til betalingskontoen til kunden for å initiere en betaling (PISP), samtidig som de får tilhørende kontoinformasjon (AISP). PSD2 vil dermed skjerpe kampen om kundene, hvor bankene mister eneretten på kundedata, samtidig som regulativet reduserer inngangsbarrierene for tredjepartsaktører. Av den grunn betegner Cortet, Rijks og Nijland (2016) PSD2 regulativet som en akselerator for den digitale transformasjonen hos bankene.

En potensiell konsekvens av PSD2 regulativet er ifølge Cortet, Rijks og Nijland (2016) at fintech aktører ikke bare vil sikte seg inn på verdikjeden tilknyttet betalinger, men muligens utfordre bankene på hver enkel del av den tradisjonelle forretningsmodellen til bankene. Cortet, Rijks og Nijland (2016) konkluderer med at PSD2 handler om bankenes strategiske evne til å posisjonere seg i verdikjeden for betaling, og knytte den opp mot bankens tilhørende tjenester.

PSD2 medførte ifølge Cortet, Rijks og Nijland (2016) med seg et strategisk veivalg for bankene. Enten kunne man ønske å fokusere på andre sentrale banktjenester som sparing, utlån eller forsikring, eller posisjonere seg for å bli «bank som en plattform». De anser PSD2 tross alt som en mulighet for bankene til å åpne sine APIer, styrke samarbeidet med nye og etablerte aktører for å skape nye inntektskilder.

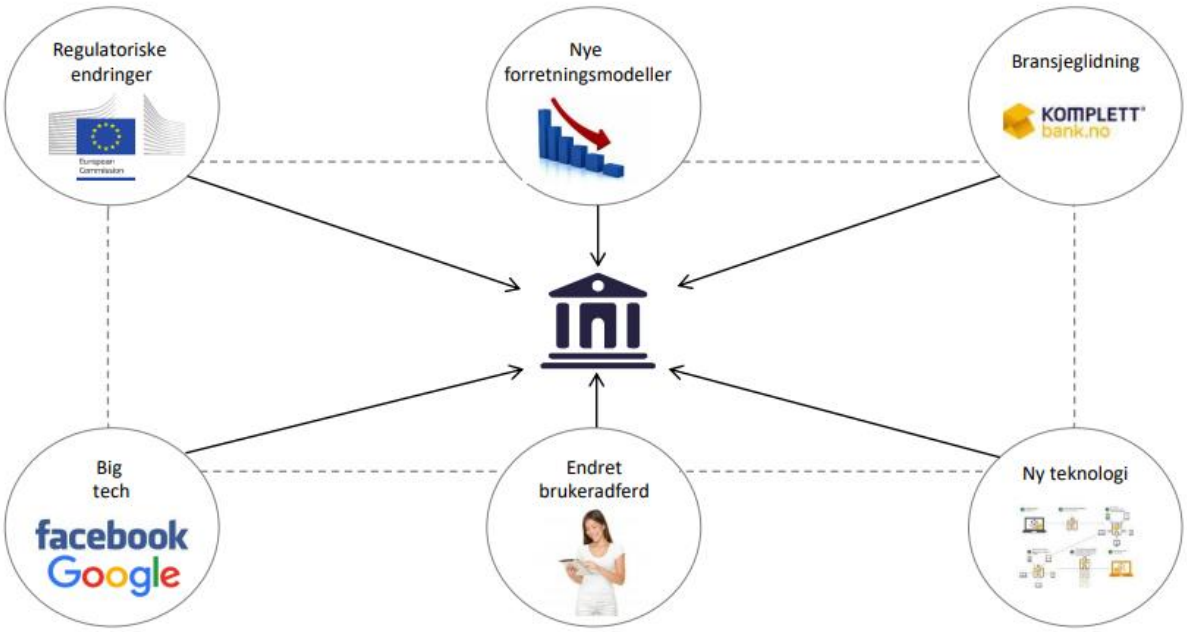
Application programmable interface (API)
Et API er en teknologi som tilbyr et standardisert grensesnitt for kommunikasjon mellom programmer. Teknologien danner grunnlaget for informasjonsdeling mellom et selskaps interne tjenester og tredjepartsaktører. Et selskaps kjerneverdier kan gjenbrukes, deles og inntektsføres via API-er, som kan utvide rekkevidden til eksisterende tjenester eller gi nye inntektsstrømmer. (Fjørtoft, Presttun og Tvedt 2019)

Analysebyrået Cicero produserte i kjølvannet av PSD2 en rapport for den norske bank- og finanssektoren, hvor de konkluderte med at bankene må se forbi PSD2. Rapporten avdekte at regulativet enn så lenge hadde ført til begrenset datautveksling mellom aktørene, hvor man nå kan se kontoinformasjonen på tvers av bankene. Bankene mente på sin side at denne tjenesten satte kundene i fokus, selv om tre av fire nordmenn svarte at de ikke har behov for å holde oversikt over kontoer i andre banker (Cicero, 2019, s. 19).

2.1.3 Driver 3: Teknologisk innovasjon og Open Banking

Open banking beskrives av Fjørtoft, Presttun og Tvedt (2019) som en trend innenfor banksektoren, som er drevet av teknologisk utvikling, endret kundeadferd og regulatoriske vedtak. Essensen i Open banking konseptet er nettopp denne produksjonen og distribusjonen av finansielle produkter i samarbeid med tredjeparter eller andre banker. Christoffer Hernæs, CDO i Sbanken, beskriver Open banking med hvordan man utnytter åpne bankplattformer til å skape verdi i kjølvannet av PSD2 (Finans Norge, 2019). Det medfører at banken får to hovedroller; der de på en side vil jobbe for å integrere tjenester med partnere for å øke verdigrunnlaget for egne kunder og på en annen side være en plattform for andre aktører som kan tilby sine tjenester på toppen av bankens produkter (Finans Norge, 2019)

Fjørtoft, Presttun og Tvedt (2019) hevder mangelen på digital innovasjon i banksektorens egne produkter og tjenester har dermed gitt teknologibedrifter en mulighet til å skape nye inntektskilder. I Norge har banksektoren allerede en spisset konkurranse på egne produkter og tjenester, hvor aktører som Komplett Bank og Bank Norwegian har tatt en posisjon innen kortsiktig finansiering.



Figur 1: Illustrasjon av driverne til Open Banking (Hentet fra Finans Norge, 2019)

På en side gir dette bankene muligheten til å adoptere teknologi og samarbeide med teknologiaktørene, men på en annen side er disse aktørene med på å endre konkurransebildet og skaper en trussel mot bankenes inntektskilder og forretningsmodell. Man kan argumentere for at potensialet til *Open banking* er enormt, hvor bankene kan bruke tredjepartsleverandører til å distribuere sine produkter og skape nettverkseffekter på innovative tjenesteplattformer. Vipps kan for eksempel anses som et resultat av *Open banking* i Norge, hvor man gjennom ny teknologi for betaling, mobile enheter og tett samarbeid med leverandører har klart å skape et sterkt samfunn på mobile enheter.

I sum ser vi en teknologisk trend i retning av Open Banking, hvor bankene samarbeider med hverandre og tredjeparter om produksjon og/eller distribusjon av sine produkter og tjenester for å vinne kampen om kundene. Som Christian Løverås i Vipps uttalte, "It's not about everybody making banks. It's about making banking available outside of the banks." (Løverås, 2018, side 3)

3. Teori og litteraturgjennomgang

3.1 Personvern og personalisering

Dataopplysninger, personalisering og personvern er elementer som er tett tilknyttet hverandre ifølge Zhu et al (2017), og økonomer var tidlig interesserte i disse sammenhengene. Allerede på 1970-tallet presenterte man et tankesett hvor man hevdet at fullstendig informasjon kunne realisere økt økonomisk effektivitet (Salop & Stiglitz, 1977). Denne påstanden ble beskrevet ved at forbrukerne delte utvalgte kunde- og personopplysninger med relevante aktører, slik at man oppnådde tilbud eller fordeler som ble oppfattet som relevante. For eksempel hevdet Salop & Stiglitz (1977) at forbrukerne kunne dele informasjon om feriebudsjettet med reisebyråene, slik at man kunne få tilbud som passet til de opplysningene man hadde gitt ifra seg. På en annen side vil en av aktørene også være i stand til å dra fordel av dette forholdet, noe som gjør at dette tankesettet fortsatt debatteres blant forskere (Zhu et al, 2017).

Personlige opplysninger og kundedata er den dag i dag blitt en av grunnsteinene for digitale bedrifter, hvor man ser at Facebook og Amazon lever av opplysningene de samler inn. Zhu et al (2017) argumenterer for at kundene selv anser kundedata som en vare med økonomisk verdi, noe som har feste i kost-nytte perspektivet til Dinev & Hart (2006). De hevder forbrukere deler personlig informasjon med leverandørene, med en rasjonell forventning om at de vil oppnå en fordel ved å dele denne informasjonen. (Zhu et al, 2017). Sluttbrukerne vurderer dermed et kompromiss mellom de potensielle fordelene og risikoen man oppnår ved å utgi personlige data.

Bellman et al (1999) fant at sikkerhet og personvern var en bekymring for kundene som handlet på internett. Studien viste at 39,1% av respondentene var bekymret for sikkerheten på deres kredittkort informasjon, selv om kun 1,9% av respondentene hadde hatt en dårlig opplevelse ved å handle på nett. Lim & Dubinsky (2004) hevdet at personvern og sikkerhet hadde utviklet seg til en kritisk faktor, hvor det var viktig at organisasjonene utviklet policyer for behandling av sensitive personopplysninger for å sikre at opplysningene ikke ble utnyttet. Av den grunn, mente Lim & Dubinsky (2004) at tillit var en faktor som var vel så viktig for netthandelen som for den fysiske butikken, hvor renomme og image var sentrale egenskaper hos tilbyderen. Hann et al (2007) utviklet forskningen ved å se på hva som motiverer kunder til å dele personlig informasjon, gjennom det som kalles *Expectancy* teorien i en kontekst av motiverte handlinger. Teorien omhandler hvordan individer vurderer en situasjon på internett, og hvordan de vurderer sammenhengen mellom et gitt valg og dets utfall. *Expectancy*

modellen resulterer i en score som beskriver hvor motivert man er til å velge de ulike alternativene, hvor individet vil velge å forfølge alternativet som resulterer i høyest score. Scoren er basert på tre oppfattelser; forventning, instrumentell verdi og valens. *Forventning* beskrives som en sannsynlighetsvurdering der individet vurderer om en gitt innsats vil lede til en gitt prestasjon. *Instrumentell verdi* er den subjektive vurderingen av om den gitte prestasjonen vil lede til en eller flere utfall, og *valens* henviser til verdien individet setter på utfallet. Hann et al (2007) hadde en hypotese som tilsa at kundene ville være villige til å dele personlige opplysninger på nett, om man vurderte at de motiverende fordelene oversteg den potensielle risikoen ved å dele sensitiv informasjon. For å forsøke å løse denne utfordringen (Bellman et al, 1999, Lim & Dubinsky, 2004) mente Hann et al (2007) at organisasjonene hadde forsøkt to forskjellige virkemidler: ved å utvikle policyer for personvern og deres håndtering av personlige opplysninger (1) og ved å tilby økonomiske og ikke-økonomiske fordeler (2).

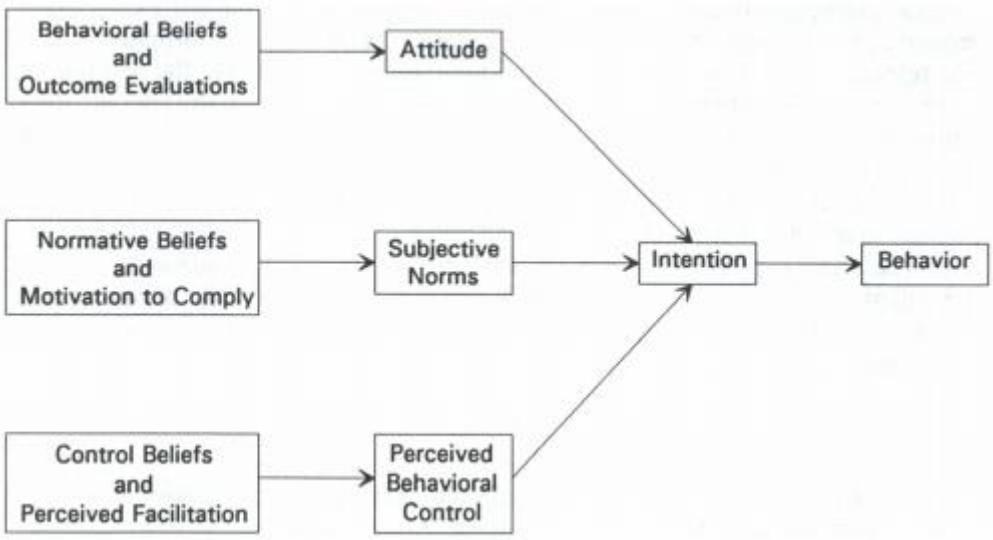
Meinert et al (2006) beskrev tre typer personlig informasjon – kontaktinformasjon, biografisk informasjon og finansiell informasjon. Kontaktinformasjon er typisk ansett som adresse, e-post og telefonnummer, og utgjør opplysninger som gjør det mulig å oppnå direkte kontakt med individet. Biografisk informasjon inkluderer navn, kjønn, sivilstatus, fødselsdato og andre opplysninger som er med på å beskrive livet til et individ. Finansielle data inkluderer data som beskriver alle økonomiske transaksjoner, for eksempel transaksjonsdata, inntektsopplysninger, kredittkortnummer og kredittscore. Studien (Meinert et al 2006) hevder kundene er mer villige til å utgi sin kontaktinformasjon enn sin biografiske informasjon, og igjen mer villig til å dele sin biografiske informasjon enn sin finansielle informasjon.

De siste årene har imidlertid denne forskningen utviklet seg mye, hvor lokasjonsdata (Zhao, Lu & Gupta, 2012) og sensitiv informasjon om familiære bånd via sosiale medier (Chang & Heo, 2014) er sentrale elementer. Denne utviklingen er drevet av den teknologiske utviklingen som har ført til økt bruk av mobile tjenester og sosiale medier, som har resultert i nye dataopplysninger som kan brukes til å beskrive kundeadferden. Studiene (Zhao, Lu & Gupta, 2012) (Chang & Heo, 2014) konkluderer med at man er villig til å dele sensitive opplysninger om hvor man er og hvilke relasjoner man har på internett, for å fremstå som sosial og vellykket foran sine bekjente.

3.2 Privacy-calculus modellen

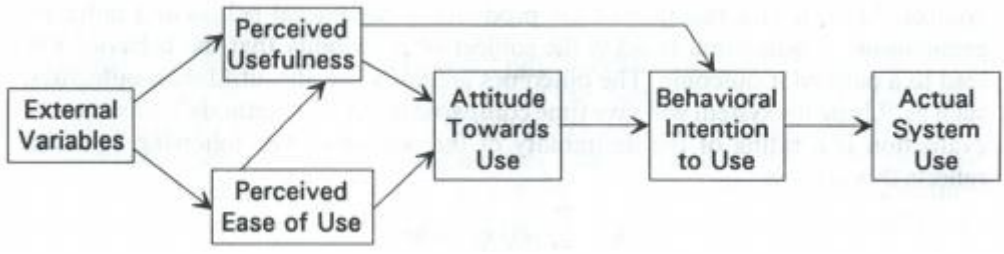
For å studere individers villighet til å dele kunde- og personopplysninger for å oppnå økt personalisering, introduserte Dinev & Hart (2006) privacy calculus modellen. Modellen har til hensikt å måle de forventede fordelene ved økt personalisering opp mot den forventede risikoen man tar ved å dele personlige data.

Dinev & Hart (2006) regnes som hovedpersonene bak forskningen innenfor personalisering og personvern, og de henviser til en rekke gjennomførte studier for å estimere individers adferd i en gitt kontekst. De baserer seg på teorien om begrunnet adferd (TRA) av Ajzen & Fishbein (1980) og senere teorien om planlagt adferd (TPB) av Ajzen (1985). Ifølge teorien om begrunnet adferd (TRA) er selve intensjonen om å utføre en gitt handling den beste indikatoren på om individet faktisk inntar en bestemt adferd. Intensjonen er igjen estimert på bakgrunn av individets egne meninger og subjektive normer og forventninger fra omverdenen. Disse faktorene skaper en motivasjon som er med på å begrunne individets adferd. Modellen ble senere utviklet av Ajzen (1985), hvor man i tillegg vektlegger individets kontrollmønster og dets evne til å kontrollere sin holdning og sin adferd. Det resulterte i teorien om planlagt adferd (TPB), som vektlegger individets evne til å reflektere over interne og eksterne faktorer, og deretter danne seg en mening som enten er med på å fremme eller hemme intensjonen om å innta en bestemt adferd. Jo sterkere evnen til å kontrollere og vurdere egne meninger er, jo sterkere blir intensjonen som igjen styrker sannsynligheten for at man inntar en gitt adferd. Teorien er kjent for å være en av de mest robuste modellene for å anslå menneskelig adferd, selv om de også er kritisert for å ikke inkludere følelsesrelaterte variabler. Det argumenteres derfor med at vår adferd og våre handlinger ikke nødvendigvis bygger på rasjonelle vurderinger, og at individene i større grad bruker sine følelser til å ta beslutninger.



Figur 2: Teorien om planlagt adferd (Hentet fra Ajzen, 1985)

Teorien om planlagt adferd (Ajzen, 1985) anses som forløperen til *The technology acceptance model*, *TAM*. Modellen er spesifikt ment for å forklare individers digitale oppførsel, og måle villigheten til å ta i bruk nye informasjonssystemer (Davis, 1989). I likhet med teorien om planlagt adferd (Ajzen, 1985) så vektlegger modellen holdningene og intensjonen om å utføre en gitt adferd. Forskjellene ligger imidlertid i de bakenforliggende driverne, hvor parameterne *anslått nytte* og *ease of use* er med på å påvirke utfallet. Anslått nytte er den subjektives vurdering av om applikasjonen vil forbedre prestasjonen i en organisatorisk kontekst, og *ease of use* sier noe om hvor brukervennlig og enkel den samme applikasjonen er å ta i bruk. Høye verdier av de to parameterne ville dermed resultere i en sterk intensjon om å akseptere den teknologiske applikasjonen.



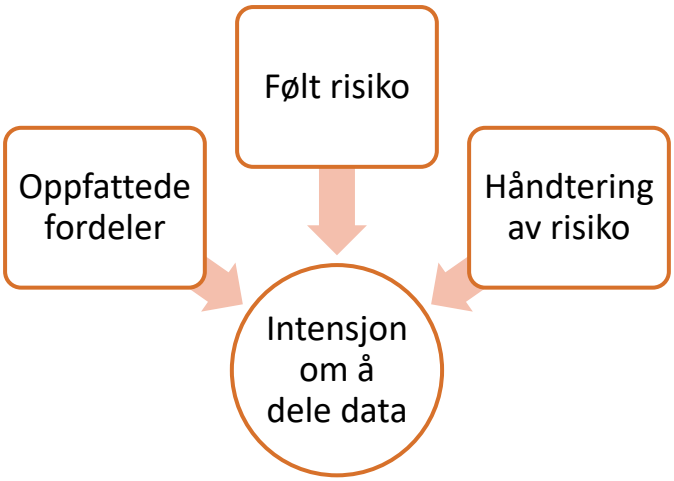
Figur 3: Technology acceptance model (Hentet fra Davis, 1989)

Disse modellene anses som forløperne til *privacy calculus modellen* til Dinev & Hart (2006), hvor man ser at vurderingen av forventet nytte er med på å påvirke villigheten til å endre adferd. På samme måte er antatte fordeler en sentral faktor i privacy calculus modellen, som

er med på å påvirke hvilken adferd man inntar, og dermed villigheten til å dele personlige data. Den opprinnelige privacy calculus modellen opererte med to parametere; *antatte fordeler* og *antatt risiko*. *Antatte fordeler* betegnes som den gevinsten man forventer å oppnå ved å dele data, og fremkommer gjerne i form av økt oppfattet kundeverdi på tjenesten som et resultat av økt personalisering. Mange av dagens digitale tjenester basert på at kunden må dele kundedata, for at man skal få tilgang til tjenesten. Dette ser man for eksempel hos en aktør som Facebook, hvor man får tilgang til den sosiale plattformen ved å opprette en konto med sine personopplysninger. *Antatt risiko* er motvekten til de antatte fordelene, og består av den oppfattede risikoen man utsetter seg for ved å dele personopplysninger. Risikoen er relatert til at man mister kontrollen over personlige data, og dermed øker den følte usikkerheten. Oppfattet risiko er igjen delt inn i to dimensjoner, hvor sannsynligheten for et sikkerhetsbrudd og konsekvensene av sikkerhetsbruddet utgjør det antatte farenivået. Modellen har dermed to dimensjoner, hvor den måler forventet nytte og potensielle negative sider assosiert ved å dele personopplysninger.

Modellen undersøker dermed nøkkelfaktorer innen personalisering og personvern for å kunne anslå individers adferd. Dette gjøres ved å avdekke forholdet i trade-offen mellom de antatte fordelene og den antatte risikoen ved å utgi personlig informasjon. Som nevnt var det opprinnelig Dinev & Hart (2006) som introduserte dette kompromisset mellom kost og nytte ved deling av personopplysninger, hvor de konkluderte med at kunden var villig til å dele personopplysninger om de antatte fordelene overgikk den antatte risikoen.

Senere forskning har utvidet privacy calculus modellen med en tredje dimensjon, hvor man også tar høyde for hvordan man kan håndtere et eventuelt sikkerhetsbrudd på personvernet. Kim & Kim (2018) delte inn privacy calculus modellen inn i tre deler; antatte fordeler, antatt risiko og *håndtering av risiko*. Håndteringsevnen betegnes som evnen man har til å kontrollere risikoen, og redusere skadeomfanget ved et sikkerhetsbrudd. Kim & Kim (2018) utarbeidet modellen for å teste om kundene ønsket å utlevere sine personlige kundeopplysninger for å oppnå relevante anbefalinger innen underholdning og/eller produkter på ulike tjenesteplattformer.



Figur 4: Utvidet privacy calculus modell

3.2.1 Oppfattede fordeler

Perceived benefits i privacy calculus modellen omhandler de positive effektene man anser som oppnåelige ved å dele personlige data. Hann (2007) redegjorde for økonomiske og ikke-økonomiske fordeler, og Kim & Kim (2018) betegner fordeler med noe som er med på å gi sluttbrukeren en nytteverdi. Fra et markedsføringsperspektiv betegnes antatt verdi eller antatte fordeler med kundens vurdering av kvaliteten på produktet eller tjenesten, og om det er i stand til å møte deres behov og forventninger (Chang et al 2009). I tillegg vurderes den antatte fordelen opp mot andre konkurrenter, og representerer en referanse for kunden. Det medfører at alle funksjonaliteter og tilbud som er med på å øke gevinsten for sluttbrukeren representeres som en antatt fordel.

Chellappa and Sin (2005) fant at fordelene knyttet til personalisering av tjenester ble oppfattet som spesielt verdifullt. Studien viste at brukerne i større grad var tilbøyelige til å dele personlige opplysninger om de oppnådde personaliserte fordeler. Siden fordelen skal kunne leveres i en B2B eller B2C relasjon, vil det alltid være forskjellige oppfatninger av hvor verdifull fordelen vil være, og man kan argumentere for at markedsføring, service og tillit kan være vel så viktig som selve produktet eller tjenesten. Markedsføring handler tross alt om å kommunisere verdien av produktet eller tjenesten til kunden, noe som vil være direkte avgjørende for hvor stor verdi kunden oppfatter at produktet eller tjenesten innehar. På samme måte kan man argumentere for at servicen man yter i forbindelse med levere produktet eller tjenesten kan være med på å påvirke den oppfattede verdien. Brukerstøtte og andre supportfunksjoner kan være med på å øke kundens utbytte av å benytte produktet eller

tjenesten, og dermed øke den oppfattede verdien. Dinev & Hart (2006) refererte også til tillit som en sentral faktor i deres studie av kundeadferden på netthandel. De hevdet tillit til organisasjonen sier noe om produktet eller tjenesten blir levert som forventet, og innehar den forventede nytten og verdien. Jeg vil også argumentere for at tillit vil ha en stor betydning i denne oppgavens kontekst, hvor kundene vurderer å dele sensitiv informasjon. Høy tillit til SpareBank 1 SMN vil kunne gi kundene en økt følelse av trygghet til at person- og kundeopplysningene blir ivaretatt på en forsvarlig måte, og potensielt fremstå som en verdi for kundene. Disse underliggende driverne er dermed med på å skape forventninger knyttet til den verdien man ønsker å levere, også er det til syvende og sist opp til organisasjonen for å holde det man lover. Konsekvensen av å miste tilliten av kundene kan være kritiske for organisasjonen, og føre til at organisasjonens produkter og tjenester oppnår en lav oppfattet kvalitet og dermed en lavere verdi. På motsatt side kan man gjennom god markedsføring, god service og gode leveranser skape tillit hos kundene, hvor man leverer det man lover. I ytterste konsekvens kan dette over tid være med på å utvikle en sterk merkevare, som igjen vil kunne øke kundens oppfattede verdi av de produktene og tjenestene man leverer.

Nettopp på grunn av at det handler om kundenes vurdering og oppfattelse av en forespeilet verdi, er det rimelig å anta at resultatene vil ha høy varians. Antakelsen baserer seg på at man som individer har forskjellige behov og forventninger, og dermed har ulike utgangspunkt for å vurdere verdien av produktet eller tjenesten. Uansett hvilken oppfatning man har av verdien man tilbys, teller denne delen av privacy calculus modellen utelukkende positivt for individers villighet til å dele data.

3.2.2 Oppfattet risiko

Risk appraisal i privacy calculus modellen omhandler på sin side de potensielle negative faktorene ved å utgi personlige data. Kim & Kim (2018) deler begrepet inn i sårbarheten av et brudd på personvernet og dets tilhørende alvorlighetsgrad. Disse negative faktorene gjør individer mer tilbakeholden med å dele personlig informasjon, og effekten er sterkere jo mer sårbar og jo mer alvorlig et brudd på personvernet er.

Fra et psykologisk perspektiv knyttes risiko opp mot usikkerhet knyttet til utfall av en situasjon. Ueland et al (2012) argumenterer for at det ikke forekommer noen risiko, om det ikke er for at det finnes usikkerhet. Usikkerhet er derfor tett relatert til begrepet risiko, hvor Strand et al (2009) hevder usikkerhet er en psykologisk faktor som kun eksisterer i de individuelle tankene våre.

Risiko kan derfor defineres som en situasjon eller en hendelse hvor noe av verdi står på spill og hvor utfallet er usikkert (Ueland et al 2012). Definisjonen har to sentrale dimensjoner, hvor risiko defineres av *verdien* som står på spill og *usikkerheten* i situasjonen. Strand et al (2009) beskriver disse dimensjonene ved begrepene *sannsynlighet* og *konsekvens*, som sikter til graden av *usikkerhet* og *den potensielle verdien* man kan miste (eller har mulighet til å oppnå). Individers oppfattelse av risiko vil dermed være subjektiv, hvor sannsynligheten for at skaden inntreffer sammen med de relaterte konsekvensene utgjør vurderingen av risikoen. Ved å koble terminologien om risiko opp mot oppgavens kontekst, betyr det at risikovurderingen består av sannsynligheten for at man opplever svindel eller brudd på personvernet, sammen med hvor omfattende de relaterte konsekvensene vil være.

Risiko beskrives som nevnt som noe menneskelig (Ueland et al, 2012) (Strand et al 2009), hvor mye av forskningen tar utgangspunkt i at mennesker er villig til å ta risiko. Enten det er å krysse et lyskryss på rødt lys, foreta en forbikjøring eller røyke sigaretter, er de alle avgjørelser hvor man utsetter seg for en eller annen risiko hvor en verdi står på spill. Risikoviljen varierer dermed fra person til person, fra de som friklatrer i fjellvegger til de som til enhver tid overholder fartsgrensen. Uavhengig av hvor stor risiko man er villig til å ta, hevder Strand et al (2009) at risiko er koblet til fordeler.

Koblingen mellom påtatt risiko og potensielle fordeler står også sentralt for oppgavens gjeldende kontekst, hvor kompromisset mellom antatte fordeler og antatt risiko er sentrale elementer i privacy calculus teorien. Teorien tar utgangspunkt i at forholdet mellom risiko og gevinst korrelerer med hverandre, men i den virkelige verden det kan være snakk komplekse kompromisser hvor det er umulig å vurdere utfallene. I tillegg kan det såes tvil om hvor nøyaktig man er i vurderingen av kost/nytten, hvor man både kan undervurdere og overvurdere de antatte fordelene og den antatte risikoen. Ueland et al (2012) vektlegger spesielt illusjonen om kontroll som en sentral faktor i situasjoner hvor man vurderer risiko. De hevder større følt kontroll fører til lavere oppfattet risiko, men gjerne fører til at man undervurderer risikoen man står ovenfor. Dette gjelder spesielt på et individuelt nivå, hvor risikoen er relatert til sin egen livsstil. Ueland et al (2012) eksemplifiserer dette med å måle risiko oppfatningen ved å kjøre bil og ved å ta fly, hvor man anser det å fly som mer risikabelt. Selv om det å kjøre bil innebærer mer risiko enn det å fly, er den oppfattede risikoen lavere på grunn av følelsen av økt kontroll over usikkerheten. Jeg vil dermed hevde at kontroll kan være en faktor som er med på å skape en skjevhet mellom risikoen man

utsetter seg for og den fordelen man potensielt oppnår, ved at man undervurderer risikoen i situasjonen.

På grunn av de nevnte utfordringene med å vurdere risiko bruker samfunnet, gjennom individer, organisasjoner og nasjoner, mer tid og ressurser på å vurdere risiko i usikre situasjoner. Ueland et al (2012) henviser til at man i Norsk politikk nå bruker tre ganger mer tid og ressurser på å vurdere risiko enn man gjorde på 60-tallet. På et individuelt nivå, benytter Ueland et al (2012) begrepet frivillig risiko for å forklare hvorfor vi som individer utsetter oss for situasjoner med risiko, og pekte på at mennesker tolererer betydelig mer risiko når de tar en frivillig risiko. I denne oppgavens kontekst er det valgfritt for bankkunden å akseptere samtykkeerklæringene hos SpareBank 1 SMN, noe som gjør at risikoen kan betegnes som en frivillig risiko for kunden. Fenomenet er relatert til illusjonen av kontroll, hvor risikoen reduseres i takt med den personlige kontrollen man føler man har i situasjonen. Dette kan eksemplifiseres med at man har en følelse av at man har mer kontroll om man kjører bilen selv, enn om man sitter på som passasjer.

Beldad et al (2011) betrakter *tillit* som en viktig faktor for oppfattet risiko, og dermed individers adferd på internett. Studien konkluderer med brukernes oppfattelse av risikoen bare kan reduseres om organisasjonene har vunnet tilliten til brukerne. Tilliten kan betegnes som to-dimensjonal, hvor organisasjonens evne og intensjon om å beskytte personopplysningene vil være med på å redusere den oppfattede risikoen. Om leverandøren ikke evner å imøtekomme kravene for tillit, hevder Beldad et al (2011) at kundene enten vil avstå fra å dele personopplysninger eller utgi feilaktige personopplysninger om seg selv.

For å avgjøre om man velger å stole på en leverandør eller ei, hevder Beldad et al (2011) at brukerne evaluerer en rekke faktorer. Personvernserklæringen er en av faktorene som er med på å øke tilliten, selv om det er kjent at de aller fleste ikke bryr seg om å lese den. Bare ved å ha en policy for personopplysningene tilgjengelig, opplever brukeren en økt kontroll, som resulterer i økt tillit til leverandøren. Beldad et al (2011) peker også på merkevaren som en avgjørende faktor som er med på å bestemme tilliten, og dermed intensjonen om å dele personopplysninger. Merkevaren er spesielt viktig i situasjoner hvor brukeren ikke har noen tidligere erfaringer med organisasjonen, hvor merkevaren fungerer som en indikator på organisasjonens troverdighet.

3.2.3 Håndtering av risiko

Håndteringsevne er den siste dimensjonen i modellen, og er opprinnelig en utvidelse av den klassiske privacy calculus modellen som undersøker kompromisset mellom fordelene og ulempene (Kim & Kim, 2018). Denne dimensjonen tar for seg hvor godt man er i stand til å håndtere og redusere skadeomfanget ved et skadetilfelle, noe som kan være med å skape en følelse av mestring og kontroll gjennom å håndtere krisesituasjoner hvor man reduser konsekvensene.

Der hvor de to første elementene i privacy calculus modellen knyttes opp mot motivasjonsteori, knyttes den antatte håndteringsevnen opp mot beskyttelsesmotivasjonsteori. Håndteringsevnen preges derfor i stor grad av frykthåndtering, og defineres som den vurderingen man gjør av sine egne muligheter til å håndtere en fryktet situasjon. (Ruiten, 2003) Faktoren er dermed med på å forklare reaksjonsmønsteret ved et skadetilfelle, med hvordan man kan benytte seg av anbefalte prosedyrer for å redusere farenivået. Reaksjonsmønsteret, som gjenspeiler en endring i adferd, kan av den grunn knyttes opp mot teorien om planlagt adferd (Ajzen, 1985) hvor interne følelser og eksterne faktorer er med på å skape en intensjon om å endre adferd. Styrken på denne intensjonen bestemmes av hvor effektive man vurderer tiltakene å være, hvor trygg man er på å være i stand til å gjennomføre tiltakene og hvor villig man er til å gjennomføre tiltakene for å redusere farenivået (Ruiten, 2003). Håndteringsevnen kan dermed kobles opp mot både personlige karakteristikker og personlige evner, noe som medfører at håndteringsevnen vil kunne variere fra individ til individ. Et individ med høy håndteringsevne kan antageligvis dermed tolerere stress, fare og usikkerhet bedre enn andre individer, samtidig som man har evnene til å gjennomføre tiltak som er med på å redusere farenivået. Som et resultat av prosessen, mener Ruiten (2003) at det skapes en mestringsfølelse hos individet, hvor man er i stand til å ivareta sin sikkerhet. Dette kan sammenlignes med en situasjon hvor man er avhengig av å overleve i naturen, der kunnskaper og ferdigheter kan være med på å legge grunnlaget for at man mestrer situasjonen eller ei. Denne tryggheten betegnes som *danger control* av Ruiten (2003), noe som sikter til hvor godt man er i stand til å håndtere farlige situasjoner. Kim & Kim (2018) bruker begrepet mestringsevne (self-efficacy) til å forklare evnen til å utføre handlinger som er med på å håndtere risikoen. Denne evnen eksemplifiseres ved at man er i stand til å vaske hendene regelmessig for å unngå influensa.

Det er vanskelig å estimere hvor stor betydning håndteringsevnen har for villigheten til å dele sensitive opplysninger, men det er rimelig å anta at denne faktoren veier i favør av å dele sine

kundeopplysninger. På en annen side kan man argumentere for at de individene som har en høy håndteringsevne og kunnskaper om tematikken, også kjenner godt til de ulike risikoelementene ved å dele sensitive data. Det er eventuelt en vinkling som medfører at individer med god oversikt over risikoen vil være ekstra påpasselige med å dele sensitive opplysninger.

3.3 Empiriske studier med privacy calculus modellen

Det som gjør en privacy calculus modell aktuell i denne oppgaven, er den antakelsen om at vi som individer oppfører oss som rasjonelle i det vi vurderer de potensielle fordelene og den potensielle risikoen med å dele data. Den rasjonelle vurderingen bygger på teorien om forventning og nytteverdi, hvor man veier opp den forventete nytteverdien mot den forventete kostnaden.

Privacy calculus modellen er også brukt en rekke ganger innen forskningen som er gjort innen netthandel og innen helsesektoren. Dette er også bransjer hvor forbrukeren utsettes for et kompromiss, hvor man kan oppnå tilgang til ønskede fordeler ved å si ifra seg opplysninger som betalingsinformasjon eller sensitive helseopplysninger.

3.3.1 Kim & Kim (2018)

Kim & Kim (2018) testet privacy calculus modellen for å måle kunders villighet til å dele personlig informasjon med digitale anbefalingssystemer for å oppnå anbefalt videoinnhold. Anbefalingssystemet baserer seg dermed på individets kundeadferd og eventuelle selvvalgte produktpreferanser. De hadde en hypotese om at oppfattet nytte ville ha en positiv effekt på villigheten til å dele data, men studien kunne ikke dokumentere noen signifikant effekt for denne sammenhengen. Følt sårbarhet viste kun en minimal negativ effekt på villigheten til å dele personlig informasjon, men følt alvorlighetsgrad hadde derimot en signifikant negativ effekt på villigheten til å dele data. Kim & Kim (2018) introduserte også en utvidet privacy calculus modell i deres studie, hvor de antok at håndteringsevnen ville ha en positiv effekt på å dele data. Studien viste at håndteringsevnen hadde en signifikant positiv effekt på villigheten til å dele informasjon tilknyttet forbruksmønsteret, personlig identitet, biografisk informasjon og informasjon om forbrukskonteksten (IP adresse, stedsdata etc.), men ikke noen effekt på brukerens intensjon om å dele data om deres egne rangeringer og anmeldelser av produktene i anbefalingssystemet. Mestringsevnen (self-efficacy) hadde derimot en signifikant positiv effekt på parameterne innenfor brukernes feedback informasjon.

Studien til Kim & Kim (2018) var med på å utvikle grunnmodellen gjennom å utdype nøkkelelementene i privacy calculus modellen. Dette gjorde forskerne ved å bryte antatte fordeler, antatt risiko og håndteringsevnen ned til mer spesifikke og detaljerte variabler som var med på å gjenspeile virkeligheten. Studien resulterte i fem typer personlig informasjon som er med på å påvirke villigheten til å dele data, og diskuterer viktigheten av å identifisere og håndtere de ulike typene personlig informasjon forskjellig fra hverandre.

3.3.2 Kim et al 2019

Kim et al 2019 testet privacy calculus modellen i en Internet of Things (IoT) kontekst, hvor IoT teknologi har tilrettelagt for en rekke personaliserte tjenester. Studien bruker IoT tjenester innenfor helse, smart hjem og smart transport til å studere individers villighet til å dele personlig informasjon. IoT markedet har ifølge studiet opplevd en voldsom vekst de siste årene, noe som gjør det relevant å studere privacy calculus modellen i denne konteksten. Noe av det mest interessante med denne studien er tilknyttet helseopplysningene, hvor sensitiviteten på opplysningene hadde en signifikant negativ effekt på villigheten til å dele data. Dette var på tross av at gevinstene ved å dele flere helseopplysninger ville øke for forbrukerne av IoT tjenesten. En variabel som måling av hjerterytme samt transport av data i sanntid ville hjulpet helsepersonell med å håndtere kroniske sykdommer på en mye bedre måte. Selv om forbrukeren er innforstått med at man oppnår en lavere verdi av tjenesten, opplevde man at risikoen med å dele helseopplysninger var for stor.

For IoT tjenester tilknyttet smart hjem og smart transport, indikerte resultatene at forbrukerne ikke viet stor oppmerksomhet til den antatte risikoen ved å dele personlige data, så lenge man fikk tilgang til en mer personalisert tjeneste. For å drifte IoT tjenester, er leverandørene helt avhengige av å tiltrekke seg kunder og samle inn deres personopplysninger. Resultatene fra studien konkluderer med at antatt verdi spiller en nøkkelrolle for kundens villighet til å dele personopplysninger. Det betyr at IoT tjenesteleverandører bør fokusere på å utvikle verdien de leverer til forbrukerne, ved for eksempel å danne eksterne strategiske nettverk for å videreutvikle tjenesten.

Det som i størst grad skiller denne studien fra tidligere privacy calculus studier, er det faktum at forholder mellom antatt risiko og villighet til å dele data ikke er statistisk signifikant. Det betyr med andre ord at forbrukerne uavhengig av verdier for antatt risiko og forventet verdi ønsket å realisere potensialet for personalisering ved å dele personlig informasjon til IoT tjenester. På motsatt side hadde høye verdier av forventet verdi på IoT tjenester tilknyttet

helsetjenester ingen signifikant positiv effekt på villigheten til å dele helseopplysninger, med bakgrunn i den høye sensitiviteten til helseopplysningene.

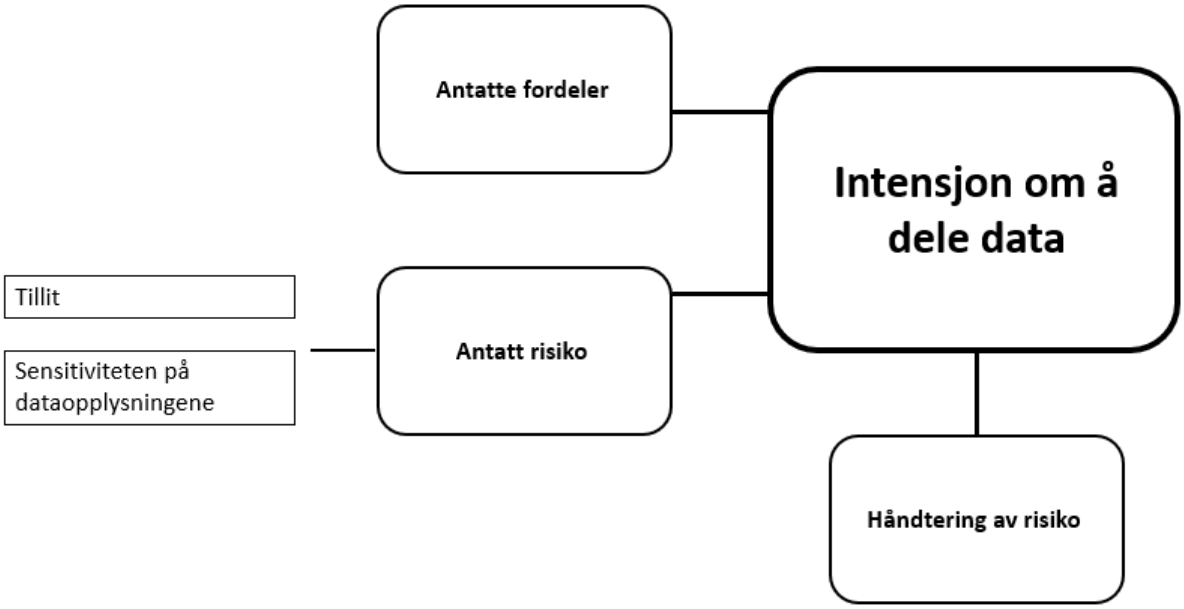
3.4 Svakheter med privacy calculus modellen

En svakhet ved modellen angår antakelsen om at individene tar et rasjonelt valg når de vurderer de potensielle fordelene og den potensielle risikoen, som i flere tilfeller har vist seg å være feil (Rogers, 1983). Rogers (1983) henviser i stedet til en rekke psykologiske faktorer som er med på å påvirke våre valg, for eksempel våre følelser, dagshumør, og tankesett. Denne forskningen indikerer at våre handlinger ikke nødvendigvis kan modelleres gjennom forenklede modeller basert på rasjonelle handlinger, da sammenhengene gjerne er mer komplekse enn hva privacy calculus modellen fremstiller. Xu et al (2011) påpekte at personlige karakteristikker hadde en vesentlig betydning for om man var villig til å dele personlige data, og pekte spesielt individets nysgjerrighet til å adoptere ny teknologi og nye tjenester. Deres resultater (Xu et al, 2011) vektlegger dermed det faktum at vi mennesker er forskjellige, og dermed vurderer gitte situasjoner ulikt.

3.5 Forskningsmodell

Privacy calculus modellen legger som nevnt grunnlaget for forskningsmodellen jeg skal benytte i denne oppgaven, hvor jeg vektlegger intensjonen om å dele data. Min antakelse er at individer vil være villige til å dele data, om de antatte fordelene overstiger den antatte risikoen ved å dele data. I tillegg vil den oppfattede risikoen reduseres, om man har en oppfattelse av at det finnes effektive mottiltak man kan iverksette ved et sikkerhetsbrudd. Denne antakelsen bygger på teorien om at individer opererer med en rasjonell adferd, og dermed har vurdert situasjonen før man tar en beslutning. I en virkelig verden vil dermed faktorer som personlighetstrekk, interesse, følelser, humør og tid være faktorer som kan være med på å bestemme adferden.

For min forskningsmodell, har jeg valgt å inndele fordelene i økonomiske og ikke-økonomiske fordeler, slik at modellen kan undersøke hvilke fordeler som har mest nytteverdi for kundene i bankbransjen. Jeg har valgt denne inndelingen, da jeg ønsker å se i hvilken grad kundene verdsetter nye innovative tjenester opp mot en direkteavkastning i form av økonomiske fordeler.



Figur 5: Forskningsmodell for studien

H1: Tillit til banken er negativt relatert til opplevd risiko ved å dele personopplysninger

H2: Sensitiviteten på dataopplysningene har en positiv påvirkning på antatt risiko

H3: Antatte fordeler har en positiv påvirkning på intensjonen om å dele data

H4: Antatt risiko har en negativ påvirkning på intensjonen om å dele data

H5: Håndtering av risiko har en positiv påvirkning på intensjonen om å dele data

4. Metode

I dette kapittelet presenteres forskningsdesignet og metoder som ligger til grunn for å innhente data, analysere data og besvare problemstillingen til studien.

Valg av vitenskapelig teori og design er ifølge Busch (2013) tett tilknyttet valg av problemstilling, metode for innsamling av data, samt analyse av data. Den vitenskapelige teorien er et fagområde som vektlegger en metodisk og kritisk fremgangsmåte med fullverdig bevisføring for de påstandene som fremsettes. Det er også essensielt at resultatene skal kunne bekreftes av andre forskere ved å gjennomføre den samme undersøkelsen med den samme metoden. Ved å forholde seg til de vitenskapelige retningslinjene, har forskningen til hensikt å være holdbar og gyldig.

4.1 Undersøkelsesdesign

Forskningsdesign er betegnelsen på den strategien man benytter for å løse en valgt problemstilling. Ved valg av design tas det utgangspunkt i hvor kompleks problemstillingen er og hvilke ressurser man har tilgjengelig (Busch, 2013). Designet deles inn i henholdsvis ekstensive og intensive design: Ekstensive design går i bredden og innhenter data fra mange respondenter og intensive design går i dybden og innhenter dyptgående innsikt fra et fåtall av respondenter. Ekstensive, eller beskrivende design har til hensikt å beskrive ulike trekk ved de utvalgte enhetene, fremfor å forklare hvorfor de ulike trekkene ved enhetene oppstår. Med tanke på problemstillingen til denne studien, vil jeg argumentere for at det passer best å benytte et ekstensivt design. Det kan begrunnes med at problemstillingen heller fokuserer på å karakterisere en større populasjon, fremfor å studere spesifikke prosesser eller adferden til utvalgte mennesker. Problemstillingen inneholder relativt få variabler og har ikke til hensikt å avdekke dype årsakssammenhenger mellom enhetene i utvalget. Jeg vil derfor argumentere for at studien står ovenfor en relativt enkel problemstilling, som ikke fremstår som veldig kompleks.

I denne oppgaven har jeg valgt problemstilling, hvor jeg ønsker å teste den etablerte teorien. Med andre ord vil jeg sammenligne min empiri med etablert teori, og se om studien kan være med på å utvikle teorilitteraturen i en eller flere retninger. Ved å gå fra teori til empiri, medfører det at jeg velger en deduktiv tilnærming. Det betyr at denne oppgaven vil trekke konklusjonene på bakgrunn av om empirien fra datainnsamlingen stemmer overens med teorigrunnlaget eller ei. På motsatt side vil en induktiv tilnærming ta utgangspunkt i empirien for å utforme ny teori.

Valg av forskningsdesign innebærer også valg av hvilken teknikk jeg ønsker å benytte for oppgavens gjennomføring. Siden studien har til hensikt å se nærmere på hva som påvirker individers ønske om å dele personlige data, er jeg interessert i å undersøke deres oppfatninger og holdninger i et gitt fenomen. Derfor har jeg valgt å benytte tverrsnittstudie til denne oppgaven, siden en tverrsnittstudie har til hensikt å beskrive et fenomen på et gitt tidspunkt. Jeg mener en tverrsnittstudie passer godt til problemstillingen, på grunn av at jeg ønsker å studere et fenomen på et gitt tidspunkt. Forskningsteknikken har til hensikt å vise forskjeller mellom respondentene i et gitt utvalg, noe jeg anser som en passende tilnærming til å svare på min problemstilling. En kvantitativ metode vil være med på å frembringe breddekunnskap i form av målbare resultater, som igjen muliggjør statistiske beregninger (Dalland, 2012). På grunn av at oppgavens problemstilling er rettet mot en større populasjon av unge bankkunder, ble det vurdert som mest gunstig å gjennomføre en spørreundersøkelse. Den kvantitative teknikken ble valg fremfor en kvalitativ tilnærming siden den er mer effektiv med hensyn på å innhente og prosessere større datamengder.

4.2 Spørreskjema

4.2.1 Utforming

For utforming av spørreundersøkelsen benyttet jeg tjenesten *Nettskjema* fra UiO, som er tilgjengelig for studenter på NTNU. Dette er et veldig enkelt og brukervennlig skjema, hvor man kan får lagret datasettet i et format som er lett overførbart til anerkjente programvarer for analyse av data. Tilgjengeligheten, samt en anbefaling fra masterveilederen gjorde det dermed naturlig å bruke denne tjenesten for utforming av spørreundersøkelsen. En annen fordel med å benytte meg av *Nettskjema* er funksjonaliteten til å publisere resultatene i ulike format, og overføre datamaterialet til andre programvarer. Dette er spesielt nyttig i en slik oppgave, hvor det er naturlig å utføre avanserte statistiske operasjoner på datamaterialet.

For å kontekstualisere studien, så jeg meg nødt til å benytte forhåndsutfylte spørsmål med avgrensede svaralternativer. I motsetning til mer åpne spørsmål og fritekstsvar, vil lukkede spørsmål med avgrensede svaralternativer gi mindre rom for egen tolkning av spørsmålet. Dette valget ble gjort for å sikre at jeg får svar på det studien ønsker å undersøke, ved å ha tydelige definerte spørsmål med tilhørende svaralternativer. Jeg håper denne utformingen av spørsmålene i studien vil resultere i gode interne reliabilitetsverdier.

De ulike svaralternativene er basert på Likert skalaen, hvor jeg har inndelt skalaen i fem deler. Likert skalaen er en teknikk for å måle holdningene hos respondenten (Likert, 1932), hvor

man benytter seg av rangerte svaralternativer for å avdekke respondentens ståsted. Svaralternativene jeg har valgt går fra «helt uenig», «litt uenig», «verken eller», «litt enig» til «helt enig», og jeg mener dette gir en balansert og forenklet beskrivelse av oppfatningen til respondenten. Spørsmålene har til hensikt å avdekke respondentenes vurdering av et gitt scenario eller en gitt faktor, hvor det kan være utfordrende for respondentene å anslå sitt nøyaktige ståsted. Dermed valgte jeg å benytte en Likert skala med fem svaralternativer for denne spørreundersøkelsen, over en mer detaljert skala hvor det kan være mer utfordrende å avgjøre sitt ståsted. Det er viktig å påpeke at distansen mellom de ulike svaralternativene ikke nødvendigvis er de samme, siden Likert skalaen benytter seg av rangerte alternativer. Fordelen med å bruke en Likert skala er at jeg får tilgang til enkle kvantitative data som kan bli analysert med statistiske operasjoner. Svaralternativene representerer dermed ord for tall, som gjør det mulig å analysere datamaterialet i etterkant av spørreundersøkelsen.

4.3 Operasjonalisering

Operasjonalisering dreier seg om hvordan man presiserer og beskriver begreper og teorier som brukes i forskningen (Clausen & Johansen, 2012). Hensikten med operasjonaliseringen er å gjøre konteksten mulig å forske på, samtidig som teorien og begrepene blir etterprøvbare å forske på.

En tverrsnittstudie bygger på en spørreundersøkelse, hvor man henter inn et kvantifiserbare data fra respondentene. Spørreundersøkelsen er utformet på bakgrunn av forskningsmodellen, og spørsmålene er utformet for å få innsikt i de ulike elementene i forskningsmodellen. De er dermed satt inn i en kontekst som passer bankbransjen og dens tjenester. Det betyr at spørsmålene tilknyttet antatte fordeler er koblet opp mot ulike fordeler som bankbransjen har mulighet til å realisere, samt at sensitiviteten på kunde- og personopplysningene måles på de samme kunde- og personopplysningene som SpareBank 1 SMN innhenter i dag.

For å operasjonalisere nøkkelbegrepene i privacy calculus modellen, har jeg benyttet studiene til Kim et al (2019), Kim & Kim (2018) og Infinedo (2012).

4.3.1 Antatte fordeler

Antatte fordeler ble av Kim et al (2019) definert som økning av prestasjonsnivået, effektiviteten, nytteverdien og ved å få tilgang på relevant informasjon. Skalaen ga en Cronbach's alfa på 0.96, som overstiger dermed den anbefalte verdien på 0.7. Kim et al (2019) har eksempelvis operasjonalisert begrepet ved påstandene: «Using this IoT service

would improve my performance» og «Using this IoT service helps me get useful information».

De påstandene som er inkludert i antatte fordeler er:

Tabell 1: Påstander for antatte fordeler

Påstander
Gi meg nyttig informasjon
Bidra til at jeg får bedre avkastning på sparepengene mine
Gi meg gode tilbud som passer min situasjon
Bidra til at jeg får bedre økonomisk oversikt
Bidra til å hjelpe meg å nå mine sparemål
Bidra til å sikte at jeg har en optimal produktsammensetning
Bidra til å styrke brukervennligheten i bankens digitale løsninger
Være med på å utvikle nye kundeorienterte bankprodukter

4.3.2 Risiko

På grunn av gode relabilitetsnivåer for begrepet antatt risiko, har jeg valgt å benytte den samme studien til å operasjonalisere begrepet. Kim et al (2019) oppnådde en Cronbach's alfa på 0.94 for antatt risiko. Denne scoren oppnådde studien ved å spørre om de personlige opplysningene kunne bli utgitt til tredjepartsaktører, bli misbrukt, bli delt med andre uten din kjennskap eller bli hacket. Begrepet er eksempelvis formulert ved: "What do you believe is the risk due to the possibility that personal information tracked by this IoT service could be misused?"

De påstandene som er inkludert i oppfattet risiko er:

Tabell 2: Påstander for oppfattet risiko

Påstander
Bli misbrukt hos SpareBank 1 SMN
Bli utgitt til tredjepartsaktører
Være dårlig sikret og havne på avveie
Bli brukt til svindel
Bankbransjens ivaretakelse av mine personopplysninger
SpareBank 1 SMNs ivaretakelse av mine personopplysninger

Tillit og sensitiviteten på dataopplysningene

Teorien argumenterer for at risikoelementet består av to underliggende faktorer; tillit og sensitivitet på dataopplysningene. Studien til Kim & Kim (2018) oppnådde en Chronbachs alfa på 0,88 for personopplysningene, og Kim et al (2019) oppnådde en Chronbachs alfa på 0,87 for tillit til aktøren.

Personopplysningene i studien til Kim & Kim (2018) er relatert til personlige anbefalinger av videoinnhold på nett. Av den grunn er personopplysningene i denne studien kontekstualisert, hvor dataopplysningene inngår i samtykkeerklæringene til SpareBank 1 SMN.

Påstandene for tillit i studien til Kim et al (2019) er målt i en kontekst for IoT tjenester. Deres mål er eksempelvis formulert som: «Organizations that provide this IoT service handle personal information in a competent fashion»

Påstandene som er inkludert i de underliggende faktorene for oppfattet risiko er:

Tabell 3: Påstander for "Tillit" og Sensitiviteten på dataopplysningene"

Påstander
Sensitiviteten på dataopplysningene
Navn
Adresse
E-post
Telefonnummer
Kunde- og produktavtaler
Transaksjonshistorikk
Kredittkorthistorikk
Inntektsopplysninger
Kundeadferd på digitale plattformer
Tillit
At det er trygt å oppbevare sparepengene mine i banken
Tillit til banksektoren i Norge
Tillit til SpareBank 1 SMN
Brukes til å dra fordel av min kundeadferd
Brukes imot meg ved fremtidige søknader i banken

4.3.2 Håndteringsevne

Begrepet håndteringsevne er som nevnt en utvidelse av den tradisjonelle privacy calculus modellen, og begrepene er dermed ikke operasjonalisert i like stor grad. Håndteringsevnen er sammensatt av effektiviteten til de tiltakene som finnes for å håndtere risikoen, kombinert

med mestringsevnen individet har til å gjennomføre tiltakene. Studien til Ifinedo (2012) operasjonaliserte begrepet mestringsevne med å spørre om individets evne til å utføre preventive og reaktive tiltak for å dempe trusselen for et sikkerhetsbrudd. Effektiviteten til de reaktive tiltakene operasjonaliseres ved å måle om de potensielle tiltakene er tilgjengelige, gjennomførbare og effektive, og dermed resulterer i å redusere alvorlighetsgraden av sikkerhetsbruddet (Ifinedo, 2012). Studien brukte måleverktøyet Composite reliabilitet for å måle konsistensen, og returnerte verdier på 0.84 for mestringsevne og 0.90 for respons effektivitet. Dette representerer verdier som er godt over 0.70, som indikerer høy intern reliabilitet.

Ifinedo (2012) har eksempelvis brukt formuleringen "I have the necessary skills to protect myself from information security violations" for å måle *mestringsevnen,* og formuleringen "The effectiveness of available measures to protect my organization's information from security violations are: 1) Inadequate to 7) Effective" for å måle *effektiviteten på tiltakene.*

Påstandene som er inkludert i håndteringsevne er:

Tabell 4: Påstander for Håndteringsevne

Påstander
Jeg er i stand til å oppdage et brudd på personvernet
Jeg er i stand til å utføre tiltak som er med på å redusere skadeomfanget ved et brudd på personvernet
Jeg er i stand til å utføre preventive tiltak som er med på å redusere risikoen for et brudd på personvernet
Potensielle mottiltak for å håndtere risikoen er tilgjengelige
Potensielle mottiltak for å håndtere risikoen er gjennomførbare
Potensielle mottiltak for å håndtere risikoen er effektive

4.4 Datainnsamling

For å innhente empiri til denne studien, var intensjonen å benytte SpareBank 1 SMN kunderegister for å gi et mest mulig representativt utvalg. Jeg fikk dessverre ikke tilgang til denne kundebasen, og SpareBank 1 SMN ønsket ei heller å være med på å administrere denne undersøkelsen. Det resulterte i at jeg ble nødt til å innhente empirien på egenhånd, noe som var svært utfordrende. Den største utfordringen var knyttet til å innhente et tilstrekkelig antall respondenter til undersøkelsen, hvor det etter hvert ble vanskelig å innhente nye svar.

Problemstillingen for denne oppgaven omhandler som nevnt de oppfatningene unge voksne har til å dele data med banken sin. Denne avgrensningen er med på å legge føringer for hvilket utvalg spørreundersøkelsen skal distribueres til, for å gi et best mulig bilde av

populasjonen. Avgrensningen er et resultat av oppgavens tilgjengelige ressurser, hvor jeg som student både er presset på økonomiske ressurser og tid. Det fører til at jeg valgte å avgrense oppgaven til den populasjonen jeg har størst mulighet til å distribuere spørreundersøkelsen til, da det vil inkludere mitt nettverk av studenter og venner.

Etter at spørreundersøkelsen ble utformet, ble den distribuert gjennom mitt private nettverk, et nettverk som hovedsakelig består av personer innenfor alderssegmentet jeg ønsker å studere. Spørreundersøkelsen ble delt fra den 4. Mai 2020 via e-post, Facebook, Twitter og LinkedIn, hvor mine venner, studiekamerater, kollegaer og andre kjente fikk muligheten til å delta. På en annen side er distribusjonen i digitale kanaler noe som gjør det vanskeligere å holde kontroll på utvalget, men på en annen side kan man dra nytte av nettverkseffekter og oppnå et stort antall respondenter. For å eksemplifisere kontrollelementet, så kan jeg ikke vite om lenken er delt videre til forum som ikke passer med den populasjonen jeg ønsker å studere, eller kontrollere om enkelte respondenter har svart flere ganger. Hallgeir Kvadsheim fra Luksusfellen delte for eksempel undersøkelsen videre på Twitter, som gjør at den spres til et nettverk jeg ikke kunne kontrollere. På en annen side kan en slik deling av undersøkelsen også bidra til å innhente flere respondenter, og dermed være med på å løse hovedutfordringen jeg hadde i datainnsamlingen. I tillegg kan jeg argumentere for at mitt private nettverk kan gi et skjevt bilde av populasjonen til SpareBank 1 SMN, siden utvalget ikke nødvendigvis representerer hele mangfoldet av bankens kunder.

Jeg har også distribuert undersøkelsen til noen organisasjoner, hvor mine kontaktpersoner i TietoEvry og Netcompany har fått tilsendt spørreundersøkelsen på e-post. Dette var avgjørelser jeg tok mot slutten av datainnsamlingen, hvor jeg så at jeg hadde behov for å hente inn flere respondenter.

Tabell 5 viser kjennetegn på utvalget:

Tabell 5: Frekvenstabell for bakgrunnsvariablene

Variabel	Alternativ	Frekvens	Prosent
Kjønn	Mann	89	67,4 %
	Kvinne	43	32,6 %
Alder	18 – 34 år	120	90,9 %
	35 – 50 år	10	7,6 %
	51 – 66 år	2	1,5 %
Antall bankforbindelser	0 – 1	24	18,2 %
	2 – 3	90	68,2 %
	4 – 5	15	11,4 %
	Flere enn 5	3	2,3 %
Antall bankprodukter	2 – 3	18	13,6 %
	4 – 5	37	28 %
	Flere enn 5	77	58,3 %

Tabellen viser at over 90% av utvalget representerer målgruppen for studiet, med en overvekt av menn. Nesten ni av ti har mindre enn tre bankforbindelser, men samtidig minst fire forskjellige bankprodukter. Det kan tyde på at den gjennomsnittlige kunden har flere produkter hos den samme banken, og gjerne en tydelig hovedbankforbindelse.

4.5 Begrepsvalidering

4.5.1 Faktoranalyse av begrepene som inngår i modellen

For å teste for konvergent validitet i målene, er det benyttet faktoranalyse. Faktoranalyse er en analysemetode som kan anvendes innen psykologien, så vel som i andre samfunnsvitenskapelige studier. Analysen har til hensikt å forklare hvor stor del av variansen som er forklart ved de ulike faktorene i det latente begrepet. En konfirmerende faktoranalyse innebærer at man har en anelse om antall faktorer på forhånd, hvor man søker etter å etterprøve dette empirisk. Målet med en slik analyse er vanligvis å undersøke om antall faktorer bestemt på forhånd er tilstrekkelige for å reprodusere korrelasjonsmatrisen i

tilfredsstillende grad og/eller kontrollere at de målte variablene som man antar henger sammen, faktisk gjør det (Ulleberg & Nordvik, 2000).

I analysen er det benyttet principal component analyse og oblimin rotasjon. Antall faktorer er basert på kriteriet om Eigenvalue større enn 1. Pallant (2013) mener at den nedre grensen for en akseptabel faktorladning er på .40, mens faktorladninger på .60 anses å være en sterk faktorladning. Dette er gitt at det eksisterer lave ladninger på de øvrige faktorene i matrisen. På bakgrunn av disse grenseverdiene, vil jeg fjerne alle faktorladningene som er under .30 i faktoranalysene, slik at tabellene blir lettere å lese.

I tillegg benyttes Chronbachs alfa som en indikator på intern konsistens i målene. Chronbachs alfa er et kjent statistisk mål for å måle den interne konsistensen til en empirisk studie av et latent begrep (Clausen & Johansen, 2012). Verdien forteller oss hvor tett variablene er knyttet sammen, og Chronbachs alfa = 0,7 regnes som en nedre verdi for hva som betegnes som tilfredsstillende intern konsistens.

Indirekte fordeler

Basert på Eigenvalue verdiene, ga faktoranalysen en en-faktorløsning som forklarer 66% av variansen. Variabelen baserer seg på åtte påstander knyttet til ulike verdier bankene ønsker å levere til kundene sine (Se 4.3.1), hvor faktorladningene lå innenfor intervallet [.686 til .829]. Spørsmålet som er brukt til å måle denne latente variabelen er «Hva oppnår du av å akseptere samtykkeerklæringene hos SpareBank 1 SMN?». Chronbachs alfa verdien for de åtte påstandene er målt til .926, som viser en veldig høy konsistens på datamaterialet.

Tabell 6: Chronbachs alfa for "Indirekte fordeler"

	Chronbachs alfa	Cronbachs alfa if Item Deleted
Indirekte fordeler	.926	
Gi meg nyttig informasjon		.914
Bidra til at jeg får bedre avkastning på sparepengene mine		.917
Gi meg gode tilbud som passer min situasjon		.913
Bidra til at jeg får bedre økonomisk oversikt		.913
Bidra til å hjelpe meg å nå mine sparemål		.917
Bidra til å sikte at jeg har en optimal produktsammensetning		.911
Bidra til å styrke brukervennligheten i bankens digitale løsninger		.924
Være med på å utvikle nye kundeorienterte bankprodukter		.922

Oppfattet risiko

Basert på Eigenverdiene, fordeles det latente begrepet følt risiko i tre komponenter som til sammen forklarer 70% av variansen i empirien.

Tabell 7: Faktoranalyse av følt risiko

Følt risiko			
	Component	Component	Component
Påstander	1	2	3
Bli misbrukt hos SpareBank 1 SMN	.620		
Bli utgitt til tredjepartsaktører	.788		
Være dårlig sikret og havne på avveie	.673		
Bli brukt til svindel	.850		
Bankens ivaretakelse av mine personopplysninger	-0,658		
SpareBank 1 SMNs ivaretakelse av mine personopplysninger	-0,657		
At det er trygt å oppbevare sparepengene mine i banken		.898	
Tillit til banksektoren i Norge		.873	
Tillit til SpareBank 1 SMN		.743	
Brukes til å dra fordel av min kundeadferd			.857
Brukes imot meg ved fremtidige søknader i banken			.855

Misbruk av kunde- og personopplysninger

Det samlede målet «Misbruk av kunde- og personopplysninger» inkluderer seks påstander tilknyttet *Oppfattet risiko*. De negative faktorladningene betyr at høye tillitsverdier til bankenes ivaretakelse av personopplysningene gir en lave verdier av de påstandene med

positive faktorladninger, og vice versa. Disse påstandene oppnår en samlet Chronbachs alfa på .864, som er høye verdier av konsistens

Tabell 8: Chronbachs alfa av "Misbruk av kunde- og personopplysninger"

	Chronbachs alfa	Cronbachs alfa if Item Deleted
Misbruk av kunde- og personopplysninger	.864	
Bli misbrukt hos SpareBank 1 SMN		.836
Bli utgitt til tredjepartsaktører		.834
Være dårlig sikret og havne på avveie		.824
Bli brukt til svindel		.850
Bankens ivaretakelse av mine personopplysninger		.848
SpareBank 1 SMNs ivaretakelse av mine personopplysninger		.836

Tillit til bankbransjen

Variabelen «Tillit til bankbransjen» er målt ved påstandene: 1) «Det er trygt å oppbevare sparepengene mine i banken», 2) «Jeg har stor tillit til bankbransjen i Norge» og 3) «Jeg har stor tillit til SpareBank 1 SMN». Målet gir en Chronbachs alfa = .831, som er tilfredsstillende verdier av konsistens.

Tabell 9: Chronbachs alfa for "Tillit til bankbransjen"

	Chronbachs alfa	Cronbachs alfa if Item Deleted
Tillit til bankbransjen	.831	
At det er trygt å oppbevare sparepengene mine i banken		.769
Tillit til banksektoren i Norge		.733
Tillit til SpareBank 1 SMN		.797

Opportunistisk adferd fra banken

Variabelen «Opportunistisk adferd fra banken» er målt ved påstandene: 1) «Brukes til å dra fordel av min kundeadferd» og 2) «Brukes imot meg ved fremtidige søknader i banken». Disse observerte verdiene var i utgangspunktet tiltenkt å beskrive *tilliten* respondentene hadde til at bankene brukte kunde- og personopplysningene på en forsvarlig måte, men faktoranalysen indikerer at påstandene utgjør en egen variabel. På grunn av at den latente variabelen kun inneholder to observerte variabler, presenteres kun Chronbachs alfa for den sammensatte variabelen. Chronbachs alfa er .728, og tilfredsstiller kravet for konsistens.

Tabell 10: Chronbachs alfa av "Opportunistisk adferd fra banken"

	Chronbachs alfa
Opportunistisk adferd fra banken	.728
Brukes til å dra fordel av min kundeadferd	
Brukes imot meg ved fremtidige søknader i banken	

Håndteringsevne

For den latente variabelen «Håndteringsevne», er det to Eigenverdier som overstiger grenseverdien på 1. De to komponentene defineres som 1) «Mestringsevne» og 2) «Effektiviteten på tiltak», og forklarer til sammen 69,8 prosent av variansen i datamaterialet.

Tabell 11: Faktoranalyse av variabelen "Håndteringsevne"

Håndteringsevne		
	Component	Component
Påstander	1	2
1) Jeg er i stand til å oppdage et brudd på personvernet	.868	
2) Jeg er i stand til å utføre tiltak som er med på å redusere skadeomfanget ved et brudd på personvernet	.906	
3) Jeg er i stand til å utføre preventive tiltak som er med på å redusere risikoen for et brudd på personvernet	.724	
4) Potensielle mottiltak for å håndtere risikoen er tilgjengelige		.678
5) Potensielle mottiltak for å håndtere risikoen er gjennomførbare		.845
6) Potensielle mottiltak for å håndtere risikoen er effektive		.744

Mestringsevne

Variabelen «Mestringsevne» er målt ved påstandene: 1) «Jeg er i stand til å oppdage et brudd på personvernet», 2) «Jeg er i stand til å utføre tiltak som er med på å redusere skadeomfanget ved et brudd på personvernet» og 3) «Jeg er i stand til å utføre preventive tiltak som er med på å redusere risikoen for brudd på personvernet». Den utvalgte variabelen gir en Chronbachs alfa på =.815, som er tilfredsstillende verdier av konsistens.

Tabell 12: Chronbachs alfa av "Mestringsevne"

	Chronbachs alfa	Cronbachs alfa if Item Deleted
Mestringsevne	.815	
1) Jeg er i stand til å oppdage et brudd på personvernet		.753
2) Jeg er i stand til å utføre tiltak som er med på å redusere skadeomfanget ved et brudd på personvernet		.650
3) Jeg er i stand til å utføre preventive tiltak som er med på å redusere risikoen for et brudd på personvernet		.816

Effektiviteten på tiltak

Det samlede målet «Effektiviteten på tiltak» er målt ved påstandene: 1) «Potensielle mottiltak for å håndtere risikoen er tilgjengelige», 2) «Potensielle mottiltak for å håndtere risikoen er gjennomførbare» og 3) «Potensielle mottiltak for å håndtere risikoen er effektive». Variabelen gir en Chronbachs alfa på = .646, og er dermed rett under grenseverdien på 0.7. Chronbachs alfa verdien ville vært på .770 om jeg hadde utelukket den tredje påstanden som går på effektiviteten til mottiltakene, men jeg velger å beholde påstanden siden jeg anser dem for relevante ut fra de teoretiske perspektivene som ligger til grunn for denne studien.

Tabell 13: Chronbachs alfa av "Effektiviteten på tiltak"

	Chronbachs alfa	Cronbachs alfa if Item Deleted
Effektiviteten på tiltak	.646	
Potensielle mottiltak for å håndtere risikoen er tilgjengelige		.545
Potensielle mottiltak for å håndtere risikoen er gjennomførbare		.298
Potensielle mottiltak for å håndtere risikoen er effektive		.770

Sensitiviteten til dataopplysningene

Faktoranalysen til «Sensitiviteten til dataopplysningene» resulterte i to Eigenverdier over 1, hvor variablene defineres som 1) «Kontaktopplysninger» og 2) «Sensitive kunde- og personopplysninger». Til sammen forklarer disse variablene 64,6 prosent av variansen i den latente variabelen.

Tabell 14: Faktoranalyse av "Sensitiviteten til dataopplysningene"

Sensitiviteten på dataopplysningene		
	Component	Component
Påstander	1	2
Navn	.788	
Adresse	.914	
E-post	.795	
Telefonnummer	.832	
Kunde- og produktavtaler		.706
Transaksjonshistorikk		.824
Kredittkorthistorikk		.899
Inntektsopplysninger		.674
Kundeadferd på digitale plattformer		.681

Kontaktopplysninger

Variabelen «Kontaktopplysninger» er sammensatt av verdiene på sensitiviteten til påstandene: 1) «Navn», 2) «Adresse», 3) «E-postadresse» og 4) «Telefonnummer». Disse har sterke faktorladninger på minst .788, og en Chronbachs alfa på =.855.

Tabell 15: Chronbachs alfa for "Kontaktopplysninger"

	Chronbachs alfa	Cronbachs alfa if Item Deleted
Kontaktopplysninger	.855	
Navn		.846
Adresse		.776
E-postadresse		.839
Telefonnummer		.798

Sensitive kunde- og personopplysninger

Variabelen «Sensitive kunde- og personopplysninger» er målt ved å måle sensitiviteten til påstandene: 1) «Kunde- og produktavtaler», 2) «Transaksjonshistorikk», 3) «Kredittkorthistorikk», 4) «Inntekstopplysninger» og 5) «Kundeadferd på digitale plattformer». Den siste påstanden er sammensatt av lokasjonsdata, trafikkdata og kommunikasjonsdata med banken, og er med på å beskrive den digitale kundeadferden. Variabelen har en Chronbachs alfa på .816, som gir tilfredsstillende grad av konsistens.

Tabell 16: Chronbachs alfa for "Sensitive kunde- og personopplysninger"

	Chronbachs alfa	Cronbachs alfa if Item Deleted
Sensitive kunde- og personopplysninger	.816	
Kunde- og produktavtaler		.786
Transaksjonshistorikk		.751
Kredittkorthistorikk		.746
Inntektsopplysninger		.795
Kundeadferd på digitale plattformer		.818

5. Resultater og analyse

I de kommende avsnittene vil jeg presentere resultatene fra analysene kjørt i SPSS. På grunn av at utvalget mitt er relativt lite, må en del av resultatene leses med forsiktighet.

Jeg har valgt å ha med relativt mange tabeller for å presentere resultatene, da jeg mener dette gjør resultatene mer leservennlige. De utvalgte uavhengige variablene vil presenteres trinnvis, hvor jeg vil presentere deskriptiv statistikk, før de vil inkluderes i en regresjonsanalyse hvor jeg kobler på den avhengige variabelen.

5.1 Deskriptiv statistikk

I avsnittene 5.1.1 – 5.1.9 vil jeg presentere og kommentere fordelingen av data på de utvalgte variablene. Jeg vil benytte de statistiske målene gjennomsnitt og standardavvik for de ulike variablene, og på den måten gi en kort presentasjon av nøkkeltallene i studien.

5.1.1 Deskriptiv statistikk for variabelen «Indirekte fordeler»

De indirekte fordelene gir en gjennomsnittlig score på 3,44 med et tilhørende standardavvik på 1,24. Spesielt faktorene knyttet til innovasjon og brukervennlighet resulterer i høye verdier, mens faktorene knyttet til sparing resulterer i en lavere verdi.

Tabell 17: Deskriptiv statistikk for "Indirekte fordeler"

Indirekte fordeler			
	Gjennomsnitt	*Standardavvik*	*N*
Gi meg nyttig informasjon	3,38	1,26	132
Bidra til at jeg får bedre avkastning på sparepengene mine	3,00	1,22	132
Gi meg gode tilbud som passer min situasjon	3,74	1,22	132
Bidra til at jeg får bedre økonomisk oversikt	3,31	1,27	132
Bidra til å hjelpe meg med å nå mine sparemål	2,97	1,31	132
Bidra til å sikre at jeg har en optimal produktsammensetning	3,49	1,27	132
Bidra til å styrke brukervennligheten i bankens digitale løsninger	3,89	1,16	132
Være med på å utvikle nye kundeorienterte bankprodukter	3,74	1,17	132
Sum	**3,44**	**1,24**	

5.1.3 Deskriptiv statistikk for variabelen «Misbruk av kunde- og personopplysninger»

Faren for at kunde- og personopplysningene skal bli misbrukt gir et gjennomsnitt på 2,58 med et tilhørende standardavvik på 1,16. Resultatene indikerer at man er rimelig fortrolig med bankenes ivaretakelse av kunde- og personopplysningene, men at man allikevel er redd for at opplysningene skal havne på avveie. Spesielt frykten for at opplysningene blir tilgjengelige for tredjepartsaktører virker å være avgjørende for variabelen *misbruk av kunde- og personopplysninger*.

Tabell 18: Deskriptiv statistikk for "Misbruk av kunde- og personopplysninger"

Misbruk av kunde- og personopplysninger			
	Gjennomsnitt	*Standardavvik*	*N*
Bli misbrukt hos SpareBank 1 SMN	2,71	1,23	132
Bli utgitt til tredjepartsaktører	3,15	1,45	132
Være dårlig sikret og havne på avveie	3,02	1,27	132
Bli brukt til svindel	2,36	1,15	132
Bankenes ivaretakelse av mine personopplysninger	2,16	0,95	132
SpareBank 1 SMNs ivaretakelse av mine personopplysninger	2,07	0,90	132
Sum	**2,58**	**1,16**	

5.1.4 Deskriptiv statistikk for variabelen «Tillit til bankbransjen»

Den latente variabelen «Tillit til bankbransjen» måler 4,42 i gjennomsnitt og 0,87 i standardavvik. Gjennomsnittsverdien reflekterer svært høye tillitsverdier til bankbransjen, og spesielt på forholdet som gjelder oppbevaring og sikring av finansielle midler.

SpareBank 1 SMN scores veldig jevnt mot bankbransjen, noe som kan anses som litt overraskende. Jeg ville antatt at SpareBank 1 SMN hadde større tillit blant kundene, enn aktører som Bank Norwegian og Komplett Bank.

Tabell 19: Deskriptiv statistikk for "Tillit til bankbransjen"

Tillit til bankbransjen			
	Gjennomsnitt	*Standardavvik*	*N*
At det er trygt å oppbevare sparepengene mine i banken	4,61	0,81	132
Tillit til banksektoren i Norge	4,35	0,84	132
Tillit til SpareBank 1 SMN	4,31	0,95	132
Sum	**4,42**	**0,87**	

5.1.5 Deskriptiv statistikk for variabelen «Opportunistisk adferd fra banken»

Variabelen «Opportunistisk adferd fra banken» består av to observerte variabler. Disse gir en gjennomsnittlig verdi på 3,32 med et tilhørende standardavvik på 1,31. Den *opportunistiske adferden* viser at kundene er redd for at banken utnytter dataopplysningene for å skape størst mulig gevinst for sin egen organisasjon. Dette kan for eksempel eksemplifiseres med at man kan få en dårligere pris på bankens produkter, basert på analyser av kundeadferden.

Tabell 20: Deskriptiv statistikk for "Opportunistisk adferd fra banken"

Opportunistisk adferd fra banken			
	Gjennomsnitt	*Standardavvik*	*N*
Brukes til å dra fordel av min kundeadferd	3,63	1,29	132
Brukes imot meg ved fremtidige søknader i banken	3,01	1,33	132
Sum	**3,32**	**1,31**	

5.1.6 Deskriptiv statistikk for variabelen «Mestringsevne»

Den latente variabelen «Mestringsevne» gir en snittscore på 3,28 med et tilhørende standardavvik på 1,12. Resultatene indikerer at man i større grad mestrer å utføre preventive tiltak, enn reaktive tiltak for å redusere risikoen.

Tabell 21: Deskriptiv statistikk for "Mestringsevne"

Mestringsevne			
	Gjennomsnitt	*Standardavvik*	*N*
Oppdage et brudd på personvernet	2,99	1,1	132
Utføre tiltak som er med på å begrense skadeomfanget ved et brudd på personvernet	3,3	1,18	132
Utføre preventive tiltak for å redusere risikoen for brudd på personvernet	3,56	1,07	132
Sum	**3,28**	**1,12**	

5.1.7 Deskriptiv statistikk for variabelen «Effektiviteten på tiltak»

Variabelen «Effektiviteten av tiltak» gir en gjennomsnittsverdi på 3,85 med et standardavvik på 0,95. Det er interessant å bemerke seg at tiltakene anses som svært tilgjengelige og gjennomførbare, at tiltakene ikke nødvendigvis er like effektive.

Tabell 22: Deskriptiv statistikk for "Effektiviteten på tiltak"

Effektiviteten på tiltak			
	Gjennomsnitt	*Standardavvik*	*N*
Tiltakene er tilgjengelige	4,08	0,91	132
Tiltakene er gjennomførbare	4,03	0,88	132
Tiltakene er effektive	3,45	1,05	132
Sum	**3,85**	**0,95**	

5.1.8 Deskriptiv statistikk for variabelen «Kontaktopplysninger»

Variabelen «Kontaktopplysninger» gir et gjennomsnitt på 2,80 med et tilhørende standardavvik på 1,05. Verdiene indikerer at kontaktopplysningene er middels sensitive, hvor telefonnummeret skiller seg noe ut som noe mer sensitivt.

Tabell 23: Deskriptiv statistikk for "Kontaktopplysninger"

Kontaktopplysninger			
	Gjennomsnitt	*Standardavvik*	*N*
Navn	2,66	1,14	132
Adresse	2,8	1,01	132
E-postadresse	2,6	0,98	132
Telefonnummer	3,14	1,07	132
Sum	**2,80**	**1,05**	

5.1.9 Deskriptiv statistikk for variabelen «Sensitive kunde- og personopplysninger»

Den latente variabelen «Sensitive kunde- og personopplysninger» gir en gjennomsnittlig verdi på 4,27 og et standardavvik på 0,89. Sammenlignet med de «Kontaktopplysninger», ser man at dataopplysningene tilknyttet «Sensitive kunde- og personopplysninger» oppnådde en vesentlig høyere score. *Kredittkorthistorikk* betegnes som den mest sensitive dataopplysningen, og betegner gjerne de kjøpene som er gjort på internett.

Tabell 24: Deskriptiv statistikk for "Sensitive kunde- og personopplysninger"

Sensitive kunde- og personopplysninger			
	Gjennomsnitt	*Standardavvik*	*N*
Kunde- og produktavtaler	3,78	0,95	132
Transaksjonshistorikk	4,42	0,85	132
Kredittkorthistorikk	4,55	0,8	132
Inntektsopplysninger	4,29	0,91	132
Kundeadferd på digitale plattformer	4,30	0,94	132
Sum	**4,27**	**0,89**	

5.2 Deskriptiv statistikk for «Samtykke 1» og «Samtykke 2»

Denne studien operer med to avhengige variabler, «Samtykke 1» og «Samtykke 2». De to variablene har informasjon om respondentene ville valgt å akseptere samtykkeerklæringene eller ei.

Tabell 25: Deskriptiv statistikk for "Samtykke 1 & Samtykke 2"

Samtykke 1 & 2			
	Gjennomsnitt	*Standardavvik*	*N*
Samtykke 1	2,97	1,31	132
Samtykke 2	2,88	1,36	132

Tabell 26: Frekvenstabell for Samtykke 1

Samtykke 1				
		Frekvens	*Prosent*	*Akk. Prosent*
Ville du akseptert samtykke 1	*1) Nei, helt sikkert ikke*	16	12,1	12,1
	2) Nei, trolig ikke	49	37,1	49,2
	3) Vet ikke	8	6,1	55,3
	4) Ja, trolig	41	31,1	86,4
	5) Ja, helt sikkert	18	13,6	100
	Totalt	132	100	

Tabell 27: Frekvenstabell for Samtykke 2

Samtykke 2				
		Frekvens	*Prosent*	*Akk. Prosent*
Ville du akseptert samtykke 2	*1) Nei, helt sikkert ikke*	20	15,2	15,2
	2) Nei, trolig ikke	49	37,1	52,3
	3) Vet ikke	5	3,8	56,1
	4) Ja, trolig	43	32,6	88,7
	5) Ja, helt sikkert	15	11,4	100
	Totalt	132	100	

Resultatene viser at respondentene i større grad var villige til å akseptere «Samtykke 1», som oppnådde et gjennomsnitt på 2,97. Gjennomsnittsverdien til «Samtykke 2» var på 2,88, noe som viser en marginal forskjell på de to variablene.

5.3 Regresjonsanalyse

5.3.1 Regresjonsanalyse for «Oppfattet risiko»

Den ytterste sammenhengen i forskningsmodellen handler om å måle tillit til bankbransjen og sensitiviteten på dataopplysningene som to underliggende faktorer for oppfattet risiko. Gjennom en lineær regresjonsmodell har vil jeg presentere funnene som er med på å dekke H1 og H2.

Modellen resulterer i et signifikansnivå på .000, som betyr at det forekommer en sammenheng mellom faktorene. Den latente variabelen «Misbruk av kunde- og personopplysninger» er avhengig variabel i modellen, hvor «Tillit til bankbransjen», «Opportunistisk adferd fra banken», «Kontaktopplysninger» og «Sensitive kunde- og personopplysninger» er uavhengige variabler. R^2 verdien er på .414 som betyr at modellen forklarer i overkant av 40% av variansen.

Tabell 28: Resultater fra regresjonsanalysen for "Oppfattet risiko"

Oppfattet risiko				
	B	***Standardavvik***	***p-verdi***	***t***
Tillit til bankbransjen	*-0,374*	*0,085*	*0*	*-4,385*
Opportunistisk adferd fra banken	*0,325*	*0,055*	*0*	*5,851*
Kontaktopplysninger	*0,061*	*0,074*	*0,41*	*0,827*
Sensitive kunde- og produktopplysninger	*0,289*	*0,097*	*0,004*	*2,973*
Konstant	*1,751*	*0,561*	*0,002*	*3,119*

Av de inkluderte variablene, er det verdt å poengtere at det kun er «Kontaktopplysninger» som ikke er statistisk signifikante. De øvrige variablene er svakt til moderat korrelert med verdiene for «Oppfattet risiko». «Tillit til bankbransjen» er negativt korrelert med «Oppfattet risiko», noe som betyr at høye verdier av *tillit* er med på å redusere verdier av oppfattet risiko. Variablene «Opportunistisk adferd av banken» og «Sensitive kunde- og personopplysninger» er svakt positivt korrelert med verdiene for oppfattet risiko. Det medfører at større verdier av de uavhengige variablene er med på å øke verdien for oppfattet risiko. Resultatene er dermed med på å bekrefte H1 og H2, hvor tillit og sensitiviteten til dataopplysningene er med på å påvirke den oppfattede risikoen.

5.3.1 Forberedelser til regresjonsanalysen for Samtykke 1 & 2

Siden jeg anser variablene «Samtykke 1» og «Samtykke 2» som dikotomiske variabler, vil jeg omformulere verdiene i en dummy variabel med klar todeling. Denne tilpasningen gjøres for å kvitte meg med verdiene for 3: «Vet ikke», da de respondentene som har svart «Vet ikke» ikke vil besvare studiens problemstilling. Det er også en relativt liten andel som har svart 3: «Vet ikke», henholdsvis 6,1 prosent for «Samtykke 1» og 3,8 prosent for «Samtykke 2».

Fordelingen på de dikotomiske variablene er dermed som følger:

Tabell 29: Frekvenstabell for "Samtykke 1"

Samtykke 1			
	Ja	*Nei*	*Sum*
Frekvens	59	65	124
Prosent	47,58 %	52,42 %	100

Tabell 30: Frekvenstabell for "Samtykke 2"

Samtykke 2			
	Ja	*Nei*	*Sum*
Frekvens	58	69	127
Prosent	45,67 %	54,33 %	100

5.3.2 Resultater fra regresjonsanalysen for «Samtykke 1»

Samtykkeerklæring 1 handler om å dele kontaktopplysninger med SpareBank 1 SMN, og dermed akseptere digital markedsføring fra banken.

Den binær logistiske regresjonsmodellen for Samtykke 1 består av variablene: 1) «Indirekte fordeler», 2) «Misbruk av kunde- og personopplysninger», 3) «Mestringsevne» og 4) «Effektiviteten på tiltak». Disse variablene representerer henholdsvis *Oppfattede fordeler, Oppfattet risiko* og *Håndteringsevnen* fra forskningsmodellen, og vil dermed være sentral for å undersøke H3, H4 og H5.

Tabell 31: Resultater fra regresjonsanalysen for "Samtykke 1"

Samtykke 1				
	B	***Standardavvik***	***p-verdi***	***Oddsratio***
Indirekte fordeler	*0,771*	*0,261*	*0,003*	*2,162*
Misbruk av kunde- og personopplysninger	*-0,387*	*0,248*	*0,118*	*0,679*
Mestringsevne	*-0,476*	*0,261*	*0,068*	*0,621*
Effektiviteten på tiltak	*0,254*	*0,299*	*0,396*	*1,289*
Konstant	*-1,217*	*1,661*	*0,464*	*0,296*

De indirekte fordelene utpeker seg som det mest sentrale funnet i regresjonsanalysen, hvor høye verdier av oppfattede fordeler gir en større sannsynlighet for at man aksepterer Samtykke 1. Mestringsevnen er den andre latente variabelen som er svakt signifikant for Samtykke 1, hvor en høy mestringsevne vil redusere sjansene for at man aksepterer Samtykke 1.

Modellens treffsikkerhet

Gjennom en Omnibus test oppnår regresjonsmodellen et signifikansnivå på 99% med 21.9 i *Chi-kvadrat* verdi. Det betyr at regresjonsmodellen er bedre skikket til å prediktere utfallene, og er dermed med på å riktigere fremstilling av resultatene. Modellen er i stand til å prediktere utfallet korrekt 65,3 % av tilfellene, som gjenspeiler en middels treffsikkerhet. Treffsikkerheten er henholdsvis fordelt 63,1 % for «Nei» og 67,8 % for «Ja» til Samtykke 1.

5.3.2 Resultater fra regresjonsanalysen for «Samtykke 2»

Samtykkeerklæring 2 handler om å dele sensitive kunde- og personinformasjon, som kan sammenstilles, behandles og analyseres på tvers av organisasjonene i SpareBank 1 alliansen.

Regresjonsmodellen inkluderer dermed variablene: 1) «Indirekte fordeler», 2) «Misbruk av kunde- og personopplysninger», 3) «Mestringsevne» og 4) «Effektiviteten på tiltak», som representerer de latente variablene *Oppfattede fordeler, Oppfattet risiko* og *Håndteringsevne* fra forskningsmodellen.

Tabell 32: Resultater fra regresjonsanalysen for "Samtykke 2"

Samtykke 2				
	B	***Standardavvik***	***p-verdi***	***Oddsratio***
Indirekte fordeler	*1,88*	*0,396*	*0*	*6,552*
Misbruk av kunde- og personopplysninger	*-0,864*	*0,317*	*0,006*	*0,422*
Mestringsevne	*-0,761*	*0,35*	*0,03*	*0,467*
Effektiviteten på tiltak	*0,87*	*0,401*	*0,03*	*2,387*
Konstant	*-5,566*	*2,178*	*0,011*	*0,004*

Modellens treffsikkerhet

Med en *Chi-kvadrat* på 68,3 og tilhørende signifikansnivå på 99 % forbedrer regresjonsmodellen resultatene i svært stor grad. Dette gjenspeiles også i den målte treffsikkerheten på 81,9%. Den fordeler seg henholdsvis på 81,2% for «Nei» og 82,8% for «Ja» til Samtykke 2.

5.4 Utvalgte bakgrunnsvariabler i studien

5.4.1 Bakgrunnsvariabelen «Deler du data med banken din i dag»

På grunn av privacy calculus modellens manglende evne til å forklare adferden ved ubevisst eller urasjonell oppførsel, har jeg implementert et kontrollspørsmål i datainnsamlingen. Uavhengig av om respondenten svarer «Ja/Nei» på om man deler data med banken i dag, kommer det et oppfølgingsspørsmål som spør om man gjorde et bevisst valg eller ei. Svarer respondenten «Vet ikke», antar jeg at vedkommende ikke har foretatt seg et bevisst valg.

Jeg har valgt å presentere denne bakgrunnsvariabelen i studiet, da variabelen kan gi et bilde av hvordan respondentene har tatt stilling til problemstillingen i sin hverdag. Til forskjell fra å svare i en hypotetisk og forskningsbasert setting, kan denne variabelen være med på å avdekke respondentenes naturlige oppførsel. Selv om spørreskjemaet var anonymt, er det vel kjent at respondentene kan innta en annen adferd når man er klar over at man blir studert.

Tabell 33: Frekvenstabell for "Deler du data med banken din i dag?"

Samtykke1 & Samtykke 2				
		Frekvens	*Prosent*	*Akk. Prosent*
Deler du data med banken din i dag	*1) Nei*	29	22,0	22
	2) Vet ikke	42	31,8	53,8
	3) Ja	61	46,2	100
	Totalt	132	100	

Tabell 34: Frekvenstabell for om respondentene gjorde bevisste valg

Samtykke1 & Samtykke 2				
		Frekvens	*Prosent*	*Akk. Prosent*
Gjorde du i den forbindelse et bevisst valg	*1) Nei*	18	20,0	20
	2) Ja	72	80,0	100
	Totalt	90	100	

Resultatene fra denne bakgrunnsvariabelen viser at totalt 60 av 132 respondenter ikke hadde foretatt seg et bevisst valg. Dette er et interessant funn, siden privacy calculus modellen legger rasjonelle handlinger til grunn for å estimere adferden. Resultatene indikerer derimot at en stor andel av respondentene ikke vet hvilket valg de foretok seg, eller at valget var ubevisst.

6. Diskusjon

Problemstillingen for studien min er: *«Hvilke faktorer kan forklare kundens villighet til å dele personlige data med banken?»*

I det kommende avsnittet vil jeg diskutere hypotesene jeg utarbeidet i forskningsmodellen til å svare på problemstillingen. Hypotesene vil testes opp mot de resultatene som fremkommer av analysene hvor jeg vil benytte signifikansnivåer på 90% og 95% til grunn for å drøfte resultatene. Funnene vil lede frem til studiens konklusjoner, som baserer seg på om hypotesene kan beholdes eller ei.

6.1 H1: Tillit til bankbransjen er negativt relatert til oppfattet risiko

Kim et al (2019) hevdet tillit til leverandøren, og deres ivaretakelse av personopplysningene hadde en betydning for villigheten til å dele data. Resultatene fra denne studien kan dermed antyde at organisasjonens tillit er en viktig faktor for at man skal være villig til å ta risiko i form av å dele data. Korrelasjonen mellom faktorene innehar moderat styrke, med et signifikansnivå på over 95%.

Jeg har tidligere i oppgavens påpekt at bankene består av organisasjoner som jevnt over nyter høy tillit blant kundene sine. Selv om driverne av den digitale transformasjonen (Cortet, Rijks og Nijland, 2016) har vært med på å utvikle banksektoren, viser undersøkelser at bankene fortsatt nyter stor tillit fra kundene. Det er vanskelig å si noe om hvordan denne faktoren vil utvikle seg i fremtiden, der mindre aktører som Komplett Bank og globale aktører som Amazon og Facebook forsøker å slå seg inn i bankbransjen. Jeg vil også anta at denne faktoren vil kunne variere i stor grad, på bakgrunn av nasjonale reguleringer og økonomi. For å eksemplifisere dette, kan man se til finanskrisen i 2008, hvor greske bankkunder ikke fikk lov til å ta ut pengene de hadde stående i banken. Jeg vil derfor anta at det kan ha satt sine spor, og at greske bankkunder har mindre tillit til greske banker, enn hva norske kunder har til norske banker.

Det kan imidlertid diskuteres om den tradisjonelle økonomiske sikkerheten er representativ for tilliten man har til at bankene ivaretar personopplysningene på en fortrolig måte. Flytting, plassering og oppbevaring av penger er ikke det samme som å oppbevare, behandle og analysere dataopplysninger. I kjølvannet av digitaliseringen hevder Lim & Dubinsky (2004) at tillit var vel så viktig for digitale organisasjoner som for fysiske organisasjoner, noe som

argumenterer for at faktoren vil være sentral i den digitale transformasjonen av bankene. Bankenes håndtering av kunde- og personopplysningene kan dermed bli like viktig som deres evne til å ta vare på de økonomiske ressursene.

Studien til Kim et al (2019) resulterte også i liknende verdier for tillit, hvor tillit hadde en signifikant effekt på oppfattet risiko ved bruk av IoT tjenester. Betaverdien i studien tilsvarte -0,21 med et signifikansnivå på 95%, og støttet opp under hypotesen om at tillit til leverandøren er med på å redusere den oppfattede risikoen. Sammenlignet med studien til Kim et al (2019), så er betaverdien høyere for denne undersøkelsen. Det kan muligens forklares av at sensitiviteten på kunde- og personopplysningene i en finansiell kontekst er høyere enn sensitiviteten på personopplysningene man deler gjennom IoT tjenester (Meinert et al 2006).

I denne studien viste faktoranalysen at opportunistisk adferd fra banken er en del av tillitsbegrepet, som fokuserte på bankens bruk av kunde- og personopplysningene. Resultatene viser at faktoren er signifikant, hvor betaverdien hadde et positivt fortegn med lavt til moderat styrkenivå (*0.325 og 95% signifikansnivå*). Dette funnet betyr at høyere målinger på opportunistisk adferd fra banken resulterer i høyere opplevd risiko. Ved å snu på fremstillingen, vil høy tillit føre til lavere målinger av opportunistisk adferd, og resultere i lavere verdier av oppfattet risiko.

Opportunistisk adferd fra banken ble også nevnt av Dinev & Hart (2006) som en faktor som kunne resultere i at kunden mistet kontrollen over sine personopplysninger, og at opplysningene kommer på avveie. Det kan i ytterste konsekvens føre til tap for kunden. Hann et al (2007) argumenterte for at kundene forventet fordeler ved å dele data. Kundene kan derfor miste tilliten til banken, om man opplever at banken bruker personopplysningene til å skape størst mulig gevinst for sin egen organisasjon. Jeg vil heller argumentere for at tilliten bygger på relasjonen mellom kunde og organisasjon, hvor formålet bør være å realisere fordeler for begge partene. Om fordelene mellom partene blir skjevt fordelt, kan det resultere i at kundene stiller spørsmål ved hvilke hensikter banken har for personopplysningene. Mangelen av følt kontroll over personopplysningene kan dermed føre til at den opplevde risikoen øker, som en konsekvens av at tilliten er svekket.

Beldad et al (2011) argumenterte for at organisasjonens evner og hensikt til å håndtere personopplysningene var sentrale elementer for å oppnå tillit hos kundene. Siden bankene i Norge opplever høy tillit blant kundene sine, kan det virke som at forutsetningene for å

innhente personopplysninger er gode. Dette underbygges ved at bankene i Norge er underlagt strenge regulatoriske krav, som er med på å fremme fokuset på sikkerhet i banken. Det er imidlertid viktig å vise frem banken som en teknologibedrift med banklisens, som evner å fornye seg samtidig som man ivaretar den organisatoriske rollen som en trygg aktør.

Tillit er også en ekstern variabel som er viktig om man skal lykkes med ny teknologi. Davis (1989) introduserte sin *technology acceptance model*, basert på eksterne variabler, oppfattet nytteverdi og brukervennlighet. Jeg vil derfor hevde at de aktørene som evner å håndtere etiske aspekter ved å innhente og analysere data har størst sjanse for å lykkes med ny teknologi.

Funnene fører derfor til at H1 beholdes for denne studien, der tillit er negativt relatert til den oppfattede risikoen.

6.2 H2: Sensitiviteten på dataopplysningene er positivt relatert til oppfattet risiko

I denne studien er sensitiviteten på dataopplysningene inndelt i kontaktopplysninger og sensitive kunde- og personopplysninger. Disse variablene representerer to forskjellige sensitivitetsnivåer på dataopplysningene som man potensielt deler med banken. Resultatene indikerer at kontaktopplysningene ikke er relatert til oppfattet risiko, men at de sensitive kunde- og personopplysningene er svakt relatert til oppfattet risiko.

Studien til Meinert et al (2006) påpekte tre typer personlig informasjon – kontaktinformasjon, biografisk informasjon og finansiell informasjon. Kim & Kim (2018) avdekte imidlertid fem forskjellige typer informasjon, og det kan dermed være at denne studien ikke går detaljert nok inn på de ulike dataopplysningene. På en annen side er bankene forpliktet til å hente inn mye av den biografiske informasjonen for å opprette et kundeforhold, og denne studien har til hensikt å undersøke de opplysningene man frivillig kan velge å dele med banken.

Kontaktopplysningene viser seg å ikke være signifikant for den oppfattede risikoen. En potensiell forklaring på dette funnet kan være lavere score på oppfattet sensitivitet på kontaktopplysningene. Med unntak av telefonnummeret, oppnådde kontaktopplysningene verdier rundt 2,60 (Se tabell 23). Deling av kontaktinformasjon via sosiale medier, 1881, LinkedIn og lignende tjenester kan være en mulig forklaring på den lave scoren for kontaktopplysninger, og dermed føre til at informasjonen ikke påvirker den oppfattede risikoen i stor grad. På en annen side er ikke utvalget i denne studien stort nok til å trekke de

sterkeste konklusjonene, selv om resultatene tyder på at kontaktopplysningene ikke fremstår som en signifikant faktor for opplevd risiko.

De sensitive kunde- og personopplysningene indikerer derimot en svak positiv korrelasjon med oppfattet risiko, innenfor et signifikansnivå på 95%. Funnet stemmer også med eksisterende teori, hvor for eksempel Kim et al (2019) oppdaget at brukerne var mindre villig til å dele helsedata enn andre personlige opplysninger ved bruk av IoT tjenester. Helsedata kan sammenlignes med finansielle data, hvor begge datasettene inneholder sensitive opplysninger. Meinert et al (2006) kategoriserte finansielle data som noen av de mest sensitive dataopplysningene, og jeg synes derfor det er rimelig å sammenligne funnet i denne oppgaven med helsedata ved bruk av IoT tjenester. I tilfellet til Kim et al (2019), så var ikke respondentene villige til å dele sine helseopplysninger med tjenesteleverandøren, selv om de var klar over at fordelene ville øke betraktelig. Funnet var begrunnet med at den oppfattede risikoen ble for stor, og dermed en hindring for å dele dataopplysningene. Sammenligner jeg de funnene i den gjeldende konteksten, kan det bety at bankkundene ikke er villige til å dele sensitive kunde- og personopplysninger selv om fordelene skulle øke betraktelig.

På en annen side er betaverdien for de finansielle dataopplysningene ikke større enn 0,289. Det indikerer at faktoren kun har en svak relevans for oppfattet risiko, hvor høye verdier av følt sensitivitet medfører en svak økning i oppfattet risiko.

På et mer generelt grunnlag, indikerer funnene at en økning av sensitivitet på dataopplysningene medfører en større oppfattet risiko. Gjennomsnittsverdien av kontaktopplysningene endte på 2,80 (Se tabell 23) mot en gjennomsnittsverdi på 4,27 (Se tabell 24) for de sensitive kunde- og personopplysningene. Forskjellen i sensitiviteten på opplysningene er betydelig, hvor økningen medfører en økning i oppfattet risiko.

Det resulterer dermed i at H2 beholdes for de sensitive kunde- og personopplysningene, men forkastes for kontaktopplysningene.

6.3 H3: Antatte fordeler er positivt relatert til intensjonen om å dele data

Hann et al (2007) argumenterte for at kundene ville være villige til å dele personlige opplysninger på internett, om man vurderte at de motiverende fordelene oversteg den potensielle risikoen ved å dele sensitiv informasjon. Denne studien har derfor undersøkt om

variabelen *Oppfattede fordeler* er positivt relatert til intensjonen om å dele data med banken sin.

Resultatene viser at *Oppfattede fordeler* er den mest sentrale variabelen for både samtykke 1 og samtykke 2. Oddsratioene (*2,16 & 95% Sig., 6,55 & 95% Sig*.) tyder på at det er en sterk korrelasjon mellom de oppfattede fordelene og villigheten til å dele sine kunde- og personopplysninger (Se tabell 31 og 32). Dette harmonerer godt med en rekke andre studier, hvor Kim et al (2019) fant fordelene ved bruk av IoT tjenester som den viktigste driveren for å dele dataopplysninger. Studien til Kim et al (2019) konkluderte med den oppfattede risikoen ikke vektlegges i like stor grad som de oppfattede fordelene, og anbefalte derfor IoT leverandørene til å søke etter å maksimere fordelene med produktene.

Ved å se disse funnene opp mot markedsrapporten fra Cicero (2019), vil jeg argumentere for at bankene i liten grad er i stand til å tilby kundeorienterte tjenester. Rapporten (Cicero, 2019) rangerte bankene etter tjenestetilbud i digitale flater, hvor testvinneren oppnådde fire av ti poeng. SpareBank 1-alliansen oppnådde et resultat på tre av ti poeng, noe som indikerer at det finnes et stort potensial for å tilby verdiøkende produkter i form av digitaliserte rådgivningstjenester. Det urealiserte potensialet kan muligens være en årsak til at banken har en utfordring med å innhente de frivillige samtykkeerklæringene i dag, da forskningen tyder på at de oppfattede fordelene spiller en viktig rolle for villigheten til å dele data. En mulig forklaring på dette, kan handle om at bankene ikke klarer å synliggjøre fordelene man tilbyr ved å dele data, eller rett og slett mangler digitale tjenester som gir kundene økt verdi. En annen forklaring kan være relatert til manglende utnyttelse av CRM systemer og algoritmer som upartisk er med på å gi digitale rådgivningstjenester.

Resultatene i denne studien viste også at nærmere 50% av utvalget ikke hadde foretatt seg et bevisst valg, eventuelt ikke visste om de delte dataopplysninger med banken sin i dag. Jeg vil derfor argumentere for at individene ikke har en nær relasjon til banken, utover basistjenestene som tilbys i nettbank og mobilbank. Personalisert rådgivning i digitale plattformer kan være en mulighet bankene har til å øke de *oppfattede fordelene*, hvor kundene opplever at deling av kunde- og personopplysninger fører til konkrete gevinster. Cicero rapporten (2019) peker på den samme muligheten, og påpeker at kundene, kompetansen og teknologien er tilgjengelig. Hva er det da bankene venter på?

Resultatene for de ulike observerte variablene av *Oppfattede fordeler* indikerer også et ønske om brukervennlige og innovative banktjenester. Det er nettopp disse observerte verdiene som

scorer høyest av de tenkte fordelene, som indikerer at bankkundene også ønsker en bredere tjenesteportefølje fra banken. Verdien av økt personalisering ble dratt frem som spesielt verdifull av Chellappa and Sin (2005), og det ser ut til å gjelde for banktjenestene også.

Spare av DNB kan for eksempel sees på som en suksesshistorie i bankbransjen, hvor den digitale tjenesten har en score på 4,6 av 5,0 i Apple Store og over 500 000 nedlastninger. Jeg vil også argumentere for at de bankene som blir hengende etter i tjenesteutviklingen kan risikere å bli utkonkurrert av tredjepartsaktører som sikter seg inn på verdikjeden til bankene. Gode digitale løsninger kan også komme fra fintech bedrifter, hvor bankene kan satse på å samarbeide med tredjepartsaktører for å kunne tilby innovative tjenester som er med på å øke de *oppfattede fordelene* ved å dele data.

Funnene i denne studien tyder derfor på at *H3* beholdes.

6.4 H4: Oppfattet risiko er negativt relatert til intensjonen om å dele data

Dinev & Hart (2006) hevdet den oppfattede risikoen var negativt relatert til intensjonen om å dele data. Studiene til Strand et al (2009) og Ueland et al (2012) dro frem kontroll og usikkerhet som to sentrale faktorer som påvirket den oppfattede risikoen.

Resultatene i denne studien viser at den oppfattede risikoen er negativt relatert til intensjonen om å dele data for både Samtykke 1 og Samtykke 2, men at faktoren kun er signifikant for Samtykke 2 (*Beta -0,864 & Sig. 95%*). Det er også verdt å merke at betaverdien for oppfattet risiko er lavere enn betaverdien for oppfattede fordeler, noe som indikerer at fordelene har større påvirkning på intensjonen om å dele data.

Studiene til Kim & Kim (2018) og Dinev & Hart (2006) støtter også opp under dette funnet, hvor den oppfattede risikoen er negativt relatert til intensjonen om å dele data. Basert på tidligere studier av privacy calculus modellen, kommer ikke dette funnet som en overraskelse. Ueland et al (2012) gjorde et poeng i at det er vanskelig å vurdere den oppfattede risikoen, men pekte på begrepet kontroll for å vise hvordan mennesker bedømmer risiko. Det er eksempelvis knyttet mer oppfattet risiko til det å ta fly enn det å kjøre bil, nettopp på grunn av at man har en følelse av kontroll om man kjører bil. Den *frivillige risikoen* en person er villig til å ta avhenger derfor av individets risikovilje, og deres illusjon om å ha kontroll over situasjonen.

Det kommer derfor ikke som en overraskelse at den oppfattede risikoen ved å dele finansielle opplysninger anses som høyere enn ved å dele kontaktopplysninger med banken. Dessuten mister man evnen til å kontrollere personopplysningene, hvor man for eksempel risikerer at de blir lekket til tredjepartsaktører eller blir misbrukt.

I motsetning til studien om bruk av IoT tjenester (Kim et al 2019), er den oppfattede risikoen for denne studiens kontekst signifikant for Samtykke 2. Det kan tyde på at den finansielle informasjonen oppfattes som mer sensitiv enn brukerdataen relatert til IoT tjenester.

Funnene medfører derfor at H4 forkastes for kontaktopplysningene, men beholdes for de sensitive kunde- og personopplysningene.

6.5 H5: Håndtering av risiko er positivt relatert til intensjonen om å dele data

Ruiten (2003) delte inn håndteringsevnen i de personlige ferdighetene man hadde for å håndtere risikoen og effektiviteten på tiltakene. Disse begrepene er definert som *Mestringsevne* og *Effektiviteten av tiltak* i denne studien. Begrepet *Danger control* (Ruiten, 2003) er passende for å beskrive denne faktoren, ved at man er i stand til å kontrollere risikoen og ivareta personvernet. Kim & Kim (2018) introduserte dette elementet i privacy calculus modellen, og argumenterte for at håndteringsevnen er positivt relatert til intensjonen om å dele data. Deres studie viste imidlertid at *Håndteringsevnen* kun var positivt relatert til intensjonen om å dele data for utvalgte typer personopplysninger. Studien til Ifinedo (2012) viste imidlertid at både *Mestringsevnen* og *Effektiviteten av tiltakene* var positivt relaterte til intensjonen om å endre adferd for å øke informasjonssikkerheten.

Denne studien viser imidlertid at en økt *Mestringsevne* er negativt relatert til intensjonen om å dele data, hvor faktoren har et signifikansnivå på 90% for Samtykke 1 og 95% for Samtykke 2. Resultatene tyder derfor på at *Mestringsevnen* ikke er positivt korrelert med intensjonen om å dele data, men heller reduserer sannsynligheten for at man deler dataopplysningene sine.

Jeg vil argumentere for at *Mestringsevnen* er tett knyttet til hvilke kunnskaper og ferdigheter man har til å ivareta personvernet. Av den grunn, er det rimelig å anta at de respondentene som scorer høye verdier på *Mestringsevne* også er klar over de potensielle konsekvensene ved et brudd på personvernet. Det impliserer igjen at man i større grad kjenner til risikoen, og ikke innehar en illusjon om at de har kontroll over personvernet. Funnet er uansett å betrakte som overraskende, og strider imot det som kan betegnes som etablert teori.

Effektiviteten av tiltakene er på sin side ikke signifikant for Samtykke 1, men positivt relatert til intensjonen om å dele data for Samtykke 2 med et signifikansnivå på 95% (Beta = .87 & Oddsratio = 2,387). Ifinedo (2012) hevdet denne faktoren var positivt korrelert med intensjonen om å dele data, noe funnene i denne oppgaven også indikerer. Funnet indikerer at bankkundene i større grad er villige til å dele data, om de opplever at de skadereduserende tiltakene er effektive.

Jeg vil dermed argumentere for at *Effektiviteten av tiltakene* kan fremstå som et sikkerhetsnett for respondentene, i tilfelle personopplysningene skulle kommet på avveie. Ved å kontekstualisere tiltakene mot bankbransjen, er det naturlig å tenke seg tiltak som å sperre kort, endre BankID osv. Dette er tiltak som vil hindre at uvedkommende får tilgang til de finansielle ressursene man har, men disse tiltakene vil ikke hindre videre spredning av dataopplysningene. Sett opp mot de observerte verdiene av denne latente variabelen, måles parameterne tilgjengelighet og gjennomførbarhet høyere verdier enn effektiviteten på tiltakene. Det er et funn som er med på å underbygge faren for videre spredning av dataopplysningene. Om sensitive personopplysninger kommer på avveie, er det rimelig å anta at man mister muligheten til å kontrollere videre spredning og eventuell bruk av opplysningene. Dette kan for eksempel eksemplifiseres med at uvedkommende klarer å opprette mobilabonnement, kredittkort eller andre tjenester i din identitet.

Resultatene indikerer dermed at H5 forkastes for *Mestringsevne*, men beholdes for *Effektiviteten på tiltakene*.

7. Avsluttende kommentarer

7.1 Begrensninger ved studien

Det er en svakhet ved oppgaven og datainnsamlingen at SpareBank 1 SMN ikke ønsket noe ansvar eller å være med på å administrere undersøkelsen. Jeg vil anta at utvalget og den påfølgende datakvaliteten derfor kunne vært av høyere kvalitet om SpareBank 1 SMN ville vært med på å gjennomføre spørreundersøkelsen. Resultatene ville eventuelt gitt en bedre ekstern validitet, og være direkte overførbare til deres egne bankkunder.

Den største utfordringen med å innhente empirien selv, var tilknyttet antallet respondenter som kreves for å gjennomføre en kvantitativ studie. Studien har totalt 132 respondenter, som er relativt lite i en forskningssammenheng. Det fører til at resultatene har større feilmargin, og gjør at funnene i denne studien ikke kan bygge de sterkeste konklusjonene.

7.2 Svakheter med spørreundersøkelser

Denne studien har benyttet tjenesten *Nettskjema,* som er et anonymisert spørreskjema. At spørreskjemaet er anonymisert vil i utgangspunktet fremme ærlige svar fra respondentene. Anonymiteten senker barrierene for å svare ærlig, i stedet for at man svarer på en måte som setter seg selv i et best mulig lys. På en annen side er spørreskjema en tydelig forskningsmetode, hvor respondentene vet at svarene deres vil bli forsket på. Det faktum at respondentene vet at de blir forsket på, kan føre til at man svarer for å fremstå sosial intelligent.

7.3 Generalisering av resultater

Hensikten med denne studien var å studere faktorer som er med på å påvirke kundenes villighet til å dele personopplysninger med banken, og sammenligne empirien med etablert teori. Generalisering av resultatene har ikke vært en sentral oppgave for denne studien, og fører til at resultatene ikke nødvendigvis kan generaliseres. Utvalget består derimot hovedsakelig av unge norske bankkunder, som er noenlunde jevnt fordelt mellom menn og kvinner. Det er også naturlig å anta at utvalget hovedsakelig består av mennesker bosatt i Trondheimsområdet, og det er derfor vanskelig å si noe om resultatene ville variert fra landsdel til landsdel. Utvalget består totalt av 132 respondenter, og er å betrakte som relativt lite. Det fører til en høyere feilmargin på resultatene, som ikke gjør det hensiktsmessig å generalisere resultatene.

Referanser

Ajzen, I. & Fishbein, M., 1980. *Understanding attitudes and predicting social behavior*, Upper Saddle River, N.J: Prentice-Hall.

Ajzen, I. 1985. *From intentions to actions: A theory of planned behavior. In Action-control: From cognition to behavior*, Edited by: Kuhl, J and Beckman, J. 11–39. Heidelberg: Springer.

Beldad, Ardion, de Jong, Menno & Steehouder, Michaël, 2011. *A Comprehensive Theoretical Framework for Personal Information-Related Behaviors on the Internet*. The Information Society, 27(4), pp.220–232.

Bellman, S, Lohse, G. L & Johnson, E. J, 1999. *Predictors of online buying behavior*. Communications of the ACM, 42(12), pp.32–38.

Busch, T. (2013). *Akademisk skriving for bachelor- og masterstudenter*. Oslo: Fagbokforlaget.

Chang, C & Heo, J, 2014. *Visiting theories that predict college students' self-disclosure on Facebook*. Computers in Human Behavior, 30, pp.79–86.

Chang, H. H, Wang, Y & Yang, W, 2009. *The impact of e-service quality, customer satisfaction and loyalty on e-marketing: Moderating effect of perceived value*. Total Quality Management & Business Excellence, 20(4), pp.423–443.

Chellappa, Ramnath K & Sin, Raymond G, 2005. *Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma*. Information Technology and Management, 6(2-3), p.181.

Cicero (2019) *Under lupen: PSD2 er her. Et luftslott eller en revolusjon innen bankbransjen.* (Innsiktsrapport, utgave 2 høst 2019) Cicero Consulting Tilgjengelig fra: https://www.cicero.no/under-lupen-psd2-er-her/

Clausen, T.H. & Johansen, V. (2012). *Chronbachs alfa. I T.A. Eikemo & T.H. Clausen (Red.), Kvantitativ analyse med SPSS*. En innføring i kvantitative analyseteknikker (2. utg., s. 268-277). Trondheim: Tapir Akademiske Forlag.

Cortet, M, Rijks, T, & Nijland, S, 2016. PSD2: *The digital transformation accelerator for banks*. Journal of Payments Strategy & Systems, 10(1), pp.13–27.

Dalland, O., 2012. *Metode og oppgaveskriving for studenter 5. utg.*, Oslo: Gyldendal akademisk.

Davis, F. D. (1989). *Perceived usefulness, perceived ease of use, and user acceptance of information technology*. Management Information Systems Quarterly,13(3), 319–340.

Dinev, T & Hart, P, 2006. *An Extended Privacy Calculus Model for E-Commerce Transactions*. Information Systems Research, 17(1), pp.61–80.

DNB (2018) *DNB blir teknologibedrift med banklisens.* Tilgjengelig fra: https://www.dnbnyheter.no/nyheter/dnb-blir-teknologibedrift-med-banklisens/

EY (2011) *The Digitisation of Everything*. *How Organisations Must Adapt to Changing Consumer Behaviour.* London.

Finans Norge (2018). *Forbruker- og finanstrender 2018.* Finans Norge. Tilgjengelig fra: https://www.finansnorge.no/aktuelt/nyheter/forbruker-og-finanstrender/forbruker--og-finanstrender-2018/forbruker--og-finanstrender-2018/

Finans Norge (2019). *Open banking - Utnyttelse av en åpen plattform for mer enn etterlevelse av PSD2*. Betalingskonferansen 2019. Fornebu, 14. November 2019, Sbanken, s. 1-21. Tilgjengelig fra: https://www.finansnorge.no/siteassets/kurs-og-konferanser/2019/betalingsformidlingskonferansen-2019/presentasjoner/open-banking_christoffer-hernas.pdf

Fjørtoft, L.E, Tvedt, K & Presttun, H, 2019. *Open Banking i Norge - samarbeid som konkurransefortrinn?* Praktisk økonomi & finans, 35(2), pp.110–121.

Forbes (2018) *10 Charts That Will Change Your Perspective Of Big Data's Growth* Tilgjengelig fra: https://www.forbes.com/sites/louiscolumbus/2018/05/23/10-charts-that-will-change-your-perspective-of-big-datas-growth/#30c715972926

Forbes (2019) *The Age Of Analytics And The Importance Of Data Quality* Tilgjengelig fra: https://www.forbes.com/sites/forbesagencycouncil/2019/10/01/the-age-of-analytics-and-the-importance-of-data-quality/#4bf3570b5c3c

Hann, Il-Horn et al., 2007. *Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach*. Journal of Management Information Systems, 24(2), pp.13–42.

Ifinedo, P., 2012. *Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory*. Computers & Security, 31(1), pp.83–95.

Kim, Dongyeon et al., 2019. *Willingness to provide personal information: Perspective of privacy calculus in IoT services*. Computers in Human Behavior, 92, pp.273–281.

Kim, Min Sung & Kim, Seongcheol, 2018. *Factors influencing willingness to provide personal information for personalized recommendations*. Computers in Human Behavior, 88, pp.143–152.

Kvistad, M.L.S (2016) *Bruk av tjenestedesigntilnærminger i arbeidet med tjenesteinnovasjon rettet mot unge bankkunder*. Mastergrad. NTNU

Likert, R. (1932). *A Technique for the Measurement of Attitudes*. Archives of Psychology, 140, 1–55.

Lim, H & Dubinsky, A.J, 2004. *Consumers' perceptions of e-shopping characteristics: an expectancy-value approach*. Journal of Services Marketing, 18(7), pp.500–513.

Løverås, C. (2018) Open Banking, *Nordic finance innovation*. Oslo, 1. Februar 2018, DNB, s. 1-85.

Meinert, D.B et al., 2006. *Privacy Policy Statements and Consumer Willingness to Provide Personal Information*. Journal of Electronic Commerce in Organizations (JECO), 4(1), pp.1–17.

Pallant, J. (2013). *SPSS. Survival Manual (6.utg.).* Berkshire: Open University Press

Regjeringen (2014) *Digitalisering i offentlig sektor*. Tilgjengelig fra: https://www.regjeringen.no/no/tema/statlig-forvaltning/ikt-politikk/digitaliseringen-i-offentlig-sektor/id2340245/

Rogers, Ronald W & Maddux, James E. 1983. *Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change*. Journal of experimental social psychology 19, 469-479 (1983).

Ruiter, Robert A.C et al., 2003. *The Role of Coping Appraisal in Reactions to Fear Appeals: Do We Need Threat Information?* Journal of Health Psychology, 8(4), pp.465–474.

Stiglitz, J.E. & Salop, S.C, 1977. *Bargains and Ripoffs: A Model of Monopolistically Competitive Price Dispersion.* Columbia University

Strand, R. et al., 2009. *Risk and uncertainty as a research ethics challenge,* Oslo: National Committees for Research Ethics in Norway.

Ueland, Ø et al., 2012. *State of the art in benefit–risk analysis: Consumer perception.* Food and Chemical Toxicology, 50(1), pp.67–76.

Ulleberg, P. & Nordvik, H., 2000. *Teststatistikk,* Trondheim: Tapir.

Xu, H, Li, H & Sarathy, R, 2011. *The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors*. Decision Support Systems, 51(3), pp.434–445.

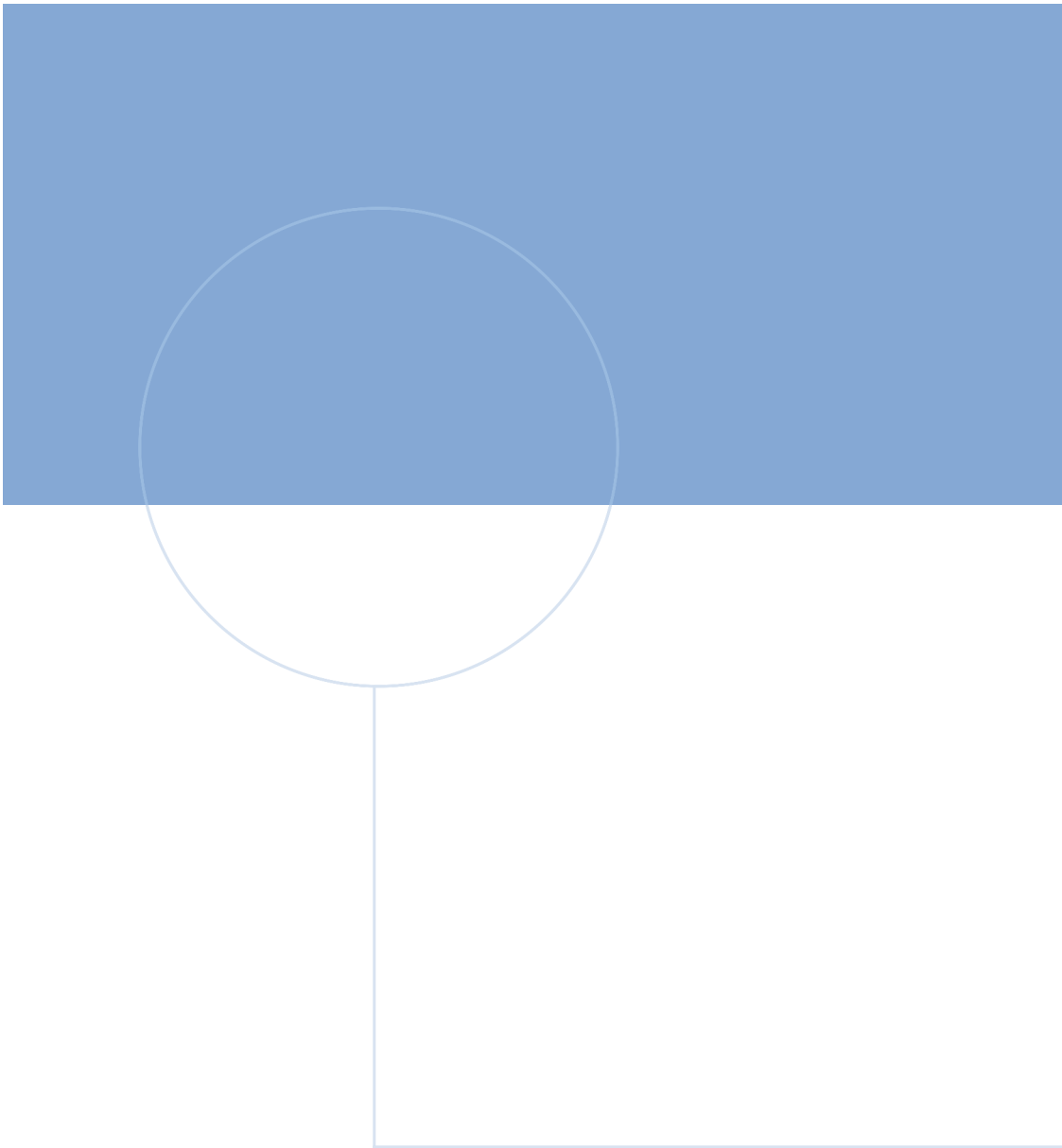
Zhao, L, Lu, Y & Gupta, S, 2012. *Disclosure Intention of Location-Related Information in Location-Based Social Network Services*. International Journal of Electronic Commerce, 16(4), pp.53–90.

Zhu, H et al., 2017. *Privacy calculus and its utility for personalization services in e-commerce: An analysis of consumer decision-making*. Information & Management, 54(4), pp.427–437.

Figurliste

Tabelliste

Vedlegg



NTNU

Kunnskap for en bedre verden