



Wearables i forsikring

En analyse av persontilpassede helseforsikringer i Norge

Johanne Falck-Pedersen & Nadia Vestre Iveland

Veileder: Knut Johannessen Ims

Masterutredning i Strategi og Ledelse

NORGES HANDELSHØYSKOLE

Dette selvstendige arbeidet er gjennomført som ledd i masterstudiet i økonomi- og administrasjon ved Norges Handelshøyskole og godkjent som sådan. Godkjenningen innebærer ikke at Høyskolen eller sensorer innestår for de metoder som er anvendt, resultater som er fremkommet eller konklusjoner som er trukket i arbeidet.

Sammendrag

Teknologisk utvikling åpner for å persontilpasse tjenester i stadig større grad, og det er i ferd med å skje store endringer innenfor forsikringsbransjen. I 2016 ble Norges første persontilpassede bilforsikring lansert, hvor forsikringspremien reguleres av forbrukernes kjøremønster. I USA og andre europeiske land finnes det også persontilpassede helseforsikringer, hvor man ved å dele aktivitetsdata med forsikringsselskapet kan trene seg til en gunstigere forsikringspremie. En slik helseforsikring har ennå ikke kommet til Norge.

En persontilpasset helseforsikring innebærer innsamling av store mengder persondata, og dette utfordrer personvernet på en helt ny måte. Er dette noe vi ønsker i Norge? Parallelt med at tjenester blir mer persontilpassede har EU vedtatt en ny personvernforordning som vil tre i kraft både i Norge og i resten av Europa i mai 2018. Denne vil påvirke hvordan forsikringsselskaper kan samle inn og bruke personopplysninger. Med bakgrunn i dette utforsker vi i denne studien hva som vil være avgjørende for om en persontilpasset helseforsikring aksepteres i Norge.

Vi finner at det er flere faktorer som vil være avgjørende for dette. Et av hovedfunnene kan knyttes til effektene av den nye personvernforordningen. For det første ser lovgivningen isolert sett ut til i større grad å tillate forsikringsselskaper å behandle personopplysninger, og følgelig øke mulighetene for å kunne tilby en persontilpasset helseforsikring i Norge. For det andre innfører lovgivningen også nye rettigheter som vil styrke forbrukernes bevissthet til personvern. Dette tror vi vil skifte maktbalansen mellom forsikringsselskapene og forbruker i favør av forbrukeren. Etterspørselen etter godt personvern vil antakeligvis øke, og vi vil få et marked hvor behandlingen av personopplysninger i tjenester vi bli mer transparent. Vår oppfatning er at dette vil ha en positiv innvirkning på aksepten av persontilpassede helseforsikringer i Norge.

Videre har vi funnet at bruken av wearables er i sterk vekst, og at teknologien anvendt i helseforsikringer gir et potensial til å skape gevinster for samfunnet, forsikringsselskaper og forbrukere. Samtidig medfører bruken av wearables utfordringer som strider mot grunnleggende prinsipper den norske velferdsstaten er bygget på, og vi tror at ønsket om å ivareta personvern og retten til et fredelig privatliv står sterkt blant norske forbrukere. Dette kan bidra til å holde tilbake aksepten av persontilpassede helseforsikringer. Mye tyder likevel på at norske forsikringsselskaper kan klare å ta i bruk wearables i helseforsikring på en akseptabel måte.

Forord

Denne masterutredningen er skrevet ved Norges Handelshøyskole som en avsluttende del av masterstudiet i Økonomi og Administrasjon, innenfor støtteprofilen Strategi og Ledelse.

En sterk interesse for teknologisk utvikling danner bakteppe for denne utredningen. Vi er begge interessert i hvordan teknologi kan brukes innenfor nye områder, og spesielt i forbindelse med persontilpasning av tjenester. Da vi oppdaget at det finnes forsikringsmodeller hvor man kan trene seg til en bedre forsikringspremie, ble vi inspirert til å utforske nærmere om et slikt forsikringsprodukt kan få innpass i Norge. I løpet av studien har vi tilegnet oss mye nyttig kunnskap om både lovverk, personvern og forsikring som vi vil ta med oss videre. Det har vært en spennende og krevende prosess som vi ikke ville vært foruten.

Vi ønsker å takke veilederen vår, Knut Johannessen Ims, for gode samtaler og nyttige innspill gjennom arbeidet med utredningen. Vi vil også rette en spesiell takk til representantene fra Storebrand, Finans Norge, Datatilsynet og Justisdepartementet som har tatt seg tid til å bli intervjuet, og som har vært svært hjelpelige gjennom hele studien. I tillegg ønsker vi å takke alle som har bidratt til å gjøre studietiden vår på NHH til en uforglemmelig opplevelse.

Bergen, juni 2017

Johanne Falck-Pedersen

Nadia Vestre Iveland

INNHOLDSFORTEGNELSE

1. INNLEDNING OG PROBLEMSTILLING	1
1.1 BIG DATA	1
1.2 PERSONTILPASNING AV TJENESTER	1
1.3 MULIGHETER I FORSIKRINGSBRANSJEN	2
1.4 WEARABLES OG HELSEFORSIKRING	3
1.5 PROBLEMSTILLING OG AVGRENSNINGER	4
1.6 UTREDNINGENS STRUKTUR	5
2. LITTERATUR	6
2.1 EN TEKNOLOGISK FREMTID	7
2.2 WEARABLES	7
2.3 PERSONVERN OG INFORMASJONSSIKKERHET	9
2.3.1 Sentrale personvernprinsipper	9
2.3.2 Personvernutfordringer	10
2.3.3 Informasjonssikkerhet	11
2.4 DEN NYE PERSONVERNLOVGIVNINGEN (GDPR)	12
2.4.1 Nye rettigheter for borgerne	13
2.4.2 Nye plikter for bedrifter	13
2.4.3 Utvidet geografisk virkeområde	15
2.4.4 Tolkninger av den nye forordningen	15
2.5 FORSIKRING	15
2.5.1 Forsikringsprinsippet	16
2.5.2 Helseforsikring	16
2.5.3 Omdømme og tillit i forsikring	17
2.5.4 Bruk av wearables i helseforsikringer	17
2.6 FORBRUKERNES HOLDNINGER	18
2.6.1 Datatilsynets personvernundersøkelse fra 2016	19
2.6.2 Norsk kultur	19
2.6.3 Den norske velferdsstaten	20
2.7 OPPSUMMERING AV LITTERATUREN	21
3. MODELL OG FORSKNINGSSPØRSMÅL	22
4. METODE OG DATAINNSAMLING	26
4.1 FORSKNINGSDSIGN	26
4.2 FORSKNINGSTILNÆRMING	26
4.3 VALG AV METODE	27
4.4 FORSKNINGSTRATEGI	27
4.5 INNSAMLING AV DATA	28
4.5.1 Intervju	28
4.5.2 Utvalg	28
4.5.3 Intervjuguide	30
4.5.4 Gjennomføring av intervjuer	30
4.6 METODE FOR ANALYSE AV DATA	31
4.7 EVALUERING AV DATA OG FORSKNINGSDSIGN	32
4.7.1 Validitet	32
4.7.2 Reliabilitet	34
4.7.3 Skjevheter	35

5. RESULTATER OG FUNN	36
5.1 TEKNOLOGISK UTVIKLING OG BRUK AV WEARABLES I FORSIKRING	36
5.1.1 <i>Teknologisk utvikling</i>	36
5.1.2 <i>Sensorbaserte forsikringsløsninger og wearables</i>	37
5.1.3 <i>Forsikringsprinsippet</i>	38
5.2 PERSONVERNUTFORDRINGER OG INFORMASJONSSIKKERHET	39
5.2.1 <i>Press på å gi fra seg samtykke</i>	39
5.2.2 <i>Kunstig intelligens og beslutninger på ukjent grunnlag</i>	39
5.2.3 <i>A- og B-lag i samfunnet</i>	40
5.2.4 <i>Informasjonssikkerhet</i>	42
5.3 PERSONVERNLOVGIVNINGEN	43
5.3.1 <i>Skjerpet krav til samtykke og innebygd personvern</i>	43
5.3.2 <i>Påvirkning på konkurranse</i>	44
5.3.3 <i>Sektorregulering</i>	46
5.3.4 <i>Bransjenormer</i>	48
5.3.5 <i>Sanksjonering</i>	48
5.3.6 <i>Hva er egentlig lovlig i dag?</i>	49
5.4 FORBRUKERNES HOLDNINGER	51
5.4.1 <i>Kunder og personvern</i>	51
5.4.2 <i>Omdømme og tillit</i>	52
5.4.3 <i>Kulturelle forskjeller</i>	53
5.4.4 <i>Kundekommunikasjon og folkeopplysning</i>	53
6. ANALYSE	55
6.1 LOVENS PÅVIRKNING PÅ FORSIKRINGSSLESKAPERS HANDLINGSROM	55
6.2 LOVENS PÅVIRKNING PÅ FORBRUKERNES BEVISSTHET TIL PERSONVERN	59
6.3 TEKNOLOGI.....	62
6.4 PERSONVERNUTFORDRINGER OG INFORMASJONSSIKKERHET	64
6.5 NORSK KULTUR OG SAMFUNNSPRINSIPPER	66
7. KONKLUSJON OG ANBEFALINGER	68
7.1 KONKLUSJON	68
7.2 STYRKER OG SVAKHETER.....	70
7.3 FORSLAG TIL VIDERE FORSKNING	70
8. LITTERATURLISTE	73
9. VEDLEGG	79
9.1 TILBAKEMELDING FRA NSD	79
9.2 INTERVJUGUIDER	81
9.2.1 <i>Justis- og Beredskapsdepartementet</i>	81
9.2.2 <i>Storebrand</i>	83
9.2.3 <i>Finans Norge</i>	85
9.2.4 <i>Datatilsynet</i>	86
FIGUROVERSIKT	
Figur 1: Ordsky med sentrale begreper brukt i utredningen.....	6
Figur 2: Modell	23
TABELLOVERSIKT	
Tabell 1: Oversikt over intervjupersoner.....	29

1. Innledning og problemstilling

1.1 Big Data

Data finnes overalt rundt oss. Gjennom kjøp og søk på nettet, bruk av sosiale medier, apper, smarttelefoner, treningsklokker og andre digitale enheter genereres enorme datastrømmer kontinuerlig (Datatilsynet, 2013). Nettverkstilkoblede sensorer plassert i millioner av fysiske gjenstander fanger opp, behandler og kommuniserer disse datastrømmene, og bidrar til at de blir digitalisert (Manyika, et al., 2011). De store mengdene med digital informasjon kan brukes til avanserte analyseformål.

I forbindelse med de enorme datastrømmene som genereres er Big Data blitt et viktig uttrykk. Big Data kan defineres som den eksponentielle veksten i tilgang til automatisert bruk av informasjon, og de gigantiske digitale datasettene som myndigheter, bedrifter og andre organisasjoner har tilgang til (Article 29 Data Protection Working Party, 2013). Big Data handler videre om de økte mulighetene teknologi gir til å samle inn data, lagre dem i store mengder, analysere dem og utnytte dem strategisk.

Big Data blir bare mer og mer relevant for verdiskapning i alle sektorer i dagens globale økonomi (Manyika, et al., 2011). Teknologien gjør det lettere å lagre og behandle data, samt utføre avanserte dataanalyser til stadig fallende kostnader. Sammen med den teknologiske utviklingen bidrar også menneskers økende digitale atferd til å drive mulighetene som ligger i Big Data raskt fremover.

1.2 Persontilpasning av tjenester

En mulighet Big Data åpner for er å persontilpasse tjenester i større grad enn før. Datatilsynets personvernrapport fra 2016 ser på hvordan innsamling og bruk av personopplysninger på nettet foregår til kommersielt bruk (Datatilsynet og Teknologirådet, 2016). Rapporten presenterer «overvåkingsøkonomien». Denne innebærer at opplysninger om vår atferd på internett blir sporet og samlet inn av aktører som Facebook og Google, for deretter å bli kjøpt og solgt på store internasjonale børser. Informasjonen vi legger igjen er blitt en handelsvare som brukes hyppig av annonseaktører, til å gi hver enkelt av oss persontilpasset reklame og innhold på nettet.

Ny intelligent teknologi gjør det mulig å få svært god innsikt i forbrukernes atferd og interesser, slik at tjenestene både kan bli personlige og forutseende (Datatilsynet og Teknologirådet, 2017). Dette skjer som følge av den økende mengden data som samles inn og lagres om oss gjennom det vi gjør på nettet, samt gjennom den økende bruken av sensorbasert teknologi i hverdagen. Atferden vår digitaliseres i større og større grad. I tillegg bidrar nye effektive metoder for å avdekke sammenhenger i store mengder data, til at tjenestene stadig kan bli mer persontilpassede.

1.3 Muligheter i forsikringsbransjen

Bruken av personopplysninger for å tilpasse tjenester er i dag blitt aktuelt på flere områder. Innenfor bank- og forsikring er det i ferd med å skje store endringer, og spesielt i forsikring åpner Big Data for nye muligheter (Brat, Heydorn, Stover, & Ziegler, 2013). Forsikringsbransjen har frem til nå ligget langt bak andre sektorer i bruken av data og teknologi. Dette skyldes at forsikringsselskaper i utgangspunktet har vært strengere regulert for bruk av teknologi enn den generelle digitale økonomien, spesielt når det gjelder personvern. I tillegg har ikke forsikringsselskaper hatt tilgang til den samme innsikten om kunder som for eksempel banker har hatt gjennom transaksjonsdata fra kredittkort og kontobruk. Bruken av sensorteknologi og Big Data er derfor forventet å ha en revolusjonerende effekt på forsikringsbransjen. Risikovurdering og prising av forsikringsprodukter er et av områdene som vil være spesielt aktuelt for dette.

Risikovurdering basert på sensorteknologi og digital overvåkning av kjøremønstre, har allerede vært i bruk i mer enn ti år i noen land (Christl & Spiekermann, 2016). Rema Forsikring var først ute med å tilby en slik type bilforsikring i Norge. De lanserte forsikringen i 2016, med mål om å «*kunne la teknologien komme kundene til gode*» (Rema 1000, 2016). Dersom kundene tar i bruk deres nye løsning «Kjør Smart», kan de få opptil 15 prosent rabatt på sin forsikringspremie (Rema Forsikring, 2017). Løsningen innebærer at kundene må akseptere å installere en sensor i bilene sine. Sensoren registrerer kjøremønstre i form av bremsing, akselerasjon, hastighet og tid på døgnet. Videre sender den dataene til en applikasjon som genererer en kjørescore, og denne scoren er avgjørende for om kundene får beholde forsikringsrabatten. Jo høyere score, jo høyere rabatt. Sparebank 1 har også lansert en lignende løsning (Sparebank 1, 2017), og Tryg Forsikring har uttalt at de planlegger å gjøre det (Bjørkeng, 2017).

I tillegg til å gi kundene en billig forsikring ønsker Rema 1000 med Kjør smart å bidra til å gjøre både miljøet og trafikken sikrere, ved å øke sjåførens bevissthet på egen kjøring (Rema Forsikring, 2017). Bruk av sensorteknologi gjør det dermed mulig for forsikringsselskapene å motivere kundene til å endre atferd, og de kan bli en del av våre liv på en helt ny måte (Datatilsynet og Teknologirådet, 2017).

1.4 Wearables og helseforsikring

Bruken av sensorteknologi for persontilpasning innenfor forsikringsbransjen begynner også å gli inn mot helsetjenester. Programmer for livs-, helse-, og tannforsikring som baserer seg på innsamling av data gjennom kroppsnær teknologi, også kalt «wearables», er i vinden (Christl & Spiekermann, 2016). Dette innebærer at personlig atferd og aktivitet overvåkes, og er med på å risikovurdere kunden og påvirke deres forsikringspremie. Bruken av wearables blir mer og mer populært ettersom sensorer blir billigere, mindre og bedre (Datatilsynet og Teknologirådet, 2014). De kan også lett integreres i kroppsnære produkter, som enkelt kan kobles til smarttelefoner og andre mobile enheter.

I USA er det en trend at forsikringsselskaper inngår avtaler med produsenter av wearables. Både FitBit, en ledende aktør innen produksjon av fitnessarmbånd, og Vitality Group, en leverandør av en komplett fitnessløsning, har inngått partnerskap med flere store aktører innenfor helseforsikring (Wheelwright, 2016). Vitality Group har utviklet et belønningssystem sammen med et av de største livsforsikringsselskapene i USA. Her belønner de forsikringskunder som ved bruk av et gratis aktivitetsarmbånd lar forsikringsselskapet overvåke deres aktiviteter (Christl & Spiekermann, 2016). På denne måten kan kundene opptjene poeng, som kan brukes til å redusere premien på livsforsikring med opp til 15 prosent.

Persontilpassede helseforsikringer er også på god vei inn i det europeiske markedet. Slike forsikringsmodeller utfordrer personvernet på en ny måte, og stiller spørsmålet: Skal vi akseptere å slippe forsikringsselskaper så tett inn på kroppen? I 2018 vil GDPR¹, EUs nye personvernforordning, erstatte dagens personvernlovgivning i både Norge og i resten av Europa (Datatilsynet og Teknologirådet, 2017). Denne lovgivningen vil være med på å utforme hvordan personopplysninger kan samles inn og brukes for å utvikle forsikringstjenester som er

¹ General Data Protection Regulation.

persontilpassede. Det er imidlertid uklart hva som konkret kommer til å skje på det norske forsikringsmarkedet.

Som tidligere nevnt prøver Rema Forsikring og Sparebank 1 seg nå med å tilby persontilpassede bilforsikringer. Hvordan dette vil mottas i det norske markedet, er foreløpig uvisst. En persontilpasning innenfor helseforsikring vil involvere bruk av det mange kan oppfatte som svært sensitiv informasjon om seg selv. Samtidig ser man at forsikringsmodeller basert på wearables allerede er introdusert i flere andre land i Europa. I tillegg ligger Norge langt fremme i bruken av ny teknologi, og er et av verdens mest digitaliserte land (Nasjonal sikkerhetsmyndighet, 2016). Det blir derfor spennende å se hvilken retning utviklingen tar i Norge.

1.5 Problemstilling og avgrensninger

Teknologisk utvikling legger et bakteppe for denne utredningen. Vi har sett at teknologi og Big Data åpner for nye muligheter innenfor de fleste næringer, og at det skjer mye spennende innenfor forsikring. Forsikringsmodeller som baserer seg på atferdsdata fra kunder er i stadig utvikling, og det har nylig blitt introdusert persontilpassede bilforsikringer i Norge. Vi har også sett at persontilpasning av helseforsikringer er fremtredende i USA, og begynner å bli utbredt i Europa. En persontilpasset helseforsikring innebærer innsamling av mer sensitive personopplysninger enn det en persontilpasset bilforsikring gjør. Vi er derfor svært interessert i å utforske om et slikt produkt ville blitt akseptert i Norge. I tillegg vil den nye personvernlovgivningen som kommer i 2018 påvirke hvordan virksomheter kan bruke personopplysninger til å utvikle tjenester.

Med bakgrunn i dette ønsker vi i denne utredningen å besvare følgende problemstilling:

Hva vil være avgjørende for om en persontilpasset helseforsikring aksepteres i Norge?

I denne studien vil vi begrense oss til å se på utviklingen av persontilpassede helseforsikringer i Norge. Vi har valgt å se på området for helseforsikring fordi dette dreier seg om et sensitivt inngrep i folks privatliv, og dermed åpner for en interessant diskusjon. Etter innledende samtaler med vår kontaktperson i Storebrand har vi også kommet frem til at helseforsikring er den mest aktuelle blant personforsikringene for persontilpasning per i dag.

Vi legger til grunn at teknologisk utvikling har skapt behov for ny personvernlovgivning, og tror denne lovgivningen vil ha betydning for utviklingen av persontilpassede helseforsikringer i Norge. Vi antar at det også er flere faktorer som vil være viktige for utviklingen av persontilpassede helseforsikringer. De faktorene vi har valgt å fokusere på i tillegg til loven, er teknologi, personvernutfordringer og informasjonssikkerhet, samt særtrekk ved norsk kultur og velferdsstat.

Vi har tatt utgangspunkt i at det er tre sentrale interessenter som påvirker og påvirkes av innføringen av persontilpassede helseforsikringer. Disse er *myndighetene*, *forsikringsselskapene* og *forbrukerne*. Ut i fra dette har vi valgt intervjupersoner som kan belyse disse aktørenes synspunkter. Dette har lagt grunnlaget for vår datainnsamling. Vi har valgt Storebrand som representant for forsikringsselskapene, fordi de ved studiens begynnelse var leverandør av den eneste persontilpassede forsikringen i Norge². Vi forutsetter også at Storebrands synspunkter er representative for andre norske forsikringsselskaper. Dette innebærer at vi ikke har intervjuet andre forsikringsselskaper. Videre har vi antatt at forbrukernes holdninger til persontilpassede helseforsikringer belyses godt nok av Datatilsynets personvernundersøkelse fra 2016, og har derfor ikke intervjuet noen forbrukere. De andre intervjupersonene vil vi gå nærmere inn på i kapittel 4.

1.6 Utredningens struktur

Utredningen er delt inn i åtte kapitler. I kapittel 2 vil vi presentere relevant litteratur som kan knyttes til vår problemstilling. Med bakgrunn i denne litteraturen har vi utviklet en modell med fem tilhørende forskningsspørsmål, som presenteres i kapittel 3. Denne modellen legger føringer for hvordan vi har valgt å gå frem for å besvare problemstillingen. I kapittel 4 vil vi presentere de metodiske valgene vi har tatt for å gjennomføre studien. Videre vil vi i kapittel 5 legge frem resultater og funn fra intervjuene. I kapittel 6 vil vi presentere analysen vår, hvor vi har knyttet resultatene opp mot modellen med sine tilhørende forskningsspørsmål. Til slutt vil vi legge frem vår konklusjon, presentere styrker og svakheter ved utredningen, samt anbefalinger til videre forskning i kapittel 7. I kapittel 8 litteraturlisten, og i kapittel 9 presenteres vedlegg, hvor vi har lagt ved alle intervjuguidene vi har utformet.

² Storebrand er underleverandør av Rema Forsikrings persontilpassede bilforsikring «Kjør Smart».

2. Litteratur

I dette kapitlet vil vi presentere litteratur som kan gi oss bedre innsikt og forståelse for vår problemstilling. Vi ønsker å avklare begreper som er relevante, samt gi mer utdypende informasjon om temaer som kan hjelpe oss å forstå vår problemstilling. Det første vi vil ta for oss er bruken og utviklingen av wearables både generelt og i Norge. Deretter vil vi se på personvern og informasjonssikkerhet. Her vil vi gå nærmere inn på tradisjonelle personvernprinsipper og ta for oss utfordringer knyttet til personvern og informasjonssikkerhet som kommer med den teknologiske utviklingen. Videre vil vi ta for oss den nye personvernlovgivningen, og presentere det vi forstår som de foreløpige implikasjonene av denne når den trer i kraft. Deretter vil vi ta for oss forsikring. Her vil vi se på forsikringsprinsippet og helseforsikring, hvor vi går nærmere inn på diskusjonen rundt helseforsikring og bruken av wearables. Vi vil også introdusere forsikringsmodellen Vitality Health for å få mer innsikt i hvordan en persontilpasset helseforsikring vil kunne se ut i Norge. Avslutningsvis vil vi se nærmere på norske særtrekk som kan påvirke holdninger til persontilpassede helseforsikringer. Her vil vi introdusere funn fra Datatilsynets personvernundersøkelse fra 2016, samt presentere trekk ved norsk kultur og den norske velferdsstaten.



Figur 1: Ordsdy med sentrale begreper brukt i utredningen

2.1 En teknologisk fremtid

Det spekuleres stadig i hvilken teknologisk retning samfunnet utvikler seg, både fiktivt og gjennom vitenskapelig forskning. I Netflix-serien *Black Mirror* settes det i flere episoder kritisk søkelys mot bruk av teknologi i hverdagen (Netflix, 2016). I en episode kalt «Nosedive» blir livet til alle mennesker styrt av hva slags score de får på sosiale medier (Jones & Schur, 2016). Med for lav score risikerer man å falle utenfor samfunnet, mens man med høy score blir tilhørende en slags elite. I episoden «Shut Up and Dance» blir faren tilknyttet datahacking satt på spissen når en tenåringsgutt blir utpresset (Bridges & Brooker, 2016). Hackere har filmet han i en sjenerende situasjon gjennom kameraet på laptopen hans, og truer med å lekke filmen dersom han ikke samarbeider.

Alt det nevnte er eksempler på hvordan populærkulturen prøver å predikere teknologiens rolle i potensielle fremtidsscenarioer. Vi ser også tendensene til at vi lever i et overvåkningssamfunn, slik George Orwell (1949) forespeilet i boken *1984*. Han beskrev det han kalte «Storebror-samfunnet», der myndighetene overvåker innbyggerne og setter rammer for livene deres. Det vi faktisk ser i dagens samfunn er at vi alle overvåker og påvirker hverandre (Bustillos, 2013). Vi blir konstant bombardert og bombarderer samfunnet med data. For eksempel kan hendelser som før var helt isolerte og ukjente nå bli filmet på en smarttelefon og sett av millioner av mennesker gjennom medier som YouTube i løpet av sekunder. Bruken av wearables bidrar til at man genererer mer og mer data, både om seg selv og om andre.

2.2 Wearables

Wearables kan defineres som elektronisk sensorteknologi, som er integrert i klær og kroppsnært tilbehør (Deel, Nadimpalli, Sahoo, Verma, & Vervuurt, 2016). Sensorene er designet til å utføre datafunksjoner på lik linje med mobiltelefoner og datamaskiner, og kan brukes til å måle fysisk aktivitet og helserelaterte verdier. Integreringen av data fra wearables med smarttelefoner gjør det lett for brukeren å få tilgang til dataene som samles inn, og å ha kontroll over egen livsstil.

Det er forventet en sterk vekst i bruken av wearables i fremtiden, og inntektene fra det globale markedet for disse produktene er estimert til å passere \$11.6 milliarder i 2020 (Deel et al., 2016). Allerede i 2014 ble det anslått at opptil 100.000 wearables ville bli solgt i Norge, og produsentene var overveldet over populariteten for disse produktene blant nordmenn (E24,

2014). I en undersøkelse gjennomført av Accenture i 2016, ble det også funnet at stadig flere nordmenn bruker wearables for å overvåke egen helse (Accenture, 2016). Dette gir en indikasjon på hvordan wearables ser ut til å bli en del av flere og flere forbrukeres hverdag i tiden fremover.

Wearable-teknologi omtales i dag som en av de mest utbredte teknologiene i vekst (Gammack, Kerr, & Marrington, 2016). Fremskrittene som gjøres innenfor wearables skaper store muligheter for å øke sosial og økonomisk velferd, og kan ha positiv effekt for både individer og organisasjoner (Berrahal & Boudriga, 2016). For individer kan overvåkning av helse gjennom wearables ikke bare bidra til å nå treningsmål, men også til å oppdage og forebygge sykdom. Wearables muliggjør måling av helseparametre som kroppstemperatur, oksygenmetning i blodet og puls, og kan varsle helsepersonell hvis et individ står i fare for å få et akutt anfall, som for eksempel et hjerteinfarkt.

Et eksempel på en norskutviklet wearable er helseklokken Contact. En av gründerne fikk ideen etter at han opplevde hjertestans i bilen sin i 2014 (ContinYou, 2017). Klokken er utstyrt med innebygd GPS og SIM-kort, og har en alarm som utløses ved fall eller unormale helseverdier. Målet med produktet er å skape trygghet for både bruker og pårørende, gi eldre mulighet til å bo hjemme lenger, samt å bidra til økonomiske besparelser i samfunnet. Dette viser hvilket potensial wearables kan ha til forbedringer innen helse fremover.

I forbindelse med wearables er *Internet of Things* et begrep som bør avklares. Internet of Things refererer til den trådløse kommunikasjonen som foregår mellom sensorutstyrte gjenstander, deriblant wearables (Datatilsynet, 2013). Begrepet belyser utviklingen mot at alle verdens ting utstyres med sensorer og blir koblet til internett (Salomonsen, 2015). Dette gjør at tingene kan oppfatte hva som skjer i omgivelsene, og kommunisere med hverandre.

Internet of Things og økt bruk av wearables skaper nye utfordringer knyttet til personvern og informasjonssikkerhet (Gammack et al., 2016). Brukere av wearables måler ofte aktiviteten sin hele døgnet, og dette fører til at det konstant genereres store mengder data om dem digitalt. Dette truer privatlivet, samt gjør brukerne sårbare hvis dataene hackes eller blokkeres. For å sikre en sunn utvikling av Internet of Things og wearable-teknologi, er det derfor viktig å ta slike implikasjoner på alvor. Utfordringer knyttet til personvern og informasjonssikkerhet vil

med andre ord stå sentralt i vurderingen av om persontilpassede helseforsikringer vil aksepteres i Norge.

2.3 Personvern og informasjonssikkerhet

Bruken av wearables og innsamling av personopplysninger for å utvikle persontilpassede tjenester utfordrer personvernet på en helt ny måte. En persontilpasset helseforsikring vil innebære innsamling av sensitive opplysninger om folks helse, noe som kan skape implikasjoner for ivaretagelsen av sentrale personvernprinsipper den norske lov er bygget på. I tillegg vil risikoen knyttet til informasjonssikkerhet øke. I dette delkapitlet vil vi først se på *sentrale personvernprinsipper*, før vi videre vil ta for oss *personvernutfordringer*. Til slutt vil vi se på utfordringer knyttet til *informasjonssikkerhet*.

2.3.1 Sentrale personvernprinsipper

Norsk personvernlov er bygget på prinsipper som dreier seg om at alle har rett til å bestemme over egne personopplysninger (Datatilsynet, 2016c). Formålet med loven er å hindre at behandling av personopplysninger fører til krenkelse av personvernet, og sikre at behandlingen skjer i samsvar med grunnleggende personvern hensyn (Lovdata, 2000). Personopplysningsloven (2000) definerer personopplysninger som «*opplysninger og vurderinger som kan knyttes til en enkeltperson*». Dette kan være navn, personnummer, adresse, telefonnummer, fingeravtrykk eller IP-adresse (Datatilsynet, 2016b). Opplysninger om atferdsmønster, som for eksempel digitale spor man legger igjen på nettet ved søk, betegnes også som personopplysninger. Informasjon om helseforhold går derimot under betegnelsen *sensitive* personopplysninger (Lovdata, 2000). Det stilles egne krav til behandling av disse.

Prinsippene som den norske loven bygger på er fastsatt av Det europeiske persondirektivet, og det er spesielt noen av dem som er relevante når det gjelder teknologisk utvikling og bruken av wearables (Datatilsynet, 2016c). Disse omfatter ivaretagelse av opplysningenes;

- *Formålsbestemthet* – Opplysningene skal kun brukes til det formålet de ble samlet inn for, og skal ikke kunne utleveres til andre uten samtykke (Datatilsynet, 2016c).
- *Relevans og minimalitet* – Det skal kun samles inn den mengde informasjon som trengs for å oppnå formålet, og all data som ikke lenger har relevans etter bruk skal anonymiseres eller slettes (Datatilsynet, 2016c).

- *Fullstendighet og kvalitet* – Det skal sikres at alle personopplysninger som lagres og brukes er korrekte, oppdaterte og nøyaktige, slik at beslutninger basert på disse ikke tas på feil grunnlag (Datatilsynet, 2016c).
- *Informasjon og innsyn* – Man har rett til å få innsyn i alle opplysninger som er samlet inn om en. Dette innebærer også at man har rett på en manuell vurdering, dersom en beslutning som er av vesentlig betydning for den det gjelder er tatt gjennom en automatisert behandling (Datatilsynet, 2016c).
- *Informasjonssikkerhet* – De som oppbevarer personopplysninger står ansvarlige for å sikre dem (Datatilsynet, 2016c)
- *Samtykke* – Alle personopplysninger som behandles skal skje etter frivillig, uttrykkelig og informert samtykke med den det gjelder (Datatilsynet, 2016c).

2.3.2 Personvernutfordringer

Flere av personvernprinsippene utfordres av teknologisk utvikling og den økende bruken av wearables, og kan gå på bekostning av at tjenester stadig blir mer persontilpassede. *Tap av kontroll over personopplysninger, press til samtykke, bånd på ytringsfrihet og fare for at beslutninger tas på feil grunnlag* er noen av personvernutfordringene samfunnet står overfor (Datatilsynet og Teknologirådet, 2017).

Tap av kontroll over personvernopplysninger

Følelsen av å miste kontroll over informasjon som er samlet inn om en, er en personvernutfordring som kan oppstå i dagens digitale samfunn (Datatilsynet og Teknologirådet, 2017). Enkeltindivider legger igjen digitale spor på stadig flere steder de ikke har full oversikt over, og det er vanskelig å vite hvem som har tilgang til denne informasjonen. Det kan derfor oppstå et ubehag knyttet til følelsen av å miste kontroll over hva slags opplysninger som egentlig er lagret, hvem som får tak i dem, og hva de kan brukes til.

Press til samtykke

En annen personvernutfordring kan knyttes til hvordan persontilpasning av tjenester kan bidra til å skape et press i befolkningen til å gi fra seg personopplysninger mot ens egen vilje (Datatilsynet og Teknologirådet, 2017). Dette kan skje dersom man for eksempel har dårlig økonomi, og kun har råd til tjenesten som krever at man gir fra seg personopplysninger. Dette

kan typisk gjelde innenfor forsikring, hvor de som lar seg overvåke får en billigere forsikringspremie. Slik kan en persontilpasset helseforsikring skape et press til å gi samtykke for bruk av personopplysninger.

Bånd på ytringsfrihet

Videre kan en økende grad av persontilpassede tjenester bidra til at folk endrer sin atferd eller ytrer seg i mindre grad enn de egentlig ønsker (Datatilsynet og Teknologirådet, 2017). Dersom man vet at måten man opptrer på tas med i prisberegningen av et produkt, kan dette føre til at man endrer atferd for å oppnå en mer fordelaktig pris. Hvis man videre er redd for at holdninger og meninger man har kan påvirke utfallet av tjenester negativt i fremtiden, kan dette også legge bånd på at man ytrer seg slik man ønsker. Dette viser hvordan persontilpassede tjenester legger press på viktige aspekter ved personvernet.

Fare for at beslutninger tas på feil grunnlag

En annen faktor som utfordrer personvernprinsippene er mulighetene de stadig sterkere algoritmene i datamaskiner gir til å ta automatiske beslutninger (Datatilsynet og Teknologirådet, 2017). Det kan være fare for at algoritmene som brukes blir påvirket av innebygde skjevheter og fordommer som preger beslutningene. Hvis algoritmesystemene gjør diskriminerende analyser som er så komplekse at man ikke forstår grunnlaget bak dem, vil dette kunne medføre at folk blir urettferdig behandlet. Dette vil være spesielt uheldig dersom beslutningen er av vesentlig betydning for den det gjelder.

2.3.3 Informasjonssikkerhet

De voksende mulighetene til å samle inn, lagre og behandle personopplysninger, øker risikoen knyttet til informasjonssikkerhet. Fra et IKT-perspektiv skal sikkerhetsarbeidet i en bedrift dreie seg om å sikre informasjonsverdiens *tilgjengelighet*, *konfidensialitet* og *integritet* (Nasjonal sikkerhetsmyndighet, 2016). Informasjonens tilgjengelighet innebærer at informasjonen skal være tilgjengelig for de som skal bruke den, mens med konfidensialitet menes det at informasjonen skal sikres mot uautorisert tilgang. Integritet innebærer at informasjonen skal forbli riktig, fullstendig og gyldig under lagring og overføring.

Systemer som oppbevarer personopplysninger kan stå i fare for å bli utsatt for dataangrep (Berrahal & Boudriga, 2016). Et dataangrep innebærer at en uautorisert aktør får tilgang til

beskyttet og konfidensiell data. Motivet bak et dataangrep kan være å utnytte sensitive opplysninger til økonomiske formål, eller ødelegge en organisasjons rykte, markedsverdi eller tillitsforhold med kunder (Miaoui & Boudriga, 2015; Berrahal & Boudriga, 2016). Trusselen for dataangrep i form av løsepengevirus er i dag en økende utfordring. Dette innebærer at et virus låser og krypterer filer som er lagret. For å få tilbake tilgang til systemene må ofrene betale en etterspurt løsepenge sum. I midten av mai 2017 ble over 200.000 datasystemer rammet av «WannaCry», det mest alvorlige og utbredte løsepengeviruset man har sett globalt hittil (Epstein, 2017). Dette belyser utfordringene knyttet til informasjonssikkerhet som følger med den teknologiske utviklingen.

Sikkerhet knyttet til kommunikasjon mellom wearables og Internet of Things-enheter er også en utfordring. Overføringen av informasjon mellom wearables og mobile enheter skjer vanligvis via Bluetooth, og denne er i de fleste tilfeller ikke kryptert (Kerr & Gammack, 2016). Dette gjør at uønskede parter enkelt kan få tilgang til informasjonen som overføres mellom enhetene. Mangel på sikring av wearables kan følgelig utgjøre en risiko for individers personvern, og er noe som bør tas i betraktning ved bruk av slike enheter.

Det finnes flere potensielle skrekksenarioer for dataangrep tilknyttet wearables. I 2012 skapte en episode i den amerikanske tv-serien *Homeland* stort oppstyr blant seerne da visepresidenten i USA ble utsatt for et dataangrep mot sin pacemaker (Wadhwa, 2012). En gruppe terrorister klarte å hacke seg inn og ta kontroll over pacemakeren, hvor de styrte den til å utføre store elektriske sjokk som påførte visepresidenten et hjerteinfarkt. Mange lurte på om dette faktisk ville være mulig. Allerede i 2008 skrev New York Times en artikkel om et datasikkerhetsteam som under et eksperiment klarte å ta kontroll over en kombinert defibrillator og pacemaker (Feder, 2008). De fikk enheten til å skru seg av, og programmerte den til å gi sterke elektriske støt som ville skapt alvorlige konsekvenser for et menneske. Forskerne demonstrerte viktigheten av å sikkerhet knyttet til bruken av wearables.

2.4 Den nye personvernlovgivningen (GDPR)

14. April 2016 ble GDPR vedtatt i EU-institusjonene, og den vil tre i kraft 25. mai 2018 både i Norge og i resten av Europa (Datatilsynet, 2017f). Den nye personvernforordningen sikter mot å innføre like personvernregler for europeiske virksomheter, og endringer som vi ser spesielt relevante for denne utredningen kan knyttes til *nye rettigheter for borgerne, større personvernansvar for bedrifter og utvidet geografisk virkeområde* (Datatilsynet, 2016a).

2.4.1 Nye rettigheter for borgerne

Et av hovedformålene bak den nye lovgivningen er å styrke borgernes kontroll over egne personopplysninger, og forordningen innfører nye rettigheter som skal bidra til dette (Datatilsynet, 2017b). Retten til *dataportabilitet* er en av dem. Dette innebærer at man som bruker har rett til å få utlevert personopplysninger som man har gitt fra seg til en tjeneste, slik at man enkelt skal kunne gi denne videre til en ny leverandør (Riisnæs & Schilvold, 2016). Dette vil gjøre det lettere for brukere å bytte tjenesteleverandør, og bidra til å skape konkurranse i etablerte markeder.

Retten til *å bli glemt* vil etter den nye lovgivningen tydeliggjøre borgernes rettighet til å kreve at egne personopplysninger blir slettet (Datatilsynet, 2017b). Dette innebærer blant annet at man kan kreve sletting av egne personopplysninger hvis man trekker sitt samtykke fra en tjeneste, hvis opplysningene som er samlet inn ikke lenger trengs for å oppnå behandlingens formål, eller hvis behandlingen av opplysningene har skjedd i strid med regelverket.

I tillegg vil det etter de nye reglene stilles strengere krav til å bruke *automatiske avgjørelser* ved behandling av personopplysninger (Datatilsynet, 2017b). Dette skal sikre at avgjørelser basert på algoritmer knyttet til for eksempel forsikringspremie ikke er tillatt med mindre virksomheten har gyldig samtykke fra brukeren.

Til slutt vil også den nye lovgivningen forsterke *kravet til samtykke* fra brukeren ved behandling av personopplysninger til bestemte formål (Riisnæs & Schilvold, 2016). Samtykke til bruk av personopplysninger må være tydelig skilt fra andre forhold i virksomhetens avtalevilkår. Brukeren må også ha avgitt en *frivillig, uttrykkelig og informert* erklæring om at han eller hun godkjenner behandling av sine personopplysninger, for at samtykket skal være gyldig. Dette vil blant annet si at samtykket ikke kan være del av en betingelse for en tjeneste, eller at passive måter for samtykke som forhåndskryssede bokser, ikke er godt nok.

2.4.2 Nye plikter for bedrifter

Alle norske virksomheter får nye plikter som følge av den nye personvernforordningen. Det blir pålagt å ha en *forståelig* personvernerklæring, hvor det blant annet stilles strengere krav til språklig klarhet, tydelighet og tilgjengelighet (Datatilsynet, 2017d). I tillegg skal det gis mer

informasjon enn det som tidligere har vært påkrevd, som for eksempel om hvilke personopplysninger som behandles.

I tillegg ser det ut til at dagens ordning med melde- og konsesjonsplikt vil bortfalle med den nye forordningen (Datatilsynet, 2016a). I dag kreves det i Norge etter hovedregelen en *meldeplikt* for behandling av personopplysninger, samt en *konsesjonsplikt* for behandling av sensitive personopplysninger til Datatilsynet (Datatilsynet, 2017e). For finans- og forsikringsnæringen er det i tillegg spesielt regulert at selv behandling av personopplysninger krever konsesjon. Det er imidlertid uklart om konsesjonsplikten for spesifikke sektorer som bank, finans og forsikring kommer til å bortfalle helt med den nye forordningen, da det er åpent for nasjonale tilpasninger på noen områder (Risung & Songe-Møller, 2016). Sammen med bortfall av den generelle konsesjonsplikten, vil virksomheters plikt til å vurdere egen risiko ved behandling av personopplysninger utvides. Dette innebærer at de får større ansvar for å identifisere risikoreduerende tiltak, og må selv ta initiativ til å søke om godkjenning fra Datatilsynet dersom de finner at risikoen er for stor (Datatilsynet, 2016a).

Videre er *innebygd personvern* noe som blir lovpålagt etter den nye forordningen. Dette innebærer at personvern skal bygges inn i alle faser av en løsning, og at det alternativet som i høyest grad skåner personvernet skal stå som standard for en tjeneste (Datatilsynet, 2017c). Systemene som behandler personopplysninger skal være sikret på en hensiktsmessig måte, for å hindre uautorisert tilgang, spredning, endring eller ødeleggelse av personopplysningene.

Samtidig som at virksomheter tillegges mer personvernansvar som følge av den nye forordningen, vil også mulighetene myndighetene har til å gi *sanksjoner* ved brudd på personvernreglene øke betraktelig (Risung & Songe-Møller, 2016). Virksomheter vil kunne ilegges bøter for opp til fire prosent av årlig omsetning eller maksimalt 20 millioner euro. Dette er en kraftig økning fra dagens regler. Det er imidlertid uklart i hvilken grad myndighetene kommer til å praktisere et strengt sanksjonsregime etter de nye reglene.

Datatilsynet påpeker at det i lys av den nye personvernlovgivningen bør samarbeides om å danne egne bransjenormer for behandling av persondata (Datatilsynet, 2017a). Dette for å sikre at behandlingen skjer på en hensiktsmessig måte. I forbindelse med helsedata må forsikringsselskaper for eksempel per i dag forholde seg til normen for informasjonssikkerhet i helse og omsorgstjenesten (Direktoratet for e-helse, 2016). Ut i fra dette vil det være interessant

å se om retningslinjene som utvikler seg i forsikringsbransjen vil spille en rolle for persontilpasning av forsikringstjenester.

2.4.3 Utvidet geografisk virkeområde

Det geografiske området som omfattes av de europeiske personvernreglene blir utvidet med den nye ordningen (Datatilsynet, 2016a). Dette innebærer at aktører som opererer fra land utenfor EU, men som leverer tjenester til europeere, også må følge de nye EU-reglene. Slike aktører vil dermed ikke lenger ha mulighet til å utnytte personopplysninger etter mer fordelaktige betingelser enn europeiske virksomheter (Riisnæs & Schilvold, 2016).

2.4.4 Tolkninger av den nye forordningen

Partner i PwC, Lars Erik Fjørtoft, hevder at et viktig aspekt som glemmes med den nye forordningen er at den legger til rette for en enklere og tryggere innsamling av personopplysninger (Fjørtoft, 2017). Han påpeker at retten til sletting, dataportabilitet og innebygd personvern skal gjøre det lettere og tryggere for borgere å gi fra seg personopplysninger mot å få fordelaktige tjenester tilbake. Dette innebærer at muligheten til å samle inn personopplysninger om kunder kommer til å bli større. Man vil kunne tilegne seg bedre innsikt i kunders atferd, og på denne måten tilby mer målrettede tjenester enn før. Han mener at den nye forordningen kommer til å redefinere oppfatningen av godt personvern, og at lovgivningen vil gå fra å være «*en utdatert begrensning, til å åpne nye muligheter for en enklere hverdag for oss alle som innbyggere og konsumenter i et digitalt samfunn*» (Fjørtoft, 2017). Fokuset på personvern skal ikke lenger bare oppfattes som en kostnad, men heller som en potensiell inntektskilde hvor virksomheter vil kunne forbedre sitt tilbud til kundene.

2.5 Forsikring

Kunnskap om hvordan tradisjonelle forsikringsmodeller er bygget opp vil være relevant for å forstå hvordan de nye forsikringsmodellene vil mottas i markedet. Vi vil derfor i dette delkapitlet presentere ulike aspekter ved forsikring. Først vil vi introdusere forsikringsprinsippet. Deretter går vi nærmere inn på helseforsikring, før vi vil ta for oss viktigheten av omdømme og tillit i forsikringsbransjen. Avslutningsvis presenterer vi en persontilpasset modell for helseforsikring som i dag tilbys i Storbritannia.

2.5.1 Forsikringsprinsippet

Forsikring defineres av Døskeland (2014) som det motsatte av en investering i finansmarkedet. I finansmarkeder ønsker man kompensasjon for å ta på seg risiko, mens i forsikring betaler man for å unngå risiko. Verdien av forsikringen er altså negativt korrelert med forsikringsobjektet. Det vil si at dersom det man har forsikret taper seg i verdi, for eksempel at telefonen blir stjålet, så vil verdien av utbetalingen fra forsikringsselskapet være positiv.

Forsikringsbransjen er bygget opp rundt *forsikringsprinsippet* (Døskeland, 2014). Dette innebærer at en gruppe mennesker står sammen om å dele risikoen for skade eller tap. Risikoen beregnes ved hjelp av statistiske modeller, og det tas utgangspunkt i at alle i gruppen står overfor samme risiko. Data og teknologi legger grunnlag for å beregne risiko på nye måter, og driver frem nye forsikringsmodeller (Datatilsynet og Teknologirådet, 2017). Med wearables vil forsikringsselskapene ha mulighet til å samle inn detaljert informasjon om sine kunders atferd, og dette gjør det mulig å beregne enkeltindividers risiko mer nøyaktig. Slik kan forsikringsselskapene i større grad tilpasse forsikringspremien til hver enkelt forsikringstaker. Da vil det ikke lenger være det samme behovet for å dele en gruppes totale risiko likt mellom medlemmene.

2.5.2 Helseforsikring

Helseforsikring er en type personforsikring som sikrer rask behandling ved sykdom (Storebrand, 2017). Storebrands helseforsikring garanterer spesialistbehandling innen 14 dager, og man kan unngå ventetid i offentlige helsekøer. I følge data fra Finans Norge (2016) hadde over en halv million nordmenn helseforsikring i 2016. Dette er en økning på fem prosent fra året før. De fleste som har helseforsikring får denne betalt av arbeidsgiver som et gode på lik linje med mobiltelefon og trening (Grymer & Strønen, 2016).

Det eksisterer delte holdninger til helseforsikring i det norske samfunnet. Forsikringsselskapene fokuserer på de positive aspektene ved forsikringen, og argumenterer for at man med en slik forsikring kommer raskere tilbake til hverdagen hvis man blir syk eller skadet (Storebrand, 2017). Andre mener derimot at helseforsikring er uheldig, fordi det skaper et klasseskille. Marte Gerhardsen, leder i Agenda, argumenterer for eksempel for at veksten i private helseforsikringer bidrar til å skape et todelt helsevesen (Dagens Næringsliv, 2016). Hun hevder dette fører til at de mest ressurssterke får bedre tilgang på nødvendig helsehjelp, og kan snike i offentlige helsekøer. Det kan derfor stilles spørsmål ved om private helseforsikringer utfordrer

den politiske tankegangen om at alle skal ha lik tilgang til helsetjenester. Dette vil være interessant å se nærmere på i forbindelse med aksepten av persontilpassede helseforsikringer i Norge.

2.5.3 Omdømme og tillit i forsikring

Forsikringsbransjen er et system som er bygget opp rundt fellesskap, ærlighet og tillit (Finans Norge, 2017a). Finans- og forsikringsbransjen er avhengig av at kundene har tillit til dem, både for å beholde eksisterende kunder, men også for å tiltrekke seg nye. Hvis forsikringsselskaper nå går inn for å persontilpasse forsikringer, vil dette innebære innsamling av store mengder personopplysninger. Lekkasje eller misbruk av disse kan føre til svekket tillit og tap av omdømme for forsikringsselskapene (Datatilsynet, 2015).

I Ciscos årlige IT-sikkerhetsrapport fra 2016 kommer det frem at 29 prosent av virksomhetene de spurte³ opplevde svikt i sin omsetning som følge av brudd på IT-sikkerhet (Cisco, 2017). Videre viser de til at 22 prosent av disse virksomhetene også tapte kunder. Tor Bang, førsteamanuensis ved Handelshøyskolen BI, påpeker at omdømme er et av en organisasjons viktigste særtrekk, og at både dette og organisasjonens lønnsomhet kan tape seg ved brudd på IT-sikkerheten (Eidem, 2017). IT-sikkerhet og ivaretagelse av personvern er altså sentrale faktorer som kan påvirke tillitsforhold med kunder, omdømme og lønnsomhet hos en bedrift. Dette vil være viktig for vår diskusjon om aksepten av persontilpassede helseforsikringer.

2.5.4 Bruk av wearables i helseforsikringer

For å forstå hvordan en persontilpasset helseforsikring vil kunne se ut i Norge, vil vi i det følgende presentere forsikringsmodellen VitalityHealth.

Innledningsvis så vi at det er en amerikansk trend at forsikringsselskaper inngår avtaler med produsenter av wearables, og tilbyr persontilpassede programmer for helseforsikring. Det globale forsikringsselskapet Discovery har gjort en slik løsning tilgjengelig i Europa (Vitality Corporate Services Limited, 2017a). De introduserte i 2014 forsikringsprogrammene *VitalityHealth* og *VitalityLife* i Storbritannia.

³ Studien hadde 2900 respondenter fordelt på 13 land (Cisco, 2017, s. 49).

VitalityHealth er Vitalitys helseforsikring, som tilbyr kundene goder gjennom et bonusprogram hvis de holder seg aktive og overvåker sin aktivitet (Vitality Corporate Services Limited, 2017b). Gjennom aktiviteter som løping, gåing, sykling og svømming kan forsikringstakerne tjene opp poeng, som registreres ved bruk av en wearable. Disse poengene kan brukes til å få rabatter hos Vitalitys mange samarbeidspartnere, som flyselskaper, hotellkjeder, treningsentre eller matleverandører (Vitality Corporate Services Limited, 2017c).

Vitality ønsker altså å motivere sine kunder til en sunnere livsstil gjennom sitt belønningssystem som omfattes av et stort nettverk av partnere. Forsikringsmodellen dreies rundt prinsippet om belønning, og Vitality straffer ikke kundene dersom de ikke er i aktivitet. De gir heller ikke en redusert pris på selve forsikringspremien, men en belønning i form av andre goder.

Forsikringsmodeller som belønner sine kunder for å være aktive har spredd seg til flere land i Europa. Forsikringsgiganten Generali Group har blant annet fått eksklusive rettigheter til å bruke Discovery's Vitality-program i sine forsikringer i kontinental-Europa, hvor de per i dag tilbyr programmet i både Tyskland og Frankrike (The Generali Group, 2016). Interessen rundt en slik forsikringsmodell ser altså ut til å øke blant de europeiske landene, og varianter har nylig også blitt lansert i Norden. I Sverige introduserte for eksempel Moderna Försäkringar i 2016 landets første syke- og ulykkesforsikring med mulighet for rabatterte forsikringspremier basert på skrittelling (Moderna, 2016). Her kan man få mellom fem og 15 prosent rabatt, avhengig av hvor mange skritt man går daglig.

Når vi nå ser persontilpassede bilforsikringer i Norge, er det tydelig at en utvikling også er i ferd med å skje i den norske forsikringsbransjen.

2.6 Forbrukernes holdninger

I dette delkapitlet vil vi først ta for oss forbrukernes perspektiv på sensorbaserte forsikringsløsninger. Vi vil her presentere Datatilsynets personvernundersøkelse fra 2016, som gir kvantitative indikasjoner på forbrukernes holdninger til persontilpassede forsikringsprodukter i Norge. Deretter vil vi se på særtrekk ved norsk kultur, samt presentere den norske velferdsmodellen som kan ha implikasjoner for innføringen av persontilpassede forsikringsløsninger i Norge.

2.6.1 Datatilsynets personvernundersøkelse fra 2016

I november og desember 2016 ble det gjennomført en personvernundersøkelse på bestilling fra Datatilsynet (Datatilsynet og Teknologirådet, 2017). Undersøkelsen belyser forbrukernes holdninger til nye forsikringsmodeller basert på innsamling av persondata. Innsikt i forbrukernes holdninger vil være viktig for å få bedre forståelse for aksepten av persontilpassede helseforsikringer i Norge.

Undersøkelsen indikerer at forbrukerne generelt er skeptiske til at forsikringsselskaper samler inn sensordata til kommersielt bruk (Datatilsynet og Teknologirådet, 2017). På spørsmål om hvordan forbrukerne stiller seg til innsamling av data om atferd og hverdagsliv for å beregne forsikringspremier, var 69 prosent negative. Den totale andelen negative ble redusert til 63 prosent da man i spørsmålet inkluderte at forsikringspremien ble *vesentlig* lavere.

Folk ble også spurt spesifikt om hvordan de stilte seg til bruk av kjøredata for å kalkulere forsikringspremien på bilforsikring (Datatilsynet og Teknologirådet, 2017). Her var andelen negative og positive cirka like store, på rundt 40 prosent. På samme type spørsmål om prisberegning på livs- eller uføreforsikring ut ifra helsedata var 64 prosent negative, og 17 prosent positive. Folk var altså langt mer positive til å gi fra seg data om sin kjøring enn sin helse. 72 prosent var også negative på spørsmål om hvorvidt man ønsket at forsikringsselskapet skulle involvere seg i forbrukernes hverdagsliv, ved å for eksempel sende ut tekstmeldinger med livsstilstips. Kun ti prosent svarte at de var positive til dette.

2.6.2 Norsk kultur

Videre vil vi se på hvordan særtrekk ved norsk kultur kan bidra til å belyse forbrukernes holdninger til innsamling av persondata. Kultur er et begrep som kan brukes i mange sammenhenger (Schackt, 2016). Det refererer ofte til en samlebetegnelse for menneskers måte å tenke, kommunisere og oppføre seg på, og kan ha både en snever, utvidet og generell betydning. I vid forstand kan det referere til fellestrekk nordmenn deler i tilknytning til atferdsmønster, holdninger og verdier.

Ims (1992) trekker frem kulturelle forskjeller som sentralt for hvordan man forholder seg til å dele personopplysninger. Han refererer til at man i Vesten har et individualistisk selvbegrep⁴.

⁴ Selvbegrep forstås her som hvordan et individ oppfatter seg selv.

Dette innebærer at man anser hvert individ for å være et fritt og selvstendig menneske, og man er opptatt av å sikre den enkeltes rettigheter. Han mener at man i Vesten vil vegre seg mot at data om en selv deles, fordi dette kan virke påtrengende og som en trussel mot selvoppfattelsen. Frihet og ønsket om å leve sitt liv i fred står sterkt. Hvert individ skal kunne tenke fritt og ytre seg kritisk, og man har et svakt forhold til fellesskapet.

2.6.3 Den norske velferdsstaten

For å forstå om en persontilpasset helseforsikring vil bli akseptert i Norge, vil det også være naturlig å forklare hvordan den norske velferdsmodellen er bygget opp.

Kuhnle og Kildal (2011) definerer kjernen i begrepet om den skandinaviske velferdsstaten som at det eksisterer en kollektiv oppfatning og forventning om at det offentlige skal sikre sosial trygghet og likhet for alle. Dette gjelder spesielt med tanke på inntekt, helse og omsorg. Velferdsstaten er en sosial forsikring som tilbys borgerne for å gi dem økonomisk sikkerhet, dersom de for eksempel blir utsatt for sykdom eller arbeidsledighet (Christensen & Berg, 2017). Den norske modellen er omfattende, og et særtrekk ved denne er at den baserer seg på universelle velferdsrettigheter. Dette innebærer at alle borgere skal ha lik tilgang til offentlige tjenester som gratis utdanning og helsehjelp. Ideen om sosiale rettigheter, som betyr at alle har rett til et godt liv, er også et viktig aspekt ved velferdsstaten.

Velferdsstaten finansieres i all hovedsak gjennom offentlige skatter og avgifter. Ettersom de med høyere inntekt betaler mer skatt, har velferdsstaten en omfattende omfordelende rolle. Dette er en viktig årsak til at det er relativt lite inntektsforskjeller i Norge sammenlignet med andre land (Christensen & Berg, 2017).

Den skandinaviske velferdsstaten skiller seg klart fra de mer liberale velferdsmodellene som man finner i for eksempel USA (Christensen & Berg, 2017). Det amerikanske systemet baserer seg på at tjenestene man har krav på bestemmes ut i fra hvor mye man betaler. Skatteytelsene i de liberale velferdsmodellene er mer beskjedne enn de man finner i Norge, og dekker kun de aller fattigste. Det finnes for eksempel ingen gratis, offentlige helsetjenester i USA. Dette har resultert i at helseforsikring er essensielt for alle amerikanere.

Solidaritet i befolkningen er en grunnstein for at prinsippet om velferdsstaten i Norge skal fungere (Christensen & Berg, 2017). Dette innebærer at man anerkjenner en gjensidig

avhengighet mellom seg som borgere i et samfunn (Tjora & Skatvik, 2017). Et annet viktig moment for oppslutningen rundt velferdsmodellen er at de offentlige tjenestene benyttes av flertallet. For at dette skal være tilfelle må tjenestene som tilbys holde så høy standard at de som har muligheten til å benytte seg av et privat tilbud, ikke gjør det.

2.7 Oppsummering av litteraturen

Vi har i dette kapitlet prøvd å samle litteratur som kan gi økt forståelse for vår problemstilling. Vi har sett at det finnes mye informasjon om hvordan teknologisk utvikling åpner for nye muligheter i forsikringsnæringen. Bruk av persondata til analyseformål og persontilpasning av tjenester er noe som blir stadig mer populært, og driver utviklingen av forsikringsmodeller i helt nye retninger. Det finnes mye litteratur om hvordan wearables brukes til å persontilpasse forsikringer i utlandet, og vi har fått god forståelse for bruksområdet til wearables, samt den voksende oppslutningen om disse produktene både på verdensbasis og i Norge.

Videre har vi samlet litteratur om utfordringer tilknyttet personvern og informasjonssikkerhet som kommer med den teknologiske utviklingen. Dette har vi prøvd å sette i sammenheng med sentrale personvernprinsipper den norske personvernloven bygger på. Vi har også dannet oss et bilde av endringene som kommer med den nye personvernforordningen i 2018, og implikasjonene dette kan ha for mulighetene til å behandle personopplysninger i forsikringsbransjen.

For å forstå konsekvensene av en persontilpasning innenfor helseforsikring, har vi også samlet litteratur som berører det overordnede temaet forsikring. Her har vi belyst de grunnleggende prinsippene tradisjonell forsikring bygger på, og sett nærmere på hva en helseforsikring i Norge i dag innebærer. Vi har også sett på betydningen av omdømme og tillit i forsikringsbransjen, samt introdusert forsikringsmodellen VitalityHealth.

Til slutt har vi presentert litteratur som kan bidra til å gi innsikt i norske forbrukeres holdninger til å gi fra seg personopplysninger. Her har vi tatt for oss resultater fra Datatilsynets personvernundersøkelse fra 2016, samt sett på særtrekk ved norsk kultur, og karakteristika ved den norske velferdsstaten.

Totalt sett har vi i dette kapitlet altså samlet litteratur som belyser flere aspekter som kan ha betydning for om en persontilpasset helseforsikring kommer til å bli akseptert i Norge.

3. Modell og forskningsspørsmål

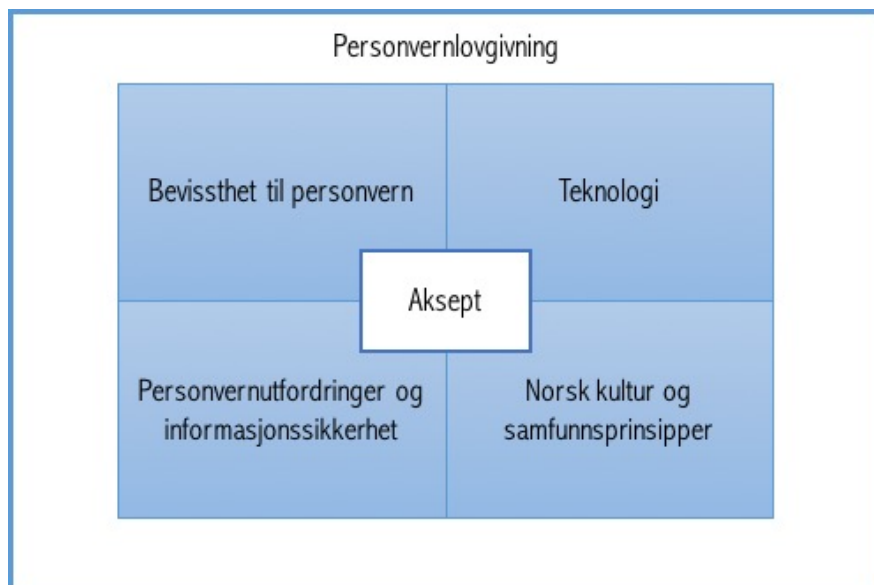
Vi har sett at det foreligger en del litteratur om temaet knyttet til bruk av wearables i helseforsikring, men vi har ikke funnet et tilfredsstillende rammeverk som kan brukes til å belyse vår problemstilling i ønsket grad. Problemet vårt er relativt komplekst og nytt, og mye tyder på at det er flere faktorer som kan være avgjørende for at en persontilpasset helseforsikring blir akseptert i Norge. Vi har derfor med utgangspunkt i litteraturkapitlet utarbeidet en modell som skal hjelpe oss å utforske vår problemstilling. Denne modellen legger grunnlag for hva slags data vi ønsker å samle inn, og vi håper med dette å kunne gi økt innsikt på feltet som omhandler persontilpassede helseforsikringer i Norge. I tillegg håper vi på å legge til rette for videre forskning. I det følgende vil vi presentere modellen med tilhørende begrepsavklaringer, og forklare våre fem avledede forskningsspørsmål.

Som det fremgår i vår problemstilling ønsker vi å utforske hva som vil være avgjørende for om en persontilpasset helseforsikring aksepteres i Norge. Vi har avgrenset oss til å ta for oss hva som skjer i det norske markedet, hvor vi ser på markedet som arenaen for kjøp og salg av forsikringsprodukter. Vi antar at det forsikringselskapene velger å tilby avhenger av det som aksepteres i markedet.

Videre legger vi til grunn at det som aksepteres først og fremst vil avhenge av det *myndighetene tillater*. Med dette antar vi at myndighetene legger føringer for forsikringselskapenes juridiske handlingsrom, og følgelig hva de har lov til å tilby. I denne studien defineres det juridiske handlingsrommet av personvernlovgivningen. Vi har fått inntrykk av at det etter dagens lovgivning vil være vanskelig for forsikringselskaper å tilby en persontilpasset helseforsikring. Vi tror dermed at den nye personvernforordningen vil være svært avgjørende for hvordan forsikringselskapene kan operere fremover. Derfor har vi valgt å visualisere lovgivningen som den ytterste faktoren i modellen.

Videre tror vi at selv om det juridisk sett er mulig å tilby et produkt, er det ikke nødvendigvis gitt at det aksepteres av forbrukerne, og dermed vil etterspørres. Derfor antar vi også at det er flere faktorer som påvirker hva som aksepteres, og følgelig hva forsikringselskapene velger å tilby. Med bakgrunn i litteraturen har vi valgt å se nærmere på fire faktorer, som vi har valgt å definere som følger: *bevissthet til personvern, teknologi, personvernutfordringer og*

informasjonssikkerhet og norsk kultur og samfunnsprinsipper. Vi vil i det følgende forklare faktorene og forholdene mellom dem nærmere.



Figur 2: Modell

Personvernlovgivningen

Det første forholdet vi ønsker å utforske er hvilke konsekvenser den nye personvernforordningen vil ha for om forsikringsselskapene har mulighet til å tilby persontilpassede forsikringer. Vi antar at den nye lovgivningen legger føringer for hva forsikringsselskaper har lov å gjøre, og på denne måten påvirker deres handlingsrom. Som vi har sett innføres det nye plikter for virksomheter som behandler personopplysninger, og kravene til å ivareta folks personvern skjerpes. Samtidig mener noen at mulighetsrommet for å tilby persontilpassede tjenester vil utvides. Det eksisterer også usikkerhet knyttet til hvordan finansnæringen vil bli regulert når den nye personvernlovgivningen implementeres. Vi har av dette utledet vårt første forskningsspørsmål:

Forskningsspørsmål 1: *Hvordan vil den nye personvernlovgivningen påvirke det juridiske handlingsrommet norske forsikringsselskaper har til å tilby persontilpassede helseforsikringer?*

Bevissthet til personvern

Den andre faktoren vi ønsker å se nærmere på er forbrukernes bevissthet til personvern. Vi har sett at forbrukernes holdninger til å dele personopplysninger med forsikringsselskaper belyses

i Datatilsynets personvernundersøkelse fra 2016. Vi tror at det eksisterer en sammenheng mellom forbrukernes bevissthet til personvern og disse holdningene, og at dette er noe som kan ha innvirkning på aksepten av persontilpassede helseforsikringer i Norge. Videre ser det ut til at den nye personvernlovgivningen vil kunne påvirke forbrukernes bevissthet til personvern, gjennom nye rettigheter. Vi ønsker derfor å utforske dette forholdet nærmere, og se på hvilken betydning det vil ha for aksepten av persontilpassede helseforsikringer. Av dette følger vårt andre forskningsspørsmål:

Forskningsspørsmål 2: *Hvordan vil den nye personvernlovgivningen påvirke forbrukernes bevissthet til personvern, og følgelig aksepten av persontilpassede helseforsikringer?*

Teknologi

Den tredje faktoren vi vil ta for oss er teknologi. Vi har sett at det med digitalisering og teknologisk utvikling åpner seg nye muligheter for datainnsamling og persontilpasning av tjenester. Internet of Things og wearables overføres stadig til nye bruksområder, og med dette kommer det både fordeler og ulemper. Blant fordelene tror vi wearables har et potensial til å skape verdi som kan virke positivt på aksepten av persontilpassede helseforsikringer. Med *verdiskapning* i denne sammenheng refererer vi til de samfunnsmessige, organisatoriske og individuelle gevinstene som kommer med bruken av wearables. For samfunnet tenker vi på mulighetene wearable-teknologi for eksempel gir til økt velferd og forbedret folkehelse. Det organisatoriske perspektivet er knyttet til forsikringsselskapers reduserte skadekostnad og økte lønnsomhet som følge av å bruke wearables i forsikring. For individer vil bruk av wearables kunne bidra til en sunnere livsstil, motivere til aktivitet, og eventuelt gi en billigere forsikringspremie.

Selv om ny teknologi aksepteres for ett bruksområde, er det ikke gitt at den passer like godt for et annet. Vi ønsker derfor å se nærmere på forholdet mellom wearable-teknologi og helseforsikring, og hvilket potensial denne teknologien har til å bli akseptert for et slikt bruksområde i Norge. Dette leder oss til vårt tredje forskningsspørsmål:

Forskningsspørsmål 3: *Hvilket potensial har wearable-teknologi til å skape aksept av persontilpassede helseforsikringer i Norge?*

Personvernutfordringer og informasjonssikkerhet

Den neste faktoren vi ønsker å se nærmere på er personvernutfordringer og informasjonssikkerhet. Vi har sett at det med digitalisering og bruken av wearable-teknologi følger en rekke utfordringer knyttet til personvern og informasjonssikkerhet. Vi vil derfor utforske om dette kan ha en påvirkning på aksepten av persontilpassede helseforsikringer i Norge. Dette leder oss til vårt fjerde forskningsspørsmål:

***Forskningsspørsmål 4:** I hvilken grad vil utfordringer knyttet til personvern og informasjonssikkerhet være avgjørende for om persontilpassede helseforsikringer vil aksepteres i Norge?*

Norsk kultur og samfunnsprinsipper

Den siste faktoren vi ønsker å ta for oss er norsk kultur og samfunnsprinsipper. Med norsk kultur benytter vi oss av kulturbegrepet i vid forstand, hvor vi refererer til fellestrekk nordmenn deler i tilknytning til atferdsmønster, holdninger og verdier. I begrepet samfunnsprinsipper legger vi til grunn verdier som er sentrale for den norske velferdsstaten, slik som trygghet og like rettigheter for alle borgere. Vi ønsker med dette å se nærmere på om det eksisterer særtrekk ved norsk kultur og norske samfunnsprinsipper som kan ha betydning for aksepten av persontilpassede helseforsikringer i Norge. Av dette har vi utledet et siste forskningsspørsmål:

***Forskningsspørsmål 5:** I hvilken grad vil norsk kultur og samfunnsprinsipper påvirke om persontilpassede helseforsikringer vil aksepteres i Norge?*

4. Metode og datainnsamling

I den følgende delen vil vi presentere og redegjøre for valg av forskningsmetoder vi har brukt i vår studie. Vi vil gå gjennom forskningstilnærming og -design, metodevalg og datainnsamling. Videre følger begrunnelse for datautvalget, samt en detaljert intervjuguide. Til slutt vil vi evaluere validitet og reliabilitet i våre data.

4.1 Forskningsdesign

Forskningsdesignet er rammeverket for hvordan man samler inn og analyserer data for å besvare problemstillingen (Saunders, Lewis, & Thornhill, 2012). Formålet med vår studie er å utforske hvordan bruk av wearables og sensordata vil utfordre personvernet i forsikringsbransjen. Når man ønsker å utvikle bedre forståelse for et tema der det fra før er lite innsikt, er en vanlig forskningsstrategi en eksplorativ tilnærming. Med det menes det at vår problemstilling stiller et åpent spørsmål der vi er usikre på sakens faktiske natur. Samtidig ønsker vi å beskrive hva som konkret skjer på feltet, hvilket impliserer at studien også til en viss grad er deskriptiv.

4.2 Forskningstilnærming

I valg av forskningstilnærming kan man velge mellom en induktiv og deduktiv tilnærming. Sistnevnte søker å forklare et kausalt forhold mellom variabler, gjennom utviklingen av hypoteser, der data brukes til å bekrefte eller avkrefte dette forholdet (Saunders et al., 2012). En induktiv tilnærming brukes når det foreligger mindre informasjon på feltet, der data brukes til å utvikle teoretiske forklaringer. I denne oppgaven ønsker vi å samle inn data for å skape forståelse for om bruk av wearables i persontilpassede helseforsikring vil bli implementert og akseptert i det norske markedet. En innledende litteraturstudie har gitt indikasjoner på at dette er en forsikringsmodell utenlandske forsikringsselskaper har begynt å benytte seg av. Samtidig ser vi at EUs nye personvernforordning legger rammer for hvordan persondata vil kunne anvendes av organisasjoner i fremtiden. Ved bruk av primær- og sekundærdata ønsker vi å gi ny innsikt på dette området, og benytter oss dermed av en induktiv forskningstilnærming (Saunders et al., 2012).

4.3 Valg av metode

Når det gjelder valg av metode for innsamling av data, skilles det vanligvis mellom kvalitativ og kvantitativ forskning. Kvalitativ forskning søker å forstå meninger, definisjoner, karakteristikk og metaforer (Berg & Lune, 2012), og brukes til å tolke og forstå subjektive oppfatninger om det fenomenet som studeres (Saunders et al., 2012). Kvantitativ forskning på sin side ser på forholdene mellom forhåndsbestemte variabler, og måler dette numerisk gjennom statistisk analyse. Ettersom vår studie er eksplorativ og vi har hatt et ønske om å tilegne oss dybdeinnsikt i et spesifikt tema, impliserer dette at en kvalitativ metode er best egnet for vår datainnsamling. Vi har derfor valgt å samle inn data gjennom semistrukturerte intervjuer, og valgt intervjupersoner med antatt spisskompetanse på området. Dette har gitt oss muligheten til å se problemstillingen fra flere forskjellige vinkler. I tillegg til intervjuer har vi brukt personvernundersøkelsen gjennomført av Datatilsynet i 2016 til å belyse forbrukernes holdninger til persontilpassede forsikringer. Dette er kvantitative sekundærdata. Da vi bruker både kvalitative og kvantitative data, kan det derfor sies at vi har en mikset metode for datainnsamling (Saunders et al., 2012).

4.4 Forskningsstrategi

Forskningsstrategi kan beskrives som en plan for hvordan en ønsker å besvare problemstillingen (Saunders et al., 2012). Det finnes mange forskjellige forskningsstrategier å velge mellom. Hvilken man velger bestemmes ut ifra problemstilling, hvilket formål man har med forskningen, eksisterende kunnskap på feltet og hva slags ressurser man har tilgjengelig. Vårt forskningsprosjekt er en casestudie. En casestudie kan kjennetegnes ved at man utforsker et spesielt fenomen eller en hendelse innenfor en gitt kontekst. Yin (2009, referert i Saunders et al., 2012, s. 179-180) skiller mellom fire forskjellige typer casestudier. Dette er enkel versus multipl case, og hver av disse kan enten bestå av én eller flere analyseenheter. Vår studie er en enkeltcasestudie, der vi ønsker å få innsikt i hva som skjer på forsikringsmarkedet i Norge som følge av personvernlovgivningen og teknologisk utvikling. For å besvare problemstillingen har vi samlet inn data fra fem forskjellige kilder: Storebrand, Datatilsynet, Justis- og Beredskapsdepartementet (heretter Justisdepartementet), Finans Norge, og personvernundersøkelsen. Dette impliserer at vi har en enkeltcasestudie med flere analyseenheter.

4.5 Innsamling av data

4.5.1 Intervju

Da vår forskning er en eksplorativ studie, fant vi at semistrukturerte intervjuer ville være den mest hensiktsmessige måten å samle inn primærdata. Denne intervjuformen har gitt oss muligheten til å legge større eller mindre vekt på temaer underveis, og stille oppfølgingsspørsmål om emner vi fant ekstra interessante eller viktige (Saunders et al., 2012). Samtidig lot det oss beholde en viss struktur i intervjuene. Intervjuformen åpnet også for at vi kunne endre og tilpasse intervjuene avhengig av hvem vi snakket med og etter hvert som forskningen utviklet seg. På denne måten har vi prøvd å få frem de forskjellige perspektivene hver intervjudeltaker hadde å tilby.

4.5.2 Utvalg

For å kartlegge hvem vi ønsket å intervjuer, tok vi utgangspunkt i boken *Informasjonsetikk i Praksis – Datasikkerhet og Personvern* (Ims, 1992). Ims beskriver interessekonfliktene og interessesammenfallene som oppstår mellom stat, enkeltperson og organisasjon som sentrale i diskusjonen om personvern. Det oppstår særlig friksjon knyttet til motsetningene mellom interessentene når det gjelder innsamlingen, lagringen og behandlingen av personopplysninger. I tillegg eksisterer det et avhengighetsforhold mellom disse tre interessentene, samtidig som hver interessent har sitt eget mandat som hovedprioritet. I vår studie vil eksempelvis forsikringsselskapet ønske å maksimere profitt, forbrukerne vil ha diskresjon rundt og korrekthet i opplysninger om dem, og myndighetene søker å minimalisere kriminalitet, og fremme økonomisk rettferdighet gjennom transparens. Ettersom personvern, informasjonssikkerhet og behandling av personopplysninger er viktige aspekter som inngår i vår studie, fant vi det derfor relevant å velge intervjupersoner som kunne belyse perspektivene til de tre interessentene nevnt av Ims (1992).

For å belyse organisasjonens perspektiv brukte vi forsikringsselskapet Storebrand. Vi har vært i kontakt med dem tidligere angående masterutredningen, og ble henvist av vår kontaktperson til de personene som var mest aktuelle å intervjuer for vår problemstilling. I tillegg ønsket vi å intervjuer Finans Norge, som er hovedorganisasjonen for finansnæringen i Norge (Finans Norge, 2017b). De ønsker å være en brobygger mellom næringen og de som setter næringens rammebetingelser, og er derfor en god kilde til informasjon om hvordan finansnæringen generelt påvirkes av og stiller seg til personvern og utviklingen av sensorbaserte forsikringer.

For å belyse myndighetenes perspektiv brukte vi Datatilsynet og Justisdepartementet. Justisdepartementet har ansvar for lovarbeid (Justis- og Beredskapsdepartementet, 2017), og vi ønsket å kontakte dem for å få noen oppklaringer i de juridiske rammene som personvernlovgivningen setter i dag, og hvordan det vil bli med den nye forordningen. Videre anså vi Datatilsynet som aktuelle å intervju, fordi de har som mandat å sørge for at personopplysningsloven overholdes, samt at opplysninger om enkeltpersoner brukes riktig (Datatilsynet, 2017g). For å belyse forbrukernes holdninger knyttet til persontilpassede forsikringsløsninger har vi benyttet oss av Datatilsynets personvernundersøkelse fra 2016. Resultatene fra denne er beskrevet i kapittel 2.6.1.

Verken Datatilsynet, Finans Norge eller Justisdepartementet hadde vi tidligere hatt kontakt med. Vi sendte derfor først en forespørsel på mail til organisasjonene der vi la frem vår problemstilling og ønske om intervju. De kom tilbake til oss med aktuelle intervjukandidater som vi avtalte tidspunkt med. Denne typen nøye utvelgelse av respondenter kalles å bruke et målrettet utvalg, og er vanlig når man bruker en liten utvalgsgruppe (Saunders et al., 2012). Vårt utvalg er basert på å få mest mulig variasjon i datainnsamlingen ved å intervju et så vidt spekter av interessentene som mulig.

På bakgrunn av dette endte vi opp med totalt åtte intervjupersoner fra Datatilsynet, Storebrand, Finans Norge og Justisdepartementet. En oversikt med stilling og hvordan de er henvist til i resultater og analysen følger i tabell 1.

Organisasjon	Stilling	Initialer brukt i resultater og diskusjon
Datatilsynet	Juridisk saksbehandler	A.A.
	Person i ledende posisjon	B.B.
Storebrand	Forretningsutvikler	C.C.
	Rådgiver	D.D.
	Person i ledende posisjon	E.E.
Finans Norge	Juridisk rådgiver	F.F.
	Person i ledende posisjon	G.G.
Justisdepartementet	Rådgiver	H.H.

Tabell 1: Oversikt over intervjupersoner

Som nevnt har vi i tillegg til å gjennomføre intervjuer brukt Datatilsynets personvernundersøkelse fra 2016 som et supplement til intervjuene. Fordelen med å bruke denne undersøkelsen er at den gir oss gode indikasjoner på forbrukernes perspektiver, uten at vi har måttet bruke store ressurser på å gjennomføre en lignende undersøkelse selv (Saunders et al., 2012). Potensielle trusler til sekundærdatas gyldighet diskuteres nærmere i kapittel 4.7.1.

Ettersom vi vet intervjupersonenes identitet og dermed har vært i besittelse av sensitive personopplysninger, har vi sendt inn meldeskjema til NSD⁵.

4.5.3 Intervjuguide

For å forberede oss til og gjennomføre intervjuene utformet vi en intervjuguide⁶ til hver av intervjudeltakerne. En intervjuguide legger rammer for hvilke temaer som skal tas opp i intervjuet, og har en løs struktur, slik at man kan gå nærmere inn på emner som dukker opp underveis (Grønmo, 2004). Vi tok utgangspunkt i litteraturen og våre forskningsspørsmål for å finne ut hva slags informasjon vi ønsket å innhente. Ettersom vi ønsket å avdekke ulike perspektiver fra hver av interessentene med hensyn til deres kompetanseområde, ble intervjuguidene noe forskjellig utformet for hvert intervju. Temaet som omhandlet den nye personlovgivningen ble for eksempel spesielt sentralt for intervjuet med Datatilsynet, mens utviklingen av nye forsikringsmodeller var mer relevant for intervjuet med Storebrand.

Det er viktig at spørsmålene man stiller under intervjuene er åpne, slik at man oppfordrer deltakerne til å reflektere og utdype svarene sine (Johannessen, Christoffersen, & Tuftes, 2011). Samtidig må de være presise. Et eksempel på et spørsmål vi stilte Datatilsynet er «*Hvilke personvernutfordringer mener dere er viktigst i vurderingen av å innføre en persontilpasset helseforsikring?*». På denne måten ga vi uttrykk for hva vi konkret ville ha svar på, samtidig som vi åpnet for refleksjon hos intervjupersonene.

4.5.4. Gjennomføring av intervjuer

Vi opplevde det som uproblematisk å avtale tidspunkt for intervjuene da vi tidlig opprettet kontakt med de aktuelle intervjupersonene, og kunne planlegge møtene lenge i forveien. Alle intervjuene ble gjennomført i Oslo i intervjupersonenes lokaler, med unntak av intervjuet med

⁵ Tilbakemelding fra NSD er vedlagt i kapittel 9.1.

⁶ Intervjuguidene er vedlagt i kapittel 9.2.

rådgiveren i Justisdepartementet som ble gjort per telefon. Vi opplevde det ikke som en ulempe at dette intervjuet ikke ble gjennomført ansikt-til-ansikt og følte vi fikk den informasjonen vi trengte. En grunn til dette kan ha vært at vi sendte representanten en veiledende temaoversikt i forkant, slik at han hadde mulighet til å tenke gjennom spørsmålene på forhånd.

Vi gjennomførte kun ett intervju per organisasjon, med alle intervjupersonene fra den aktuelle organisasjonen til stede samtidig. En fare ved en slik gjennomføring er at intervjupersonene ikke tør å være helt åpne under intervjuet fordi det er andre til stede (Saunders et al., 2012). I vårt tilfelle var vi ikke ute etter å avdekke sensitive opplysninger om hver enkelt intervjuperson, og så det derfor heller som en fordel at de kunne utnytte hverandres kunnskap og spille videre på poenger som ble trukket frem underveis i intervjuet.

I forkant av intervjuet sendte vi som nevnt intervjudeltakerne en temaoversikt, slik at de kunne ha mulighet til å forberede seg. Dette gjorde at intervjupersonene kunne føle seg trygge på det de skulle snakke om, og at samtalene fikk god flyt. I tillegg bidro det til at intervjupersonene kunne lede samtalen slik de ville, samtidig som at vi fikk dekket de temaene vi ønsket. Før intervjuet startet spurte vi også om det var greit at vi brukte lydopptaker. Alle intervjupersonene godtok dette. På denne måten kunne vi konsentrere oss fullt om hva som ble sagt, samt stille oppfølgingsspørsmål til poengene som ble trukket frem.

4.6 Metode for analyse av data

Intervjuene foregikk over tre dager, og vi satt igjen med totalt fire lengre intervjuer å transkribere fra lydopptak. Transkriberingen gjorde vi dagen etter at intervjuene var gjennomført. På denne måten hadde vi de umiddelbare inntrykkene fortsatt klart for oss og kunne få ut all nødvendig informasjon fra intervjuene, slik som tonefall og ikke-verbal kommunikasjon. De transkriberte intervjuene ble lagret som separate Word-dokumenter, med anonymiserte filnavn. Opptakene ble slettet etter studiens slutt.

Etter at vi hadde transkribert intervjuene kunne vi starte med kategorisering av dataene. Dette tillot oss å sile ut informasjon som ikke var relevant for å besvare problemstillingen. Hvordan man velger å analysere datamaterialet vil komme an på hvilken forskningstilnærming man har valgt (Saunders et al., 2012). Vi har en induktiv tilnærming med et element av deduksjon. Dette reflekteres i hvordan vi kategoriserte dataene. Når man kategoriserer kan man enten ta utgangspunkt i teorien, dette kalles konseptdrevet kategorisering, eller man kan ta utgangspunkt

i kategorier som man finner i dataene. Sistnevnte kalles datadrevet kategorisering, som vi hovedsakelig benyttet oss av.

Da transkriberingen var gjennomført satt vi igjen med store mengder ustrukturerte data. Første ledd i analyseringen av dataene var derfor å systematisere informasjonen (Saunders et al., 2012). For å gjøre dette benyttet vi oss av konseptdrevet kategorisering, hvor vi tok utgangspunkt i intervjuguiden. Dette var en praktisk måte å komme i gang på, og for å kontrollere at de mest sentrale emnene fra litteraturen ble dekket. Ettersom intervjuene var semistrukturerte, krevde dette at vi måtte gå dypere inn i datamaterialet og vi ga derfor hvert sitat en overskrift som kort refererte til hva det handlet om.

Etter å ha laget en systematisk oversikt over datamaterialet, satt vi igjen med rundt 70 forskjellige overskrifter som representerte relevante sitater. Disse overskriftene ble lagt inn i et Excel-skjema. Vi gikk deretter over til en datadrevet kategorisering. Dette gjorde vi ved å sammenstille overskrifter som vi mente omhandlet det samme undertemaet, og tildelte disse temaene tallkoder. Antall kategorier ble da redusert til rundt 40. Denne prosessen fortsatte vi med til vi ble sittende igjen med syv hovedkategorier. Disse ble oppsummert til fire overskrifter som ga grunnlag for fremstilling av resultatene i kapittel 5. Metoden vi brukte var tidkrevende, men ga oss en strukturert forståelse for dataene, og var essensiell for da vi videre skulle presentere resultatene og analysere disse opp mot modellen.

4.7 Evaluering av data og forskningsdesign

Vi har tatt utgangspunkt i kriteriene reliabilitet og validitet for å sikre at våre innsamlede data reflekterer faktiske forhold.

4.7.1 Validitet

Validitet refererer til dataens gyldighet og relevans for å kunne besvare det fenomenet man ønsker å utforske (Johannessen et al., 2011). Man skiller mellom intern og ekstern validitet. Først vil vi diskutere denne studiens interne validitet og deretter den eksterne validiteten.

Intern validitet handler om man klarer å måle det man ønsker å måle og om studien produserer troverdige resultater (Johannessen et al., 2011). I vår studie har vi gjort flere tiltak for å sikre så høy grad av intern validitet som mulig. Med datainnsamling gjennom semistrukturerte

intervjuer, kunne vi etterprøve svarene og stille oppfølgingsspørsmål dersom noe var uklart. Vi hadde også mulighet til å stille oppklarende spørsmål i etterkant av intervjuet dersom dette var nødvendig. Dette bidro til at vi fikk samlet inn tilstrekkelig informasjon til å dekke hvert tema.

I forkant av datainnsamlingen sørget vi for å ha lest oss godt opp på fenomenet vi har ønsket å undersøke og organisasjonene vi skulle ha intervju hos. Dette bidro til at vi visste *hva* vi burde spørre om for å kunne besvare problemstillingen, samt *hvordan* vi skulle formulere spørsmålene for å fange opp de nødvendige dataene. At vi leste oss godt opp på forhånd sikret også at vi hadde nok kompetanse til å kunne tolke meningsinnholdet i respondentenes svar på riktig måte. Da vi hadde ferdigstilt resultatene sendte vi dem i retur til intervjupersonene for respondentsjekk. Johannessen et al. (2011) forklarer at en slik tilbakeføring av resultatene kan styrke studiens troverdighet. Ingen sitater ble brukt uten at respondentene godkjente det, og på denne måten kunne vi bekrefte at vi hadde tolket utsagnene riktig.

Videre er våre intervjupersoner nøye utvalgt. Vi ønsket å sikre at de hadde mye kunnskap om og jobbet tett på det fenomenet vi har utforsket. I tillegg la vi vekt på å intervju folk med *ulik* kompetanse innenfor de forskjellige organisasjonene, for å kunne utforske de aktuelle temaene fra flere vinkler. For å styrke troverdigheten til våre resultater ytterligere, sendte vi intervjupersonene en temaoversikt i forkant av intervjuene. Dette tillot dem å forberede seg, samt sikret at de forstod hensikten med intervjuet, og kunne komme med spørsmål i forkant dersom noe var uklart.

Alle de overnevnte tiltakene har bidratt til å gi oss dybdeinnsikt om innføringen av persontilpassede helseforsikringer i Norge, og vi mener derfor denne studien har en høy grad av intern validitet.

Ekstern validitet i kvalitative studier refererer til hvorvidt studiens resultater er *overførbare* til lignende fenomener (Johannessen et al., 2011). Vi går nærmere inn på denne studiens overførbarhet under styrker og svakheter ved utredningen i kapittel 7.2.

I forbindelse med ekstern validitet, ønsker vi å vurdere hvorvidt resultatene fra Datatilsynets personvernundersøkelse fra 2016 kan overføres til vår studie, ettersom vi har brukt denne som en viktig sekundærkilde. Undersøkelsen ble ikke utført med hensikt å besvare vår problemstilling, og det er derfor viktig at vi er bevisste på at operasjonaliseringen av begrepene

i spørsmålene ikke nødvendigvis fanger opp det vi har ønsket å måle. Til tross for dette mener vi at undersøkelsen kan gi oss relativt gyldige indikasjoner på forbrukernes holdninger tilknyttet vår studie. Dette fordi noen av spørsmålene i undersøkelsen spesifikt har som formål å fange opp forbrukernes holdninger til innsamling av persondata til forsikringsformål. Det er akkurat det vi har hatt som formål å undersøke. Undersøkelsen ble også utført nylig i november 2016 (Datatilsynet og Teknologirådet, 2017), noe som styrker gyldigheten til denne i vår studie. Videre har undersøkelsen brukt et utvalg på 1001 respondenter (Datatilsynet og Teknologirådet, 2017). I følge Saunders et al. (2012) er dette et stort nok utvalg til å generalisere resultatene til Norges befolkning på rundt fem millioner mennesker. Dette styrker undersøkelsens eksterne validitet og gjør den anvendelig for å belyse forbrukernes holdninger i vår studie.

4.7.2 Reliabilitet

Reliabilitet refererer til hvorvidt en lignende studie ville avdekket de samme funnene, dersom den ble gjennomført på et annet tidspunkt og/eller med andre forskere (Saunders et al., 2012).

Marshall og Rossman (2006, referert til i Saunders, et al., s. 382) stiller seg kritiske til verdien av reliabilitet i semistrukturerte intervjuer. De argumenterer for at det er urealistisk å kunne replikere denne type forskning, og mener det vil undergrave muligheten til å kunne gå dypere i komplekse og dynamiske problemstillinger som slike intervjuer tillater. Samtidig foreslår Johannessen et al. (2011) at det er noen tiltak man kan iverksette for å sikre en viss grad av reliabilitet i kvalitativ forskning som vi har benyttet oss av. Vi har gitt en grundig presentasjon av bakgrunnen for vår utredning og en detaljert fremstilling av forskningsprosessen.

Reliabilitet for vår sekundærkilde kan vurderes ut ifra det vi vet om hvordan undersøkelsen ble gjennomført og av hvem. Personvernundersøkelsen fra 2016 ble gjort på bestilling av Datatilsynet. Datatilsynet er et norsk, uavhengig forvaltningsorgan administrativt underlagt Kommunal- og moderniseringsdepartementet (Datatilsynet, 2017g). Undersøkelsen ble gjennomført av Opinion AS, et markedsanalyse- og meningsmålingsbyrå (Datatilsynet og Teknologirådet, 2017). Da undersøkelsen er gjennomført og brukt av anerkjente organisasjoner antar vi at dataen som leveres er et pålitelig komplement våre primærdata.

4.7.3 Skjevheter

I semistrukturerte intervjuer kan det stilles spørsmål ved om det har oppstått skjevheter underveis i intervjuprosessen som kan ha påvirket påliteligheten til intervjupersonenes svar (Saunders et al., 2012). Skjevheter refererer til systematiske feil i menneskelig beslutningstaking (Kahneman, 2011). Under intervjuprosessen i en forskningsstudie kan slike skjevheter oppstå ved at for eksempel intervjuer blir oppfattet på en måte som leder intervjupersonen til å svare annerledes eller mer mangelfullt enn hva vedkommende ellers ville gjort (Saunders et al., 2012). Dette er spesielt en fare i semistrukturerte intervjuer, som særlig krever at intervjupersonen er villig til å forklare og utdype temaene som utforskes.

For å forhindre at slike skjevheter skulle oppstå gjorde vi flere tiltak. Vi var nøye med å informere om at all data som ble samlet inn ville holdes anonymt, at sensitiv informasjon ville forbli konfidensiell og at lydopptak skulle slettes når vi ikke lenger trengte de. Dette gjorde vi for at intervjupersonene skulle kunne snakke åpent om de temaene vi ønsket å belyse, uten å føle at de måtte holde noe tilbake. Det at tre av fire intervjuer ble holdt i intervjupersonenes lokaler bidro videre til at de kunne være komfortable under intervjuet.

Ved å sende ut temaoversikten på forhånd ga vi intervjupersonene mulighet til å tenke gjennom hva de ønsket å formidle i forkant av intervjuet. Dette mener vi bidro til å lage god flyt i samtalene, og at svarene vi fikk var gjennomtenkte. Vi opplyste også om at vi skulle sende intervjupersonene de ferdige resultatene for godkjenning før den endelige innleveringen av utredningen. Slik kunne de snakke friere, uten å frykte at de skulle bli fremstilt på en ugunstig måte. Med disse tiltakene mener vi å ha unngått de største farene for at skjevheter skulle oppstå i intervjuene, og har på denne måten sikret dataens pålitelighet.

5. Resultater og funn

I det følgende kapitlet vil vi presentere funn fra våre intervjuer. Her vil vi beskrive synspunkter som fremkommer av representantene A.A. og B.B. i Datatilsynet, C.C., D.D. og E.E. i Storebrand, F.F. og G.G. i Finans Norge, samt H.H. i Justisdepartementet. Vi har valgt å strukturere dette kapitlet på den måten vi mener gir den mest pålitelige gjengivelsen av intervjuene. Funnene er følgelig presentert under fire overordnede temaoverskrifter: *Teknologisk utvikling og bruk av wearables i forsikring, personvernutfordringer og informasjonssikkerhet, personvernlovgivningen og forbrukernes holdninger.*

5.1 Teknologisk utvikling og bruk av wearables i forsikring

5.1.1 Teknologisk utvikling

Teknologisk utvikling er et gjennomgående tema i intervjuene. Det første B.B. i Datatilsynet bemerker er at det kommer til å skje en stor utvikling i forsikringsmarkedet i årene fremover. Han belyser at Datatilsynet i årets personvernrapport har jobbet med å kartlegge folks holdninger til innsamling av personopplysninger, som stadig blir viktigere for tjenesteformål.

«Vi konstaterer at det er personopplysninger som er motoren i hele denne økonomien. At det er personopplysninger man trenger for å få segmentert markedet i tilstrekkelig grad.»

B.B. i Datatilsynet

C.C. i Storebrand understreker også at det skjer store teknologiske fremskritt innenfor forsikringsbransjen. Det som tradisjonelt har vært en gammeldags næring ser nå behovet for å fornye løsningene sine og måten man samhandler med kundene på. Hun påpeker at teknologi kan skape økt konkurranse, men også åpner for nye muligheter på tvers av sektorer.

«Enten kan man se på det som at andre aktører kommer inn og ødelegger, eller så kan man se på det som at vi går over i økosystemer der man er partnere og sammen tilbyr en komplett tjeneste til kunden.»

C.C. i Storebrand

Det skjer særlig en stor digital utvikling innenfor helsesektoren. E.E. i Storebrand forteller at noe som vitner om dette er nye nisjeprodukter, slik som helseklokken Contact fra ContinYou. Lignende produkter utvikles innenfor for eksempel diabetes, hjerte- og karsykdommer eller luftveisproblemer. I tillegg ble en oversikt over hjertestartere i Norge nylig lansert. E.E. argumenterer for at denne kan bidra til å redusere dødsraten relatert til hjerteårsaker, og var noe Storebrand tenkte på å legge inn i sin egen mobilapplikasjon for et år siden. I dette tilfellet er det ikke teknologien som har vært avgjørende – en slik oversikt har vært tilgjengelig i Danmark lenge – men heller Datatilsynets restriksjoner på bruken av posisjonsdata. D.D. i Storebrand poengterer videre at Datatilsynet må bidra og være en muliggjører for digitalisering i norsk næringsliv, også av samfunnsmessige hensyn.

«Det er så mange syke, så mange liv som kan reddes med digitale løsninger, men som man ikke kan ta i bruk fordi det er strengt personvernmessig.»

E.E. i Storebrand

5.1.2 Sensorbaserte forsikringsløsninger og wearables

I det følgende vil vi beskrive hvilke tanker representantene fra Storebrand har rundt wearables og sensorbaserte forsikringsløsninger, og hvordan utviklingen ligger an i Norge. D.D. forteller at Storebrand i samarbeid med Rema 1000 var de første på det norske markedet til å tilby en sensorbasert forsikring. Hun poengterer at man som kunde av Rema Forsikring kjøper et forsikringsprodukt som driftes av Storebrand. Det innebærer at Storebrand behandler og har ansvar for alle personopplysninger. Lansering av Rema Forsikring har vært en måte for dem å forsiktig prøve seg med sensorbaserte forsikringer. E.E. bekrefter at de også har vært inne på tanken om å lansere en sensorbasert helseforsikring, med utgangspunkt i skrittelling som aktivitetsmål. Rasjonaliseringen bak forsikringen er den samme som Kjør Smart-løsningen til Rema Forsikring;

«Hvis folk kjører penere blir det færre bilulykker. Og hvis folk behandler seg selv penere blir de friskere.»

D.D. i Storebrand

E.E. forklarer at dette er et produkt som vil hjelpe bunntinjen ved at kundene aktiviseres, og som i sin tur vil gjøre dem friskere og føre til lavere skadekostnad. Han foreslår at Storebrand

for eksempel kan knytte seg opp mot Den Norske Turistforeningen og Yr, og anbefale turer til kundene basert på aktivitetsnivå og posisjon. Ved å ta en slik innfallsvinkel påtar de seg også en samfunnsrolle:

«Hvis vi kan bidra til å få kundene våre i aktivitet, så mener vi at det må være fornuftig for hele samfunnet.»

E.E. i Storebrand

5.1.3 Forsikringsprinsippet

I lys av de økte mulighetene teknologi og wearables gir til å optimalisere tjenester, diskuteres det utfordringer dette skaper for forsikringsprinsippet og den kollektive tankegangen det er bygget på.

Både F.F. og G.G. i Finans Norge bemerker at et forsikringssystem i dag er basert på en kollektiv ordning, hvor mange betaler inn og er med å dekke skadene til de få som får problemer og trenger utbetaling. Dersom man begynner å beregne priser og risiko basert på enkeltindivider, vil ikke dette systemet lenger fungere. Skreddersøm kontra forsikringskollektivet er noe G.G. belyser som en vanskelig diskusjon, og slike dilemmaer vil komme til overflaten når man individualiserer tjenester stadig mer.

«Jeg er veldig usikker på om næringen ønsker å nærme seg de amerikanske tendensene, hvor det er enkelte som rett og slett ikke kan få forsikring, eller i så fall må betale en svært dyr premie.»

F.F. i Finans Norge

B.B. i Datatilsynet kommenterer at man ser en oppsplitting i marked etter marked, og at tjenester stadig blir mer persontilpassede. Man får ikke lenger beregnet forsikringspremien sin basert på en statistisk modell, men i mye større grad på individuell risikoestimering. I lys av dette bemerker A.A. fra Datatilsynet at han tror det vil fremtvinges en diskusjon om hvor grensen vil gå for å utvikle tjenester ut i fra reglene om personvern. Han poengterer at det med slike tjenester vil oppstå utfordringer knyttet til den grunnleggende tankegangen personvernlovgivningen er bygget på. Personopplysninger er ikke en handelsvare, og skal beskyttes.

5.2 Personvernutfordringer og informasjonssikkerhet

A.A. beskriver at Datatilsynet er opptatt av retten til at privatliv og databeskyttelse ivaretas i den teknologiske utviklingen, og at det er viktig å gi betydelig handlingsrom for individet til å leve sitt liv i fred. Dette innebærer kanskje at man ikke alltid fremmer det som er mest samfunnsøkonomisk effektivt, men at man taper i andre enden dersom man ikke sikrer godt personvern. Det er spesielt noen personvernutfordringer som både han og de andre intervjupersonene trekker frem som relevante for finans- og forsikringsbransjen.

5.2.1 Press på å gi fra seg samtykke

A.A. i Datatilsynet trekker frem at det kan oppstå et press til å gi fra seg samtykke for bruk av personopplysninger, dersom prisen på en tjeneste blir vesentlig billigere. Dette utfordrer det grunnleggende prinsippet som han kaller «fairness». Han peker derfor på at det er viktig at tjenester har et utgangspunkt hvor prisen ikke endrer seg hvis man velger å ikke gi samtykke. Bruk av metoder for prisdifferensiering der man blir straffet for å si nei til å gi fra seg personopplysninger er ikke rettferdig, og kan bidra til at samtykket ikke er frivillig.

«Essensen i samtykke er respekt for privatlivet – man lar det være opp til den enkelte, og respekterer den enkeltes ønske. Hvis man bruker mekanismer for å presse noen til å gi samtykke, er det ikke helt forenlig med tanken om respekt. Kan man si: ”Ja, det er fritt valg, men vi gjør alt i vår makt for å få deg til å si ja?”»

A.A. i Datatilsynet

5.2.2 Kunstig intelligens og beslutninger på ukjent grunnlag

Mulighetene teknologi skaper til å ta beslutninger ved hjelp av maskindrevne algoritmer blir bare større og større, og personvernutfordringer dette medfører belyses av representantene fra både Datatilsynet og Finans Norge. A.A. og B.B. i Datatilsynet beskriver at utfordringene knyttet til situasjoner hvor maskiner som tar en beslutning er så avanserte at det er vanskelig å forklare hvilke faktorer som er avgjørende i vurderingen. B.B. påpeker at algoritmene ofte har innebygde bias, hvor ulike fordommer er med på å styre beslutningene som tas. Spørsmålet er om dette er noe man ønsker å tillate. Han fremmer at Datatilsynet er positive til bruken av teknologi, men at det er viktig å styre utviklingen i en retning som er ønskelig.

«Det er ikke sånn at det er fritt frem å slippe kunstig intelligente maskiner løs på befolkningen og la dem treffe beslutninger. Det er viktig at det fortsatt settes grenser for bruken av teknologi.»

B.B. i Datatilsynet

Videre kommenterer A.A. i Datatilsynet at en datadreven risikoberegning i forsikring heller ikke vil være spesielt gjennomiktig. Den enkelte vil ha få forutsetninger for å vite om han eller hun har blitt behandlet rettferdig, og fått en «rettferdig» pris på sin risiko. Når risikoen blir fastsatt på en så kompleks måte, er det vanskelig å si om man som forbruker vil ende opp med den beste behandlingen.

F.F. i Finans Norge trekker også frem utfordringen knyttet til algoritmer og automatisert behandling. Han påpeker at jo mer data som kjøres gjennom algoritmer, jo mer mister man kontroll over beslutningsgrunnlaget. Samtidig bør det være mye data for at beslutningene skal bli treffsikre, så dette er en avveining som må tas.

F.F. kommenterer i tillegg utfordringer knyttet til kriteriene algoritmene baserer sine risikoberegninger på. Rema 1000 beregner risiko gjennom sine bilsensorer på bakgrunn av blant annet akselerasjon og bremsing. Noen steder på veien vil det kanskje være mer aktsomt enn uaktsomt å akselerere brått for å unngå ulykker, for eksempel i vanskelige utkjøringer. Dette fanger ikke nødvendigvis sensorene opp, og sjåføren risikerer å automatisk bli kategorisert som en høyrisikokunde. F.F. belyser dilemmaet ved slike tilfeller, og er opptatt av at det er mange utfordringer i forsikringsbransjen som knytter seg til algoritmebaserte beslutninger.

«På et eller annet tidspunkt, når man putter alt inn i en stor kvern, så mister man perspektivet, og man kan ikke forklare hvorfor det blir som det blir.»

F.F. i Finans Norge

5.2.3 A- og B-lag i samfunnet

D.D. i Storebrand uttrykker at det er noen utfordringer knyttet til datadrevne tjenester som Storebrand føler ansvar for å ta hensyn til når de utvikler persontilpassede forsikringer. Hun peker på at det eksisterer store forskjeller i befolkningen, og at noen grupper er flinkere til å ta vare på helsen enn andre. Skal de som i utgangspunktet har høy utdanning, beveger seg mye

og sørger for at barna sine holder seg aktive, få alle godene fordi de allerede er friske og raske? Dette kan gå utover andre som i større grad trenger helseforsikring, og som ender opp med å betale en mye høyere premie. D.D. mener at dette er et tankekors som kommer med den datadrevne utviklingen, og som forsikringsselskapene må ta hensyn til som samfunnsaktører. Man kan ikke stoppe utviklingen, men man må finne andre mekanismer som veier opp.

«Spesielt hvis man reiser fanen for samfunnsansvar høyt, betyr det at man også må ta vare på de som ikke har så gode forutsetninger for å få de billigste forsikringene.»

D.D. i Storebrand

Helseforsikring er en forsikring som noen hevder at bidrar til å skape et todelt helsevesen i samfunnet, der de mest ressurssterke får bedre tilgang på nødvendig helsehjelp, og kan snike i offentlige helsekøer. E.E. i Storebrand hevder derimot at forsikringen deres bidrar til å redusere sykehuskøene og er positivt fordi den får folk raskere tilbake i jobb. Han uttaler:

«Vi ser hvor viktig forsikringen vår egentlig er i dette samfunnet; Vi sniker ikke i køene, vi tar kundene ut og over i det private, og lar andre komme lenger frem i køen.»

E.E. i Storebrand

B.B. i Datatilsynet kommenterer at detaljert segmentering i helsemarkedet er en utfordring, og at dersom den går for langt, kan det bli et politisk spørsmål. Det kan være at man ønsker en regulering dersom det blir slik at de som trenger forsikringen mest har så høy premie at det heller lønner seg for dem å spare pengene.

5.2.4 Informasjonssikkerhet

Utfordringer knyttet til informasjonssikkerhet som kommer med teknologisk utvikling og bruk av wearables er noe vi har diskutert med både Finans Norge og Datatilsynet. Vi vil i det følgende beskrive funnene fra denne diskusjonen.

«Med wearables og Internet of Things blir mulighetene store for de som vil gjøre ugagn, om man kan kalle det det.»

G.G. i Finans Norge

F.F. i Finans Norge kommenterer at en utfordring for forsikringsselskaper er at de sitter på store mengder sensitive personopplysninger som må beskyttes tilstrekkelig. Opplysninger som omfatter uttalelser fra leger og helsejournaler er noe de ikke ønsker at skal utsettes for et dataangrep. Det samme gjelder for banker, som blant annet sitter på data om betalingstransaksjoner. Ettersom Internet of Things og wearables blir en økende del av hverdagen, vil trusselen om dataangrep bare bli større, og det blir viktigere å bruke nok ressurser på å sikre seg. Finansnæringen bruker allerede mye krefter, både virksomhetene hver for seg, og i fellesskap, på å stoppe og oppdage forsøk på inntrenging i sine datasystemer. Det er snakk om organisert datakriminalitet, hvor de som driver er profesjonelle aktører.

«Det er litt gutteromsstreker, men i hovedsak organisert kriminalitet. I de verste tilfellene er det statlig støttede institusjoner som står bak, og de har gjennomgående minst like god kompetanse som det finansnæringen har, om ikke bedre, og minst like mye penger å sette inn på å bryte ned som vi har til å forsvare oss. Det kommer til å bli et kappløp som fortsetter.»

G.G. i Finans Norge

I tillegg påpeker G.G. at de aktørene som oppbevarer store mengder personopplysninger, som forsikringsselskaper, vil være mer sårbare for dataangrep. Hvis en aktør for eksempel sitter på opplysninger som inkluderer posisjonsdata, internetthistorikk, betalingshistorikk og helsedata, vil denne bli svært attraktiv å angripe, fordi man vil få ut mye verdifull informasjon.

B.B. i Datatilsynet kommenterer også at Datatilsynet er svært opptatt av sikkerhetsdimensjonen av personvernet. Det er viktig at man bruker gode krypteringsløsninger, slik at

kommunikasjonen mellom Internet of Things-enheter beskyttes. Han påpeker at mange selskaper som lager slike produkter i dag ikke har sikkerhet som sin høyeste prioritering.

5.3 Personvernlovgivningen

Vi vil i det følgende beskrive funn som belyser hvordan den nye personvernlovgivningen påvirker handlingsrommet norske forsikringsselskaper har til å implementere persontilpassede helseforsikringer ved bruk av wearables i Norge.

5.3.1 Skjerpet krav til samtykke og innebygd personvern

F.F. i Finans Norge trekker frem at den nye personvernforordningen for det første kommer til å stille strengere krav til samtykke. Samtykkene må spisses og gjøres mer forståelige, og det skal komme klarere frem hva man egentlig godtar når man velger å bruke en tjeneste. Dette vil kunne skape begrensninger for noen selskaper. F.F. påpeker at veldig mange forbrukere i dag ikke vet hva de samtykker til, og at man ofte aksepterer ulike vilkår for en tjeneste uten å egentlig sjekke hva det innebærer. Når det nå vil kreves at det skal komme klarere frem hva man samtykker til, vil folks oppfatning av bruk av personopplysninger kunne endres.

Videre trekker F.F. frem kravet til innebygd personvern, og peker på begrensninger dette kan skape for bedrifter som i dag bruker personopplysninger i sine tjenester. Etter den nye forordningen skal alle tjenester være standardinnstilte for det tiltaket som gjør minst inngrep mot personvernet – hvis ikke må ytterligere samtykke innhentes. For å demonstrere konsekvensene av dette brukes Google Maps som eksempel; det første man som forbruker vil få valget om å samtykke til er om man tillater Google å bruke sine lokasjonsdata. Dette vil utfordre virksomheter som i dag automatisk bruker slik data i bakgrunnen av sine tjenester uten at man merker det og har fått spørsmål om å godkjenne det.

F.F. påpeker også at det vil være fullt mulig å fortsette med å bruke personopplysninger i tjenester, men at det kan bli mer utfordrende fordi man må klare å skrive svært presise samtykker. Samtidig poengterer han at bank- og finansnæringen i Norge i dag ligger på et høyt nivå når det gjelder utforming av samtykker, og at de er nært knyttet til kravene som kommer med den nye forordningen. Dette vil derfor ikke skape store utfordringer for forsikringsselskaper.

«Bank og forsikring har ikke noe tradisjon for å tukle med halvveissamtykker, her skal man ha sitt på det tørre. Når det gjelder personopplysninger i forbindelse med forsikring og helsedata, driver man per i dag ikke i grenseland. Så jeg tror ikke det blir noen stor forandring der.»

F.F. i Finans Norge

D.D. i Storebrand forteller at samtykke i forbindelse med innhenting av personopplysninger går igjen i de aller fleste prosesser knyttet til forsikring. En utfordring vil være å tydelig skille ut behandlingsgrunnlaget man har for personopplysninger i hvert enkelt forsikringstilfelle. I kollektive ordninger har for eksempel de ansatte ikke gitt personlig samtykke til å gi fra seg helseopplysninger når forsikringen tegnes, men så fort de har behov for å bruke helseforsikringen, så trengs opplysningene om dem.

Videre kommenterer D.D. at dersom man i utgangspunktet er god på databehandling og har kontroll på all data i selskapet, så vil nesten alle kravene i det nye lovverket være oppfylt. Man skal legge til rette for å bruke data slik man ønsker, og gjøre det som er best for kundene. Er man dyktig på digitalisering av tjenester, så vil man også være dyktig på personvern.

«Når man skal bruke data mye mer aktivt, som digitalisering innebærer, så må man vite; hvor er denne dataen, hvordan er den tilgjengelig, når kan man bruke den og hvor god kvalitet har den? Mange av spørsmålene som den nye lovgivningen handler om, vil man automatisk være god på, hvis man er god på digitalisering.»

D.D. i Storebrand

5.3.2 Påvirkning på konkurranse

Et av formålene med den nye lovgivningen å skape like konkurransevilkår over hele Europa, og den vil omfatte alle selskaper i verden som behandler data om europeiske kunder. Det diskuteres derfor i intervjuene i hvilken grad internasjonale aktører vil påvirkes av den nye lovgivningen, og hvordan dette vil ha betydning for konkurransen i forsikringsmarkedet.

G.G. i Finans Norge kommenterer at finansbransjen i Norge tradisjonelt har blitt grundig regulert, og at det har vært krevende for deres medlemmer å kunne utnytte personopplysninger

innenfor finanssektoren. Sammenligner man for eksempel med hvordan Google opererer i dag, og skal prøve å konkurrere mot dem om å levere finansielle tjenester, vil man stille svakt. Mye av styrken med den nye forordningen er derfor at den skal harmonisere kravene for personvern internasjonalt, slik at det blir så likt som mulig. En utfordring har også vært at internasjonale aktører forholder seg til personvern på en helt annen måte enn selskaper i Norge, og at norsk finans- og forsikringsnæring har vært relativt forsiktige med å utnytte persondata sammenlignet med andre aktører.

«Vi håper jo at dette skal bety at Google og Facebook må løfte seg opp på et nivå som ligner mer på det som velregulerte næringer har hatt lenge.»

G.G. i Finans Norge

Representantene i Storebrand forteller i likhet med G.G. i Finans Norge at det er stor forskjell på hvordan den nye personvernlovgivningen vil påvirke ulike aktører. D.D. påpeker at Norge per i dag har blant Europas strengeste personvernlovgivninger, og hadde man etterlevd den til punkt og prikke, så ville ikke steget opp til den nye forordningen vært spesielt stort. Norge har også hatt et aktivt datatilsyn i forhold til de fleste andre europeiske land, som har laget mange gode veiledere slik at det har vært lettere å etterleve lovgivningen. E.E. i Storebrand opplever for eksempel store forskjeller på hvordan deres tilknyttede virksomheter i både Sverige og Tyskland stiller seg til personvern i forhold til dem.

D.D. i Storebrand peker også på at den nye personvernloven er en viktig lovgivning for EU. Det har vært en stor ulempe for europeiske selskaper å behandle persondata sammenlignet med for eksempel amerikanske, på grunn av strengere personvernlovgivning. Alle som skal behandle opplysninger om europeere må nå gjøre det i tråd med den nye forordningen, det handler ikke lenger om hvor i verden man befinner seg. Her trekker hun spesielt frem Google og Facebook som eksempler på selskaper som har hatt virksomheten sin stasjonert utenfor Europa, og benyttet seg godt av å ha friere handlingsrom. Hun legger til at disse selskapene også har vært mye flinkere på teknologi, men at denne konkurransefordelen vil utjevne seg når de må konkurrere på like vilkår som de europeiske selskapene.

I tillegg spesifiserer D.D. at det ikke vil være mulig å gi samtykke til amerikanske selskaper for å behandle europeiske personopplysninger på dårligere vilkår enn personvernlovgivningens krav.

«Nei, du kan aldri samtykke deg til dårligere vilkår. De kan ikke si at hvis du skal ha denne tjenesten, så mister du rettighetene dine. Rettighetene er lovpålagt, og loven vil alltid gå foran et samtykke eller en avtale. Så hvis de skal tilby helseprodukter, altså wearables- helseforsikringer i EU eller i Norge, så må de gjøre det i tråd med den nye forordningen.»

D.D. i Storebrand

B.B. i Datatilsynet kommenterer også at alle juridisk sett skal likebehandles når den nye lovgivningen trer i kraft. I forbindelse med dette mener han at kulturen for å utvikle produkter innenfor selskapet kommer til å være avgjørende for hvem som lykkes i markedet. Bank- og forsikringsselskaper har i utgangspunktet hatt tunge og trege strukturer som har satt begrensninger for innovasjon, og de vil utfordres når de møter Google, Facebook og andre voksende start-ups som har en helt annen tilnærming til produktutvikling.

«Vi har alltid hørt at det er lovgivningen som gjør at de amerikanske selskapene er så mye mer innovative enn oss. Jeg har ment lenge at dette er tull. Fra og med mai neste år er lovgivningen lik, så da får vi se om vi klarer å matche dem. Og det er ikke sikkert.»

B.B. i Datatilsynet

5.3.3 Sektorregulering

Ettersom forordningen på enkelte områder gir rom for nasjonal tolkning, er det uklarerhet knyttet til hva som spesifikt vil skje med regulering i forsikringsbransjen i Norge. Konesjonsplikt og sektorregulering er derfor noe vi har diskutert med flere av våre intervjupersoner.

D.D. i Storebrand forklarer at Storebrand ikke bare forholder seg til personvernlovgivningen, men også til egne konsesjonsreguleringer for finansnæringen. Dette innebærer blant annet Datatilsynets forsikringskonsesjon, som setter særskilte rammer for forsikringsselskapers behandling av personopplysninger. Hun uttrykker at denne begrenser dem i ytterligere grad enn det lovgivningen gjør.

Videre kommenterer hun at det er utfordrende at myndighetene ikke gir tydeligere signaler om hva som kommer til å skje med konsesjonsordningen i finansnæringen. Selv om konsesjonsregimet generelt ser ut til å bortfalle, vil det i enkelte spesiallovgivninger være mulig å sektorregulere. Det er derfor mulig at Datatilsynet og Justisdepartementet ønsker å fortsette med konsesjonsbeleggelse av finansnæringen gjennom for eksempel finansforetaksloven. Dette er noe D.D. anser som svært ugunstig for Storebrands konkurransevne.

D.D. peker på at man nå er i en avgjørende fase, hvor det bestemmes om det skal være muligheter for norsk forsikrings- og finansnæring å være med på å utvikle datadrevne tjenester i Norge. Hun uttrykker at de persontilpassede produktene med tiden vil komme til Norge uansett, og at dersom forbrukerne ikke får tak i det her, vil de kunne gå til utlandet. E.E. legger til at det allerede er to konkurrenter av dem i Sverige som har lansert løsninger for helseforsikring hvor aktivitetsbasert data brukes.

F.F. i Finans Norge uttaler at Datatilsynet overfor dem har gitt ganske klare signaler om at det ikke er rettsgrunnlag for å ha konsesjoner i regi av den nye forordningen. Han kan opplyse om at Datatilsynet og Justisdepartementet har konkludert med at det ikke er behov for å innføre konsesjoner for behandling av personopplysninger i medhold av finansforetaksloven. Forenklet sett innebærer dette at man får en slags forhåndsgodkjennelse for behandling av personopplysninger. Større forpliktelse legges over på de behandlingsansvarlige i bedriften, og man har ansvar for å sikre interne rutiner og gjøre grundige konsekvensanalyser.

«Sånn som jeg tolker det, så er vi ikke så veldig redde for konsesjonsregimet etter møtet med departementet.»

F.F. i Finans Norge

A.A. i Datatilsynet bekrefter at konsesjonsplikten med aller høyeste sannsynlighet kommer til å bortfalle. Det vil ikke lenger være spørsmål om særnorske reguleringer – konkurransen kommer til å gå på tvers av landegrenser, og det vil bli et mer harmonisert marked. Likevel poengterer han at selv om konsesjonsplikten bortfaller, er det en del andre mekanismer som er innbakt i de nye reglene, og som kan sies å komme i stedet for konsesjonsordningen. Han bemerker at Datatilsynet kommer til å være involvert i utviklingen av persontilpassede produkter, fordi det innebærer monitorering av intime forhold som berører enkeltindividets personvern.

«Som tilsynsmyndighet vil vi bli involvert i utviklingen og designet av denne typen produkter, fordi det per definisjon, er ganske høy risiko for inngrep i sentrale rettsgoder man har som individ når man bruker den type teknologi.»

A.A. i Datatilsynet

5.3.4 Bransjenormer

Både representantene i Finans Norge og Storebrand nevner utviklingen av bransjestandarder som en viktig oppgave for finansnæringen i lys av den nye forordningen. D.D. i Storebrand påpeker at den nye forordningen legger til rette for at den skal etterleves med bransjenormer. Storebrand er representert i en gruppe i Finans Norge hvor det arbeides med å oppdatere og utvikle slike normer, og D.D. poengterer at denne jobben er svært krevende. Hun peker også på at forslag til godt utformede bransjenormer kan bidra positivt til dialogen med Datatilsynet om ulike personvernutfordringer.

«Vi oppfordres tydelig av Datatilsynet til å lage egne bransjenormer.»

D.D. i Storebrand

F.F. i Finans Norge omtaler i likhet med D.D. i Storebrand at jobben med å utvikle bransjenormer er omfattende, og at det er vanskelig å få et klart inntrykk av hva som vil skje i finansnæringen. Han trekker også frem Normen.no som en svært tidkrevende bransjenorm å holde oppdatert, og at det vil kreve mye ressurser å skrive en bransjestandard for hele finansnæringens behandlinger av personopplysninger. En fordel for finansnæringen er at dagens særskilte konsesjonsordning vil være et godt utgangspunkt å bygge videre på.

5.3.5 Sanksjonering

Virksomheter som bryter reglene for håndtering av personopplysninger kan etter den nye forordningen risikere store bøter. Det er imidlertid uklart hvor strengt myndighetene kommer til å praktisere det nye sanksjonsregimet. Dette har vi derfor diskutert med Datatilsynet.

A.A. i Datatilsynet forteller at det ikke er et mål i seg selv å sanksjonere, men at et betydelig strengere strafferegime er et politisk signal fra EU om at de mener alvor. Det er en direkte respons på hvordan eksisterende regler har fungert, og at de i dag ikke er godt nok akseptert.

Man har derfor valgt å bytte ut en del mekanismer i den nye lovgivningen, hvor da dette overtredelsesgebyret også kommer inn med en betydelig styrke.

«Sanksjonsregimet er en klar trussel. Målet med det er å vise at nå mener vi alvor, og det krever nok også at det tas i bruk. Man kommer nok til å se reaksjoner, men de store bøtene som man snakker om, det får vi vente å se med.»

A.A. i Datatilsynet

B.B. i Datatilsynet nevner at etterlevelse av reglene handler like mye om firmapolitikk som at man gjør det for å unngå bøter. Det er noe med holdningen til hvorfor man behandler data i utgangspunktet, og hva man skal bruke den til, som burde reflektere bedriftens bevissthet på personvern. Han trekker frem Schibsted som et godt eksempel. Schibsted følger ikke personvernreglene for å unngå bøter, men er helt åpne om at det er fordi de skal bruke data de besitter om sine kunder til å tjene penger, samtidig som de ønsker å gi bedre tjenester til forbrukerne.

«Det er noe med holdningen til hvorfor man behandler data, og hva man skal bruke data til – da liker jeg mye bedre Schibsted sin holdning; De skal følge alle lover og regler, men jaggu om de skal bruke disse dataene også. Jeg tror etterlevelsen blir mer ekte, og kanskje litt bedre også, hvis man gjør det på Schibsted-metoden.»

B.B. i Datatilsynet

5.3.6 Hva er egentlig lovlig i dag?

H.H. fra Justisdepartementet forklarer forskjeller mellom dagens lovgivning og den nye forordningen. Representantene fra Finans Norge har også noen relevante kommentarer på dette området. I tillegg forteller Datatilsynet om hvilke forhold de ser på når de i dag vurderer konsesjonssøknader.

H.H. fra Justisdepartementet stiller seg kritisk til at bortfall av konsesjonsplikten vil ha noen betydning for om forsikringsselskaper kan utvikle tjenester ved hjelp av kundedata. Han hevder at dersom data behandles på en lovlig måte i dag, så skal det mye til å nekte denne behandlingen

i en konsesjon. Han er usikker på om forordningen vil ha noe særlig betydning for, eller medføre endringer, som gjør det mer eller mindre mulig å tilby persontilpassede tjenester.

Han påpeker at han ikke vet hva Datatilsynet bestemmer i sine konsesjoner, men at det i dag ikke burde være umulig å lage en applikasjon hvor folk premieres basert på hvordan de beveger seg, gitt at de samtykker til datainnsamlingen. Han understreker at verken den nåværende eller den nye forordningen gjør det umulig å behandle personopplysninger til tjenesteformål. Norske myndigheter ønsker ikke å gjøre det umulig å drive teknologisk utvikling, som i stor grad baserer seg på behandling av personopplysninger i mange bransjer. Slik han ser det er det heller ikke noe stort handlingsrom som åpner seg som følge av den nye forordningen.

«Det kan hende at jeg ikke vet nok om det forsikringsregulatoriske, men jeg klarer ikke å se at forordningen trigger noe nytt når det gjelder muligheten for den type datainnsamling til bruk i forsikring.»

H.H. i Justisdepartementet

F.F. i Finans Norge kommenterer også at det lovmessig ikke virker umulig å tilby persontilpassede forsikringer verken etter dagens lovgivning eller etter den nye forordningen.

«Det er ikke bare jussen som er problemet og utfordringen her. Det kommer an på hvilken vei man ønsker å gå. Sånn som jeg ser det, er det mulig å gjøre det i dag, og det er mulig å gjøre det etter forordningen. Man må nok justere litt, og det blir nok litt vanskeligere, men det er ikke umulig, det tror jeg absolutt ikke.»

F.F. i Finans Norge

A.A. i Datatilsynet forteller litt om hva de har vurdert når de har fått inn konsesjonssøknadene for persontilpassede bilforsikringer. For det første ser de på samtykke, og undersøker om det finnes alternative produkter slik at man ikke blir presset til å si ja fordi man er avhengig av å ha produktet. De ser også på hvordan bedriften har tenkt å informere kundene sine om hvordan de bruker opplysninger, og hvor transparent de opererer. Videre ser Datatilsynet på rutiner for sletting av opplysninger, hvor opplysningene overføres, og hva slags kryptering som brukes for å beskytte dem. I tillegg ser de på typen informasjon som samles inn, og undersøker om det er proporsjonalitet i mengden data som samles inn og hva som egentlig trengs for å levere tjenesten. Når det gjelder sensorbaserte bilforsikringer peker A.A. for eksempel på at de

vurderer innsamling av posisjonsdata som problematisk, fordi det kan oppleves som invaderende og ikke nødvendig for tjenestens formål.

5.4 Forbrukernes holdninger

I det følgende vil vi beskrive funn tilknyttet ulike aspekter som kan påvirke forbrukernes holdninger til persontilpassede helseforsikringer.

5.4.1 Kunder og personvern

D.D. i Storebrand forteller at kundene deres viser variert grad av oppmerksomhet til forvaltningen av sine personopplysninger. De fleste ser for eksempel på Storebrand som ett selskap, og tenker ikke på at det er delt opp i Storebrand Bank, Storebrand Helse og Storebrand Forsikring. Hun forklarer derfor at noen blir veldig frustrerte når de skjønner at det ikke er fri informasjonsflyt mellom disse selskapene og må gi fra seg de samme opplysningene flere ganger. Samtidig påpeker hun at dersom man spør kundene konkret om de ønsker at selskapet skal vite alt, så sier de gjerne nei. Dette mener hun gir en indikasjon på at folk ikke helt forstår hva de egentlig ønsker.

I tillegg erfarer E.E. i Storebrand at det er få privatkunder som i dag spør om lagringen av deres persondata og ber om å få dem slettet. D.D. tror den nye forordningen vil øke bevisstheten hos privatkunder, slik at antall henvendelser vil øke. I dag er det hovedsakelig kunder som har fått avslag på forsikring som ønsker at deres personopplysninger skal slettes.

F.F. i Finans Norge snakker også om holdninger hos forbrukerne. Han refererer til personvernundersøkelsen og at det er relativt lav interesse blant norske forbrukerne til å dele opplysninger med forsikringsselskapet. Under Finansnæringens Dag, arrangert av Finans Norge 4. april 2017, ble de 400 første deltakerne spurt, som hovedsakelig var folk fra finansnæringen, om de var villigere til å gi fra seg detaljerte sensordata til forsikringsselskapet i bytte mot en *vesentlig lavere* forsikringspris. Her var 29 prosent enige, mens 49 prosent var uenige. Videre ble deltakerne spurt om hvilke aktører de var mest villige til å gi fra seg persondata til for å få skreddersydde tjenester. I dette tilfellet rangerte man på en skala fra 1 til 6 (hvor 6 var høyest vilje). Forsikring scoret da 4,32. På et lignende spørsmål om tillit scoret forsikring 4,28.

5.4.2 Omdømme og tillit

G.G. i Finans Norge poengterer at tillit tar lang tid å bygge opp og kort tid å bryte ned. F.F. nyanserer at man kan gjøre noe lovlig eller ulovlig, og man kan gjøre ting lovlig, men bryte tilliten.

«Dette blir en personlig refleksjon, men jeg tror at det er noe med den allmenne oppfatningen av innsamling av personopplysninger som kommer til å få en forandring.»

F.F. i Finans Norge

F.F. trekker frem et eksempel Datatilsynet og Teknologirådet har brukt i en av rapportene sine der en forbruker blir spurt om å bli fotfulgt rundt på et kjøpesenter, for å kunne bli tilbudt den beste kundeopplevelsen. Han påpeker at de aller fleste, i en fysisk verden, ville sagt nei, fordi de synes det er for påtrengende. Samtidig ser man at når folk i prinsippet blir spurt om det samme på internett, så har de ikke noe problem med det. F.F. kommenterer at dette er fordi den samme «fotfølgingen» da skjer mer i det skjulte. Han mener at organisasjoner som Google og Facebook, som hovedsakelig opererer med personopplysninger, kan støte på utfordringer når den nye forordningen kommer. I dag gir forbrukerne fra seg store mengder personopplysninger i bytte mot relativt lite, mens de med ny forordning forhåpentligvis vil bli klar over verdien av egne data.

«Jeg tror folk kommer til å få en større forståelse for verdien av egne personopplysninger, og et helt annet forhold til dem enn tidligere. Når det skjer, tror jeg at man kan komme i en situasjon hvor den behandlingen man har bedrevet – som er fullt lovlig, fordi man har samtykke – vil stå til omdømmestryk.»

F.F. i Finans Norge

F.F. argumenterer videre for at folk i større grad kan komme til å trekke tilbake samtykke og be om sletting av sine personopplysninger når bevisstheten til personvern øker. Selv om det selskaper som Google gjør i dag i teorien er helt lovlig, kan det bli sterke reaksjoner når man skjønner hva disse selskapene faktisk vet om en.

D.D. i Storebrand har også noen tanker rundt personvern og omdømme. Hun peker på at omdømme ikke nødvendigvis er noe som holder Storebrand igjen når de nå vurderer å lansere persontilpassede helseforsikringer, men hun kan bekrefte at personvern er en komponent som i økende grad påvirker omdømmet deres og pris på selskapet.

«Det øker veldig, dette ansvaret vi føler for at personvern i stor grad kan påvirke omdømmet vårt.»

D.D. i Storebrand

Hun forteller videre at noen av Storebrands investorer nå viser interesse for og er opptatte av at personvern og informasjonssikkerhet skal være i orden i selskapet. Yahoos personvernutfordringer og den følgende prisreduksjonen av deres aksjer blir lagt frem som en mulig bakenforliggende årsak for den økte interessen. Hun understreker at personvern har en reell økonomisk verdi, så vel som omdømmeverdi, og er noe de tar seriøst.

5.4.3 Kulturelle forskjeller

A.A. i Datatilsynet foreslår at kulturelle forskjeller mellom land i Europa vil være med på å påvirke hva forbrukerne sier ja til å dele av personopplysninger. Nordmenn er kanskje mindre villige til å dele informasjon om seg selv mot en billigere forsikring, enn det man er sammenlignet med andre land. I tillegg har nordmenn relativt god kjøpekraft, som betyr at man kan ta seg råd til å si nei. I andre land i Europa vil kanskje situasjonen være annerledes. Dette vil kunne ha innvirkning på hvilken retning norske selskaper velger å ta.

5.4.4 Kundekommunikasjon og folkeopplysning

D.D. i Storebrand bemerker at hver enkelt forbruker eier sine personopplysninger, og at de selv bør få bestemme hva disse skal brukes til. Hun påpeker at Storebrand i utgangspunktet forvalter mange viktige verdier for kundene sine, og at kundene også burde ha mulighet til å gi fra seg helseopplysninger for å få en persontilpasset forsikringstjeneste dersom de ønsker det. I forbindelse med dette er D.D. opptatt av at Storebrand skal være helt åpne og ærlige om hva de gjør, og at dataene de samler inn ikke skal misbrukes. Hun mener at det handler mye om kundekommunikasjon og å skape tillit, og at det er opp til Storebrand som selskap å være ansvarlige nok til å få tillit fra kundene til å kunne tilby tjenester som drives av personopplysninger.

D.D. hevder videre at bruk av ord som *overvåkning* er problematisk når man snakker om innsamling av persondata, fordi det har en ordlyd som er ubetinget negativ. Derfor foreslår hun at *monitorering* er en bedre beskrivelse når formålet er å tilby en bedre tjeneste til kundene. Samtidig argumenterer hun for at bruk av ord som *overvåkning* gjør det vanskelig for forbrukerne å skjønne hva Datatilsynet prøver å formidle, fordi det kan være vanskelig å relatere det til virkeligheten. Med bakgrunn i dette understreker hun at ordlyd og språk har stor betydning når man skal formidle noe til forbrukere for at de skal forstå hva man mener:

«Det må kanskje brukes et annet språk eller en annen måte å snakke på for at man skal skjønne: Vil du at de skal vite hvor mange skritt du tar? Eller vil du at de skal overvåke hvordan du oppfører deg? Det er veldig stor forskjell på de to!»

D.D. i Storebrand

D.D. påpeker at folkeopplysning er et effektivt virkemiddel for å påvirke forbrukernes holdninger, og derfor kan være et bedre tiltak enn restriksjoner. I Norge er man spesielt gode på, og har mye erfaring med, opplysning om folkehelse. Sier man for eksempel til det norske folk at de skal spise mindre sukker, så spiser de mindre sukker. Hun argumenterer for at det å lære både barn og voksne å ta bevisste valg og passe på personopplysningene sine, er viktigere enn å ikke tillate bruk av for eksempel wearables for å få billigere helseforsikring. Folkeopplysning kan bidra til å gjøre forbrukerne mer ansvarlige samtidig som at Norge kan fortsette med å ligge langt fremme i bruken av teknologi. Hun poengterer også at hun tror markedet vil tilpasse seg dersom forbrukerne blir mer bevisste og etterspør bedre personvern, og at Datatilsynet i denne sammenheng kan dra nytte av forbrukerne som ressurser.

«Jeg tror at hvis forbrukerne hadde vært mer bevisste og etterspurt bedre personvern, så hadde markedet tilbudt det i større grad. Og siden Datatilsynet har relativt lite ressurser, hvorfor ikke bruke de viktigste ressursene de har; Det er aktive forbrukere som er de beste vaktbikkjene.»

D.D. i Storebrand

6. Analyse

I det følgende kapitlet vil vi analysere funn fra intervjuene opp mot studiens modell med sine forskningsspørsmål.

6.1 Lovens påvirkning på forsikringsselskapers handlingsrom

Forskningsspørsmål 1: *Hvordan vil den nye personvernlovgivningen påvirke det juridiske handlingsrommet norske forsikringsselskaper har til å tilby persontilpassede helseforsikringer?*

I kapittel 2 fremgår det at to av de overordnede endringene som kommer med den nye personvernforordningen kan knyttes til *nye plikter for bedrifter* og *utvidet geografisk virkeområde*. I det følgende vil vi bruke innsikt fra resultatene til å diskutere hvilke effekter disse endringene kan ha på handlingsrommet til norske forsikringsselskaper.

Sektorregulering vil erstattes av nye plikter for bedrifter

Et av momentene som har vært oppe til diskusjon under studien er hvorvidt finansnæringen i Norge vil fortsette å bli regulert, og i så fall hvordan. Ut i fra resultatene sitter vi igjen med inntrykket av at melde- og konsesjonsplikten ser ut til å bortfalle helt med den nye forordningen, også for finansnæringen. Slik vi forstår det vil dette innebære at alle virksomheter får en slags forhåndsgodkjennelse til å behandle personopplysninger, og at man i prinsippet kan tilby de tjenestene man ønsker, så lenge det skjer i tråd med regelverket. Samtidig kommer det frem at det foreligger andre mekanismer innbakt i den nye forordningen som vil kunne fungere som regulering i stedet for konsesjonsordningen. Dette tyder på at Datatilsynet som tilsynsmyndighet fortsatt vil ha muligheten til å involvere seg i utviklingen av datadrevne tjenester i Norge.

En av mekanismene som ser ut til å kunne fungere som regulering, er bruken av bransjenormer. Aktørene i ulike bransjer må samarbeide seg imellom og med Datatilsynet om å utforme retningslinjer for hvordan man ønsker at personopplysninger skal behandles innenfor bransjen. Dette indikerer at bruken av personopplysninger til å utvikle tjenester vil komme til å skje innenfor rammer som må godtas av Datatilsynet, og at dialogen man har med dem om hva som er akseptabelt fortsatt vil være gjeldende. Vi sitter også igjen med inntrykket av at bransjenormer er svært tids- og ressurskrevende å utvikle, men at finansnæringen har et godt

utgangspunkt når det gjelder utforming av nye retningslinjer. Dette fordi de allerede har en gruppe som jobber med utvikling av normer, og kan bygge videre på dagens særskilte konsesjonsordning for forsikring.

En annen mekanisme som vil kunne virke regulerende er det *skjerpede kravet til samtykke* og *kravet til innebygd personvern* som kommer med den nye forordningen. Alle virksomheter må spisse sine samtykkeerklæringer og gjøre dem mer forståelige for kunden. Den innstillingen som er mest skånsom mot personvernet i en tjeneste skal også alltid stå som standard. Dette kan ha to effekter. For det første, vil klarere avtalevilkår kunne få forbrukerne til å forstå hva de egentlig samtykker til når de bruker en tjeneste. Dette kan føre til at de blir mer bevisste på hva de faktisk gir fra seg av personopplysninger, og bidra til at de ikke lenger ønsker å akseptere vilkår som de tidligere har gjort. For det andre, ser det ut til at flere tjenester som i dag baserer seg på bruk av personopplysninger uten at samtykke er innhentet, ikke vil overleve. Dette indikerer at vi kan få et marked med mer transparente tjenester, hvor det ikke vil være mulig å utnytte overflødig persondata. Mekanismene som regulerer bedriftens plikter vil på denne måte se ut til å skyve maktbalansen mellom produsent og forbruker mer over til forbrukeren.

I tillegg fremkommer det av resultatene at sanksjonsordningen som innføres er ment som et sterkt virkemiddel for å forhindre overtredelser av regelverket, og at det ikke vil bli holdt tilbake med å ta det i bruk. Vi har dermed inntrykk av at trusselen om streng sanksjonering vil kunne fungere som en regulerende mekanisme som er innbakt i den nye forordningen. Dette impliserer at selv om virksomheter får mer ansvar og ikke trenger å søke om godkjenning til å behandle personopplysninger, vil de antakeligvis operere på en måte som ville blitt akseptert etter dagens ordning.

Et annet interessant funn vi ønsker å diskutere i tilknytning til sanksjonering er Schibsteds holdning til behandling av personopplysninger. Schibsted trekkes frem som et eksempel på en bedrift som ikke følger personvernreglene for å unngå bøter, men fordi det er en del av deres underliggende firmapolitikk; de ønsker å være dyktige på databehandling fordi de skal tjene penger på å tilby forbrukerne tilpassede tjenester. Dersom en bedrift som lever av personopplysninger ikke ivaretar personvern og informasjonssikkerhet, vil den trolig kunne rammes hardt hvis den misbruker personopplysninger eller blir utsatt for et dataangrep. Som det fremkommer i intervjuet med Storebrand sank for eksempel prisen på Yahoos aksjer betraktelig som følge av selskapets personvernutfordringer. Dette impliserer, som vi også har

sett i litteraturen, at mangel på godt personvern og fokus på datasikkerhet vil kunne føre til omdømmetap og tillitsbrudd hos tusenvis av kunder. Omdømmetap kan derfor koste selskaper som både Schibsted og Storebrand mer enn en bot fra Datatilsynet, og bidra til at etterlevelse av regelverket også er av egen interesse.

Utvidet geografisk virkeområde og påvirkning på konkurranse

Et av formålene med den nye forordningen er å skape like konkurransevilkår for alle virksomheter som behandler personopplysninger om europeere. I lys av resultatene ser det ut til at den nye forordningen vil påvirke konkurransesituasjonen på to måter: Den vil ha innvirkning på konkurranseevnen til norske selskaper, og den vil påvirke hvordan aktører utenfor Europa kan operere med europeiske kunder.

De skjerpede kravene som bedrifter pliktes å følge, er noe vi i lys av våre funn tolker at kan skape en konkurransefordel for norske forsikringsselskaper. Vår oppfatning er at Norge har hatt en strengere personvernlovgivning enn andre land, med et aktivt Datatilsyn som har bidratt til å gjøre det enklere for virksomheter å etterleve lovgivningen. I tillegg har den norske finansbransjen vært spesielt strengt regulert, gjennom blant annet forsikringskonsesjonen. Det har blitt påpekt at norske finans- og forsikringsinstitusjoner allerede er dyktige på å utforme samtykker, og at de er vant med å forvalte personopplysninger på en transparent måte. Utgangspunktet de har for å behandle data i tråd med regelverket synes derfor å være bedre enn for de fleste andre internasjonale aktører.

Videre ser utjevningen av konkurransevilkårene ut til å kunne ha stor innvirkning på amerikanske selskapers handlingsrom på det europeiske markedet. Det vil ikke lenger være en trussel at for eksempel aktører som Facebook og Google skal kunne utkonkurrere norske selskaper ved å tilby finanstjenester i Norge på grunn av ulike personvernregler. En forbruker kan aldri samtykke seg vekk fra rettigheter som er fastsatt i europeisk lov. Dette impliserer at hvis Google for eksempel skal tilby en persontilpasset helseforsikring i Norge, må de gjøre det på like vilkår som norske selskaper.

I forbindelse med utjevningen av konkurransevilkårene, kan det åpnes for en interessant diskusjon. På den ene siden argumenterer noen av representantene fra finansnæringen for at den norske personvernlovgivningen har vært en begrensning for utvikling av datadrevne tjenester i Norge. Det antydes at forskjeller i lovgivningen kan forklare hvorfor amerikanske

selskaper er så mye bedre på teknologi og innovasjon enn europeiske selskaper. På en annen side påpekes det av en av representantene i Datatilsynet at mange norske finansselskaper i dag er preget av trege organisasjonsstrukturer, og at dette i større grad kan forklare hvorfor de ligger bak på innovasjon og produktutvikling. Vi ser derfor at det eksisterer delte meninger om lovgivningens innvirkning på norsk konkurranseevne.

Dagens handlingsrom

Diskusjonen over gir rom for å stille spørsmål ved hvilken betydning dagens lovgivning faktisk har for muligheten til å tilby persontilpassede helseforsikringer i Norge. Et av våre mest interessante funn er at det kan se ut til at det verken etter dagens lovgivning eller den nye forordningen er lovteknisk umulig å tilby en slik tjeneste. Dersom databehandlingen i dag skjer i tråd med regelverket virker det som at den i prinsippet ikke kan nektes i en konsesjon, og at dersom man oppfyller kravene etter den nye forordningen skal man i prinsippet kunne tilby de tjenestene man ønsker.

Tatt i betraktning at Datatilsynet nylig har gitt konsesjoner til sensorbaserte bilforsikringer, har vi derfor inntrykk av at det lovteknisk også burde være mulig for et forsikringsselskap å tilfredsstille kravene til en tilsvarende konsesjon for helseforsikring. Slik vi har forstått det er det likevel ingen som tidligere har søkt om en konsesjon spesifikt til dette. Det er derfor vanskelig å si om Datatilsynet ville godkjent en slik søknad i dag. En persontilpasset helseforsikring vil innebære et mer sensitivt inngrep i enkeltindividets privatliv enn en persontilpasset bilforsikring, og det er mulig at Datatilsynet på grunn av dette ville vurdert søknadene ulikt. Hvis det er tilfelle at man faktisk ville fått et avslag selv om man i prinsippet behandler personopplysninger på riktig måte, kan det argumenteres for at konsesjonsordningen holder tilbake utviklingen av persontilpassede helseforsikringer i dag. Dette kan i så fall støtte argumentet om at innovasjon i forsikringsbransjen begrenses av lovgivningen.

Det kan videre stilles spørsmål ved hvorfor ingen har søkt om konsesjoner for verken persontilpassede bil- eller helseforsikringer i Norge tidligere, når det har eksistert i flere år i blant annet USA. Her kan det trekkes inn at det ble nevnt i intervjuet med Finans Norge at norsk forsikrings- og finansnæring har vært relativt forsiktige med å utnytte persondata i forhold til andre aktører. Dette impliserer at det ikke nødvendigvis kun er regelverket som har stoppet dem fra å utvikle datadrevne forsikringstjenester tidligere. Som F.F. i Finans Norge peker på, «*er det nok ikke bare jussen som er problemet og utfordringen her*». Mye kan tyde på at de andre

faktorene vi har utforsket vil være avgjørende for hva som tilbys av produkter i det norske markedet i dag og i tiden fremover.

Delkonklusjon

Ut ifra det vi nå har sett kan vi trekke at den nye personvernlovgivningen kommer til å påvirke hvordan forsikringsselskaper kan anvende teknologi til tjenesteformål. Generelt ser det ut til at kravene i personvernlovgivningen blir strengere enn i dag, men at det for den norske finansnæringen likevel kan bli enklere å behandle personopplysninger. Dette fordi forsikringsselskapene slipper å bli særregulert med konsesjonsplikt, og fordi de allerede har et høyt nivå på sin databehandling, som vil gjøre det lettere for dem å etterleve lovgivningens nye krav. I tillegg ser det ut til at den nye lovgivningen vil påvirke norsk konkurranseevne positivt, samt gjøre det vanskeligere for aktører utenfor Europa å utnytte persondata om europeere. Våre funn tyder også på at det lovteknisk ikke burde være umulig å kunne tilby en persontilpasset helseforsikring verken i dag eller etter den nye forordningen, men det er uvisst om Datatilsynet faktisk ville godkjent det. Mye tyder på at det er andre faktorer enn det juridiske som også vil være avgjørende for både Datatilsynet og forsikringsselskaper når de vurderer nye produkter.

6.2 Lovens påvirkning på forbrukernes bevissthet til personvern

***Forskningsspørsmål 2:** Hvordan vil den nye personvernlovgivningen påvirke forbrukernes bevissthet til personvern, og følgelig aksepten av persontilpassede helseforsikringer?*

I det følgende vil vi bruke funn fra intervjuene til å belyse hvordan vi tror *nye rettigheter for borgerne* vil ha en innvirkning på forbrukernes aksept av persontilpassede helseforsikringer. I kapittel 2 ble resultater fra Datatilsynets personvernundersøkelse fra 2016 brukt for å belyse forbrukeres holdninger til å dele personopplysninger med forsikringsselskaper mot å få en *vesentlig billigere* forsikringspremie. Her kom det frem at 63 prosent stilte seg negative til dette. I intervjuet med Finans Norge ble disse holdningene diskutert, og det ble påpekt at de 400 første deltakere på Finansnæringens dag i 2017 ble spurt om det samme. Her var andelen negative 49 prosent. Svarene fra undersøkelsen på Finansnæringens dag peker altså i samme retning som resultatene fra undersøkelsen i 2016, og i lys av dette kan det diskuteres flere interessante aspekter knyttet til forbrukernes holdninger.

Vi finner det for eksempel svært interessant at utvalget som ble spurt på Finansnæringens dag hovedsakelig bestod av representanter fra finansnæringen. Da det er finansnæringen som i størst grad virker aktive med å fremme de fordelaktige sidene ved persontilpassede forsikringstjenester, vil det kanskje være rimelig å tro at representantene fra denne næringen ville stille seg mer positive til å dele helsedata med forsikringsselskaper. Hvis ikke de som jobber med å kunne tilby disse produktene er mer villige til bruken av dem, hvordan kan man da anta at de blir mottatt av «vanlige» forbrukere?

Videre kan det fra resultatene virke som at selv om nordmenn på papiret sier «nei» når de får spørsmål om de ønsker å dele personopplysninger til tjenesteformål, så gjør de det i praksis ofte likevel. Det kan derfor tyde på at mange forbrukere ikke helt forstår hvor mye opplysninger de egentlig godtar å dele når de bruker tjenester og er på internett, og at de ikke er spesielt bevisste på å ivareta eget personvern. Det kan også tenkes at de i noen sammenhenger ikke har god nok innsikt i hva de egentlig vil når det gjelder deling av opplysninger. Dersom de ikke forstår at det er nødvendig å gi fra seg personopplysninger for at det skal være mulig å få en tjeneste tilpasset slik de ønsker, kan det være at de isolert sett svarer «nei» når de får spørsmål om de ønsker å dele, uten å egentlig vite hva de da gir avkall på. I forbindelse med dette tyder mye på at økt bevissthet til personvern og deling av egne personopplysninger vil bli viktigere for at forbrukerne skal kunne gjøre seg opp en mening om hvilken retning de ønsker at markedet skal bevege seg.

Vår oppfatning er at den nye personvernforordningen, gjennom *nye rettigheter til borgerne*, vil bidra til å styrke forbrukernes bevissthet til personvern og forståelse for verdien av egne personopplysninger. For det første vil det skjerpede kravet til samtykke bidra til å skape økt forståelse hos forbrukerne for hva de faktisk samtykker til. Dette kan føre til at de ikke lenger ønsker å akseptere vilkår som de tidligere har gjort, og at de slutter å bruke visse tjenester. For det andre vil klarere og mer forståelige avtalevilkår kunne bidra til at de i større grad forstår formålet med hvorfor og hva personopplysningene deres skal brukes til, og at de derfor kan føle seg tryggere på at det de deler ikke vil bli misbrukt. Dette impliserer at den nye forordningen kan bidra til å redusere personvernutfordringen knyttet til følelsen av at man ikke har kontroll over egne personopplysninger.

I tillegg tyder mye på at de nye rettighetene som kommer med den nye forordningen kan føre til at maktforholdet mellom produsent og forbruker flyttes i favør av forbrukeren. Forbrukerne

vil i større grad kunne være med å bestemme hva som aksepteres i markedet når de forstår verdien av egne personopplysninger og hva de skal brukes til. Med retten til dataportabilitet og retten til sletting kan de også enkelt be om at alle personopplysninger som er lagret hos en virksomhet skal overføres til en ny leverandør eller slettes helt dersom de ikke er fornøyde med en tjeneste. Dette indikerer at økt fokus på personvern antakeligvis vil bli viktigere for alle virksomheter fremover, fordi forbrukerne kommer til å etterspørre det.

Mye tyder videre på at godt personvern vil bli en essensiell faktor for tillitsforholdet mellom kunde og leverandør, og at en lite gjennomslagskraftig behandling av personopplysninger i tjenester, kan føre til «omdømmestryk». Dette kan underbygge argumentet fra tidligere diskusjon, om at en bot fra Datatilsynet antakeligvis ikke er det eneste som vil gjøre skade hos en virksomhet ved misbruk av personopplysninger eller brudd på kravene til informasjonssikkerhet.

Til slutt kan det også nevnes at D.D. i Storebrand argumenterer for at folkeopplysning om personvern vil være et bedre virkemiddel for å beskytte innbyggernes personvern, enn at Datatilsynet skal gå inn og regulere hva virksomheter har lov til å gjøre. I forbindelse med dette kan det argumenteres for at kravene i den nye forordningen i praksis kan føre til en slags folkeopplysning. Alle virksomheter vil gjennom sine nye plikter bidra til å øke folks forståelse for personvern, og forhåpentligvis gjøre dem mer bevisste på de valgene de tar knyttet til deling av personopplysninger. På denne måten sitter vi igjen med inntrykket av at poenget til D.D. i Storebrand vil ha gjennomslagskraft; forbrukerne vil etterspørre bedre personvern, og de vil fungere som «vaktbikkjer» i markedet. Virksomheter som bryter med lovgivningen eller forbrukernes forventninger kan risikere å bli skjøvet ut av markedet.

Det er imidlertid vanskelig å si hvordan økt bevissthet til personvern vil påvirke aksept av persontilpassede helseforsikringer i det norske markedet. På den ene siden kan det forsterke negative holdninger hos forbrukerne fordi de innser utfordringene som kommer med slike tjenester. På den andre siden kan de bli mer villige til å dele personopplysninger fordi de føler seg trygge på hvordan disse behandles. Vi tror derfor forbrukernes aksept av persontilpassede tjenester vil avhenge av forsikringsselskapenes evne til å utvikle attraktive og transparente tjenester som tilfredsstillende forbrukernes nye krav til personvern.

Delkonklusjon

Vi har nå sett at nordmenn har gitt uttrykk for at de generelt er skeptiske til å gi fra seg personopplysninger mot å få en vesentlig billigere forsikringspremie. Det har blitt påpekt at mange i dag likevel gir fra seg store mengder opplysninger til ulike tjenester, og at man kanskje ikke er helt bevisste på egne valg. I lys av våre funn ser det ut til at mekanismene i den nye personvernforordningen kan øke forbrukernes bevissthet til eget personvern, og gjøre dem mer bevisste på verdien av egne personopplysninger. Dette vil kunne påvirke maktforholdet mellom forbruker og produsent, og føre til en økt etterspørsel etter personvern blant forbrukerne. Dette kan i sin tur bidra til at noen av dagens tjenester vil dø ut, men også til at etterspørselen etter andre fintilpassede tjenester vil øke. Totalt sett ser det ut til at den nye forordningen derfor vil kunne få noen forbrukere til å bli mer skeptiske til persontilpassede helseforsikringer, mens den kan få andre til å akseptere dem i større grad. Det vil være opp til forsikringsselskapet å overbevise forbrukerne om at tjenestene deres er gode nok.

6.3 Teknologi

***Forskningsspørsmål 3:** Hvilket potensial har wearable-teknologi til å skape aksept av persontilpassede helseforsikringer i Norge?*

I lys av resultatene ser det ut til at wearables åpner for verdiskapning på flere nivåer som kan bidra positivt for aksepten av persontilpassede helseforsikringer i Norge. For forsikringsselskapet har vi inntrykk av at lønnsomhet naturlig inngår som et viktig argument for innføringen av persontilpassede helseforsikringer. Ved å aktivisere kundene gjennom bruk av wearables håper forsikringsselskapene på å gjøre dem friskere, noe som i sin tur vil redusere deres skadekostnader. For samfunnet som helhet kan dette bidra til forbedret folkehelse. For kundene personlig kan bruk av wearables i forsikring virke motiverende for å komme i gang med en sunnere livsstil, samt gi dem muligheten til å få en gunstigere forsikringspremie. Potensialet bruken av wearable-teknologi i forsikring har til å skape verdi både for samfunnet, forsikringsselskapet og for kunden mener vi derfor vil kunne ha en positiv effekt på aksepten av persontilpassede helseforsikringer i Norge.

I tillegg fremkommer det av resultatene at bruken av wearables til helseformål allerede er i rask fremvekst i Norge. Helseklokken Contact er et godt eksempel på et norsk nisjeprodukt som nylig har blitt lansert. Vi har også sett at det generelt har skjedd en kraftig økning i populariteten rundt bruk av wearables til personlige formål. Dette mener vi gir indikasjoner på at wearables

er godt akseptert som teknologi av norske forbrukere i dag. Det kan også tenkes at eksisterende kjennskap til wearables og deres tilhørende programvare og applikasjoner kan gjøre forbrukere mer tilbøyelige til å akseptere bruken av dem i forsikringer. Det kan for eksempel være lettere for en forbruker å la et forsikringsselskap få tilgang til data fra en tjeneste han eller hun allerede bruker og er kjent med, enn en tjeneste som krever at man setter seg inn i noe helt nytt. På denne måten har vi inntrykk av at eksisterende popularitet og kjennskap til wearable-teknologi, kan virke positivt på aksepten av persontilpassede helseforsikringer i det norske markedet.

Til tross for de positive effektene som kommer med bruken av wearables i helseforsikring, er det også fremtredende av resultatene at denne bruken skaper utfordringer på flere områder. Det fremkommer for eksempel at bruken av teknologi ikke bør komme i veien for ivaretagelsen av personvernet eller samfunnsverdier som settes høyt. Våre funn tyder på at det er flere utfordringer man bør ta hensyn til når man vurderer å ta i bruk wearables i persontilpassede helseforsikringer, og disse vil belyses videre i analysen.

Delkonklusjon

Vi har nå sett at wearable-teknologi har potensial til å skape verdi på tre hovedområder; For samfunnet som helhet, for forsikringsselskapet og for forbrukeren. Wearables er i rask fremvekst, og bruken av dem er populær. I tillegg kan det argumenteres for at eksisterende kjennskap til produktene kan bidra til å gjøre det lettere å overføre bruken av dem til nye områder, der i blant forsikring. Dette indikerer at wearables har et verdiskapningspotensial som kan virke positivt på aksepten av persontilpassede helseforsikringer. Samtidig må det tas i betraktning at det med teknologisk utvikling og bruk av wearables kommer en rekke nye utfordringer, som vi tror vil være avgjørende for om persontilpassede helseforsikringer blir akseptert i Norge.

6.4 Personvernutfordringer og informasjonssikkerhet

***Forskningsspørsmål 4:** I hvilken grad vil utfordringer knyttet til personvern og informasjonssikkerhet være avgjørende for om persontilpassede helseforsikringer vil aksepteres i Norge?*

Flere utfordringer knyttet til personvern og informasjonssikkerhet som oppstår som følge av teknologisk utvikling og bruk av wearables har blitt beskrevet i litteraturen. Vi vil i det følgende bruke funn fra intervjuene til å belyse effekten slike utfordringer kan ha på aksept av persontilpassede forsikringer i Norge.

Press til samtykke

Vi sitter igjen med inntrykk av at personvernutfordringer er noe alle intervjupersonene anser som en viktig diskusjon i forbindelse med den teknologiske utviklingen. Press til å gi fra seg samtykke er en av utfordringene som trekkes frem som spesielt relevant. Dersom man i praksis blir straffet for å si nei til å dele persondata, kan dette sies å være uforenlig med tanken om rettferdighet og respekt for folks privatliv. Dette vil for eksempel være tilfelle hvis forsikringen blir så mye billigere at man føler seg tvunget til å si ja, og det ikke finnes et annet godt alternativ. En implikasjon av dette er at tanken om at et individ skal ha rett til å leve sitt liv i fred, kanskje ikke alltid er forenelig med det som er mest samfunnsøkonomisk lønnsomt.

Det kan argumenteres for at press til samtykke ikke vil være en fremtredende utfordring for helseforsikring i Norge, da alle nordmenn har et godt alternativ i de offentlige helsetjenestene. Som en del av den norske velferdsstaten står lik tilgang til helsetjenester sterkt, og man skal i prinsippet ikke ha behov for å tegne en privat helseforsikring, slik man må i USA. Utfordringen blir imidlertid større dersom man begynner å vurdere persontilpasning på andre essensielle forsikringer hvor man ikke har et like godt alternativ. Man kan derfor diskutere om en aksept av persontilpassede helseforsikringer vil øke faren for at man lettere godtar en persontilpasning innenfor andre forsikringstjenester, som i sin tur kan føre til et press på forbrukeren som ikke er ønskelig. I lys av dette tyder mye på at man også bør være varsom for eventuelle ringvirkninger som en persontilpasset helseforsikring kan skape, når man vurderer å tillate produktet.

Videre kan det antydes at presset til å gi fra seg samtykke forsterker utfordringen knyttet til bånd på ytringsfrihet. Ved at man føler press til å gi fra seg persondata til en tjeneste, risikerer man at man også endrer sin atferd for å leve opp til kravene tjenesten setter. Dette indikerer at slike tjenester kan føre til at individer lar være å ytre seg eller handle på en måte som de egentlig ønsker, fordi konsekvensene for eksempel vil være en forsikringspremie som de ikke har råd til. Dersom man skal ivareta prinsippene personvernlovgivningen er bygget på, er det ønskelig å unngå situasjoner med «frivillig» tvang som slike tjenester kan medføre.

Algoritmeutfordringen

Bruken av kunstig intelligens for å ta beslutninger, og faren knyttet til at beslutningene tas på feil grunnlag, blir også trukket frem i intervjuene som en sentral utfordring. Det fremkommer som bekymringsfullt at algoritmene etter hvert blir så avanserte at man ikke lenger har oversikt over hvorfor eller hvordan en beslutning blir tatt. Det bemerkes også at algoritmer kan utvikle innebygde skjevheter som hindrer transparens i beslutningene. Dette impliserer at man kanskje bør sette grenser for bruken av teknologi, og at man bør være bevisst på hvilke beslutninger som skal vurderes manuelt og hvilke som kan tas ved hjelp av kunstig intelligens. Dette er noe man bør ta hensyn til når man bestemmer hva som skal være lov, og som vi også tolker at den nye lovgivningen delvis gjør gjennom å stille strengere krav til bruk av automatiske avgjørelser.

Informasjonssikkerhet

Informasjonssikkerhet blir videre belyst som en utfordring i intervjuene. Det påpekes at forsikringsselskaper allerede sitter på store mengder data om sine kunder, og at dette gjør forsikringsselskapene mer sårbare for dataangrep. Selv om finansnæringen i dag bruker store summer på å sikre seg, er aktørene som utfører angrepene ofte profesjonelle og organiserte. Dette impliserer at det alltid vil være en risiko for at uønskede hendelser kan oppstå. Jo mer sensitive opplysninger en virksomhet behandler, desto viktigere er det derfor at de bruker ressurser på å sikre sine datasystemer. Ettersom en persontilpasset helseforsikring vil innebære innsamling av store mengder helsedata, vil misbruk eller lekkasje av disse opplysningene kunne føre til alvorlige konsekvenser for forsikringsselskapenes lønnsomhet, omdømme og tillitsforhold med kunder. Dette impliserer at utfordringer knyttet til informasjonssikkerhet vil være viktig i vurderingen av om forsikringsselskaper skal tilby en persontilpasset helseforsikring. I tillegg tror vi at risikoen for dataangrep kan påvirke forbrukernes vilje til å gi fra seg personopplysninger, og dermed også deres aksept for produktet.

Delkonklusjon

Vi har nå sett at det følger flere personvernutfordringer med utviklingen av persontilpassede tjenester. Press til å gi fra seg samtykke samsvarer ikke med prinsippene om rettferdighet og respekt for privatlivets fred, og kan bidra til å legge bånd på enkeltindividers ytringsfrihet. Det er også utfordrende at algoritmer som tar avgjørelser kan ha uklare beslutningskriterier og innebygde skjevheter som fører til at forbrukeren blir urettferdig behandlet. I tillegg har vi sett at utfordringene knyttet til informasjonssikkerhet øker med bruk av personopplysninger. Dette er noe forsikringsselskaper må ta hensyn til når de vurderer å innføre persontilpassede helseforsikringer. Totalt sett tyder mye på at utfordringer knyttet til personvern og informasjonssikkerhet er noe som vil bidra til å begrense aksepten av persontilpassede helseforsikringer i Norge.

6.5 Norsk kultur og samfunnsprinsipper

***Forskningsspørsmål 5:** I hvilken grad vil norsk kultur og samfunnsprinsipper påvirke om persontilpassede helseforsikringer vil aksepteres i Norge?*

Vi vil i det følgende bruke funn fra intervjuene til å belyse hvordan norsk kultur og samfunnsprinsipper vil kunne påvirke om persontilpassede helseforsikringer vil aksepteres i Norge.

Frem til nå har vi sett at en av grunnene til at norske forbrukerne stiller seg negativt til deling av personopplysninger kan skyldes mangel på kunnskap om og bevissthet til personvern. Et annet aspekt som trekkes frem i intervjuene er at kulturelle forskjeller også kan forklare hvorfor nordmenn er lite villige til å dele personlig informasjon mot å få en billigere forsikring. Her mener vi det kan trekkes paralleller til hvordan man i Vesten har et individualistisk selvbegrep og derfor vegrer seg mot å dele data om seg selv. Frihet og retten til å leve et liv i fred er fremtredende i norsk kultur, og kan bidra til å forklare hvorfor nordmenn generelt virker negative til persontilpassede forsikringer.

Videre belyses det i intervjuene hvordan forsikringsløsninger basert på individuell risikoestimering utfordrer forsikringsprinsippet og den kollektive tankegangen det er bygget på. Det fremkommer at skreddersøm kontra forsikringskollektivet er et vanskelig dilemma, og at man i Norge kanskje ikke ønsker å nærme seg «de amerikanske tendensene». Den norske velferdsmodellen bygger på en kollektiv oppfatning om at sosial trygghet og likhet skal sikres

for alle, uavhengig av om man er fattig eller rik. De persontilpassede forsikringsmodellene kan sies å utfordre denne tankegangen, fordi man i slike modeller legger opp til å segmentere så mye som mulig. Det kan argumenteres for at dette fører til en forskjellsbehandling av deltakerne i kollektivet som strider mot velferdsprinsippene om likhet. Ettersom solidaritet står sterkt i den norske befolkningen tyder mye på at nordmenn vil være lite villige til å akseptere en slik forsikringsmodell sammenlignet med for eksempel amerikanere.

Det fremkommer av intervjuene at persontilpassede helseforsikringer kan forsterke utfordringer knyttet til at det skapes et A- og B-lag i samfunnet. Ved at markedet segmenteres, risikerer man at de som allerede er aktive og friske får alle de positive fordelene ved en persontilpasset forsikring. De andre som ikke har de riktige forutsetningene vil få en mye høyere premie, eller i verste fall ikke ha råd til forsikring. Ved persontilpasning vil man også kunne risikere å forsterke det todelte helsevesenet som noen hevder helseforsikring i utgangspunktet skaper. Ettersom prinsippene i den norske velferdsstaten strider mot å skape forskjeller i samfunnet på denne måten, kan mye tyde på at dette er noe som vil holde tilbake aksepten av persontilpassede helseforsikringer i Norge.

Samtidig bør de positive sidene ved helseforsikring som belyses i intervjuene også nevnes. Det hevdes for eksempel at helseforsikring er viktig i samfunnet fordi den bidrar til å redusere sykehuskøene fremfor at den tillater folk å snike, samt at den får folk raskere tilbake i jobb etter sykdom. Det kan derfor argumenteres for at persontilpassede helseforsikringer vil kunne forsterke disse positive aspektene, fordi den kan motivere folk til å bli mer aktive, og på denne måten forbedre folkehelsen og redusere sykehuskøene.

Delkonklusjon

Vi har sett at kulturelle trekk som omhandler individualisme og ivaretagelse av privatlivet kan bidra til å forklare hvorfor nordmenn generelt virker negative til å gi fra seg helseopplysninger mot reduserte forsikringspremier. Vi har også diskutert hvordan grunnprinsipper i den norske velferdsmodellen kan øke forståelsen for hvorfor nordmenn kan virke skeptiske til persontilpassede helseforsikringer. Dette fordi segmenteringen av markedet disse forsikringsmodellene legger opp til, strider i mot prinsippene om likhet og rettferdighet. Norsk kultur og samfunnsprinsipper vil antakeligvis derfor påvirke aksepten av persontilpassede helseforsikringer i Norge negativt.

7. Konklusjon og anbefalinger

7.1 Konklusjon

Vi har i denne utredningen utforsket hva som vil være avgjørende for om persontilpassede helseforsikringer vil aksepteres i Norge.

Etter endt studium ser vi at den nye personvernlovgivningen på den ene siden vil stille strengere krav til hvordan virksomheter generelt kan behandle og bruke personopplysninger i tjenester. Det innføres en rekke nye plikter, og kravene til sikring av datasystemer kommer til å være gjennomgående strengere. For finansnæringen har vi derimot inntrykk av at det isolert sett vil bli enklere å behandle personopplysninger. Dette fordi det ser ut til at konsesjonsplikten vil bortfalle helt, og fordi aktørene i næringen har gode forutsetninger for å oppfylle kravene etter den nye lovgivningen. Samtidig fremkommer det at det lovteknisk ikke burde være umulig å få konsesjon til en persontilpasset helseforsikring i dag. Likevel vet vi ikke om Datatilsynet faktisk ville gitt godkjenning til en slik forsikring, da den utfordrer flere av prinsippene de jobber for å ivareta. Våre funn tyder altså på at lovgivningen vil påvirke forsikringssektorens handlingsrom, men vi tror de andre faktorene vi har sett på vil være vel så avgjørende for om en persontilpasset helseforsikring aksepteres i Norge.

Vi har funnet at flere av faktorene vi har utforsket kan bidra til å begrense aksepten av persontilpassede helseforsikringer. For det første medfører teknologisk utvikling og bruk av wearables flere utfordringer knyttet til personvern og informasjonssikkerhet. For det andre kan særtrekk ved norsk kultur gi økt forståelse for hvorfor nordmenn er opptatt av å prioritere ivaretagelsen av personvern og retten til et fredelig privatliv når nye tjenester utvikles. Videre kan en persontilpasset helseforsikring sies å utfordre den kollektive tankegangen både forsikringsprinsippet og den norske velferdsstaten er bygget på. Mye tyder derfor på at norsk kultur og samfunnsprinsipper bidrar til å holde tilbake aksepten av persontilpassede helseforsikringer i Norge.

Til tross for utfordringene er Norge et land som i dag ligger langt fremme i bruken av teknologi. Vi ser at bruken av wearables er populær, og har potensial til å skape verdi for samfunnet, organisasjoner og forbrukere. Kjennskap til wearable-teknologien vil også kunne bidra til å gjøre det lettere å overføre den til nye bruksområder. I forbindelse med dette mener vi at

bevissthet til personvern vil være svært avgjørende for om wearables vil aksepteres i bruk i helseforsikringer. Mye tyder på at norske forbrukere er lite bevisste på hva de gir fra seg av personopplysninger, og at det ikke alltid er konsistens mellom det de sier at de ønsker og hva de faktisk gjør. Her mener vi den nye personvernlovgivningen vil spille en viktig rolle. De nye rettighetene som innføres vil kunne bidra til å gjøre forbrukerne mer bevisste på eget personvern, og få dem til å forstå verdien av egne personopplysninger. Dette vil i sin tur flytte markedsmakt over fra produsent til forbruker, og føre til økt etterspørsel etter personvern i markedet. Vi tror derfor at lovgivningen vil bidra til å skape et marked med mer transparente tjenester som ivaretar forbrukerens interesser i større grad enn tidligere.

Videre tror vi økt bevissthet til personvern kan ha to effekter på aksepten av persontilpassede helseforsikringer. På den ene siden kan mer kunnskap om personvern føre til at forbrukerne i større grad stiller seg kritiske til å gi fra seg personopplysninger. Mange forbrukere er i dag ikke klar over hvor store mengder data de egentlig godtar å gi fra seg til tjenester, og bedre innsikt i dette vil kunne føre til at de blir mer skeptiske.

På den andre siden kan økt bevissthet til personvern bidra til at forbrukerne føler seg tryggere på at personopplysninger blir behandlet på en måte som samsvarer med deres ønsker. Med de nye rettighetene skal forbrukerne kunne forstå alt de samtykker til, og dataene som samles inn skal utelukkende benyttes til å oppnå tjenestens formål. De vil på denne måten få større kontroll over egne personopplysninger. Dette er noe vi mener vil kunne medføre at forbrukerne lettere aksepterer persontilpassede helseforsikringer. Vi tror dermed at det som blir mest avgjørende for hva forbrukerne aksepterer vil være forsikringsselskapenes evne til å utvikle en tjeneste som er så attraktiv og transparent at forbrukerne «bare må ha den».

Til slutt vil vi påpeke at Norge har et aktivt Datatilsyn som lager gode veiledere til virksomheter for hvordan de skal behandle personopplysninger og etterleve lovgivningen. Vi har også en finansnæring som tilsynelatende samarbeider godt med Datatilsynet om å utvikle retningslinjer for hvordan det skal være akseptabelt å operere. Med bakgrunn i dette mener vi norske forsikringsselskaper har gode forutsetninger for å klare å ta i bruk wearables i forsikring på en måte som ivaretar både egne og forbrukernes interesser på en akseptabel måte. Vi vil derfor antyde at det kun er spørsmål om tid før vi ser den første persontilpassede helseforsikringen i Norge.

7.2 Styrker og svakheter

En potensiell svakhet ved utredningen er antall intervjuer vi har gjennomført. På grunn av begrenset tid og ressurser hadde vi kun mulighet til å gjennomføre fire intervjuer, med totalt åtte intervjupersoner. Dersom vi hadde hatt muligheten ville vi snakket med flere forsikringsselskaper, for å på den måten kunne belyse deres synspunkter i enda større grad. Det er for eksempel ikke gitt at andre forsikringsaktører forholder seg til utviklingen av persontilpassede forsikringsprodukter på samme måte som Storebrand, men dette er noe vi har tatt en antakelse om. På den annen side var de personene vi intervjuet nøye valgt ut, og har alle vært viktige deltakere i debatten om personvern og implikasjonene dette har for forsikringsbransjen. Vi mener derfor at vi likevel har klart å belyse de viktigste faktorene ved utviklingen av persontilpassede helseforsikringer.

For casestudier er en viktig kritikk at det kan være vanskelig å generalisere resultatene til andre sammenhenger (Saunders, et al., 2012). Vi har i denne studien kun fokusert på finans- og forsikringsnæringen, og denne har visse særtrekk relatert til vår problemstilling som ikke gjelder for andre næringer. Vi har heller ikke benyttet oss av noe eksisterende teoretisk rammeverk for å besvare problemstillingen. Dette bidrar til å gjøre funnene våre mindre overførbare til andre studier. Samtidig mener vi at mange av resultatene som fremkommer i studien vil kunne gi nyttig innsikt til andre næringer som står overfor utfordringer knyttet til innsamling av persondata. Vi mener for eksempel at utfordringer knyttet til personvern og datasikkerhet som avdekkes i studien, vil være gjeldende og bør tas hensyn til når man utvikler persontilpassede tjenester, uavhengig av hvilken bransje man opererer i.

7.3 Forslag til videre forskning

I løpet av arbeidet med denne studien har det fremkommet flere interessante aspekter vi kunne tenkt oss å forske videre på.

Vårt første forslag til videre forskning er å se nærmere på det at arbeidsgiver betaler for helseforsikring, og om dette vil ha noen betydning for hvordan persontilpassede helseforsikringer vil se ut i Norge. Det fremgår i litteraturen at de aller fleste nordmenn som har denne forsikringen i dag får den dekket gjennom arbeidsgiver. Vi har to perspektiver knyttet til dette som vi kunne tenkt oss å se nærmere på. Det første er knyttet til rabatten og insentivene til å bli mer aktiv, som en persontilpasset helseforsikring legger opp til. Dersom det er

arbeidsgiver som betaler forsikringen, vil en pris som reguleres av aktivitet i prinsippet ikke påvirke forsikringstakeren direkte. Vil dette hindre effekten forsikringsselskapene ønsker å oppnå – nemlig å skape insentiver til å trene mer – når forsikringstaker uansett ikke selv drar nytte av rabatten på forsikringspremien? I så fall vil kanskje ikke forsikringsselskapene klare å redusere skadekostnadene i den grad de ønsker, og poenget med hele forsikringsmodellen faller bort?

Det andre vi kunne tenkt oss å forske videre på, fremdeles med bakgrunn i at arbeidsgiver betaler forsikringen, er om en persontilpasning vil kunne gi bedriftens ledelse insentiver til å iverksette interne programmer for å øke ansattes aktivitetsnivå. Jo mer aktive de ansatte er, desto lavere vil i så fall bedriftens forsikringsutgifter være. Kanskje vil dette føre til at bedriften ønsker å belønne sine ansatte for å trene mye. I så fall vil insentivene hos de ansatte kunne holdes oppe av bedriften selv, og ikke av forsikringsselskapet.

I tillegg syns vi det kunne vært interessant å forske på om utfordringen knyttet til at det kan skapes et A- og B-lag i samfunnet som følge av helseforsikring, vil reduseres dersom arbeidsgiver dekker forsikringen. Det kan tenkes at når arbeidsgiver betaler for at alle ansatte skal få ha helseforsikring, vil det ikke nødvendigvis bare være de som har «best» forutsetninger som drar nytte av å ha forsikringen. Dersom arbeidsgiver velger å sette i gang et program for å få ansatte i aktivitet, vil forsikringen kunne ha positive effekter for samfunnet som helhet. Det kan hjelpe mange med å komme i gang med trening og en sunnere livsstil, uten at de uønskede effektene knyttet til klasseskille blir like fremtredende.

Et annet aspekt vi foreslår at kan forskes videre på er om bruken av wearables i forsikring kan gi inspirasjon til å bruke wearables i offentlige helsetjenester. Det kom frem i et av intervjuene at bruk av teknologi i privat sektor ofte legger grunnlaget for hva som skjer videre i det offentlige. Det kunne derfor vært interessant å se nærmere på om bruken av wearable-teknologi i det private vil fungere som en katalysator for å bruke den i det offentlige. Det ville vært spennende å forske på om og hvordan bruk av wearables kan skape verdi i for eksempel eldreomsorgen. Vil offentlige institusjoner akseptere bruken av slik teknologi, til tross for utfordringene dette medfører som har blitt diskutert i denne studien?

Vårt siste forslag til videre forskning er knyttet til konkurranse i det norske forsikringsmarkedet. Det fremgår av vår studie at noen parter mener at personvernlovgivningen har hindret norske

forsikringselskaper i å ligge langt fremme på innovasjon, mens andre hevder at mangelen på innovasjon skyldes tung organisasjonsstruktur. Det kunne derfor vært interessant å studere nærmere hva slags struktur tradisjonelle forsikringselskaper har, og sammenlignet med selskaper som for eksempel Schibsted. Schibsted kan antydes å være Norges svar på Google, og vi synes det hadde vært svært spennende å utforske om dette selskapet kan være en potensiell trussel for norske forsikringselskaper når det gjelder persontilpassede forsikringer. Schibsted er svært dyktige til å behandle persondata, og de besitter mye informasjon om sine brukere som potensielt kan anvendes til å persontilpasse tjenester. Det virker samtidig som at de har en mer «frempå» holdning når det gjelder å utnytte persondata, sammenlignet med finansinstitusjoner. Det blir derfor spennende å se om innovative selskaper som Schibsted kommer til å innta nye arenaer hvor behandling av personopplysninger står sentralt, og utfordre forsikringselskaper slik man har fryktet at Google og Facebook kan komme til å gjøre.

8. Litteraturliste

- Accenture. (2016, 8. Juni). *Consumers' Use of Health Apps and Wearables in Norway Increased in Past Two Years, Accenture Survey Finds*. Hentet 6. Juni, 2017, fra Accenture News Release: <https://newsroom.accenture.com/industries/health-public-service/consumers-use-of-health-apps-and-wearables-in-norway-increased-in-past-two-years-accenture-survey-finds.htm>
- Article 29 Data Protection Working Party. (2013). *Opinion 03/2013 on purpose limitation (WP 203)*. Brussels: Directorate C of the European Commission, Directorate General Justice.
- Berg, B. L., & Lune, H. (2012). *Qualitative Research Methods for the Social Sciences*. Pearson.
- Berrahal, S., & Boudriga, N. (2016). Chapter 2 - The Risks of Wearable Technologies to Individuals and Organizations. In J. Gammack, D. Kerr, & A. Marrington, *Managing Security Issues and the Hidden Dangers of Wearable Technologies* (s. 18-46). Hershey, Pennsylvania: IGI Global.
- Bjørkeng, P. K. (2017, 3. April). *Er du villig til å la deg overvåke for å spare penger? Nå kommer trenden for fullt*. Hentet 12. April, 2017, fra Aftenposten: <http://www.aftenposten.no/viten/Er-du-villig-til-a-la-deg-overvake-for-a-spare-penger-Na-kommer-trenden-for-fullt-617017b.html>
- Brat, E., Heydorn, S., Stover, M., & Ziegler, M. (2013, 25. Mars). *Big Data: The Next Big Thing for Insurers?* Hentet 20. Februar, 2017, fra Boston Consulting Group: https://www.bcgperspectives.com/content/articles/insurance_it_performance_big_data_next_big_thing_for_insurers/
- Bridges, W., Brooker, C. (Manusforfattere), & Watkins, J. (Regissør). (2016). *Black Mirror: Shut up and Dance* [TV-serie].
- Bustillos, M. (2013, 22. Mai). Little Brother is Watching You.
- Christensen, J., & Berg, O. T. (2017, 12. Januar). *Velferdsstat*. Hentet 22. Mai, 2017, fra Store Norske Leksikon: <https://snl.no/velferdsstat>
- Christl, W., & Spiekermann, S. (2016). *Networks of Control - A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*. Wien: Facultas Verlags- und Buchhandels AG.
- Cisco. (2017). *Cisco 2017 Annual Cybersecurity Report*. Cisco.
- ContinYou. (2017). *Om oss*. Hentet 4. April, 2017, fra ContinYou: <https://continyou.no/about/>
- Dagens Næringsliv. (2016, 24. November). *Agenda vil beskatte helseforsikring*. Hentet 7. Mars, 2017, fra Dagens Næringsliv: <http://www.dn.no/nyheter/2016/11/24/0458/Politikk/agenda-vil-beskatte-helseforsikring>
- Datatilsynet. (2013). *Big Data - Personvernprinsipper under press*. Datatilsynet.

- Datatilsynet. (2015, 5. Mars). *Syv Steg til Innebygd Personvern*. Hentet 22. Mars, 2017, fra Datatilsynet: <https://www.datatilsynet.no/Teknologi/Innebygd-personvern/>
- Datatilsynet. (2016a, 18. Februar). *Hva blir nytt med forordningen?* Hentet 1. Mars, 2017, fra Datatilsynet: <https://www.datatilsynet.no/Regelverk/EUs-personvernforordning/hva-blir-nytt-med-forordningen/>
- Datatilsynet. (2016b, 27. Januar). *Hva er en personopplysning?* Hentet 27. Februar, 2017, fra Datatilsynet - Personvern på 1-2-3: <https://www.datatilsynet.no/personvern/Personopplysninger/>
- Datatilsynet. (2016c, 11. August). *Personvernprinsippene*. Hentet 27. Februar, 2017, fra Datatilsynet: <https://www.datatilsynet.no/personvern/Personvernprinsipper/>
- Datatilsynet. (2017a). *Alle bør samarbeide i egne nettverk og følge bransjenormer*. Hentet 6. Mars, 2017, fra Datatilsynet - Hva betyr de nye personvernreglene for din virksomhet: <https://www.datatilsynet.no/Regelverk/EUs-personvernforordning/hva-betyr/alle-bor-samarbeide-i-egne-nettverk-og-folge-bransjenormer/?showContentList=true&showDetailedContentList=false&readMode=false>
- Datatilsynet. (2017b). *Alle må kunne oppfylle borgernes nye rettigheter*. Hentet 3. Mars, 2017, fra Datatilsynet - Hva betyr de nye personvernreglene for din virksomhet?: <https://www.datatilsynet.no/Regelverk/EUs-personvernforordning/hva-betyr/alle-ma-kunne-oppfylle-borgernes-nye-rettigheter/>
- Datatilsynet. (2017c). *Alle skal bygge personvern inn i nye løsninger*. Hentet 6. Mars, 2017, fra Datatilsynet - Hva betyr de nye personvernreglene for din virksomhet?: <https://www.datatilsynet.no/Regelverk/EUs-personvernforordning/hva-betyr/alle-skal-bygge-personvern-inn-i-nye-losninger/?showContentList=true&showDetailedContentList=false&readMode=false>
- Datatilsynet. (2017d). *Alle skal ha en forståelig personvernerklæring*. Hentet 3. Mars, 2017, fra Datatilsynet - Hva betyr de nye personvernreglene for din virksomhet?: <https://www.datatilsynet.no/Regelverk/EUs-personvernforordning/hva-betyr/punkt-1/?showContentList=true&showDetailedContentList=false&readMode=false>
- Datatilsynet. (2017e, 25. Januar). *Melding og konsesjon*. Hentet 6. Mars, 2017, fra Datatilsynet: <https://www.datatilsynet.no/personvern/Melding-og-konsesjon/>
- Datatilsynet. (2017f). *Nye personvernregler fra 2018*. Hentet 1. Mars, 2017, fra Datatilsynet: <https://www.datatilsynet.no/Regelverk/EUs-personvernforordning/>
- Datatilsynet. (2017g). *Om Datatilsynet*. Hentet 20. Februar, 2017, fra Datatilsynet: <https://www.datatilsynet.no/Om-Datatilsynet/Oppgaver/>
- Datatilsynet og Teknologirådet. (2014). *Personvern, Tilstand og trender 2014*. Oslo: Datatilsynet og Teknologirådet.
- Datatilsynet og Teknologirådet. (2016). *Personvern 2016, Tilstand og Trender*. Oslo: Datatilsynet og Teknologirådet.

- Datatilsynet og Teknologirådet. (2017). *Personvern 2017, Persontilpasning og kunstig intelligens*. Oslo: Datatilsynet og Teknologirådet.
- Døskeland, T. (2014). *Personlig Finans*. Bergen: Fagbokforlaget.
- Deel, L. v., Nadimpalli, R., Sahoo, D., Verma, S., & Vervuurt, M. (2016, 18. Januar). *Wearable Devices and Their Applicability in the Life Insurance Industry*. Hentet 20. Februar, 2017, fra Capgemini: https://www.capgemini.com/resource-file-access/resource/pdf/wearable_devices_and_their_applicability_in_the_life_insurance_industry.pdf
- Direktoratet for e-helse. (2016). *Normen for informasjonssikkerhet - Helse- og omsorgstjenesten*. Oslo: Direktoratet for e-helse. Hentet fra <https://ehelse.no/Documents/Normen/2%20Normen%20prosessdok/Norm%20for%20informasjonssikkerhet%205.2%20%20utgave.pdf>
- E24. (2014, 5. Juni). *Titusenvis av nordmenn kjøper teknoarmbånd*. Hentet 6. Juni, 2017, fra E24: <http://e24.no/digital/titusenvis-av-nordmenn-kjoeper-teknoarmbaand/23222439>
- Eidem, M. (2017, 1. Februar). *Dårlig Datasikkerhet Gir Bedrifter Store Tap*. Hentet 22. Mars, 2017, fra Dagens Næringsliv: <http://www.dn.no/nyheter/2017/02/01/1959/Teknologi/darlig-datasikkerhet-gir-bedrifter-store-tap>
- Epstein, Z. (2017, 15. Mai). *WannaCry: Everything you need to know about the global ransomware attack*. Hentet 7. Juni, 2017, fra BGR: <http://bgr.com/2017/05/15/wannacry-ransomware-virus-windows-wannacry-explainer/>
- Feder, B. J. (2008, 12. Mars). *A Heart Device Is Found Vulnerable to Hacker Attacks*. Hentet 10. April, 2017, fra New York Times: http://www.nytimes.com/2008/03/12/business/12heart-web.html?_r=0
- Finans Norge. (2016). *Statistikk og Nøkkeltall for Skadeforsikring 2016*. Finans Norge.
- Finans Norge. (2017a). *Det er viktig å være forsikret*. Hentet 28. Mars, 2017, fra <https://www.finansnorge.no/tema/ny-i-norge-bank--og-forsikringstjenester/det-er-viktig-a-vare-forsikret/>
- Finans Norge. (2017b). *Om Finans Norge*. Hentet 23. Mai, 2017, fra Finans Norge: <https://www.finansnorge.no/om-finans-norge/>
- Fjørtoft, L. E. (2017, 15. Februar). *Personopplysninger til begjær (og besvær)*. Hentet 8. Mars, 2017, fra PwC - @stake, God styring og kontroll: <http://blogg.pwc.no/styringogkontroll/personopplysninger-til-begjaer-og-besvaer>
- Gammack, J., Kerr, D., & Marrington, A. (2016). Chapter 1 - The Promise and Perils of Wearable Technologies. In J. Gammack, & A. Marrington, *Managing Security Issues and the Hidden Dangers of Wearable Technologies* (s. 1-17). Hershey, Pennsylvania: IGI Global.
- Grønmo, S. (2004). *Samfunnsvitenskapelige Metoder*. Bergen: Fagbokforlaget.

- Grymer, T., & Strønen, A. (2016, 27. Mai). *Nesten en halv million nordmenn har privat helseforsikring*. Hentet 1. Mars, 2017, fra NRK.no: <https://www.nrk.no/norge/nesten-en-halv-million-nordmenn-har-privat-helseforsikring-1.12967399>
- Ims, K. J. (1992). *Informasjonsetikk i praksis: Datasikkerhet og personvern*. Oslo: Tano.
- Johannessen, A., Christoffersen, L., & Tufte, P. A. (2011). *Forskningsmetode for Økonomisk-Administrative Fag* (3. utgave ed.). Oslo: Abstrakt Forlag.
- Jones, R., Schur, M. (Manusforfattere), & Wright, J. (Regissør). (2016). *Black Mirror: Nosedive* [TV-serie].
- Justis- og Beredskapsdepartementet. (2017). *Justis- og Beredskapsdepartementet*. Hentet 29. Mai, 2017, fra Justis- og Beredskapsdepartementet: <https://www.regjeringen.no/no/dep/jd/id463/>
- Kahneman, D. (2011). *Thinking Fast and Slow*. Farrar, Straus & Giroux.
- Kerr, D., & Gammack, J. (2016). Chapter 12 - Conclusions: Where Next for Wearables? In D. Kerr, & J. Gammack, *Managing Security Issues and the Hidden Dangers of Wearable Technologies* (s. 289-299). Hershey, Pennsylvania: IGI Global.
- Kuhnle, S., & Kildal, N. (2011). Velferdsstatens Idégrunnlag i Perspektiv. In A. Hatland, S. Kuhnle, & T. I. Romøren (Ed.), *Den Norske Velferdsstaten* (4. utgave, s. 15-39). Oslo: Gyldendal Akademisk.
- Lovdata. (2000, 4. April). *Kapittel 1. Lovens formål og virkeområde*. Hentet 27. Februar, 2017, fra Lov om behandling av personopplysninger: https://lovdata.no/dokument/NL/lov/2000-04-14-31/KAPITTEL_1#§1
- Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Hung, A. (2011). *Big data: The next frontier for innovation, competition, and productivity*. McKinsey Global Institute.
- Marshall, C., & Rossman, G. B. (2006). *Designing Qualitative Research*. Thousand Oaks, CA: Sage.
- Miaoui, Y., & Boudriga, N. (2015). Economics of Pricacy: A Model for Protecting Against Cyber Data Disclosure Attacks. (72), s. 569-579.
- Moderna. (2016, 11. Februar). *Nu kan vardagsmotionen ge dig rabatt på din sjuk- och olycksfallsförsäkring*. Hentet 12. April, 2017, fra Moderna Försäkringar: <http://news.cision.com/se/moderna-forsakringar/r/nu-kan-var-dags-motion-ge-dig-rabatt-pa-din-sjuk--och-olycksfallsforsakring,c9911996>
- Nasjonal sikkerhetsmyndighet. (2016). *Helhetlig IKT-risikobilde 2016*. Sandvika: Nasjonal sikkerhetsmyndighet.
- Netflix (Produksjonsselskap). (2016). *Black Mirror Season 3* [Tv-serie].
- Orwell, G. (1949). *1984*. New York: Harcourt.
- Rema 1000. (2016, 20. August). *Rema lanserer forsikring*. Hentet 20. Februar, 2017, fra Rema 1000 Nyheter: <https://www.rema.no/nyheter/rema-lanserer-forsikring/>

- Rema Forsikring. (2017). *Spørsmål og svar om Kjør smart*. Hentet 20. Februar, 2017, fra Rema Forsikring: <https://www.remaforsikring.no/forsikringer/bil/kjor-smart/>
- Riisnæs, R., & Schilvold, S. S. (2016, 9. Mai). *Ny personvernforordning*. Hentet 1. Mars, 2017, fra Wikborg Rein: <https://www.wr.no/aktuelt/nyhetsbrev/2016/ny-personvernforordning/>
- Risung, K. M., & Songe-Møller, J. (2016, 4. Mai). *Nyhetsbrev - Slik blir de nye personvernreglene*. Hentet 7. Mars, 2017, fra Schjødt: <http://www.schjodt.no/aktuelt/nyhetsbrev/nyhetsbrev-slik-blir-de-nye-personvernreglene/>
- Salomonsen, J. (2015, 2. November). *Hva skjer når alle tingene dine kobles til internett?* Hentet 7. Juni, 2017, fra Forskning.no: <http://forskning.no/internett-teknologi/2015/10/internet-things-gir-forskere-hodebry>
- Saunders, M., Lewis, P., & Thornhill, A. (2012). *Research Methods for Business Students* (6. utgave ed.). Pearson.
- Schackt, J. (2016, 21. April). *Kultur*. Hentet 30. Mai, 2017, fra Store Norske Leksikon: <https://snl.no/kultur>
- Sparebank 1. (2017). *Smart Bilforsikring*. Hentet 6. Juni, 2017, fra Sparebank 1: Forside Smart Helseforsikring: <https://www.sparebank1.no/nb/bank/privat/forsikring/bil-bat-og-andre-kjoretoy/bilforsikring/smart-bilforsikring.html>
- Storebrand. (2017). *Helseforsikring*. Hentet 1. Mars, 2017, fra Storebrand: Forside Helseforsikring: <https://www.storebrand.no/privat/forsikring/helseforsikring>
- The Generali Group. (2016, 6. September). *Generali launches Generali Vitality in France*. Hentet 14. Mars, 2017, fra <http://www.generali.com/media/News/Generali-launches-Generali-Vitality-in-France>
- Tjora, A. (2010). *Kvalitative Forskningsmetoder i Praksis*. Oslo: Gyldendal Akademisk.
- Tjora, A., & Skatvik, F. (2017, 1. Februar). *Solidaritet*. Hentet 23. Mai, 2017, fra Store Norske Leksikon: <https://snl.no/solidaritet>
- Vitality Corporate Services Limited. (2017a, 14. Mars). *About Us*. Hentet 14. Mars, 2017, fra Vitality: <https://www.vitality.co.uk/about/>
- Vitality Corporate Services Limited. (2017b, 14. Mars). *How Vitality rewards work*. Hentet 14. Mars, 2017, fra Vitality: <https://www.vitality.co.uk/rewards/>
- Vitality Corporate Services Limited. (2017c, 14. Mars). *Partners and rewards*. Hentet 14. Mars, 2017, fra Vitality: <https://www.vitality.co.uk/rewards/partners/>
- Wadhwa, T. (2012, 6. Desember). *Yes, You Can Hack A Pacemaker (And Other Medical Devices Too)*. Hentet 10. April, 2017, fra Forbes: <https://www.forbes.com/sites/singularity/2012/12/06/yes-you-can-hack-a-pacemaker-and-other-medical-devices-too/#d3e380c6853c>

- Wheelwright, G. (2016, 21. November). *Wearable technology: gathering data from tooth to toe*. Hentet 20. Februar, 2017, fra Financial Times:
<https://www.ft.com/content/9b00b05c-70fe-11e6-a0c9-1365ce54b926>
- Yin, R. K. (2009). *Case Study Research: Design and Methods* (4. utgave). Thousand Oaks, CA: Sage.

9. Vedlegg

9.1 Tilbakemelding fra NSD



Knut Oddvar Ims
Institutt for strategi og ledelse NHH
Helleveien 30
5045 BERGEN

Vår dato: 31.05.2017

Vår ref: 54199/3/HIT/IRH

Deres dato:

Deres ref:

TILBAKEMELDING PÅ MELDING OM BEHANDLING AV PERSONOPPLYSNINGER

Vi viser til melding om behandling av personopplysninger, mottatt 25.04.2017. All nødvendig informasjon om prosjektet forelå 29.05.2017. Meldingen gjelder prosjektet:

54199
Daglig ansvarlig
Student

Digitalisering i Forsikring
Knut Oddvar Ims
Nadia Vestre Iveland

Det fremgår at prosjektet allerede er påbegynt ved at informasjon er gitt til utvalget og datainnsamling er påbegynt. Personvernombudet finner dette beklagelig, og minner om at prosjekter som omfattes av meldeplikten skal meldes senest 30 dager før oppstart. Personvernombudet har vurdert prosjektet og finner at behandlingen av personopplysninger omfattes av meldeplikten iht. personopplysningsloven forskrifter § 31.

Prosjektvurdering

Utvalget ble informert skriftlig om prosjektet og samtykket til deltakelse. Informasjonsskrivet var noe mangelfullt utformet, men studenten opplyser at det vil bli gitt nødvendig tilleggsinformasjon jf. epost 29.05.2017.

Personvernombudet legger til grunn at forsker etterfølger Norges Handelshøyskole sine interne rutiner for datasikkerhet. Dersom personopplysninger lagres på mobile enheter, bør opplysningene krypteres tilstrekkelig.

Det oppgis at indirekte identifiserende opplysninger skal publiseres. Studenten opplyser at det vil innhentes eksplisitt samtykke fra den enkelte til dette. Vi anbefaler at deltakerne gis anledning til å lese igjennom egne opplysninger og godkjenne disse før publisering.

Forventet prosjektslutt er 08.06.2017. Ifølge prosjektmeldingen skal innsamlede opplysninger da anonymiseres. Anonymisering innebærer å bearbeide datamaterialet slik at ingen enkeltpersoner kan gjenkjennes. Det gjøres ved å:

- slette direkte identifiserende personopplysninger (som navn/koblingsnøkkel)
- slette/omskrive indirekte identifiserende personopplysninger (identifiserende sammenstilling av bakgrunnsopplysninger som f.eks. bosted/arbeidssted, alder og kjønn)
- slette digitale lydopptak

Avslutning

Personvernombudets vurdering forutsetter at prosjektet gjennomføres i tråd med opplysningene gitt i meldeskjemaet, korrespondanse med personvernombudet, samt personopplysningsloven med forskrifter.

Det gjøres oppmerksom på at det skal gis ny melding dersom behandlingen endres i forhold til de opplysninger som ligger til grunn for personvernombudets vurdering. Endringsmeldinger gis via et eget skjema, http://www.nsd.uib.no/personvernombud/meld_prosjekt/meld_endringer.html. Det skal også gis melding etter tre år dersom prosjektet fortsatt pågår. Meldinger skal skje skriftlig til ombudet.

Personvernombudet har lagt ut opplysninger om prosjektet i en offentlig database,
<http://pvo.nsd.no/prosjekt>.

Personvernombudet vil ved prosjektets avslutning, 08.06.2017, rette en henvendelse angående status for
behandlingen av personopplysninger.

Ta gjerne kontakt dersom noe er uklart.

Vennlig hilsen


Kjersti Haugstvedt


Hildur Thorarensen

Kopi:
Nadia Vestre Iveland, Østre Murallmenningen 12, 5012 BERGEN

9.2 Intervjuguider

9.2.1 Justis- og Beredskapsdepartementet

Informasjon før intervjuet starter

- Fortelle kort om oss og hva oppgaven handler om.
- Forklare intervjuets hensikt.
- Spørre om konfidensialitet og anonymitet.
- Spørre om vi kan bruke lydopptaker.
- Informere om intervjuets varighet.

Generelt

- Hva er din rolle i arbeidet med og implementeringen av den nye personvernforordningen?
- Hvordan arbeider dere med loven nå?
- Vi har lest at en forordning ikke får direkte virkning i Norge, men at den skal «gjøres til del av avtalepartenes interne rettsorden». Samtidig har vi lest at EUs forordning kommer til å erstatte den gamle loven. Hvordan kommer den til å implementeres?
- Videre er det skrevet at forordninger krever «gjennomføring i norsk rett». Hva betyr dette?

Mulighet for nasjonal regulering

Bortfall av konsesjons- og meldeplikt

I forbindelse med at de nye reglene fører til forenklinger, leser vi at melde- og konsesjonsplikt helt eller delvis faller bort med den nye forordningen. Vi har likevel forstått at forordningen åpner for nasjonale tilpasninger på enkelte områder, og at det ikke er helt klart hva som vil skje med konsesjonsplikten innenfor spesifikke sektorer. Her er forsikringsbransjen nevnt.

- Tror du det vil utvikles spesielle regler for konsesjonsplikt i forhold til forsikring?

Begrenset mulighet for nasjonal tolkning

Vi har også lest at den nye forordningen vil begrense nasjonale muligheter for fortolkning i forhold til i dag, og at det vil skape nye utfordringer knyttet til sikring av ønskede særnorske bestemmelser.

- Vet du hva slags type særnorske bestemmelser dette eventuelt gjelder, og tror du det kan knyttes til forsikringsbransjen?

Bransjenormer

Datatilsynet påpeker at det i lys av den nye personvernlovgivningen bør samarbeides om å utarbeide egne retningslinjer for behandling av persondata innenfor ulike bransjer.

- Hvordan pleier det å fungere rettslig med bransjenormer?
- Tror du det vil utvikles bransjenormer som kan påvirke hvordan forsikringsselskapene opererer?

Muligheter

- Det er mye fokus på begrensninger og sikkerhet når det prates om den nye lovgivningen. Hvilke muligheter skaper den?
- Opplever du at normen for praktisering av sanksjoner er mild i dag? Tror du dette vil skjerpes med den nye forordningen?
- Hva er myndighetenes holdning til bruk av persondata til kommersielle forhold?

Avsluttende spørsmål

- Er det noe du ønsker å tilføye innenfor de temaene vi har snakket om?
- Spørre om det er mulig å ta kontakt ved en senere anledning om det skulle bli behov for mer informasjon.
- Takke for hjelpen og informere om at vi vil oversende resultatene for sitatsjekk og godkjenning.

9.2.2 Storebrand

Informasjon før intervjuet starter

- Fortelle kort om oss og hva oppgaven handler om.
- Forklare intervjuets hensikt.
- Informere om konfidensialitet og anonymitet.
- Spørre om vi kan bruke lydopptaker.
- Informere om intervjuets varighet.

Personvern

- Hvordan jobber dere med den nye personvernforordningen?
- Hvordan vil den påvirke deres forretningsvirksomhet?
- Hvordan opplever dere at kundene deres stiller seg til personvern?
 - Ser dere en sammenheng mellom kundelojalitet og fokus på personvern?
 - Opplever dere at kundene deres er kritiske til å gi fra seg personopplysninger?
- Hvordan opplever dere at personvernlovgivningen legger føringer for deres tilbud av produkter?
- Hvilke utfordringer mener dere er viktigst i vurderingen av å innføre en persontilpasset helseforsikring? Er det loven, holdninger i samfunnet, datasikkerhet?

Helseforsikring og wearables

- Hvordan jobber dere med å utvikle nye forretningsmodeller innenfor helseforsikring?
- Har dere vurdert å kombinere wearables med helseforsikringer?
 - Hvordan ville en slik løsning blitt implementert?
 - Ville en aktuell løsning være at kunden kan påvirke forsikringspremien direkte, eller gjennom et belønningssystem hvor de får belønning i form av andre goder?
- Hvordan opplever dere markedssituasjonen i Norge for persontilpassede forsikringstjenester i dag?
 - Er dette noe som vil bli godt mottatt - tatt i betraktning generelle holdninger til helseforsikringer i det norske samfunnet?
 - Opplever dere press fra internasjonale forsikringsaktører som tilbyr persontilpassede helseforsikringer?
- Hva slags holdninger tror dere norske forbrukere vil ha til persontilpassede helseforsikringer?
 - Vil det påvirke omdømme?
 - Hvordan opplever dere at en persontilpasning av forsikringstjenester vil påvirke deres omdømmebelastning?
 - Er det en grunn til at dere leverer løsningen Kjør Smart gjennom Rema Forsikring og ikke selv?
- Hvordan vil kravene til datasikkerhet påvirke om dere tilbyr persontilpassede helseforsikringer?
- Hvordan ser veksten i helseforsikring ut fremover?

Bransjenormer

- Hva er de eksisterende bransjenormene i dag?
- Hvordan tror dere disse vil endre seg som følge av den nye lovgivningen?
- Jobber dere aktivt sammen med andre selskaper for å utvikle bransjenormer?

Avsluttende spørsmål

- Er det noe dere ønsker å tilføye innenfor de temaene vi har snakket om?
- Spørre om det er mulig å ta kontakt ved en senere anledning om det skulle bli behov for mer informasjon.
- Takke for hjelpen og informere om at vi vil oversende resultatene for sitatsjekk og godkjenning.

9.2.3 Finans Norge

Informasjon før intervjuet starter

- Fortelle kort om oss og hva oppgaven handler om.
- Forklare intervjuets hensikt.
- Informere om konfidensialitet og anonymitet.
- Spørre om vi kan bruke lydopptaker.
- Informere om intervjuets varighet.

Generelt

- Hvordan arbeider dere med den nye personvernforordningen?

Den nye forordningen

- Hvordan vil personvernforordningen påvirke forsikringsselskapers muligheter til å samle inn og behandle personopplysninger?
 - Hvilke tanker har de rundt melde- og konsesjonsplikten?
 - Samtykke, dataportabilitet, retten til å bli glemt, innebygd personvern.
- Hvilke muligheter gir den nye forordningen til nasjonal tolkning?
- Skaper forordningen utfordringer for ivaretagelsen av særnorske bestemmelser?
- Hvilke utfordringer mener dere forsikringsselskaper står overfor når det gjelder innføring av persontilpassede forsikringer?
 - Er det loven, holdninger i samfunnet eller fokus på datasikkerhet som er viktigst?
- Tror dere en persontilpasset helseforsikring kommer til å bli lansert i Norge i nærmeste fremtid? Hvorfor/hvorfor ikke?
- Tror dere det vil utvikles normer i forsikringsbransjen som setter begrensninger utover lovgivningen?
- Hvordan tror dere disse vil endre seg som følge av den nye lovgivningen?

Muligheter

- Hva tror dere er mest avgjørende for om persontilpassede helseforsikringer blir innført i Norge? Er det loven, holdninger i samfunnet, datasikkerhet og omdømmerisiko, konkurranse fra utlandet?
- Det er mye fokus på begrensninger og sikkerhetskrav når det gjelder den nye lovgivningen. Skaper forordningen nye muligheter for å utvikle persontilpassede tjenester?
- Tror dere omdømmerisiko vil begrense forsikringsselskapers handlinger?

Avsluttende spørsmål

- Er det noe dere ønsker å tilføye innenfor de temaene vi har snakket om?
- Spørre om det er mulig å ta kontakt ved en senere anledning om det skulle bli behov for mer informasjon.
- Takke for hjelpen og informere om at vi vil oversende resultatene for sitatsjekk og godkjenning.

9.2.4 Datatilsynet

Informasjon før intervjuet starter

- Fortelle kort om oss og hva oppgaven handler om.
- Forklare intervjuets hensikt.
- Informere om konfidensialitet og anonymitet.
- Spørre om vi kan bruke lydopptaker.
- Informere om intervjuets varighet.

Personvern

- Ville et forsikringsselskap fått tillatelse til å tilby en persontilpasset helseforsikring i dag?
 - Hvis ja, hvorfor tror dere det ikke er blitt lansert enda?
 - Er det forskjellige hensyn som tas med tanke på bilforsikring og helseforsikring?
- Hvordan vil den nye personvernforordningen påvirke forsikringsselskapers muligheter til å samle inn og behandle personopplysninger (spesielt med tanke på helse)?
 - Tilrettelegger eller begrenser det forsikringsselskapene?
 - Diskutere samtykke, dataportabilitet, retten til å bli glemt, innebygd personvern
- Bortfall av konsesjonsplikt: vil dere fortsette å sektorregulere forsikring/finans?
 - Hvilke implikasjoner vil dette ha for forsikringsselskaper når de samler inn data? Vil det være uheldig for konkurranse med tanke på utenlandske aktører?
 - *Moderna Smärt Helse* og *Skandia*: Er dere kjent med om de vil implementere noe i Norge?
 - Skal det være mulig for norske forsikringsselskaper å utvikle så datadrevne produkter som tilbys i utlandet?
- Hvordan kommer dere til å etterleve de nye sanksjonsmulighetene? Kommer dere til å bruke de mulighetene dere har?
- Hvordan tror dere myndighetene vil gripe inn for å regulere utviklingen som utfordrer den kollektive tankegangen bak forsikringsprinsippet?
- Hvordan jobber dere sammen med myndighetene for å regulere muligheter for persontilpassing av produkter?

Muligheter

- Hvilke utfordringer mener dere forsikringsselskaper står overfor når det gjelder innføring av persontilpassede forsikringer?
- Hva tror dere er mest avgjørende for om persontilpassede helseforsikringer blir innført i Norge? Er det loven, holdninger i samfunnet, datasikkerhet og omdømmerisiko, konkurranse fra utlandet?
- Hva skjer på denne fronten i dag i den norske forsikringsbransjen?

Forsikringsprinsippet og holdninger

- Hvordan ser dere for deg at persontilpasset forsikring vil endre fremtidens forsikringsmodeller?
- Hvilke utfordringer tror dere dette byr på?
- Hvilke forretningsmodeller tror dere vil slå mest an? Rema 1000 sin modell der man får redusert pris, eller Vitalitys modell, der man får poeng som kan brukes på andre goder?
- Tror dere holdninger til et kollektivt forsikringsystem står sterkere i Norge enn i andre land?

Datasikkerhet

- I hvilken grad mener dere at datasikkerhet knyttet til wearables, for eksempel med tanke på kobling mellom FitBit og smarttelefon, utfordrer personvernet?
- Hvilke sikkerhetsutfordringer mener dere er mest sentrale for forsikringsbransjen?
- Mener det er sikkert for forbrukere å benytte seg av wearables?

Forbrukere

- Mener dere at det er uheldig for forbrukerne med persontilpassede forsikringer? Tror dere at det er risikabelt å gi fra seg data i dag med tanke på hva som vil skje med reguleringer i fremtiden?
- Diskutere ordlyd: Overvåke vs. monitorere. Hva er best?

Avsluttende spørsmål

- Er det noe dere ønsker å tilføye innenfor de temaene vi har snakket om?
- Spørre om det er mulig å ta kontakt ved en senere anledning om det skulle bli behov for mer informasjon.
- Takke for hjelpen og informere om at vi vil oversende resultatene for sitatsjekk og godkjenning.