Handelshøyskolen BI - campus Bergen

BTH 11411

Bacheloroppgave - Forretningsutvikling og digitalisering

Bacheloroppgave

På hvilken måte påvirker GDPR bruk og utvikling av kunstig intelligens, og hvordan kan teknologien utnyttes?

Navn:	Celine Ekornrud, Karoline Gurholt Haaland, Tale Staveteig Taalesen

Utlevering:	06.01.2020 09.00
Innlevering:	03.06.2020 12.00

Bacheloroppgave

ved Handelshøyskolen BI

«På hvilken måte påvirker GDPR bruk og utvikling av kunstig intelligens, og hvordan kan teknologien utnyttes?»

BTH1141
Forretningsutvikling og digitalisering

Utleveringsdato
06.01.2020

Innleveringsdato
03.06.2020

Studiested
Handelshøyskolen BI Campus Bergen

Forord

Denne bacheloroppgaven er skrevet i fordypningskurset forretningsutvikling og digitalisering ved Handelshøyskolen BI, Bergen. Oppgaven avslutter tre år med bachelorstudier innen Økonomi og administrasjon.

Utformingen av undersøkelsens tematikk begynte allerede tidlig i semesteret. Til tross for at vi gjennom hele arbeidsprosessen har hatt retningen for oppgaven, har vi hatt behov for endringer underveis. Vi har vært bevisste på at vi har valgt et omfattende emne, og dette har resultert i at vi har arbeidet hardt og målrettet. Avslutningsvis er vi svært fornøyde med resultatet på oppgaven, og ser problemstillingen som svært nyttig for oss å ta med oss videre inn i arbeidslivet.

Vi ønsker å takke vår veileder ved Handelshøyskolen BI for god veiledning, tilrettelegging og undervisning i faget. Samtidig vil vi også rette en stor takk til våre respondenter (A, B, C, D), som alle har hjulpet oss i arbeidet med innhenting av data. Resultatet hadde ikke vært komplett uten deres ekspertise.

Bergen, juni 2020.

Sammendrag

EUs personvernforordning, GDPR, trådte i kraft 20. Juli 2018 og skal sikre at regler om personvern overholdes, og sørger for at data ikke misbrukes. Ny teknologi utfordrer personvernet dersom det ikke settes grenser. Behovet for satsninger på langsiktig teknologi står sentralt i det norske samfunnet. Teknologien kunstig intelligens kan bidra til å effektivisere, automatisere og standardisere arbeidsoppgaver i forretningsdrift.

Følgende problemstilling drøftes i denne oppgaven: **«På hvilken måte påvirker GDPR bruk og utvikling av kunstig intelligens, og hvordan kan teknologien utnyttes?»** Personvern-implikasjonene er viktig for å ivareta individers frihet, samfunnets utvikling og etiske retningslinjer. Oppgaven fokuserer på hvordan bruk og utvikling av kunstig intelligens påvirkes av personvernhensyn i norske virksomheter, med hovedvekt på norske banker.

Datagrunnlaget baserer seg på primærdata gjennom kvalitative intervjuer og sekundærdata fra supplerende litteratur. Oppgaven vil derfor være undersøkende og eksplorativt med et kausalt forskningsdesign.

I analyse og drøftingskapittelet vil funn fra informanter knyttes opp mot relevant teori. Drøftingen inneholder avveininger om innebygd personvern, personvernkonsekvenser og tre av personvernprinsippene knyttet opp mot kunstig intelligens. Siste del av oppgaven vil trekke ut slutninger om sammenhenger som kan besvare problemstillingen, og trekke konklusjoner.

Innholdsfortegnelse

Begrepsforklaring

Algoritmer
Algoritmer defineres som en fremgangsmåte eller oppskrift for løsning av en modell.

Behandlingsansvarlig
Den som alene eller sammen med andre bestemmer formålet med behandlingen og hvilke midler som skal benyttes, er behandlingsansvarlig, jf. forordningen artikkel 4 (7).

De fem store techgigantene
Google, Apple, Microsoft, Amazon og Facebook

Databehandler
Den som behandler personopplysninger på vegne av den behandlingsansvarlige, jf. Forordningen artikkel 4 (8).

Den registrerte
Enkeltpersonen som de lagrede opplysningene kan knyttes til (Datatilsynet, 2020)

DPIA
Data Protection Impact Assessment
Vurdering av personvernkonsekvenser

Entitet
En entitet er en enhet du ønsker å lagre informasjon om i en database. Dette kan være en person, en vare, et dokument eller lignende. En samling like entiteter kalles en entitetstype (Heggernes, 2017)

EØS
Det europeiske økonomiske samarbeidsområde
Samarbeid mellom EU-land, EUs medlemstater og EFTA-landene. Norge inngår som et av EFTA-landene

EU
Den europeiske unionen
Samarbeidsorganisasjon i Europa som består av 27 medlemsland

Formålsglidning
Formålet glir over fra å være noe til å bli noe annet.

GDPR
General Data Protection Regulation
EUs personvernforordning som gjelder for alle land innenfor EU/EØS, og inkluderer alle land som behandler opplysninger med land innenfor EØS

Hype
Betegnelse på opphausende og eventuelt manipulerende omtale eller markedsføring; reklame som skaper store forventninger til et produkt eller fenomen ved hjelp av overdrivelser (Store norske leksikon, 2018)

Nevrale nettverk
Samlebetegnelse for datastrukturer, med tilhørende algoritmer, som er inspirert av måten nervecellene i en hjerne er organisert på (Dvergsdal, 2019)

Omdømmerisiko
Omdømmerisiko utgjøres av det potensialet handlinger og begivenheter har til å assosiere en organisasjon med konsekvenser som negativt påvirker forhold av verdi for mennesker (Brønn & Arnulf, 2019)

Personvernfremmende teknologi
Teknologi som muliggjør innebygd personvern. Omtales også som Privacy Enhancing Technologies (PET) (Datatilsynet, 2017)

Teknisk gjeld
Etterslep som oppstår når en bedrift venter for lenge med å oppdatere bruken av teknologi (Heggernes, 2017)

1.0 Innledning

Direktør i Datatilsynet, Bjørn Erik Thon, uttaler at en av effektene som har kommet frem etter innføringen av GDPR er at både nordmenn og europeere generelt har fått et mye mer bevisst forhold til innsamling og bruk av egne personopplysninger. Dette underbygger hvor viktig det er at virksomheter opptrer lovlydig og holder seg oppdaterte på endringer. Denne holdningsendringen fører til at virksomheter trolig er mer skjerpet i behandling av personopplysninger enn tidligere.

«80 % av det tekniske arbeidet rundt utvikling av en analysemodell handler om data» (PrivatewaterhouseCoopers, 2020). Det er kritisk at regler overholdes slik at data ikke misbrukes, og her står personvern og GDPR sentralt. Kunstig intelligens (heretter omtalt som KI) forutsetter store mengder data for at det skal kunne tas intelligente avgjørelser. «Potensialet for bedre tjenester, forskningsmessige gjennombrudd og økonomisk gevinst, setter KI høyt på agendaen i de fleste sektorer» (Datatilsynet, 2018).

Personvernforordning, GDPR, trådte i kraft 20. juli 2018 (Regjeringen, 2019), og er derfor høyst dagsaktuell. Det er klart at innføringen av GDPR har satt fokus på de registrertes rettigheter, og det er her problematikken oppstår når KI skal understøtte samfunnsoppdrag på best mulig måte.

Økonomiske og effektivitetsfremmende samfunnsgevinster må veies opp mot grunnleggende personvernhensyn. «Kunnskap om personvern-implikasjonene ved bruk og utvikling av kunstig intelligens er nødvendig for å bevare samfunnsbehov utover personvernet og for å ivareta enkeltmenneskers personvernrettigheter» (Datatilsynet, 2018). Møtet mellom KI og personvern er interessant fordi det skaper utfordringer, samtidig som det åpner for digitaliserte muligheter i samfunnet.

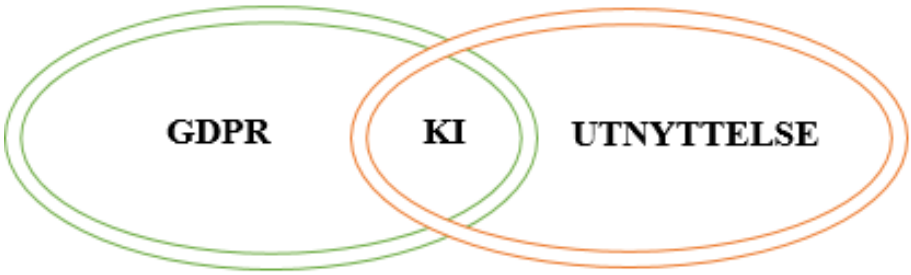
1.1 Problemstilling

I takt med digitaliseringen er det et økt behov for diskusjon rundt GDPR, spesielt knyttet opp mot KI. Vi har derfor valgt å ta utgangspunkt i følgende problemstilling:

«På hvilken måte påvirker GDPR bruk og utvikling av kunstig intelligens, og hvordan kan teknologien utnyttes?»

For å forklare problemstillingen er det nødvendig å sette KI i sentrum. Det første spørsmålet som reiser seg, vil være hvordan KI påvirkes av GDPR-regelverket. Det andre spørsmålet vil fokusere på hvordan KI som teknologi kan utnyttes. Kombinasjonen av personvern og utnyttelse vil kunne være motstridende, og sammenhengen vil reise interessante spørsmål. Derfor vil denne problemstillingen være høyst relevant å undersøke.

Problemstillingen er omfattende, og vil derfor avgrenses ytterligere i delkapittel 1.3. Videre, har vi med hovedvekt på våre hypoteser undersøkt hva begrepet KI innebærer, som legger grunnlag for å besvare problemstillingen. Oppgaven skal gi leseren innsikt i relevante personvernproblematikker norske virksomheter står ovenfor ved bruk og utvikling av KI-systemer.



Figur 1: Illustrasjon av problemstillingen i et venndiagram

1.2 Avgrensninger

Vi har valgt å avgrense oppgaven med å drøfte hvordan personvernet påvirker bruk og utvikling av KI hos norske virksomheter med hovedvekt på bank- og finansbransjen, derav norske banker. Bank- og finansbransjen er hjørnesteiner i samfunnet. Dette med tanke på forvaltning av midler, investeringer og at bransjen er med på å skape forutsigbarhet. Banker har et stort samfunnsansvar både for å motivere økonomisk vekst, men også for å skape trygghet. Grunnen til at vi ønsker å vektlegge norske banker er fordi bank- og finansbransjen er høyst digitalisert, og behandler store mengder personopplysninger.

Oppgaven setter søkelys på GDPR og avgrenses til tre personvernprinsipper: formålsbegrensing, dataminimering og gjennomsiktighet. Disse prinsippene er særlig knyttet opp mot KI, men det er viktig å presisere at alle områder ved personopplysningsloven vil gjelde. For å unngå å begrense kvaliteten på innholdet i undersøkelsen, har vi valgt å drøfte utfordringer og muligheter ved KI.

2.0 Bakgrunn

Internett og digitalisering har de siste 20 årene ført til omfattende samfunnsmessige endringer (NHO, 2018). Den teknologiske utviklingen har bidratt til nye muligheter for utvikling av innovative produkter og tjenester. Dette er med på å utfordre virksomheters data- og informasjonssikkerhet på andre måter enn tidligere, og skaper økt behov for IKT-sikkerhet generelt og for personvernet spesielt. Hensikten med kapittelet er å sette problemstillingen i kontekst. Vi vil derfor trekke frem personvern og samfunnsmessig verdi som relevante punkter for å få frem viktigheten av tematikken som problemstillingen reiser.

2.1 Personvern

«Personvern handler om retten til privatliv og retten til å bestemme over egne personvernopplysninger» (Datatilsynet, 2019). Personopplysninger inkluderer opplysninger og vurderinger som kan knyttes til en enkeltperson, for eksempel navn, adresse, telefonnummer, e-postadresse, bilnummer, bilder og fødselsdato (Datatilsynet, 2019).

Personvern skal sikre hensynet til den enkeltes privatliv og integritet og inngår som en viktig menneskerettighet. I et demokratisk samfunn, er personvern avgjørende for at den enkelte skal kunne skape rom og utvikle refleksjoner og vurderinger på et selvstendig grunnlag uten forstyrrelser og kontroll fra andre. Retten til privatliv står her sentralt. Innføringen av EU/EØS personopplysningslov i 2018 har ytterligere bidratt til å styrke retten til å kunne bestemme over egne personopplysninger. Rett til innflytelse på bruk og spredning av opplysninger om seg selv er viktig innenfor personvernbegrepet (Datatilsynet, 2019).

Sensitive opplysninger skal behandles særskilt. Dette er personopplysninger som er mer omfattende å behandle og innebærer blant annet opplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion eller helseopplysninger (Datatilsynet, 2019).

2.2 Samfunnsmessig verdi

Behovet for IT og teknologiske prosesser har gått fra å være et støtteverktøy til at det i dag forventes at forretningsmodellen skal være designet med hensyn på å utnytte dagens og morgendagens teknologi (Heggernes, 2017). Dagens teknologiutvikling har derfor ført til et skifte i den digitale forretningsdriften, og genererer nye måter å både skape og fange verdi på. For at digitalisering skal være mulig, vil det nødvendigvis ligge et behov for å kunne bruke og analysere store datamengder.

«90% av verdens data har blitt generert de siste fem årene» (Heggernes, 2017). Som et resultat av «datahavet» som blir produsert, ligger det i dag til rette for unike kommersielle og samfunnsøkonomiske muligheter. «Potensialet for bedre tjenester, forskningsmessige gjennombrudd og økonomisk gevinst, setter KI høyt på agendaen i de fleste sektorer» (Datatilsynet, 2018). Det er nettopp tilgangen på mengden data og regnekraften som i dag gjør at virksomheter kan dra nytte av denne teknologien. KI forutsetter store mengder data for at det skal kunne tas intelligente avgjørelser. Virksomheter er avhengige av sine registrerte og derfor vil personopplysninger være driveren bak datainnsamlingen.

Data som innhentes, lagres og brukes, og som kan trekke slutninger om et individ, må behandles som personopplysninger. Ny teknologi vil i mange tilfeller utfordre personvernet, og det er kritisk at virksomheter arbeider for å sikre at disse ikke kommer på avveie eller misbrukes. Samtidig vil en økt generell bevissthet på personopplysninger føre til at virksomheter blir nødt til å vurdere de potensielle samfunnsgevinstene opp mot grunnleggende personvernhensyn, dette for å ivareta enkeltmenneskers personvernrettigheter (Datatilsynet, 2019).

Personvern som ikke ivaretas, vil utfordre demokratiet i ytterste konsekvens. Den registrerte vil kunne oppleve å føle frykt for at opplysninger om personlige forhold misbrukes. Dette kan resultere i at den registrerte begrenser deltakelse i å uttrykke holdninger og i kommunikasjon med andre (Datatilsynet, 2019).

3.0 Teoretisk rammeverk

Kapittelet representerer og gjennomgår det teoretiske rammeverket som er anvendt i oppgaven. Formålet med teorikapittelet er å gi leseren en overordnet forståelse av emnene oppgaven berører. Teorifundamentet er hentet inn gjennom relevant litteratur, artikler og rapporter.

3.1 General Data Protection Regulation (GDPR)

Personvernloven, GDPR, trådte i kraft 20. Juli 2018 (Regjeringen, 2019). GDPR er EUs personvernforordning og er gjeldende for alle land innenfor EØS. Lovverket gjelder også for behandlingsansvarlige som befinner seg utenfor EØS-området, dersom det behandles personopplysninger av EØS-borgere. Personopplysningsloven inneholder bestemmelser som er nødvendige for å gjennomføre personvernforordningen i norsk rett. Lovverket vil gjelde for alle som skal innhente, bruke og lagre personopplysninger, og inneholder bestemmelser som presiserer adgangen til å gjennomføre behandlinger av personopplysninger (Datatilsynet, 2019).

3.1.1 Formålsbegrensning

Prinsippet om formålsbegrensning innebærer at personopplysninger skal behandles dersom det foreligger et eller flere formål. Personopplysningene kan kun brukes dersom formålet er legitimt. Formålet må være lovlig, og formulert klart og presist. Følgelig, kan ikke opplysningene gjenbrukes til formål som er uforenlig med det opprinnelige formålet (Datatilsynet, 2019).

3.1.2 Dataminimering

Dersom det ikke foreligger behandlingsgrunnlag for personopplysninger som er nødvendige for å oppnå formålet, skal disse heller ikke samles inn. Prinsippet om dataminimering innebærer å begrense mengden innsamlede data til det nødvendige (Datatilsynet, 2019).

3.1.3 Gjennomsiktighet

Prinsippet om gjennomsiktighet går ut på at behandlingen av personopplysninger skal være forståelig og oversiktlig for den personen de enkelte opplysningene gjelder for. Den registrerte skal ha innsyn i behandlingsgrunnlaget (Datatilsynet, 2019).

3.2 Stordata

Det genereres 2,5 trillioner bytes med data hver dag, hvor store mengder av dataen som genereres har blitt produsert de siste årene (PricewaterhouseCoopers, 2020). Datamengdene er så store og komplekse at det ikke lenger er tilstrekkelig med tradisjonell programvare. Det kreves egne analyseverktøy for å håndtere og analysere dataene og dette omtales som stordata. «Betegnelsen referer både til dataene i seg selv og aktiviteten knyttet til å samle, lagre og analysere dem» (Datatilsynet, 2017).

Stordata benyttes om mye, og det finnes ingen gitt definisjon på hva stordata er. EU-kommisjonens rådgivende organ i personvernspørsmål definerer stordata på følgende måte: «Stordata refererer til den enorme økningen i tilgang til, og automatisert bruk av, opplysninger: det refererer til gigantiske mengder digitale data som er kontrollert av selskap, myndigheter og andre store generasjoner, og som gjøres til gjenstand for omfattende analyse ved bruk av algoritmer» (Bergsjø & Bergsjø, 2019).

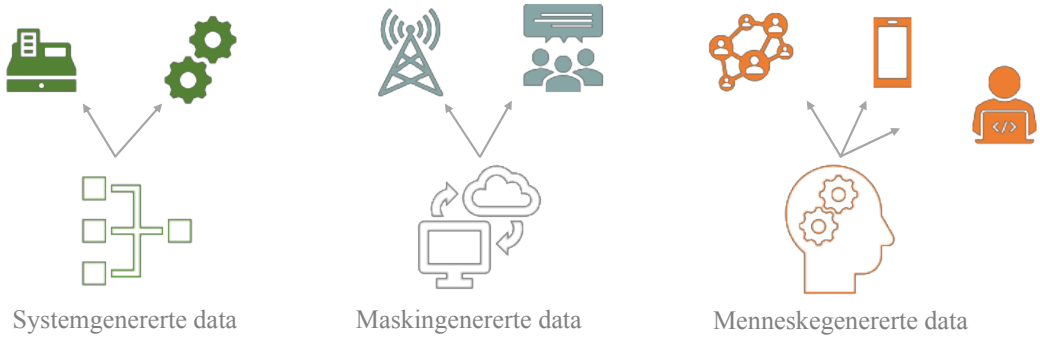
3.2.1 Innsamling av data

Nesten all bruk av digitale tjenester legger igjen elektroniske spor, noe som gjør at det nå er mulig å følge med på hva mennesker interesserer seg for og hvor de beveger seg i det fysiske rom. Det benyttes mangfoldige datakilder ved innsamlingen av data, og disse kan deles inn i tre kategorier: systemgenererte, maskingenererte og menneskegenererte data (Heggernes, 2017).

Systemgenererte data er data som genereres i virksomhetenes egne IT-baserte systemer. Informasjon som registreres er eksempelvis salg, henvendelser fra kunder og oppfølging av kunder. Ved systemgenererte data er den enorme mengden data som er tilgjengelig den største utfordringen (Heggernes, 2017).

Den andre kategorien handler om maskingenererte data. Det er store maskiner som generer data til enhver tid. Dette fenomenet omtales som Internet of Things (IoT). «Det som muliggjør denne datastrømmen, er sensorer» (Heggernes, 2017). Slike sensorer er svært små og kraftfulle, og vil føre til at det er få begrensninger for bruksområdene til en sensor. Informasjon som samles inn fra sensorer registreres fra blant annet biler, datamaskiner og mobiltelefoner.

Menneskegenererte data gjelder all type data som skapes og deles av mennesker gjennom ulike plattformer. Delingen av data foregår primært via sosiale medier gjennom eksempelvis Instagram, Facebook, Youtube og Twitter (Heggernes, 2017).



Figur 2: Kategorisering av stordata

Nesten all bruk av digitale tjenester legger igjen elektroniske spor. Dette gjør at det vil være mulig å følge med på hva mennesker interesserer seg for og hvor de beveger seg i det fysiske rom. Ved å identifisere generelle trender og sammenhenger, kan virksomheter benytte stordata til å hente ut verdifull informasjon. Videre kan dette brukes til å skaffe ny innsikt, foreta forbedrede beslutninger og optimalisere egne prosesser (PricewaterhouseCoopers, 2020). Sammensetningen av de ulike datakildene er et sentralt aspekt ved stordata, og kan klargjøre sammenhenger som ikke hadde vært mulig ved en manuell analyse.

3.3 Kunstig intelligens

Store teknologiske omveltninger fører til at mange i dag mener at vi befinner oss i det som er omtalt som den «fjerde industrielle revolusjon» (Heggernes, 2017). Tidsepoken kjennetegnes ved at de eksisterende teknologiene nå har nådd et visst digitalt modenhetsnivå. Dett legger til rette for sammenkobling av ulike systemer, omtalt som kyberfysiske systemer, og KI står sentralt.

KI er et komplisert og sammensatt fagfelt og gir opphav til en rekke definisjoner. Vi har valgt å ta utgangspunktet i definisjonen fra Ekspertgruppen i Europakommisjonen, for å gi undersøkelsen en mer målbar retning:

«Kunstig intelligente systemer utfører handlinger, fysisk eller digitalt, basert på tolkning og behandling av strukturerte eller ustrukturerte data, i den hensikt å oppnå et gitt mål. Enkelte KI-systemer kan også tilpasse seg gjennom å analysere og ta hensyn til hvordan handlinger har påvirket omgivelsene» (Astrup, 2020).

Med utgangspunkt i bruk og utvikling av KI vil beskrivelsen som regel benyttes samtidig, men kan likevel forklares separat. Bruken er ofte forbundet med hva som skal til for å kunne anvende og drifte KI-systemer. Bruk omfattes av mange elementer, og disse kan for eksempel være data, etiske retningslinjer, IT-sikkerhet, lover og regler, eller forvaltning av systemer som tar i bruk KI. Utvikling ses gjerne i sammenheng med KI-forskning, IKT-forskning, hvordan teknologien kan dra nytte av utviklingen i teknologiske trender eller gjennom innovasjon og verdiskapning. Utvikling og bruk kan totalt sett vurderes som gjensidig avhengige begreper, da utvikling sjeldent kan utnyttes maksimalt uten bruk, og omvendt.

Hva som inngår i KI-systemer varierer med tanke på tilnærming og hvilke teknikker som brukes. KI er et bredt begrep og det trekkes grovt sett et skille mellom KI-systemer som har til hensikt å ligne menneskelig intelligens, kalt kunstig generell intelligens, og regelbaserte systemer for automatisering. Sistnevnte er bygget opp av regler gitt av mennesker, og kan danne kompliserte beslutningstrær. Disse er blant annet mye brukt i forretningssystemer. Systemer som tar i bruk KI analyserer data, tar beslutninger og utfører handlinger. Dette ofte som en del av et større IT-system eller

som en fysisk løsning (Astrup, 2020). Hvordan løsningen innretter seg avhenger av hvilke området systemet er ment å treffe. «Sterk» KI vil underligge kunstig generell intelligens og «svak» KI er utviklet med tanke på en bestemt oppgave (Astrup, 2020).

De fleste systemer som i dag tar i bruk KI benytter seg av «svak» KI. Dette er sammenfallende med at disse igjen som regel baserer seg på trening og læring, også kalt maskinlæring (heretter omtalt som ML) (Astrup, 2020). ML er en viktig byggestein for KI (PricewaterhouseCoopers, 2017), og er systemer som lærer basert på egne erfaringer, eller fra tilbakemeldinger fra bruker eller operatør (Astrup, 2020). Maskinlæringsalgoritmer gir opphav til ulike læringsmetoder; Veiledet læring, ikke-veiledet læring og forsterkende læring. Eksempel- og treningsdata lager modeller, som igjen brukes til å ta beslutninger.

3.4 DPIA - Personvernkonsekvenser

Alle virksomheter som skal behandle personopplysninger plikter også å vurdere personvernkonsekvenser (heretter omtalt som DPIA) og reguleres av artikkel 35 i GDPR lovverket. Datatilsynet legger vekt på at vurderingene er gjentakende og skal hjelpe virksomheter å kartlegge hvilke tiltak som kan igangsettes for å redusere høy risiko. I tillegg må virksomheter også iverksette nødvendige tiltak for å oppfylle de registrertes rettigheter. Dette for å forsøke å kombinere lovverket, personverninteresser og virksomhetens interesser (Datatilsynet, 2019).

En DPIA skal foregå i forkant av en behandlingsprosess og burde kontrolleres kontinuerlig. DPIA burde oppdateres jevnlig slik at systemene som tas i bruk er tilrettelagt for å kunne etterleve kravene. Dette for å korrigere for endringer i risiko, organisatoriske eller sosiale sammenhenger. «Når risikoen vurderes, skal det tas hensyn til arten, omfanget, sammenhengen og formålet med behandlingen» (Datatilsynet, 2018). Virksomheter må ta et spesielt hensyn til sensitive personopplysninger ved automatiske beslutninger, og dersom det benyttes ny teknologi.

Et minimumskrav for en konsekvensanalyse omfatter blant annet om behandlingen er nødvendig for dens formål, gjennomføring av risikovurdering opp mot personvernet og andre tiltak som identifiserer risiko. Behandlingen er lovlig dersom det ivaretas en berettiget interesse hos den behandlingsansvarlig. Dersom en virksomhet bevisst eller ubevisst utsetter de registrertes personopplysninger for høy risiko, kan dette medføre brudd i mindre eller større grad. Konsekvenser av mulige mislighold eller avvik ved vurdering av DPIA kan føre til at tilsynsmyndighetene pålegger virksomheten sanksjoner, administrative bøter. Ved manglende overholdelse kan disse bøtene gi alvorlige økonomiske konsekvenser.

3.5 Innebygd personvern

Innebygd personvern, beskrevet i artikkel 25 i forordningen, innebærer at det må tas hensyn til personvern i alle utviklingsfaser av et system eller en løsning, samt i rutiner og den daglige bruken. Prinsippet sørger for at informasjonssystemene oppfyller kravene i personvernloven og at de registrertes rettigheter ivaretas, uten at det går på bekostning av systemet. For virksomheter som oppretter et system for behandling av personopplysninger, vil det være avgjørende å kjenne til personvernprinsippene (Datatilsynet, 2018).

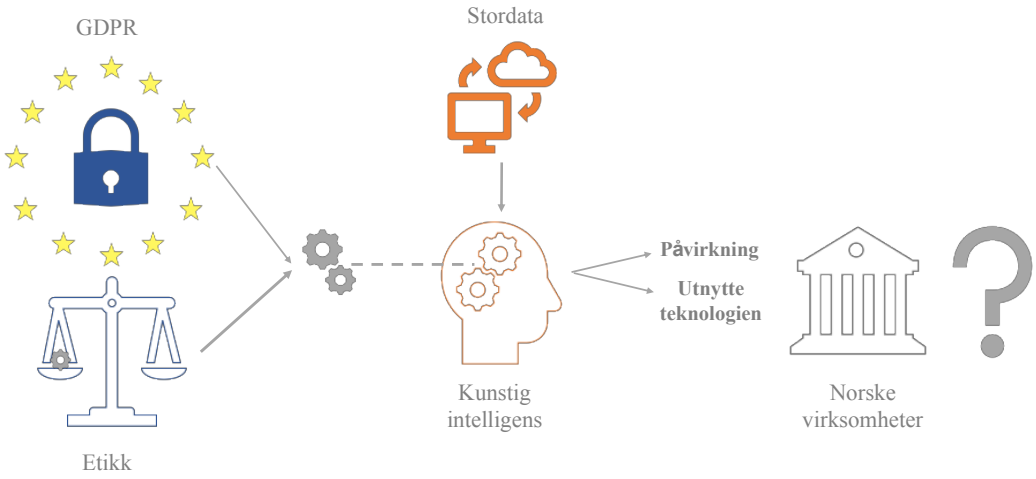
I likhet med en vurdering av DPIA, vil innebygd personvern skje i forkant av og under en utviklingsprosess. Dette for å arbeide forebyggende, og for å unngå i størst mulig grad å bruke unødvendige ressurser for å reparere. Ved å bygge personvernet funksjonelt for brukeren inn i designet, og samtidig gjøre personvernet til en standardinnstilling, vil virksomheter kunne ivareta informasjonssikkerheten og personvernet fra start til slutt. Spesielt er det viktig for virksomheter å vise åpenhet og respekt. Prinsippene om dataminimering og gjennomsiktighet vil stå sentralt for dette kravet (Datatilsynet, 2018).

3.6 Digital etikk

I Global Risk Report 2017 blir KI betegnet av World Economic Forum som «en av de fremvoksende teknologiene med størst nytteverdi, men også med størst skadepotensial» (Astrup, 2020). Dette skaper behov for diskusjon vedrørende ansvarlig og ønsket fremgang ved bruk av KI. Videre, vil diskusjonen om hvordan virksomheter kan arbeide preventivt mot en uønsket utvikling være essensiell. Nøkkelen til suksess innen utvikling og bruk av KI, avhenger av om det skapes en norm for ansvarlig bruk, tillit og gjennomsiktighet. Digital etikk blir dermed en viktig faktor i vurderingen av hvordan teknologien kan utnyttes uten at det truer personvernet.

Økt digitalisering har de siste årene satt digital etikk på agendaen. Digital etikk er analyse av ny teknologi, som stiller spørsmål til hva den nye teknologien er, hvilken sosial påvirkning den kan ha, og hvordan den bør utvikles og brukes (Moor, 1985). Digital etikk kan anvendes som et verktøy til å identifisere fordelene og styrke de positive mulighetene som teknologiske nyvinninger gir. Dette både for samfunnet og den enkelte. Samtidig anvendes digital etikk for å minske mulige risikoer (Bergsjø & Bergsjø, 2019). Diskusjon og kunnskap vedrørende digital etikk er viktige fokusområde for å fremme en ansvarlig og bærekraftig utvikling av bruken av KI.

3.7 Sammenheng mellom teori og problemstilling



Figur 3: Sammenheng mellom teori og problemstilling

Modellen over illustrerer sammenhengen mellom problemstilling og utvalgt teori. GDPR og etikk vil påvirke bruk og utvikling av KI, og stordata og KI vil knyttes opp mot sammenhengen av hvordan teknologien utnyttes.

4.0 Metode

Data er innhentet gjennom kvalitative intervjuer, med supplerende relevant litteratur og sekundærdata. Oppgaven vil derfor være undersøkende og eksplorativt med et kausalt forskningsdesign. I dette kapittelet vil vi legge frem forberedelser til oppgaven, datainnsamling, intervjuguider, analyse av data og evalueringskriterier.

4.1 Forskningsprosessen

Ifølge Johannesen deles forskningsprosessen seg over fire faser (Johannessen, 2011):

1. Forberedelse
2. Datainnsamling
3. Dataanalyse
4. Rapportering

De fire fasene danner grunnlaget for oppgavens struktur. Forberedelsesfasen og datainnsamlingen representeres her i kapittel 4, metode. I dette kapittelet trekkes det også inn relevante empiriske vurderinger. De to siste fasene danner dataanalyse og rapportering.

4.2 Forberedelse

Forberedelsesfasen gikk i hovedsak ut på å finne en eller annen virkelighet for et fenomen vi ønsket mer kunnskap om. Forskningsprosessen startet med at vi leste oss opp på all litteratur som vi tenkte oss at kunne omhandle emnene for oppgaven. Problemstillingen er presentert innledningsvis, og ble utarbeidet på en måte som gjorde det mulig å finne en sammenheng mellom to valgte fenomener.

Etter å ha utformet en problemstilling var neste steg å sette oss inn i relevant litteratur, som dermed dannet grunnlaget for teorikapittelet. Ved å sette oss inn i teoriene, var det lettere å sette oss inn i neste steg; å finne hypoteser. Hypotesene la føringer i arbeidet med å svare på problemstillingen, og ga oss retning for valg av undersøkelsesdesign og metode. Dette fremkommer i delkapittelet om datainnsamling, som danner neste fase i forskingsprosjektet.

4.3 Datainnsamling

For å bygge opp til analyse og diskusjon har vi samlet inn dokumentasjon og data, som skal fungere som støtte for undersøkelsen. Fasen inneholder en presentasjon av utvalgsstørrelse, utvalgsstrategi og rekruttering (Johannessen, 2011).

4.3.1 Valg av forskingsdesign og metode

Problemstillingen presenterer fenomenet KI og personvern, og etter å ha fordypet oss i litteraturen utviklet det seg en felles oppfatning om at begge fenomener var relativt komplekse. For å velge hvordan vi skulle angripe datainnsamlingen vil det være nødvendig å legge frem forskningsdesign.

Vi skiller mellom tre forskjellige forskningsdesign (Gripsrud, Olsson, & Silkoset, 2018):

- **Undersøkende (eksplorativt):** Formålet er å skaffe dypere innsikt og forståelse om et fenomen.
- **Beskrivende (deskriptivt):** Formålet er å kartlegge situasjonen på et bestemt område.
- **Kausalt (årsak-virkning):** Formålet er å undersøke årsakssammenhenger mellom variabler

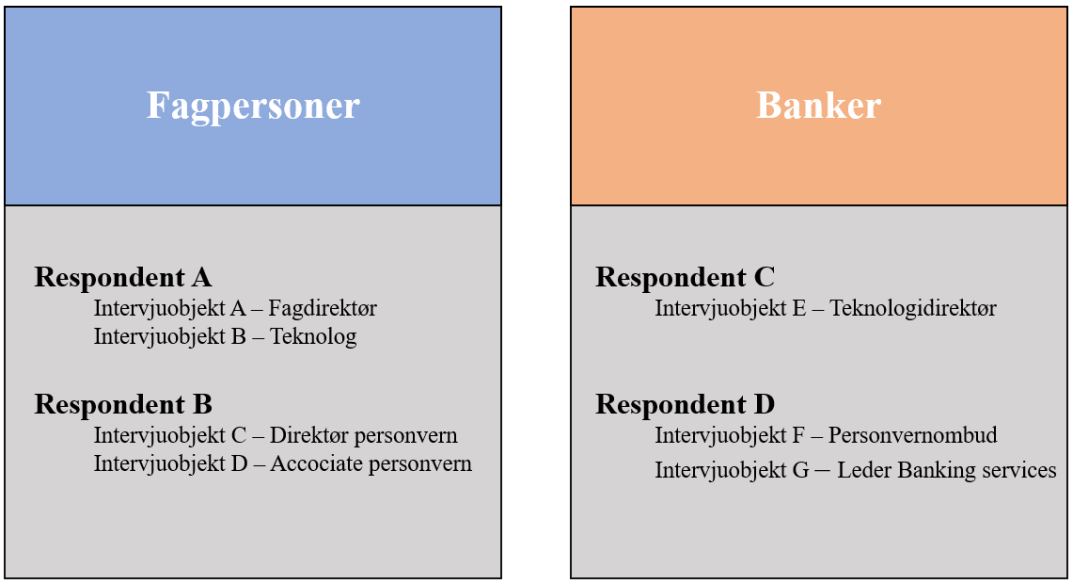
Ved komplekse fenomener vil det være fordelaktig å benytte et undersøkende (eksplorativt) design, da vi hadde behov for å skaffe dyp innsikt i KI og personvern. I empiriske forskningsprosjekter, skiller vi mellom kvantitativ og kvalitativ metode. Ved kvantitative metoder er målet å generalisere og analysere data og å vise sammenhengen mellom variabler. Ved kvalitative metoder er formålet å undersøke et fenomen som er lite kjent og lite forsket på for å få en bedre forståelse (Johannessen, 2011).

Videre ble det bestemt at det ville være mest hensiktsmessig med en kvalitativ metode med en induktiv tilnærming, for i korthet å trekke slutninger fra det spesielle til det mer allmenne. Undersøkelsen har et teoretisk utgangspunkt og vi har konkretisert fenomenet med en empirisk forskningsmetode (Johannessen, 2011).

4.3.2 Utvalg av informanter

I motsetning til andre næringer har bank- og finansbransjen lenge hatt strenge krav for å etterleve personvernet, samtidig som de er assosiert med høy digitaliseringsgrad. Av praktiske og naturlig årsaker, falt valget derfor på denne bransjen. Ved utvalg av informanter ved en kvalitativ tilnærming var det vesentlig å finne nøkkelpersoner innenfor bank- og finansbransjen som kunne gi oss mest mulig kunnskap om KI og personvern.

Ved strategisk utvelgelse var det for vår tilnærming mest hensiktsmessig å benytte snøballmetoden. Grunnet kompleksiteten for oppgaven var det vesentlig å komme i kontakt med informanter som kunne gi god innsikt i tematikken, og som samtidig kunne hjelpe oss å komme i kontakt med andre nøkkelpersoner. For å strukturere informantene har vi valgt å dele de inn i to hovedgrupper; Fagpersoner og Banker. Noen av informantene ønsket å holdes anonyme, og vi har derfor valgt å anonymisere alle. Under følger en oversikt over inndelingen:



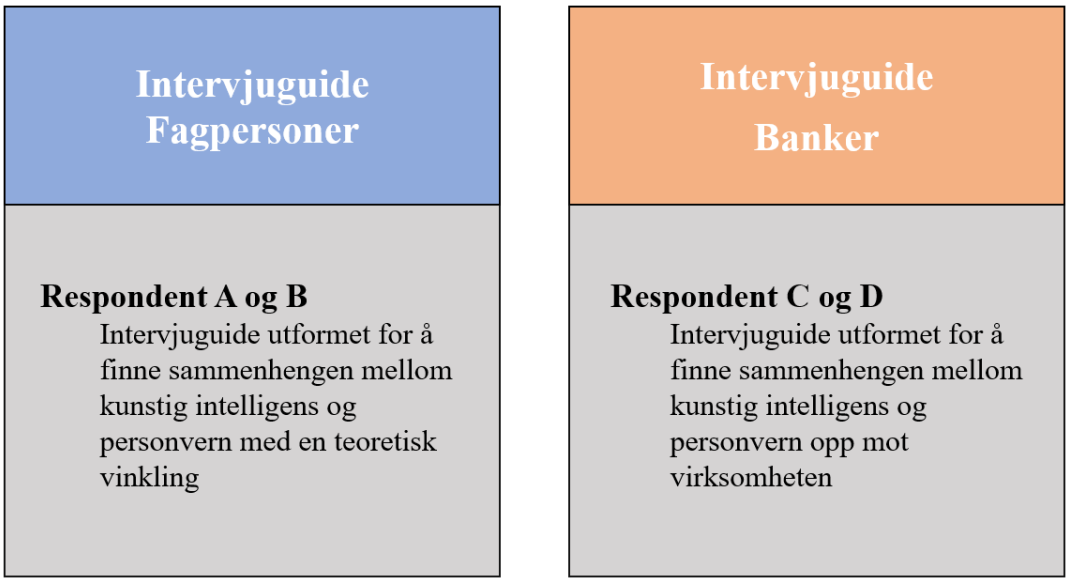
Figur 4: Inndeling av informanter

4.3.3 Kvalitative intervjuer

Med et eksplorativt forskningsdesign med kvalitativ tilnærming vil direkte kontakt for dybdeintervjuer kunne gi oss et utgangspunkt for utfyllende svar på problemstillingen. For å vurdere hvordan intervjuene burde gjennomføres, skilles det mellom tre ulike typer av kvalitative intervjuer (Johannessen, 2011):

- **Ustrukturert intervju:** Uformelt, bestående av åpne spørsmål. Tema er gitt på forhånd, men spørsmål tilpasses den enkelte intervjusituasjonen.
- **Semi-strukturert intervju:** Overordnet intervjuguide som utgangspunkt for intervjuet. Spørsmål, temaer og rekkefølge kan variere.
- **Strukturert intervju:** Fastsatt tema på forhånd med spørsmål og svaralternativer

Med våre intervjuer, ønsket vi at intervjuobjektene kunne ha muligheten til å svare fritt på spørsmålene og utdype og analysere disse etter behov. I tillegg ønsket vi å oppfordre til refleksjon, og alle våre kvalitative intervjuer er derfor lagt opp med en semi-struktur. For denne typen intervjuer har vi valg å utarbeide to sett med intervjuguider. Dette er forklart i figuren under:



Figur 5: Kategorisering av intervjuguider

Alle intervjuene vi gjennomførte tar utgangspunkt i problemstillingen vår og baserer seg på det teoretiske rammeverket. Spørsmålene i de to intervjuguidene er utformet med 9-10 spørsmål, hvor rekkefølgen på spørsmålene er forsøkt inndelt emnevis. Spørsmålene er stilt for å åpne for diskusjon, da vi ønsket dialog fremfor monolog. Fordelen ved å velge semi-strukturerte intervjuer er nettopp at det gir muligheter for oppfølgingsspørsmål og nyanserte svar. Dette gjorde at intervjuobjektene fikk mer frihet og samtidig gjorde det enklere for oss å kunne bevege oss på tvers av teori. Spørsmålene fremkommer under kapittel 9, vedlegg.

Intervjuguide, problemstilling og informasjon om oppgaven ble sendt over til intervjuobjektene i god tid før intervjuet. Dette gjorde vi for at intervjuobjektene skulle være forberedt og ha muligheten til å se og reflektere over spørsmålene før selve intervjuet. I forberedelsesfasen av prosjektet ønsket vi i utgangspunktet å gjennomføre intervjuene i person, men grunnet dagens situasjon, måtte selve gjennomføringen foregå i form av video- og telefonmøter på cirka en time. For praktiske formål var det en talsperson som stilte spørsmål og to som noterte svar fra respondentene.

4.3.4 Datareduksjon

Dataene innsamlet for undersøkelsen vil være strukturert grunnet kategorier av spørsmålene, men for å kunne bruke denne datapoolen i en analyse ble vi nødt til å redusere datamengden. Dette ble gjort ved å ta i bruk kategorisert inndeling i relevante temaer med fellestrekk. Metoden ble brukt på hele datamaterialet med fortolkende lesing i forsøk på å sette seg inn i informantenes normer, miljø og hva de er påvirket av. Som hjelpemiddel for en inndeling har vi tatt i bruk et diagram som representerer de ulike kategoriene, presentert i modellen under:

Figur 6: Kategoribasert inndeling

Modellen over er utformet slik at det på en oversiktlig måte avdekker viktige sammenhenger mellom KI og personvern. I kombinasjon med dataene fra intervjuene og relevante sekundærdata, er kategoriseringene benyttet som struktur for analysedelen. For å etterleve personvernet for oppgaven, har vi i etterkant slettet intervjuene.

4.4 Dataanalyse og kvalitetskriterier

Vi vil ta for oss kvalitetskriterier for kvalitative data. Ifølge Guba og Lincoln (1989), må kvalitative undersøkelser vurderes med begrepene pålitelighet, troverdighet, overførbarhet og bekreftbarhet (Johannessen, 2011).

4.4.1 Reliabilitet (Pålitelighet)

«Reliabilitet handler om undersøkelsens data: hvilke data som brukes, hvordan de samles inn, og hvordan de bearbeides» (Johannessen, 2011). Ved kvalitative undersøkelser er kravet om reliabilitet mindre relevant, likevel vil det være nødvendig å vurdere ulike aspekter. Teknikken for datainnsamling er styrt av samtalen, og intervjuene vil være noe situasjonsavhengige. Kunnskapen vi som forskere sitter på utgjør et unikt utgangspunkt for dialog, og gjør det dermed utfordrende for andre å duplisere. Analysen vil også være unik for undersøkelsen, da vi vil tolke resultatene ulikt andre.

For å styrke påliteligheten har vi gjennomgående forsøkt å fremstille konteksten og fremgangsmåten detaljert. Metodekapittelet er ment for å gi leseren et innblikk og en forståelse av undersøkelsens innhold, drøftinger og konklusjon. Med disse aspektene, vil dermed vurdering og evaluering av hensiktsmessige kriterier være med på å styrke reliabiliteten av metode og datainnsamling.

4.4.2 Begrepsvaliditet (Troverdighet)

Validitet dreier seg om hvorvidt forskeren måler det han eller hun har til hensikt å undersøke. I kvalitative undersøkelser handler begrepsvaliditet om i hvilken grad forskerens fremgangsmåter og funn reflekterer formålet med studien (Johannessen, 2011)

Formålet med undersøkelsen reflekteres i problemstillingen, og legger retning for oppbygningen og analysen. Dataene som presenteres kategorisk er ment for å gi en oversikt over de innsamlede ustrukturerte dataene, og drøftingen skal gi leseren god forståelse av resultatene og konklusjonen. Gjennom intervjuene har vi forsøkt å minimere intervjueffekten ved å stille åpne drøftingsspørsmål, holde et nøytralt kroppsspråk og prøvd å imøtekomme informantenes informasjon på en profesjonell måte.

Det er ikke noe spørsmål om personvern enten påvirker eller ikke i en bransje, men heller i hvilken grad. Informantene for oppgaven er plukket ut strategisk for å representere den bransjen som har kommet langt med KI, og hvor personvern samtidig lenge har vært underlagt strengt regulatorisk. Vi kan klassifisere intervjuobjektene som ledende fageksperter innenfor begge fenomener. Dette er med på å styrke troverdigheten både til våre intervjuobjekter og datainnsamlingen. Likevel vil datainnsamlingen kunne inneholde noe form for skjevhet eller metodefeil. Grunnet omfanget av undersøkelsen og praktiske årsaker vil det forekomme noe utvalgsskjevhet, og kan vurderes til å svekke validiteten og representativiteten.

4.4.3 Ekstern validitet (Overførbarhet)

Ekstern validitet handler om hvorvidt resultater fra et forskningsprosjekt kan overføres til andre sammenlignbare områder (Johannessen, 2011).

For å sikre anonymitet for undesøkelsen kan vi ikke oppgi navn på virksomhetene som er benyttet som respondenter. Vi kan derimot nevne at ekspertisen de utvalgte sitter på er overførbare resultater til både virksomheter i samme bransje og andre næringer. Til tross for at ikke alle virksomheter benytter seg av digitale løsninger i like stor grad som våre respondenter, vil det være rimelig å vurdere deres beskrivelser, begreper, fortolkninger og forklaringer overførbare. Med dette mener vi at resultatene fra datainnsamlingen er nyttig for andre bransjer med lignende formål.

4.4.4 Objektivitet (bekreftbarhet)

Objektivitet går ut på at det er viktig at funnene ikke er et resultat av forskernes subjektive holdninger, men er et resultat av forskning (Johannessen, 2011).

For å sikre en høy grad av objektivitet har vi detaljert forklart alle beslutninger gjennom hele forskningsprosessen, slik at leseren skal kunne følge og vurdere disse. Påstander og konklusjon er kontinuerlig drøftet, og har forankring i funn fra informantene. Vi styrker også objektiviteten ved at fortolkningene er støttet opp av supplerende teorier og litteratur. Mange av påstandene er også støttet opp av informantene, og gir grunnlaget for en objektiv vurdering. For drøfting og analyse har vi forsøkt å være så objektive som mulig, og det vil være umulig å si med sikkerhet at

det ikke forekommer noen skjevheter. Både intervjuguiden, gjennomføringen av selve intervjuet, analysen og konklusjonen vil kunne bære noe preg av subjektivitet, og kan dermed være med på å svekke bekreftbarheten.

5.0 Analyse og drøfting

Formålet med analysen er å kunne gi en oppklarende fremstilling av hvilke personvernproblematikker våre respondenter opplever ved bruk og utvikling av KI. Samtidig vil det drøftes de muligheter som kan utnyttes ved KI.

5.1 Begrepet kunstig intelligens

For å forstå og utnytte endringer i teknologiutviklingen skal Norge ha avansert kompetanse både innenfor IKT-forskning og KI-forskning (Astrup, 2020). KI er «hype» å snakke om blant norske virksomheter (Respondent A), og KI settes derfor høyt på agendaen i dagens teknologiske samfunn. Som en effekt av at KI er «hype», uttrykker respondent B at hovedgrunnen til at bedrifter etterspør KI, er ønsket om å fremstå som troverdige og tidsriktige.

"Artificial intelligence is like teenage sex: Everyone talks about it, nobody really knows how to do it, everyone thinks everyone else is doing it, so everyone claims they are doing it" (Ariely, 2020).

Tolkningen av begrepet vil kunne gi en pekepinn på om virksomheter har tilegnet seg tilstrekkelig kunnskap knyttet til KI eller om de bare omtaler begrepet som en trend. Flere virksomheter omtaler programmering basert på statistikk som det nye KI (Respondent A). Det kan her se ut som virksomheter ikke har et bevisst forhold til begrepet, og dermed uttrykker at de tar det i bruk, når de egentlig tar i bruk ML og beslutningstrær. Respondent D vil ikke gi en spesifikk definisjon på KI, fordi dette i seg selv vil være å bestemme hva som er riktig. Med bakgrunn i dette utsagnet vil norske banker i utviklingsfasen av KI ofte stille spørsmål: hva er KI, og hvordan skal det brukes eller ikke brukes (Broomfield & Reuter, 2019).

Likeledes, opplyser Respondent C om at de i banken ikke har en uttalt definisjon på KI og at det er ulike meninger om begrepet. Det vil her avhenge av hvem som definerer KI og om vedkommende retter begrepet populistisk eller akademisk. «Den akademiske definisjon på kunstig intelligens vil være at det er en entitet, noe annet enn et menneske, som tar smarte valg basert på en kombinasjon av nevrale nettverk, maskinlæring, dyp læring, Natural language prosessing og statistikk» (Respondent C). Det spesifiseres at KI handler om at entiteten faktisk tar smarte beslutninger selv og ikke at den forer et menneske som tar beslutninger. Flere norske virksomheter definerer ML som KI (Respondent A). Videre, vil respondent C definere maskinlæring som et verktøy i verktøykassen til KI.

Norge har ikke like muligheter til å skaffe kunnskap og kompetanse i hele bredden av KI-feltet sett opp mot et høyt internasjonalt nivå, men fokuset på kvalitet og kvantitet på nasjonal kompetanse vil stå sentralt (Astrup, 2020). Begrepet kunstig intelligens er såpass nytt for norske virksomheter og vil derfor oppleves som et tverrfaglig og komplekst fenomen (Respondent A; B; C; D). Det kan her virke som norske banker har ulike oppfatninger av begrepet, men at de har god innsikt i hvordan kunstig intelligente systemer kan effektivisere innad i virksomheten. Tilstrekkelig kunnskap til teknologien vil være avgjørende for å kunne forstå og ta i bruk kunstig intelligens.

5.2 Innebygd personvern

Datatilsynet legger frem innebygd personvern som spesielt viktig for virksomheter som tar i bruk systemer som bygger på KI. Til tross for at kravet har tydelige retningslinjer, er det en felles enighet blant våre respondenter om at innebygd personvern i praksis ofte er omfattende og dermed også vanskelig å overholde (Respondent A; B; C; D). Ny teknologi medfører et behov for oppdateringer i rutiner og prosesser ved behandling av personopplysninger, og vil stå like sentralt ved gamle som for nye systemer.

Innebygd personvern kan sies å stå i nær tilknytning til virksomheters digitale intensitet. Virksomheter som har dårlige tekniske systemer, og som ikke har de ressursene som kreves til å implementere automatiserte prosesser, vil nødvendigvis utbygge et mer manuelt regime (Respondent B). Respondentene uttrykker at de i stor grad har digitaliserte prosesser og rutiner, men at de opplever svingninger i næringslivet med lav digital kvalitet og høy grad av teknisk gjeld (Respondent A; B; C; D). Regelverket er lovfestet, og problemet vil derfor ikke ligge i om virksomheter har innebygd personvern eller ikke, men i hvordan og i hvilken grad disse er bygget inn i systemene.

Personvernproblematikken som oppstår når virksomheter skal ta i bruk og utvikle KI vil ofte være størst hos virksomheter med et teknologisk etterslep og tyngre, eldre IT-systemer (Respondent A). Dette vil ofte være knyttet til at personvernet i liten grad er bygget inn som en del av systemet, og heller lagt til og beskrevet av respondentene som omfattende manuelle rutiner og prosessbeskrivelser (Respondent A; B). Virksomheter som opererer slik vil derfor kunne oppleve utfordringer ved å etterleve prinsippet om gjennomsiktighet og de registrertes rettigheter til sletting og innsyn. Dette fordi manuelle oppgaver hvor en eller flere mennesker skal involveres som regel er mer ressurs- og tidkrevende enn automatiske oppgaver.

Norsk bank-, finans- og forsikringsbransje vurderes i dag til den mest digitaliserte bransjen i Europa (PricewaterhouseCoopers, 2020), og dette vil i stor grad også gjelde våre respondenter. Respondent C viser til at det også er mulig å bygge personvernet inn i eldre systemer. Dette vil som regel skje i form av større oppdateringsprosjekter, hvor hver linje i systemet blir gjennomgått og vurdert for etterlevelse av personvernet. I vurderingen, blir det lagt vekt på at systemet ikke støtter kravet om innebygd personvern (Dahl, 2020). Ved implementering av nye digitale prosjekter eller systemer, vil respondentene allerede i en utviklingsfase bygge personvernet inn. Det vil være rimelig å anta at virksomheter i samme bransje med samme størrelse, slik som våre respondenter, vil angripe løsninger for innebygd personvern på noe samme måte.

KI har som mål å gi en mer effektiv forretningsdrift og forvaltning (Thon, 2018), og virksomheter som ønsker å benytte seg av denne teknologien vil kunne styrke personvernet dersom dette er bygget inn som automatiske prosesser. Respondent B sier at hovedgrunnen til at det forekommer avvik ved personvernet er menneskelig svikt. KI som en automatisering vil kunne redusere tilfellene av menneskelige svikt, og dermed også antall avvik.

Planleggingsfasen ved innebygd personvern vil være kritisk, og respondentene fremlegger viktigheten av proaktivt arbeid i designfasen som en avgjørende faktor for å lykkes med utviklingen av systemer som baserer seg på KI. Respondent A og B uttrykker begge at det å være i forkant, i seg selv kan medføre utfordringer. Norske virksomheter oppdager ofte i kommersialiseringsstadiet at systemet ikke overholder kravene til personvernet, og avvik oppstår. For å lette på denne problematikken er det vesentlig med et tverrfaglig samarbeid, eksempelvis mellom teknikere, jurister og analytikere. Disse bør involveres tidlig i utviklingsprosessen for å unngå teknisk gjeld (Respondent B).

5.3 DPIA – En risikovurdering

«Kunstig intelligens skal være bygget på systemer med teknisk robuste løsninger som forebygger risiko og som bidrar til at systemene fungerer slik de er tiltenkt. Risikoen for uintenderte og uventede skader skal minimeres. Teknisk robusthet er også viktig for systemenes nøyaktighet, pålitelighet og etterprøvbarhet» (Astrup, 2020). På samme måte som innebygd personvern, vil en vurdering av risiko for personvernet være spesielt viktig for virksomheter som tar i bruk systemer som bygger på KI.

Respondent B uttrykker at virksomheter må avdekke alle områder hvor det er en fare for at personopplysninger kan lekkes. I tillegg må risikoreduserende tiltak bygges inn i løsningen etter at risikoen er identifisert, og alle vurderinger må dokumenteres. For å redusere sannsynligheten for risiko for den registrertes rettigheter og friheter, må de behandlingsansvarlige foreta en risikovurdering i designfasen. Respondent D sier at bank handler om mennesker og de registrerte, og at utsagnet støttes opp mot et viktig

aspekt ved risikovurdering. Verdien ligger i å gi sine kunder medbestemmelse, utøve åpenhet, forutsigbarhet og skape tillit.

KI-systemer er avhengige av data i bruk og utvikling, og dermed er det også nødvendig for de registrerte at personopplysningene de gir fra seg er tilknyttet minst mulig risiko. Gjennomsiktighet, retten til sletting og innsyn vil blant annet være sentrale behov for de registrerte, og vesentlig for at KI systemene skal kunne utnyttes. Dette må bygges inn i løsningene, slik at personvernet begrenser prosessene minst mulig.

Dersom virksomheter mot formodning ikke skulle klare å redusere risiko, vil dette kunne medføre økonomiske eller sosiale ulemper. KI-systemer har lenge hatt sin rot i teknologien, men det er ikke før nå at vi faktisk ser en endring i bruk av KI for å treffe slutninger. Dette gjelder særlig for bank- og finansbransjen som behandler mer personopplysninger enn andre. Risikoen anses derfor å være relativt høy (Datatilsynet, 2020). Med utgangspunkt i at våre respondenter underligger bank og finans vil det derfor være relevant å vurdere avvikene i denne bransjen.

Datatilsynet har mottatt totalt 3.000 avviksmeldinger etter innføringen av GDPR. 1.916 av disse avvikene er mottatt i 2019, og bank- og finansbransjen står for 30 prosent. Til tross for at dette er den største prosentandelen av alle områdene, skyldes dette i stor grad at bransjen er preget av høy grad av etterlevelse av GDPR. I tillegg er bransjen preget av høy kompetanse (Datatilsynet, 2020).

Til tross for at respondent C og D uttrykker at bransjen er preget av høy digitaliseringsgrad, vil KI kun i dag modellere et resultat som veileder for menneskelige beslutninger. Ifølge Datatilsynets årsrapport skyldes 83 prosent av avvikene som forekommer manglende rutiner, kunnskap, opplæring, uhell eller teknisk svikt internt i virksomheten (Datatilsynet, 2020). Siden 30 prosent av disse gjelder for bank- og finansbransjen, vil bruk og utvikling av KI-systemer være spesielt relevant for denne bransjen. Med en mulighet til å redusere svikt i manuelle prosesser eller menneskelige feil, medfølger også en reduksjon i antall avvik.

Datatilsynet gir hvert år ut overtredelsesgebyr for større avvik, noe som gjør bransjen sårbar for økonomiske konsekvenser.

Respondent B legger vekt på at løsningen grundig må kartlegge risikoen for hacking og brudd på datasikkerheten. Formålet med å ta i bruk KI er at modellen kan gjenkjenne mønstre, for personvern vil dette gjelde avvik. KI-systemer kan brukes til å avdekke bank- og forsikringssvindel eller brudd på datasikkerhet (Astrup, 2020). Dersom risikoen reduseres ved bruk av KI, vil også personvernet i høyere grad kunne etterleves, og mange av avvikene potensielt unngås.

5.3.1 Skade på omdømme

«En ofte glemt risiko er risikoen forbundet med organisasjonens omdømme» (Brønn & Arnulf, 2019). Enhver organisasjon som behandler personopplysninger vil oppleve at deres kunder eller brukere har visse forventinger til at deres personopplysninger skal bli behandlet sikkert og profesjonelt. Dette blir definert som kritisk for grad av tillitsforhold, og er uavhengig av hvilke teknologier virksomheten benytter seg av. Dette vil gjelde behandling av personopplysninger i systemer, og dermed også stå sentralt for KI.

Brudd på tillit kan føre til skade på omdømme i mindre eller større grad for en virksomhet. Hvilke konsekvenser virksomheten opplever som konsekvens av et brudd, avhenger av hvilken alvorlighetsgrad de har ved mislighold av personopplysninger. Respondent D sier at dersom en virksomhet blir tatt for å ikke melde fra eller bruke opplysninger ulovlig, kan de risikere å miste lisensen. Bank- og finansbransjen har en høyere risiko ved brudd på GDPR grunnet de store mengdene personopplysninger de behandler i forretningsdriften. Det er felles enighet blant våre respondenter om at misbruk av personopplysninger er nært tilknyttet tap av tillit. Virksomheter innenfor denne bransjen har derfor et spesielt høyt fokus på å etterleve GDPR-kravene for å unngå konsekvensene som medfølger ved et brudd (Respondent A; B; C; D).

5.4 Kunstig intelligens og prinsippet om formålsbegrensning og dataminimering

Formålsbegrensing innebærer at man skal begrense behandlingen av personopplysninger til det formålet det er samlet inn for. Det betyr at formålet som er angitt er bestemmende for i hvilken grad man klarer å overholde prinsippet om dataminimering (Respondent B).

«Presset på bruken av personopplysninger øker i takt med at analyser basert på KI kan bidra til effektivisering og bedre tjenester» (Datatilsynet, 2018). Innsamling av data fra de registrerte er nødvendig for utvikling og bruk av kunstig intelligente systemer. Gjenbruk av data vil kunne gjøre det beste for samfunnet; det blir bedre, billigere og raskere (Broomfield & Reuter, 2019). Samtidig som bankene skal gjennomføre prosjekter basert på KI med store mengder data, vil det være avgjørende med et relevant utvalg av datamengder (Astrup, 2020).

5.4.1 Stordata og GDPR

Norske banker sitter på registre med stordata. De lagrer mer opplysninger om den enkelte enn de trenger (Respondent A), og de er pålagt å beholde data til bruk for politiet i kriminalsaker og regnskapslovverk. Maskingenererte, systemgenererte og menneskegenererte data kan i mange tilfeller isolert sett ikke knyttes opp mot enkeltpersoner. Sammensetningen av disse dataene vil potensielt kunne utgjøre sensitive opplysninger, og kan derfor ikke gjenbrukes til annet enn formålet. Her trekkes formålsbegrensning inn. Respondent C opplyser om at de har utviklet en egen mobilapp som baserer seg på KI med lokasjonsdata, timestamps, locationstamps og identifikasjon av hva den registrerte kjøper. Banken har muligheten til å kunne ta en helhetsvurdering av den registrerte som menneske, men disse dataene skal ikke brukes som grunnlag for vurdering av en kunde.

Det er kontroversielt å skulle bruke personopplysninger til andre formål enn det dataene er innhentet for og det er derfor viktig å etterleve GDPR-regelverket. «Vi har kun lov til å behandle data som vi har samtykke til» (Respondent C; D). Respondent C stiller spørsmål til hvorvidt de virkelige verdifulle opplysningene faktisk reguleres

av GDPR, og om data som genereres blir tatt hensyn til. Respondent C og D spesifiserer her at motivasjonen ikke er å benytte denne dataen til annet formål enn det formålet dataen er innhentet for. «Vi sletter mye data kontinuerlig» (Respondent D). Dataene slettes dersom banken har muligheten til det, fordi det besittes så mye opplysninger som de ikke trenger.

5.4.2 Formålsglidning

Planlegging av innebygd personvern, i forkant og i forberedelsesfasen av kunstig intelligente systemer i realiteten føre til formålsgliding (Respondent A). Utviklingsperspektivet av KI er problematisk når alt skal avgjøres på forhånd fordi det ikke er mulig å forutse hva algoritmen vil være. I ettertid, vil det være lett å trekke slutning om at man skulle valgt en annen løsning. Her forutsettes det at man kan foré KI-systemet med tilstrekkelig informasjon. Det er vanskelig å vite formålet fra start og hvilke data som er nødvendig for at KI-systemer skal fungere optimalt. Etterhvert som maskinen lærer, kan formålet imidlertid endres (Datatilsynet, 2018).

5.5 Kunstig intelligens og prinsippet om gjennomsiktighet

Respondent A legger vekt på at det er knyttet en del praktiske utfordringer til hvordan en virksomhet skal overholde sine plikter om åpenhet rundt bruk av personopplysninger. I arbeidet med utviklingen av KI systemer, er det vanskelig å kartlegge hvilke data man trenger i utviklingsfasen, og hvilke sammenhenger og slutninger som trekkes basert på dette. Dette skaper utfordringer vedrørende bruk av personopplysninger. Ettersom formålet ikke er forhåndsbestemt kan det være vanskelig å være åpen om hvilke data som blir benyttet. Dette blir trukket frem som høyst relevant og viktig i diskusjonen vedrørende håndtering av personopplysninger (Respondent A; B; C; D).

For å sikre åpenhet, vil det være hensiktsmessig å gi de registrerte spisset og rettet informasjon om hvordan behandlingen av data foregår (Astrup, 2020). Dette formuleres gjerne i form av en samtykkeerklæring. Respondent B presiserer at en viktig nøkkelfaktor vil være å gi nødvendig informasjon, gjennom bruk av et klart og brukertilpasset språk slik at det er lett å oppfatte for den registrerte. For å kunne gi

tilstrekkelig og god nok innsikt til den registrerte, forutsetter dette at virksomhetene kan forklare hvilken informasjon det automatiserte systemet baserer beslutningen på (Datatilsynet, 2018). Ved systemer som bygger på ML kan det være komplisert å skaffe tilstrekkelig innsyn og overblikk for hvordan systemet fungerer. Dette kalles svart boks-problematikk, og vil utdypes videre.

5.5.1 Svart boks-problematikken

Enkelte algoritmer som benyttes i systemene er så komplekse at man ikke har nok innsyn i modellen til å kunne forklare hvilke data som er benyttet eller hvordan resultatet er produsert (Astrup, 2020). Denne problematikken er ikke relevant for alle typer av KI, men er en aktuell utfordring ved ML.

Prinsippet om gjennomsiktighet vil ikke overholdes dersom det er mangel på transparens i systemene. Dette er særlig en trussel mot personvernet, dersom systemet behandler persondata. En nødvendighet for videreutvikling og bruk av systemer basert på ML, vil derfor være å utvikle algoritmer som forklarer hvordan systemet tar beslutninger (Bergsjø & Bergsjø, 2019).

«Forklarbar KI» vil kunne være en løsning på svart boks-problematikken. Dette er en løsning som tar utgangspunkt i å analysere hvilke data som har hatt påvirkningskraft for resultatet. I tillegg vil også vektingen av de ulike elementene følge av analysen (Astrup, 2020). Utviklingen av slike algoritmer er svært komplisert, og det foregår mye forskning på dette området (Datatilsynet, 2018). Respondent D trekker frem at deres bank benytter seg av noe de kaller «hvit boks». Denne løsningen gjør det mulig å forklare modellen, og begrunne resultatet ovenfor kunden.

Med utgangspunkt i samme datagrunnlag, så ser vi ved sammenligning av svart og hvit boks algoritmene, at svart boks algoritmene signifikant er bedre enn hvit boks algoritmene i de fleste tilfeller (Respondent D). Derfor vil det være aktuelt å benytte løsninger med svart boks algoritmer ved enkelte dataanalyser. Svart boks kan benyttes til å kategorisere resultatene, men for å overholde prinsippet om gjennomsiktighet er det et menneske som er nødt til å foreta en beslutning. Dette krever at vedkommende har forståelse og innsikt i beslutningen.

5.6 Muligheter ved bruk og utvikling av kunstig intelligens

På generell basis, ser vi at KI anvendes i mindre komplekse prosjekter som rapporter og enkeltanalyser. I virksomheter med større grad av digitalisering har vi eksempler på anvendelse av KI på et mer avansert plan. I disse tilfellene benyttes KI blant annet til produksjonssatte beslutningsstøtte- og kontrollverktøy (Broomfield & Reuter, 2019). Dette tyder på at det er muligheter for større grad av automatisering i flere bransjer, og utvidelse av bruksområder utover det KI benyttes til i dag. Forskning på nasjonal agenda blir dermed en viktig faktor for å utnytte mulighetene ved bruk av KI.

I en rapport utgitt i regi av regjeringen ser vi en økning i midler til forskning innen IKT. I 2019 ble det tildelt omtrent 400 millioner som gikk til forskning på prosjekter innen KI, robotikk og stordata (Astrup, 2020). I Norge og Europa er det spesielt fokus på pålitelig KI, for å sikre at systemene ivaretar personvernet. Det kommer frem fra respondent B at det etableres grupper i offentlig sektor som arbeider med å finne en løsning for hvordan man skal ivareta kravene i GDPR, ved utvikling og bruk av KI. Slike initiativ og samarbeid er avgjørende for en positiv utvikling. Opprettelse av slike nettverk i privat sektor blir en viktig faktor for forskning innen KI, gjennom samarbeid og deling av løsninger.

Utvikling og bruk av KI vil nødvendigvis reguleres av GDPR. Dette er sentralt i utviklingen av pålitelig KI, som tar hensyn til personvern og etiske vurderinger. I finansnæringen kan KI blant annet brukes til rekruttering, lånesøknader, tolke kontrakter, registrere kundeatferd og avdekke kortsvindel (Teknologirådet, 2018). Samtidig kan det benyttes som overvåkning til å avdekke økonomisk kriminalitet som for eksempel hvitvasking. Respondent C og D nevner at de anvender systemer i dag som bygger på ML og modellering, som de kan benytte til avdekking av svindel og til å se sammenhenger i kundeatferd. Respondent D legger også til at de har egne team som eksplisitt arbeider med utvikling og bruk av KI. En generell tendens i bank- og finansbransjen at de systemene de benytter i dag, beveger seg mer over i en form for KI (Respondent D).

Bruk og utvikling av KI i næringslivet er viktig for verdiskapning, og kan bidra til konkurransefortrinn for virksomheter som finner gode løsninger på pålitelig KI. Automatisering av arbeidsoppgaver og prosesser vil bidra til å effektivisere driften og frigjøre ressurser i form av arbeidskraft. En del banker anvender blant annet systemer med elementer fra KI som beslutningsstøtte ved lånesøknader (Respondent C; D). I tillegg vil systemer basert på ML benyttes for å kartlegge kundeatferd, og til å forstå interne prosesser bedre. Dette gjør det mulig å drive med tilpasset markedsføring, noe som skyldes at ML ser sammenhenger som ikke har vært mulig tidligere ved manuell analyse (Respondent A; B; C; D).

I 2019 ble det vedtatt en ny lov om behandling av opplysninger i kredittopplysningsvirksomhet (Datatilsynet, 2020). Det er forventet at den nye kredittopplysningsloven vil tre i kraft i løpet av 2020. Målet med den nye loven er at bankene skal kunne foreta grundigere kredittvurderinger av kunder, samtidig som de vil hindre at kunder tar opp mer gjeld enn de kan betjene.

Loven vil åpne for at bankene skal kunne få innsikt i den registrertes kredittopplysninger og gjeldsopplysninger fra gjeldsinformasjonsforetak (Kredittopplysningsloven, 2019). Dette betyr at bankene vil ha større vurderingsgrunnlag, som også vil ha betydning for utviklingen av KI systemer. Det vil øke mulighetene for mer treffsikre analyser og beslutninger. Samtidig vil loven bidra til å redusere risiko for utnyttelse av bankens tjenester.

5.7 Samfunnsansvar, etikk og personvern

Samfunnsansvar handler mye om å bygge kompetanse i miljøet og samfunnet rundt oss (Respondent D). Dersom norske banker ikke forstår og har tilstrekkelig innsikt i teknologien, vil det ikke være mulig å opprettholde trykk i endringstakten i næringslivet. Dersom virksomheter ikke tar i bruk KI, vil det kunne resultere i teknologiske etterslep. Respondent D sier fokuset på å bruke tid på egne ressurser og egen forståelse rundt systemene er avgjørende for å forhindre teknisk gjeld, fremfor å kun kjøpe ferdige systemer.

Respondent D spesifiserer at dersom det ikke er et klart «ja», så vil det være et «nei». Med dette menes at banken innehar «nei-soner» fremfor «gråsoner». Prinsippet er viktig for å opprettholde og styrke en god organisasjonskultur innad i banken, samt trygghet for de registrerte. Et tydelig samfunnsansvar står her sentralt. Personvernet begrenser bruksområdet for KI; bankene har data liggende, men de må vurdere om det er etisk riktig og lovlig å bruke disse. Det oppstår her en gråsone med hvilke data som kan tas i bruk og hva som er etisk forsvarlig. Respondent C sier at de er opptatt av å følge de etiske retningslinjene og at verdien personvernet tilfører et samfunn er viktig i det store bildet.

5.7.1 Mennesket i fokus

Det er mange som har uttrykt bekymring rundt utvikling av KI, blant annet fysikeren Stephen Hawking, teknologi-gründerne Elon Musk og Bill Gates (Fugelsnes, 2018). Kritikken er hovedsakelig rettet mot et manglende fokus på det å verne om den registrertes rettigheter. Foreløpig vil ikke bruk og utvikling av KI kunne sammenlignes med de komplekse kognitive evner mennesker besitter, og er en av de mest sentrale utfordringene ved KI systemer. Ved mer komplekse vurderinger og kundebehandlinger er det en risiko for at utfallet ved bruk av KI resulterer i deterministiske svar, som potensielt kan utfordre personvernet (Respondent D). Det er derfor essensielt at det vil være en menneskelig vurdering ved minst et steg i prosessen, noe som også er et lovmessig krav (Respondent A; B; C; D).

Innføringen av GDPR har dermed vært viktig for utvikling av teknologi i fremtiden. GDPR bidrar til at den registrertes personvern ivaretas uavhengig om prosessene er automatisert eller manuelle, og det stilles krav til virksomheter som benytter seg av KI. Den registrerte har blant annet rett til innsyn og rett til etterprøving av resultatet dersom en beslutning er foretatt av en maskin (Datatilsynet, 2018). Det kan stilles spørsmål til om dette vil bremse effektivisering av driften, ettersom lovverket krever menneskelig involvering i deler av prosessene. Hovedsakelig vil dette avhenge av hvor godt innebygd personvern er implementert som en kjernefunksjonalitet i KI-systemet, og i hvilken grad man kan stole på KI til å foreta egne beslutninger.

Respondent D trekker frem at en positiv egenskap ved KI er at systemet vil være objektivt, og gjøre som den læres opp til. Samtidig er det noen utfordringer med å utvikle objektive systemer. «Fordommer eller manglende bevissthet blant utviklerne kan også føre til en fordomsfull og lite objektiv KI». Respondent B uttrykker at det ikke er lett å forutse hvordan dataen vil påvirke resultatet, og at det ikke alltid finnes godt nok datagrunnlag til at løsningen gir svar som er mindre preget av utvalgsskjevhet. Dette kan bidra til at systemene trekker urettferdige beslutninger, eller i enkelte tilfeller opptrer diskriminerende. Et viktig poeng er at systemer som baseres på KI er nødt til å vedlikeholdes (Respondent A).

5.7.2 Insentiver for kunstig intelligens

«Kunstig intelligens (KI) representerer store muligheter for oss som enkeltmennesker, og for samfunnet som helhet. KI kan bidra til nye og mer effektive forretningsmodeller i næringslivet og effektive og brukerrettede tjenester i offentlig sektor» (Astrup, 2020).

Ifølge respondent A, vil makt og økonomisk vinning være sentrale insentiver for KI. Manipulering av KI vil kunne gi tilgang til stor makt, og det er derfor viktig at virksomheter ikke utnytter data for manipulering. De fem store techgigantene har stor makt og lager algoritmer som er så kraftige at de registrerte blir avhengige (Respondent A). Parallelt med denne makten følger GDPR-regelverket som må etterleves, og en av utfordringene vil her være at de enkelt kan manipulere meningene til den registrerte. Friheten som ligger i personvernet faller bort når maskiner er sterkere manipulatorer enn mennesket. Det strider imot demokratiet at noen mennesker besitter stordata og setter slutning på hva som er rett og galt.

Det er en felles enighet blant våre respondenter om at etterlevelsen av GDPR vil være en sentral driver for å fremme og opprettholde personvernet (Respondent A; B; C; D). Personvernkonsekvensene ved brudd på GDPR er kritisk og bidrar dermed til å sikre enkeltmenneskets frihet til sine egne personopplysninger. Teknologiske fremskritt er viktig for effektivisering og utvikling av samfunnet. Respondent C antar at det vil det ta en stund før KI blir en stor del av samfunnet, fordi det oppstår endel etiske

problemstillinger som begrenser denne utviklingen. Denne utfordringen vil potensielt kunne legge noen føringer ved utvikling av KI.

Det vil være avgjørende å ikke utnytte folkets velvilje, integritet og mangel på kunnskap. «Ved bruk av KI beveger man seg på en knivsegg, der det er en sammenheng med der den virkelige verdien av KI ligger og viktigheten med å ikke misbruke tillit» (Respondent C). I Norge er vi velvillige til å ta i bruk ny teknologi og vi har god tillit til selskaper og organisasjoner, men det er her avgjørende at det settes krav til etiske retningslinjer.

Hovedproblemstillingen ved insentiver for KI vil være å oppnå samfunnsmessig verdi, men samtidig vil det også stilles spørsmål til om denne utviklingen i det lange løp vil gagne enkeltindivider.

5.7.3 Tillit til kunstig intelligens og personvern

Det norske samfunnet innehar grunnleggende verdier som bærer preg av høy grad av tillit; nordmenn respekterer menneskerettighetene og personvernet i den teknologiske verden. Regjeringen legger frem at de vil at Norge skal gå foran i bruk og utvikling av kunstig intelligens med respekt for den enkeltes rettigheter og friheter (Astrup, 2020). Nye tjenester, produkter og personopplysninger baseres på data, digitalisering og effektivisering av tjenester avgjøres ved folkets grad av tillit til å dele personopplysninger. For utvikling av KI er det derfor avgjørende at de registrerte har tillit til virksomhetene.

«Personvernidealet tilsier at de registrerte i størst mulig grad skal kunne ha tillit til den som behandler opplysninger om dem» (Regjeringen, 2019). Hvilke holdninger den registrerte har til innsamling av data avgjøres av hvilken tillit de har til virksomheten. Tillit bør ikke tas for gitt og norske virksomheter må vise seg tillitsverdige (Datatilsynet, 2018).

Dersom virksomheter misbruker personopplysninger vil det kunne føre til en eventuell nedkjølingseffekt. Systemene vil da anses som mindre pålitelig og følgelig vil tilliten til virksomhetene svekkes. De registrerte vil kunne oppleve bekymring, frykt eller uro for at de blir overvåket (Datatilsynet, 2019). Våre respondenter

spesifiserer her at det er avgjørende med samtykke fra den enkelte, slik at virksomhetene ikke overskrider hva som er lovlig innen rettens grunnlag (Respondent A; B; C; D). Både respondent A og C konkretiser at tillit er nøkkelen for å lykkes med innebygd personvern, og muliggjør forretningsutvikling.

6.0 Konklusjon

GDPR-regelverket påvirker bruk og utvikling av kunstig intelligens på flere områder. Innledningsvis presenterte vi følgende problemstilling:

«På hvilken måte påvirker GDPR bruk og utvikling av kunstig intelligens, og hvordan kan teknologien utnyttes?»

Tilgangen på innovative og høyteknologiske løsninger i kombinasjon av verdifull data, vil kunne gi virksomheter unike forretningsmuligheter. Teknologien utvikler seg over tid, og oppblomstringen av systemer som tar i bruk KI står sentralt i dagens IT-norm. Norske virksomheter vil imidlertid ikke kunne skape verdi dersom løsningene ikke tar hensyn til hvilke aspekter som gjør KI mulig. Stordata er drivkraften bak kunstig intelligens, og er en naturlig utvikling av markedsøkonomien. Riktig og lovlig bruk av data er avgjørende for at virksomhetene skal kunne utnytte løsningen, og personvern vil derfor være en nøkkelfaktor.

I analysen avdekkes det at mulighetene ved bruk og utvikling av KI er mange. Virksomheter som ser verdien av å ta i bruk og utvikle KI-systemer vil kunne oppleve en økonomisk og samfunnsmessig verdiøkning. Samtidig som verdi står sentralt, vil det oppstå flere utfordringer i etterlevelsen av GDPR. Respondentene trekker frem formålsbegrensning, dataminimering og gjennomsiktighet som spesielt utfordrende i tilknytning til KI.

Det største problemet ved bruk og utvikling av KI systemer er at det i forkant vil være vanskelig å forutse hvilke data som vil være relevant å hente inn for en analyse. Samtidig vil dette også skape utfordringer knyttet til dataminimering, fordi stordata gjør KI mulig. Prinsippene vil i kombinasjon kunne skape problemer ved utforming av samtykkeerklæringen. Dersom norske virksomheter skal dra nytte av KI og kunne redusere de overnevnte utfordringene, vil det være nødvendig med forskning og videreutvikling av kunstig intelligente systemer. Nødvendige tiltak for effektiv utvikling av KI vil være kunnskapsdeling, innovasjon og samarbeid.

Formålet med KI er å systematisere data for videre analyse, men særlig vil norske virksomheter oppleve flere problemstillinger til forklarbarheten av hvordan systemene fungerer. Prinsippet om gjennomsiktighet begrenser KI med at det er utfordrende å forklare algoritmene modellen bygges på. Dette gjør at virksomheter i dag ser at systemet ikke kan ta beslutninger på egenhånd, men at det kun kan brukes som et analyseverktøy. Til tross for at svart boks algoritmer er mer treffsikre enn hvit boks algoritmer, kan sistnevnte i dag benyttes som en løsning på forklarbarhet.

Personvernfremmende teknologi gjør innebygd personvern mulig, og det vil være rimelig å konkludere med at dette er en løsning for å etterleve personvernet. KI-systemer er fortsatt i en tidlig utviklingsfase, og virksomheter som drar nytte av å bygge personvernet inn som en kjernefunksjonalitet, vil kunne oppnå konkurransefortrinn. Virksomheter som ser verdien av innebygd personvern allerede i en designfase, vil kunne reduserer risiko, personvernkonsekvenser og samtidig sørge for at de registrertes friheter og rettigheter blir ivaretatt. Innebygd personvern vil kunne gi en mer åpen og trygg behandling, og kontroll som kan være med på å styrke tillit mellom systemet og den registrerte.

For å konkludere vil GDPR isolert sett ikke medføre noen utfordringer i bruk og utvikling av KI, men derimot heller hvilke insentiver som legges til grunn for behandling av personopplysninger. Behandlingsansvarlig må derfor kontinuerlig tilstrebe å finne en balanse mellom de samfunnsmessige og økonomiske gevinstene. Samtidig kan vurderinger om at GDPR ikke tar tilstrekkelig hensyn til den teknologiske utviklingen, forklares med konflikten mellom KI og etiske retningslinjer. Avslutningsvis, vil det være rimelig å anta at det er mulig å ivareta personvernet med bruk og utvikling av KI. Hvordan teknologien utnyttes avhenger av hvilke behov norske virksomheter ser ved bruk og utvikling av KI, og at det er i tråd med samfunnsmessige verdier.

7.0 Refleksjonsnotat

I denne avhandlingen har vi forsket på hvordan GDPR påvirker bruk og utvikling av KI, og hvordan norske virksomheter kan dra nytte av denne teknologien. Tematikken som danner grunnlaget for oppgaven er kompleks, noe som har ført til utfordringer vedrørende avgrensning av oppgaven. Vi har forsøkt å avgrense uten å svekke innholdet og utgangspunktet for drøftelsen og analysen.

KI og personvern er abstrakte begreper som er krevende å måle. Mangel på ressurser, samt tilgang på respondenter begrenset utvalgsstørrelsen. Et lavt antall respondenter er en typisk svakhet ved kvalitative studier. Samtidig åpner et smalt utvalg for økt fokus på de som intervjues, og legger dermed til rette for innhenting av dybdeinformasjon. Dette er formålstjenlig i en oppgave som søker innsikt i et tema.

Det var krevende å finne respondenter som hadde kapasitet til å stille seg disponibel til gjennomførelse av intervju, og antall informanter er dermed ikke tilstrekkelig. Utvelgelsen av intervjuobjektene veier noe opp for dette, ettersom flere av intervjuobjektene har gjennomført prosjekter eller samarbeid med andre norske virksomheter. Dette er prosjekter som berører både overholdelse av GDPR-regelverket og utvikling av teknologiske løsninger, og var dermed svært relevante funn.

Utarbeidelsen av bacheloroppgaven har vært en svært lærerik og krevende prosess. Under høstsemesteret i fordypningskurset forretningsutvikling og digitalisering opplevde vi datasikkerhet som et spennende område. Vi ønsket å fokusere på den registrertes personopplysninger. Forskningsprosessen startet med at vi leste oss opp på litteratur, før vi avgjorde retning for oppgaven. Etter hvert, kom vi frem til at utfordringene og mulighetene knyttet til KI og personvern, og hvordan denne teknologien utnyttes, ville være en interessant vinkling på oppgaven.

I oppstartfasen satt vi med et inntrykk av at KI var mer utbredt i norske virksomheter enn det som er faktum. Dette skapte begrensninger i utvelgelsen av aktuelle intervjuobjekter. For å oppnå større grad av reliabilitet burde vi i tillegg til dybdeintervju, benyttet oss av kvantitative spørreundersøkelser. Med tanke på

omstendighetene, har vi vært tvunget til å gjøre endringer og tenke alternativt i arbeidsprosessen. Dette er noe vi mener vi har taklet godt, og vi har erfart nytten av gode teknologiske løsninger.

8.0 Referanseliste

Ariely, D. (2020). *Digital Transformation*. Hentet fra tgo-consulting.com: https://www.tgo-consulting.com/digital

Astrup, N. (2020, Januar 14). *Nasjonal strategi for kunstig intelligens*. Hentet fra Regjeringen.no: https://www.regjeringen.no/contentassets/1febbbb2c4fd4b7d92c67ddd353b6ae8/no/pdfs/ki-strategi.pdf

Bergsjø, L. O., & Bergsjø, H. (2019). *Digital etikk* . Universitetsforlaget.

Broomfield, H., & Reuter, L. (2019, September). *Kunstig intelligens/Data Science: En kartlegging av status, utfordringer og behov for norsk offentlig sektor.* Hentet fra NTNU: https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2634733/KI%252C%2Bdata%2Bscience%2B-%2BKartlegging%2Bav%2Bstatus%252C%2Butfordringer%2Bog%2Bbehov%2Bi%2Bnorsk%2Boffentlig%2Bsektor.pdf?sequence=1&isAllowed=y

Brønn, P. S., & Arnulf, J. K. (2019). *Kommunikasjon for ledere og organisasjoner.* Bergen: Fagbokforlaget.

Datatilsynet. (2017, Juni 05). *Big Data - Personvernprinsipper under press.* Hentet fra Datatilsynet: https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/rettigheter-og-plikter/rapporter/big-data_web.pdf

Datatilsynet. (2017, oktober 12). *Må styrke forskning på personvern for å sikre tillit til digitale tjenester*. Hentet fra Datatilsynet.no: https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/hoeringsuttalelser/2017/horing-forskning-utdanning/

Datatilsynet. (2018, 06 25.). *Formålsbegrensning*. Hentet fra Datatilsynet.no: https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/formalsbegrensning/

Datatilsynet. (2018, juni 23.). *Innebygd Personvern*. Hentet fra Datatilsynet.no: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/

Datatilsynet. (2018, januar 11). *Kunstig intelligens og personvern.* Hentet fra Datatilsynet.no: https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/kunstig-intelligens/

Datatilsynet. (2018, Januar). *Personvern 2018 Tillit og følelser*. Hentet fra datatilsynet.no: https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/rettigheter-og-plikter/rapporter/tilstand-og-trender-20182.pdf

Datatilsynet. (2019, 07 17.). *Hva er en personopplysning?* Hentet fra Datatilsynet.no: https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/

Datatilsynet. (2019, juli 17). *Hva er personvern?* Hentet fra datatilsynet.no: https://www.datatilsynet.no/rettigheter-og-plikter/hva-er-personvern/

Datatilsynet. (2019, august 08.). *Nødvendig for å ivareta legitime interesser - interesseavveiing*. Hentet fra datatilsynet.no: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/?id=10831

Datatilsynet. (2019, august 21.). *Om personopplysningsloven med forordningen og når den gjelder*. Hentet fra datatilsynet.no: https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/om-personopplysningsloven-og-nar-den-gjelder/

Datatilsynet. (2019, juli 16). *Personvernprinsippene*. Hentet fra Datatilsynet.no: https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/

Datatilsynet. (2019, juli 17). *Vurdering av personvernkonsekvenser*. Hentet fra Datatilsynet.no: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/

Datatilsynet. (2020, mars 28). *Hvilke rettigheter har den det tas opptak av?* Hentet fra Datatilsynet.no: https://www.datatilsynet.no/personvern-pa-ulike-omrader/overvaking-og-sporing/lydopptak/?id=8414

Datatilsynet. (2020, Mai 4). *Årsrapport for 2019 - Tall og tendenser fra Datatilsynets virksomheter*. Hentet fra Datatilsynet.no: https://www.datatilsynet.no/om-datatilsynet/arsmeldinger/arsmelding-for-2019/

Dvergsdal, H. (2019, 11 11). *Nevralt nettverk*. Hentet fra snl.no: https://snl.no/nevralt_nettverk

Fugelsnes, E. (2018, Oktober 22). *Kunstig intelligens: Frelsende eller fatalt?* Hentet fra Forskning: https://forskning.no/data/kunstig-intelligens-frelsende-eller-fatalt/1251311

Gripsrud, G., Olsson, U. H., & Silkoset, R. (2018). *Metode og Dataanalyse.* Bergen: Fagbokforlaget.

Heggernes, T. A. (2017). *Digital forretningsforståelse.* Bergen: Fagbokforlaget.

Johannessen, A. (2011). *Forskningsmetode for økonomisk-administrative fag.* 0130 Oslo: Abstrakt forlag AS.

Kredittopplysningsloven. (2019, Desember 20). Hentet fra Lovdata: https://lovdata.no/dokument/NL/lov/2019-12-20-109?q=kredittopplysningsloven

Kunstig intelligens. (2020). Hentet fra dnvgl.no: https://www.dnvgl.no/karriere/kunstig-intelligens.html?gclid=EAIaIQobChMIwJa7we_G6QIVicmyCh0FygVWEAAYAiAAEgK25vD_BwE

Lied, H. (2018, Juni 17). *Ryddet opp etter at kunstig intelligens begikk rasist-blemme*. Hentet fra NRK beta : https://nrkbeta.no/2018/06/17/ryddet-opp-etter-at-kunstig-intelligens-begikk-rasist-blemme/

Moor, J. H. (1985). *What is Computer Ethics* . Metaphilos .

Morgenbladet. (2017, Januar 27). *Advarer mot kunstig intelligens* . Hentet fra Morgenbladet: https://morgenbladet.no/aktuelt/2017/01/advarer-mot-kunstig-intelligens

NHO. (2018). *Næringslivets perspektivmelding; Digitalisering.* Hentet fra Næringslivets hovedorganisasjon: https://www.nho.no/siteassets/publikasjoner/naringslivets-perspektivmelding/pdf-er-sept18/nho_perspektivmeldingen_5_digitalisering.pdf

PricewaterhouseCoopers. (2017, Juni 08). *Digitalisering på 1-2-3*. Hentet fra pwc.no: https://www.pwc.no/no/teknologi-omstilling/digitalisering-pa-1-2-3/maskinlaering.html

PricewaterhouseCoopers. (2020). *Big Data.* Hentet fra pwc.no: https://www.pwc.no/no/publikasjoner/Digitalisering/big-data.pdf

PricewaterhouseCoopers. (2020, Mai 15). *Med ambisjon om å bli best på digitalisering*. Hentet fra pwc.no: https://www.pwc.no/no/pwc-aktuelt/med-ambisjon-om-a-bli-best-pa-digitalisering-.html

PrivatewaterhouseCoopers. (2020). *Fra strategi til AI*. Hentet fra pwc.no: https://www.pwc.no/no/pwc-aktuelt/fra-strategi-til-ai.html

Regjeringen. (2019, 10 30). *Hva er personvern?* Hentet fra Regjeringen.no: https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/hva-er-personvern/id448290/

Regjeringen. (2019, oktober 30.). *Ny personopplysningslov*. Hentet fra Regjeringen.no: https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/ny-personopplysningslov/id2340094/

Store norske leksikon. (2018, februar 20). *Hype*. Hentet fra snl.no: https://snl.no/hype

Succarat, G. (2017). *Metode og økonometri - en moderne innføring.* Oslo: Fagbokforlaget.

Teknologirådet. (2018, September). *Kunstig Intelligens - Muligheter, utfordringer og en plan for Norge.* Hentet fra Teknologirådet: https://teknologiradet.no/wp-content/uploads/sites/105/2018/09/Rapport-Kunstig-intelligens-og-maskinlaering-til-nett.pdf

Thon, B. E. (2018, februar 21). *Personvern og kunstig intelligens*. Hentet fra Personvernbloggen.no: https://www.personvernbloggen.no/2018/02/21/personvern-og-kunstig-intelligens/

9.0 Vedlegg

9.1 Figuroversikt

9.2 Intervjuguide

9.2.1 Intervjuguide I

1. Hvilke emner tenker dere umiddelbart at berøres av problemstillingen?
2. Hvilke utfordringer tenker dere ligger i prinsippene om dataminimering, formålsbegrensning og gjennomsiktighet?
3. Hvordan oppfatter dere at norske bedrifter håndterer personvernopplysninger etter innføring av GDPR?
4. Kan dere redegjøre for hvorfor innebygd personvern er viktig for virksomheter?
5. Hva vurderer dere som godt personvern, og hvilke utfordringer møter bedrifter i dag?
6. Kan dere redegjøre for hva dere mener er forskjellen på utvikling og bruk av kunstig intelligens?
7. Hvordan kan kunstig intelligens utvikles og brukes personvernfremmende?
8. Finnes det en korrelasjon mellom utvikling/bruk av kunstig intelligens og brudd på personvernet?

9. Noe tilleggsinformasjon dere tenker at er relevant for oppgaven? Eventuelt noen rapporter eller artikler som kan hjelp.

9.2.2 Intervjuguide II

1. Hvilke systemer i arbeidet deres baseres på kunstig intelligens?
2. Hva definerer dere som kunstig intelligens?
3. I hvilken grad tar dere i bruk digitale løsninger (digitaliseringsgrad) i dag, og hvordan er personvern bygget inn i disse?
4. Hvilke rutiner og holdninger har dere knyttet til etterlevelse av GDPR?
5. Innebygd personvern er et av kravene i personvernforordningen, hvordan arbeider dere for å etterleve dette kravet?
6. Opplever dere noen utfordringer ved personvern i sammenheng kunstig intelligens?
7. Digital etikk har også en avgjørende rolle for personopplysninger, hvordan behandler dere dette?
8. Hva vil du si er drivere for kunstig intelligens? Her mener vi hva som understreker motivasjonen ved kunstig intelligens som utfordrer viktigheten ved personvern.
9. Data fra kunder er åpenbart nødvendig for utvikling av kunstig intelligente systemer:
    a. Hvilke data samler dere inn fra kunder/brukere?
    b. Hvordan sikrer dere at virksomhetens interesse ikke overgår kundenes/brukerens interesse ved innhenting, lagring og bruk av personopplysninger?
10. Noe tilleggsinformasjon du tenker at er relevant for oppgaven? Eventuelt noen rapporter eller artikler som kan hjelpe?