Fordeler og ulemper med ansiktsgjenkjenningsteknologien

MAY KRISTIN AAS

VEILEDER
Camilla S. Flodin

Universitetet i Agder, 2023
Fakultet for Humaniora og pedagogikk
Institutt for religion, filosofi og historie

Forord

Det at jeg nå sitter og skriver forordet på denne masteroppgaven, betyr at et halvt år med mange emosjonelle bølgedaler, spennende lesing, frustrasjon og maktesløshet straks er over! Det er fascinerende hvor fort det har svingt fra at dette går utrolig bra, til hvordan i alle dager skal jeg komme meg videre?! Denne masteroppgaven hadde ikke vært mulig uten god hjelp og oppfølging fra min veileder Camilla S. Flodin. Jeg vil takke deg for at du har kommet med gode, konkrete og konstruktive tilbakemeldinger underveis i arbeidet. Dette kom også godt med da panikken tok overhånd i noen sekunder. Jeg vil også benytte meg av sjansen til å takke Håvard Løkke, som var til god hjelp under masterseminarene vi har hatt denne våren. Du har også kommet med gode tilbakemeldinger og tips jeg kunne bruke på veien videre. Min medstudent, Ruben Solér, skal heller ikke glemmes. Du betrygget meg underveis om at jeg var inne på noe i arbeidet mitt, og du kom også med fine tilbakemeldinger som jeg kunne jobbe videre med! Den siste jeg vil takke for hjelpen er min mor, Eli Berit Aas, som leste korrektur og har måtte tåle de forskjellige bølgedalene av følelser som har dukket opp underveis. Men alt i alt har dette vært en lærerik og spennende prosess.

May Kristin Aas

Abstract

We live in an era where digital technologies constitute a large part of our daily life. This is also true for Facial Recognition Technologies (FRT). This Master thesis is divided into five parts: Introduction, methods, and the research approach, historical background, discussion, and a conclusion. The research question I address is: "*What are the advantages and disadvantages with FRT?"*. To answer this question, I explore ethical problems, from the perspective of consequentialism, and more specifically utilitarianism. Utilitarianism is a theory that prescribes right from wrong, by focusing on what will provide happiness and well-being for the greatest number of people in society. Jeremy Bentham (1748—1832) and John Stuart Mill (1800-1873) are proponents of utilitarianism, which is a relevant theory for addressing my research question, since I investigate what can bring us happiness and well-being. It is a relevant theory when examining advantages and disadvantages to judge what will provide happiness for the majority of the people. One of the arguments for using FRT in surveillance concerns society's safety and well-being. It is a claimed to prevent crimes. Even though privacy is not usually something that is usually discussed from the point of view of utilitarianism, I have a strong focus on this in my examine. This is because from my point of view society will be a better for all when people know which rights, they have for protecting their privacy. This Master thesis has a theoretical framework, and I used academic work from several research fields (e.g. philosophy, criminology, and computer science) that addresses both the advantages and the disadvantages of using FRT.

In the discussion, I examine issues about privacy, how FRT is used in Norway, so called "chilling effects", crime vs surveillance and bias in the technology. The use of FRT implies both advantages and disadvantages. For example, FRT verification and identification in different social medias, banks etc. FRT also makes it easier for the police to look for evidence for criminal activity by looking at surveillance material, and this has had some positive effects in public places, where criminal acts have decreased. Some of the disadvantages of using FRT are its chilling effects, which means that we change our behavior and become watchful with what we are doing. The greatest disadvantages concern the problem of bias in the data that is used to train the technology. If we are going to use FRT in the future the bias need be fixed with more data that is more representative of the whole population, and not just for one group of people.

Innhold

1.0 Innledning

Dagens samfunn er preget av nyutvikling av teknologien, som skjer i en stor fart. Dette er på mange måter med på å forenkle hverdagen vår, og noe vi har blitt helt avhengige av. Spesielt etter Apple utviklet ansiktsgjenkjenningsteknologien ved at man kunne låse opp telefonen med ansiktet, har vært med på å gjøre teknologien lettere tilgjengelig for oss forbrukere. Tenk så flott at man ikke lenger må ha en egen bok med oversikt over hvilke passord som er til hvilken nettside. Man kan logge seg inn på ting bare ved å vise fram ansiktet sitt. Ansiktsgjenkjenningsteknologien er på mange måter bra, men den har også noen etiske problemer i forhold til bruken.

1.1 Inspirasjon og bakgrunn for masteren

Inspirasjonen til denne masteroppgaven kom fra min store interesse for blant annet overvåkningen, og metodene benyttet av STASI (Ministerium für Staatssicherheit) under den kalde krigen i Øst-Tyskland. Denne interessen kommer nok av at en del av familien vokste opp under dette regimet, og det vil alltid være en del av min families historie. I utgangspunktet var tanken å skrive rundt det som skjedde i Tyskland mens landet var delt, men jeg fant også en interesse av å se det i et nyere perspektiv, og hvordan teknologien har utviklet seg i forhold til hvor lett overvåkning har blitt.

Et annet punkt som var med på å vekke interessen for overvåkning kom da jeg så dokumentaren «En overvåket verden», på NRK. Det at myndigheter verden over har tatt i bruk forskjellige overvåkningssystemer er i seg selv ganske interessant. Begrunnelsen som ofte blir benyttet handler om sikkerheten til deg og meg. Man skal få ned kriminaliteten, og det skal bli lettere å kunne fange opp ulovlige aktiviteter og aktører. Kanskje også før noe katastrofalt skjer. Det er også fascinerende å se på hvordan den vestlige delen av verden kritiserer det strenge regimet og utviklingen av overvåkningen som skjer i Kina, mens de selv kjøper akkurat de samme programvarene for å overvåke sin egen befolkning. Det er ingen tvil om at Kina er en stor aktør når det kommer til overvåkning, og som det kom fram i dokumentaren; ligger Kina et tiår foran den vestlige verden når det kommer til denne teknologien.

Etter å ha sett denne dokumentaren satt jeg igjen med flere spørsmål. Hvor går egentlig grensen mellom det offentlige og det private? Med teknologien i utvikling ser vi at selv

om man snakker i telefonen ute i det offentlige, er det fortsatt regnet som en privat samtale (Rössler, 2005, s. 173) Hva kan være følgende av dette? Har vi igjen blitt naive, og tenker at «jeg har ingenting å skjule, så det gjør ikke meg noe»? Jeg syntes også det var interessant å se at etter forskjellige terrorangrep forskjellige steder i vestlige land, ble ansiktsgjenkjenningsteknologien kjøpt fra kinesiske aktører, og deretter videreutviklet, og brukes i dag over store deler av verden som et verktøy for å forutse kriminelle handlinger.

1.2 Problemstilling og andre forskerspørsmål

Hovedtematikken i denne masteroppgaven er privatliv og overvåkning gjennom bruken av ansiktsgjenkjenningsteknologi. Denne masteroppgaven vil handle om følgende problemstilling:

«Hva er fordelene og ulempene med å bruke ansiktsgjenkjenningsteknologien?»

For å kunne besvare denne problemstillingen, ønsker jeg å se på følgende forskningsspørsmål:

- Hvilken påvirkning har teknologien for vår rett til privatliv og personvern?
- Hvordan fungerer teknologien i Norge, og hva er Datatilsynets oppgaver i forhold til bruken av ansiktsgjenkjenningsteknologien?
- Hvilke etiske problematikker oppstår ved bruken av teknologien?
- På hvilken måte kan teknologien ha nedkjølende effekt på hvordan vi utfører en handling?
- Har det blitt mindre kriminalitet med økt overvåkning?
- Hvilken rolle spiller bias inn på bruken av teknologien?

1.3 Masteroppgavens oppbygging

For å kunne svare på problemstillingen i denne masteroppgaven, har jeg valgt å dele opp teksten i fem kapitler. Først vil jeg ta for meg forskningstilnærmingen, hvor jeg går igjennom framgangen for å utforske etiske problem for denne oppgaven. Deretter tar jeg for meg litteraturgjennomgangen. Her vil jeg gå igjennom mine valg av kilder og litteratur jeg har funnet relevant for oppgaven. I neste kapittel har jeg valgt å fremstille den teoretiske tilnærmingen, ved å se nærmere på historien til overvåkningen og hvordan ansiktsgjenkjenningsteknologien har utviklet seg spesielt det siste tiåret.

Deretter vil jeg ta for meg dagens overvåkningssituasjon, hvor jeg går nærmere inn på hva egentlig ansiktsgjenkjenningsteknologien er, hvordan den benyttes og hvordan den har blitt en del av vår hverdag. Videre i dette kapitlet vil jeg se på hva «big data», algoritmer og bias er. Disse tre punktene er vesentlige med tanke på å kunne forklare hvordan teknologien fungerer, og hvordan man er avhengig av en stor database for i det hele tatt kunne ha en teknologi som fungerer. I kapittel 4 vil jeg analysere og diskutere teorien jeg har benyttet meg av i denne oppgaven, og ta for meg flere underpunkter og forskningsspørsmål for å kunne gi et svar til problemstillingen. Disse underpunktene vil ta for seg vår rett til privatliv og personvern, hvordan bruken av ansiktsgjenkjenningsteknologien er i Norge, hva rollen til Datatilsynet er og hvilke betingelser som gjelder for bruken av Facebook og Snapchat. Deretter tar jeg for meg et kapitel jeg har valgt å kalle «Etisk problematikk rundt ansiktsgjenkjenningsteknologien». Her ser jeg på kjølende effekter, om kriminaliteten har blitt mindre med masseovervåkning og jeg går mer inn i bias i teknologien og hvilke utfordringer dette kan ha for bruken. Helt til slutt har jeg kapittel 5, hvor jeg vil avslutte masteroppgaven med en analyse av funnene i kapittel fire, som vil ende med en konklusjon til problemstillingen.

2.0 Forskningstilnærming

Dette kapitlet handler om de metodiske perspektivene som vil være grunnlaget for masteroppgaven. Akkurat som i filosofien, finnes det ingen konkret metode man benytter seg av tekster skrevet innenfor etikken. Det blir derfor viktig å kunne stille spørsmål om hvorfor ting er som det er, kverulere mot hvorfor ting er som det er, argumentere for det man mener og ikke minst tegne opp et bilde for å få fram poengene sine, både bokstavelig og metaforisk. I all hovedsak er denne masteren basert på et litteraturgrunnlag. Den teoretiske tilnærmingen vil dermed være vesentlig igjennom oppgaven. Derfor vil jeg også i dette kapitlet ta for meg en gjennomgang av litteraturgrunnlaget som en disposisjon denne masteroppgaven er basert på.

2.1 Framgang for å utforske etiske problem

Når man skal jobbe med en etisk preget problemstilling, innser man hvor mange etiske områder som eksisterer. Før jeg begynte med oppgaven visste jeg at etikk handlet om

handlinger som enten er rette eller gale. Da jeg begynte å se litt nærmere inn på etikken, innså jeg at det var utrolig mange veier innenfor etikken enn hva jeg var klar over. I denne masteroppgaven valgte jeg å se på materialet for oppgaven med moralfilosofi, som vil si at man vektlegger å søke etter en allsidig basiske prinsipper for moral. Moralfilosofi blir dominert av idéen om at vår moralske tankegang trenger støtte av en moralsk teori, og om de fundamentale prinsippene innenfor moralteori. Dette er grunnlaget for hvordan all vår etisk dømmekraft burde baseres på (Hansson, 2017, s. 3). Innenfor moralfilosofi finnes det et underområde som kalles for normativ etikk, som handler om hvilke regler og prinsipper vi bør handle etter. Den normative etikken deles igjen inn i flere områder, men jeg har valgt å fokusere på konsekvensetikken og særlig utilitarismen.

2.1.1 Konsekvensetikk – Utilitarisme

Utilitarismen er en teori innenfor konsekvensetikken. Ifølge Frode Nyreng finnes det tre grunnleggende kjennetegn ved konsekvensetikken. Det første går på handlinger. Her vil man ta utgangspunkt i handlinger, som har et godt utfall for flertallet. Det andre punktet er hvordan en god handling frembringer gode konsekvenser. Det tredje, som binder de to andre punktene er verdilære. Her ser man på hva som gjør en konsekvens bra eller dårlig. Et annet punkt den også tar for seg er «på hvilken måte man skal begrense *hvem* konsekvensene skal beregnes *for*» (Nyreng, 1999, s. 37). Utilitarisme går ut på hvordan de bra og de dårlige alternativene av en handling kan bli målt opp mot det å handle riktig. Det handler om å velge det alternativet som vil gi en maksimal grad av det som er bra (Hansson, 2017, s. 3). Med andre ord blir fordeler og ulemper veid opp mot hverandre, for å finne det beste alternativet som er moralsk riktig. I dette feltet ser man på det moralske gode med hensyn i forhold til nytte (Hansson, 2017, s. 7). I denne masteroppgaven har jeg sett på hvilke bra og dårlige konsekvenser AGT kan ha. Her kommer mange poenger innenfor utilitarismen fram i forhold til at AGT agerer på mange måter for flertallet og er også på mange måter bra for de fleste av befolkningen. Det er lettere for den enkelte personen å logge seg inn på mobilen, banken også videre. Man slipper å huske på alle versjoner av passord til alle de forskjellige stedene. Det er gøy å leke med for befolkningen, om hva som kan gjøres med ansiktet også videre i forskjellige filter på sosiale medier. Det er også gøy å kunne tagge venner i forskjellige

bilder på forskjellige plattformer. Det er også en stor fordel at man kan bruke det til å forhindre kriminalitet, og ikke minst finne igjen savnede personer.

Utilitarismen ble utviklet av Jeremy Bentham (1748—1832), som var en engelsk filosof og jurist. Han argumenterte for at lyst og behag er det eneste som er godt i seg selv, og at man skal derfor velge handlinger som gir mer lyst enn smerte. Han står også bak den klassiske retningen, hedonisme, innenfor utilitarismen. Hedonisme går ut på hvordan menneskelig lyst og behag er det eneste som er godt for seg selv (Carson & Kosberg, 2022, s. 35). Denne kan igjen deles inn i psykologisk og etisk hedonisme, hvor psykologisk går ut på det som får oss til å utføre en handling, som gjør at vi unngår smerte. Mens etisk går ut på hvordan vi bør handle for å maksimere lyst og minimere smerte. Ifølge Nyreng (1999) handler verdilæren om at vi mennesker har potensiale til å ta innover oss forskjellige konsekvenser, og dermed handle riktig. Nyreng skriver videre at Bentham mente også at denne psykologien hadde påvirkning på politiske og juridiske områder. Man ser på hva som er det beste for folket, ved at det lages lover og regler man må følge. For de som ikke følger disse, er det tilknyttet en stor mengde straff. Dette for at man skal velge det som er lønnsomt, og som selv gir deg glede. Allerede her blir straffen benyttet som forebygging til kriminelle handlinger, og ikke i forhold til å ta hevn (Nyreng, 1999, s. 40). Denne teorien er sammenlignbar i forhold til overvåkningen av befolkningen. Ser man for eksempel på Kina, benytter de akkurat dette for at folk ikke skal velge kriminalitet ovenfor det å være lovlydig. Dette er også noe vi ser i vestlige liberale land. Man jobber for at det ikke skal lønne seg å gjøre en kriminell handling og at det vil bli ubehagelig for den som eventuelt blir tatt for en kriminell handling.

John Stuart Mill (1800—1873), som var en engelsk filosof og økonom, er en annen sentral person i videreutviklingen av utilitarismen. Han utviklet det vi kan kalle for nytteprinsippet. Dette går ut på at han vektlegger formålet/intensjonen med en handling til den som er tilsiktet handlingen, mer enn de faktiske konsekvensene som kan oppstå av en handling. Man skal også velge den handlingen som gir lykke til flest mulige mennesker (Carson & Kosberg, 2022, s. 39). De høyeste målene i utilitarismen er lykke, nytte, lyst og glede. Selv om mange kan tenke at nytte er en motsetning til glede, er det ikke det i denne sammenhengen (Carson & Kosberg, 2022, s. 39). Selve målet er lykke, siden dette er noe folk etterstreber. Siden lykke er en mental tilstand, kan det ikke

sammenlignes som velferd. Man må også ha i bakhodet at selv om alle ytre forutsetninger ligger til rette, betyr det ikke at man er lykkelig. I konsekvensetikken ser man at man vurderer handlinger ut fra konsekvensene de fører til (Carson & Kosberg, 2022, s. 42—43).

Ifølge Carson og Kosberg (2022) kan man dele utilitarismen inn i to deler, hvor den ene delen er regelutilitarismen og den andre handlingsutilitarismen. Regelutilitarismen blir regnet som å være indirekte. Her vurderer man konsekvensene ut ifra reglene som ligger til grunn for handlingen. Man skal følge regler som fører til mest mulig nytte og lykke moralsk sett. Handlingsutilitarisme er mer direkte, og går på de direkte konsekvensene av den enkelte og aktuelle handlingen. Man skal her vurdere hver enkelt handling og vurdere mulige framtidige konsekvenser av å utføre den enkelte handlingen (Carson & Kosberg, 2022, s. 45). Dette har fått mye kritikk i forhold til at det det tar for lang tid å skulle vurdere og tenke over konsekvensene ved hver eneste handling man skal foreta seg. Carson og Kosberg referer til Richard M. Hare (1919—2002), som svarer på denne kritikken ved å kunne nivådele den moralske tekningen. Dette blir kalt for totrinnsutilitarisme, en syntese mellom handlings- og regelutilitarisme. Nivå 1 går på generelle regler, normer og moralske intuisjoner. Det er dette som skjer når vi handler ut ifra vane, og kan begrunne våre handlinger på gitte regler vi er vant til å følge. Nivå 2 er mer krevende for aktøren. Her skal avgjørelser tas uavhengig av regler og normer, og man må vurdere hvert enkelt tilfelle. Dette skal igjen føre til at man kan komme fram til den beste løsningen upartisk. Med andre ord blander han både regel- og handelsutilitarismen ved at regler går på hverdagslige og rutinemessige avgjørelser, mens ved handling må man ta større og vanskelige avgjørelser som man må tenke seg om før man tar et valg (Carson & Kosberg, 2022, s.47).

På mange måter kan man si at utilitarismen er en tilpasningsdyktig teori. Den er derfor fortsatt aktuell i dagens samfunn. Det er vanskelig å avvise teorien om nytteprinsippet, siden denne har en stor appell i samfunnet den dag i dag. Vi streber fortsatt etter å få finne lykke og vil helt unngå smerte. På mange måter kan man si at utilitarismen er en prosedural etikk, som fokuserer på prosedyrene som må følges for at vi skal handle på best mulig måte. Vi må på mange måter tenke selv, og stå til ansvar for våre egne

handlinger. Utilitarismen er også en bra motvekt i et samfunn som i stor grad blir detaljstyrt av regler, som vi ser iblant annet Kina (Carson & Kosberg, 2022, s.52).

Denne masteroppgaven vil vise at selv om AGT har store fordeler for majoriteten av befolkningen, er det fortsatt en stor ulempe for minoriteter. Myndighetene spiller på frykt som et argument for å bedrive full overvåkning av befolkningen. I det store og hele bildet er det ikke tvil om at vi vil jo være trygge, og vi ønsker å være beskyttet. Vi er dermed villige til å gi fra oss privilegiet til å ha full frihet til å gjøre som vi vil. Når man blir overvåket hele tiden, kan dette medføre en «chilling effect»/ «kjølende effekt», som vil si at man begrenser seg på hvordan man skal oppføre seg i forskjellige settinger. Til daglig blir hver enkeltes privatliv utfordret av overvåkning og AGT. Dette med tanke på steder ute i offentligheten de ikke nødvendigvis forventer at de skal bli overvåket som man blir ved for eksempel flyplasser. Konsekvensene for full overvåkning kan være ganske stor for befolkningen. Det at man argumenterer for «om man ikke har noe skjule, har du ikke noe å frykte» blir på mange måter feil. I forhold til rettigheten til privatliv, handler det om at man selv skal kunne bestemme hva slags informasjon om en selv som skal ut i forskjellige settinger. Selv om man ikke har noe skjule, er det fortsatt enkelte ting man ikke vil at andre skal vite om. Det blir derfor et argument som på mange måter sier at vi skal frasi oss rettigheten til å ha et privatliv. Etter avsløringene til Edward Snowden i 2013, kom han med et godt utsagn: «Your rights matters because you never know when you may need them» (Lyon 2015, s. 113).

Dette utsagnet er veldig godt beskrivende i forhold til når man ser på hvilke konsekvenser hva som er bra for den enkelte, eller for fellesskapet. På mange måter kan man si at det går utover folks rettigheter ved at alle er ikke lenger lik for loven. Dette med tanke på store bias til enkelte minoritetsgrupper, raser og etnisitet. Dette fører igjen til at ulempene for denne grupperingen av befolkningen blir enda større. Man kan se at diskrimineringen har blitt større, med hjelp av AGT. Man kan også få en falsk-positiv match som fører til at man kan bli kategorisert som en kriminell, selv om man ikke har gjort noe.

Selv om rettigheter ikke er noe som står sentralt i en utilitaristisk tenkemåte (Carson & Kosberg, 2022, s. 46), vil dette fortsatt ha et sterkt fokus i oppgaven. Dette med tanke på

viktigheten for befolkningens vinning av å ha rett til et privatliv og et godt personvern. Samfunnet generelt vil kunne vinne på at man er klar over rettighetene man har i forhold til bruk av AGT og privatliv. Det at man selv kan bestemme hva slags informasjon andre skal vite om deg gir en frihetsfølelse, som igjen vil føre til bedre velferd for både samfunnet og som enkeltperson. Dette er et aspekt som er viktig i den vestlige liberale delen av verden. I kontrast kan man for eksempel se på Kina, som operer med at staten har kontroll over hele befolkningen. På denne måten har de full kontroll på at befolkningen skal oppføre seg best mulig, siden de vil ha en vinning på dette. Oppfører de seg dårlig, vil dette bli statuert som et dårlig eksempel ved at man vanærer den som har brutt loven (Bu, 2021).

2.2 Disposisjon og litteraturgrunnlag

Da jeg startet med denne masteroppgaven, var planen i hovedsak å skrive om hvordan overvåkning påvirker privatlivet vårt. Etter jeg gjorde flere søk innenfor overvåkning og privatliv, så jeg ganske raskt at forskningsfeltet der er stort. Jeg måtte derfor gjøre noen valg for å kunne snevre inn mitt forskningsfelt. Selv om jeg har snevret det inn mye, ser jeg fortsatt at det er uendelig med forskning akkurat på feltet om ansiktsgjenkjenningsteknologien. Av forskningsøkonomiske grunner har jeg måtte velge ut enkelte forskningsfelt, som jeg har brukt som analysegrunnlag i denne oppgaven.

Denne oppgaven er en master som har et teoretisk rammeverk innenfor etikken som grunnlag for å kunne besvare problemstillingen. I all hovedsak har jeg basert litteraturgrunnlaget på tekster min veileder har anbefalt, og igjennom søk i databaser som: Springer.com, elsivier.com, scholar.google.com, datatilsynet.no, oria.no og amazon.com. Jeg har også vært aktivt på utkikk etter litteratur når jeg har vært på reise til blant annet London.

I denne masteroppgaven vil jeg se på fordelene og ulempene ved å benytte ansiktsgjenkjenningsteknologien. Jeg har derfor valgt å dele opp oppgaven inn i ulike punkter. Først tar jeg for meg en teoretisk tilnærming, hvor jeg tar for meg historien til overvåkning og teknologien rundt denne. Videre tar jeg for meg dagens overvåkningssituasjon, og har med hva ansiktsgjenkjenningsteknologien, algoritmer, bias og «big data» som underpunkter.

I kapittel fire, som jeg har valgt å kalle «analyse og diskusjon», har jeg fordelt teksten inn i forskjellige punkter som er vesentlige å se på i forhold til å kunne sammenligne fordeler og ulemper med bruken av ansiktsgjenkjenningsteknologien. Disse har jeg delt inn som: privatliv/personvern, ansiktsgjenkjenningsteknologien og personvern i Norge, etisk problematikk rund ansiktsgjenkjenningsteknologien. Her har jeg flere underpunkter som går på kjølende effekter, kriminalitet vs. overvåkning og bias i teknologien.

2.2.1 Historie

Selve historiekapitlet har jeg delt inn i generelt om historien om overvåkning. Deretter tar jeg for meg flere tiår med utvikling, før jeg tar for meg korte trekk om historien til ansiktsgjenkjenningsteknologien.

I kapitlet «3.1.1 Tiår med utvikling», har jeg benyttet meg av litteraturen til David Lyon, og boka *Surveillance after Snowden* (2015). David Lyon er nå en pensjonert professor og leder for Surveillance Studies Centre, ved Queens University i Kingston i Ontario. Han har forsket mye på overvåkning, og har flere bøker om emnet. Han tar for seg på en god og strukturert måte hvordan vi lar oss overvåke, og hva som er framtiden når det kommer til overvåkningsteknologien. Jeg har benyttet to av hans verk i denne mastergraden, som jeg vil komme tilbake til. I forhold til tiåret med utviklingen, fremstiller han historien på en oversiktlig måte, som er relevant for min oppgave og for å kunne forstå bakgrunnen for hvordan overvåkningssituasjonen har blitt som den har blitt.

I kapitlet «3.1.2 Historien til ansiktsgjenkjenningsteknologien i korte trekk», har jeg benyttet meg artikkelen «A brief history of Facial Recognition», som er publisert av NEC New Zealand, som er et internasjonalt teknologikonsern (2022). Denne tok jeg med, siden jeg syntes den ga et oversiktlig overblikk på hva som har skjedd i forhold til teknologien rundt ansiktsgjenkjenning. Den tar for seg oppstarten på 1960-tallet og fram til dagens bruk. Jeg har også sammenlignet denne informasjonen med andre kilder, som viser at det de skriver er forenelig med andre kilder også. Jeg har også benyttet meg her av artikkelen «The Bias in the Machine: Facial Recognition Technology and Racial

Disparties» (2021), skrevet av Sidney Perkowitz (vitenskapsmann, vitenskapsforfatter og professor emeritus i fysikk ved Emory University). Han tar for seg hvordan forskerne utviklet teknologien til å kunne gjenkjenne ansikter i et bilde ved å benytte en binærkode.

2.2.2 Dagens overvåkningssituasjon

I kapitlet «3.2.1 Ansiktsgjenkjenningsteknologien» er hovedgrunnlaget mitt å se på hva egentlig AGT er. Her har jeg nok en gang benyttet med av David Lyon som kilde. I boken *The Culture of Surveillance* (2018) tar han for seg hvordan AGT fungerer, og hvordan vi benytter oss av denne teknologien i det daglige. Han tar for seg forskjellige utfordringer enkelte mennesker kan møte med bruken av AGT, og hvordan denne er med på å diskriminere enkelte grupper. Han tar også for seg sentrale deler som har skjedd med utviklingen de senere årene. Mye av det han skriver om blir også støttet opp av Kate Crawford (forsker hos Microsoft reasearch) sin bok *Atlas of AI* (2021). Crawford har en 20 års karriere innenfor å jobbe med å forstå kunstig intelligens, og har dermed drevet med mye forskning innenfor feltet med store datasett, maskinlæring og AI i kontekst med historien, politikk, arbeidskraft og miljøet. I boken *Atlas of AI* (2021), tar hun for seg flere etiske grunnlag i forhold til hvordan vi skal forholde oss til kunstig intelligens og lignende. Det som var interessant i boken hennes var hvordan AGT har blitt utviklet fra såkalte «mugshots» til det produktet de fleste av verdens befolkning benytter seg av i dag. Jeg har også benyttet boken hennes flere steder som en relevant kilde i andre underpunkter. Videre har jeg benyttet meg av Tore Tennøe, Adele Flakke Johannessen og Marianne Barland sin artikkel «Ansiktsgjenkjenning og personvern» (2020). Disse tre jobber i Teknologirådet, hvor blant annet jobben består i å gi råd til Stortinget og regjeringen om ny teknologi. I artikkelen tar de opp blant annet hvordan AGT blir brukt, og hvordan den påvirker livene våre i hverdagen. De skriver også om argumentasjonen for hvorfor man bør fortsette med å utvikle AGT. Jeg har også benyttet meg av artikkelen deres som et supplement i kapitlet om personvern. Scott Robins (doktorgrad i etikken ved AI, ved Technical University of Delft) støtter opp mye av det Tennøe et. al. tar opp i sin artikkel, med å forklare bruksområdene til AGT. Begge kildene tar for seg hvordan teknologien kan deles inn i tre hovedområder: identifisere, verifisere og kategorisere. Jeg har også benyttet med av artikkelen hans «Facial Recognition for Counter-Terrorism: Neither a Ban Nor a Free-for-all» (2021) flere steder i oppgaven, da han kommer med gode argumenter for hvorfor man ikke bør legge inn et totalforbud av bruken til AGT.

Han har også forsket mye på området med sin doktoravhandling om AI, terrorisme og etikken rundt dette. Den siste kilden jeg har benyttet meg av i dette underkapitlet er Denise Almeida, Konstantin Shmarko og Elizabeth Lomas sin artikkel «The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulator frameworks» (2021). Disse tre forskerne jobber henholdsvis i forskjellige departement i London innenfor informasjonsstudier og økonomi. De tar blant annet for seg hvordan Kina er et ledende land i forhold til utvikling av teknologi, og hvordan de benytter seg av AGT med å kategorisere befolkningen inn i forskjellige rangeringer. Jeg syntes her at det var interessant å kunne sammenligne den vestlige bruken, og hvordan det blir brukt i østlige land, som for eksempel Kina. Jeg har også benyttet denne teksten som kilde flere steder i oppgaven.

I kapitlet «3.2.2 «Big data», algoritmer og bias», er poenget å få fram hvordan systemet er satt sammen og hvordan den fungerer i forhold til store datainnsamlinger for å kunne benytte programvaren, og hvordan dette henger sammen med algoritmer og bias. Her har jeg fortsette med å benytte meg av Lyon (2015) og Crawford (2021), som begge forklarer hvordan «big data» og algoritmene henger sammen. De tar også for seg punkter i forhold til hva man må tenke over ved bias og hvordan disse kan oppstå. Jeg har også benyttet meg av boken til Mark Coeckelbergh (professor i filosofi av media og teknologi, ved Department of Philosophy i Wien) *AI Ethics* (2020). Coeckelbergh har forsket mye på AI og etikken rundt bruken av AI. Han har også mange vesentlige poenger i sin bok, som jeg syntes var hensiktsmessige å ha med. Han tar blant annet opp hvordan maskinens læringsprosess er, som også støtter opp det det Lyon og Crawford skriver. I forhold til bias, har han et eget kapitel dedikert til hva dette er og hvordan det kan oppstå. Spesielt bekymringsfullt er det om vi lar systemene fungere uten at funnene de finner blir bare tatt for gitt at det stemmer. Dette går utover forskjellige grupper med mennesker, noe som igjen er med på å føre til skille i samfunnet og mer diskriminering. Helt til slutt i dette kapitlet har jeg benyttet meg av filmen *Coded bias* (2020) (regi av Shalini Kantayya), hvor man følger blant annet Joy Buolamwini (dataforsker ved MiT) sin oppdagelse på at det var store bias i systemene for spesielt mørkhudede kvinner og AGT. Hun har forsket en del på området, og er en aktiv motstander av bruken for AGT.

Hun har blant annet vært i flere høringer med politikere og domstoler for å få til et forbud mot bruken av AGT.

2.2.3 Retten til privatliv

I kapittel «4.1 Retten til privatliv», har jeg nok en gang tatt i bruk Lyon (2018) som en relevant kilde. Han skriver om konseptet rundt argumentene rundt masseovervåkningen henger sammen med at den er der for «vår egen trygghet». Det å spille på borgernes frykt for kriminelle handlinger kan skje, er et politisk virkemiddel som blir benyttet i hele verden. Jeg har også benyttet meg av boken til Beate Rössler (professor i etikk og filosofi), *The value of privacy* (2005). I denne boken tar hun for seg mange viktige aspekter rundt dette med hva som defineres som privat, selv ute i den offentlige sfære og hvilke rettigheter vi har i forhold til etikken rundt overvåkning.

Før man kan gå inn på hvordan AGT påvirker privatlivene våre, syntes jeg det var vesentlig å ta et kapittel om hva som defineres som privatliv. I underkapitlet «4.1.1 Hva defineres som privatliv?», har jeg benyttet meg av artikkelen «Privacy» (2018), skrevet av Judith DeCew (professor i filosofi). Hun tar for seg mange viktige elementer i forhold til utviklingen av privatlivet. Hun gir eksempler på hvordan det var tilbake på 1960-tallet, og hvordan det har utviklet seg til lovverk ved blant annet General Data Protection Regulation (GDPR), og European convention of Human rights, artikkel 8. Dette er viktige punkter i forhold til dagens diskusjon rundt hvor grensene til privatlivet går, og hva som kan regnes med som offentlighetens beste i forhold til hva slags informasjon som skal ut som allmenninformasjon og ikke. Videre har jeg benyttet meg av artikkelen til Stefan Strauß (forsker innenfor sosialfag og data, spesialfelt innenfor sosio-tekniske systemer, privatliv, sikkerhet og overvåkning, digital identitet og privatlivets konsekvensanalyse), «Privacy Analysis – Privacy Impact Assesment» (2017). Han forklarer på en god måte hva privatliv defineres som, og rettigheten vi mennesker har til å bestemme over hvilken informasjon om oss som kan deles og ikke. Han beskriver også veldig god hvordan grensene for hva som regnes som privat og offentlig på en oversiktlig måte i forhold til hvordan overvåkning har blitt en normalisert ting i vår hverdag. Jeg har også i dette underkapitlet benyttet meg av Lyon (2015), som tar for seg hvordan overvåkningen fungere i forhold til privatlivet i et demokratisk liberalt land, som de vestlige landene regnes som. Han tar også for seg hvordan myndighetene kan invadere privatlivet, ved å

overvåke oss uten at vi selv er klar over det. Dette kom også tydelig fram i 2013 med Edward Snowdens avsløringer om hvordan staten overvåket befolkningen i USA.
Det neste underkapitlet har jeg valgt å kalle «4.1.2 Privatliv og personvern». Her definerer jeg hva som regnes som personvern, og hvordan dette henger sammen med vårt privatliv. Her har jeg benyttet med av datatilsynets hjemmeside som kilde, hvor de tar opp hvordan loven GDPR fungerer, og hvordan personvernet har blitt noe man må ta hensyn til i forhold til masseovervåkning. Man må blant annet ha samtykke fra befolkningen for å kunne overvåke dem, og det er det ikke alle steder med overvåkning som overholder. De går også inn på hvordan vår informasjon skal behandles i forskjellige områder som innhenter informasjon, hvordan den skal lagres og hvordan den skal brukes.

I underkapitlet «4.1.3 Ansiktsgjenkjenningsteknologien og privatliv», tar jeg for meg utfordringene rundt å benytte seg av AGT som overvåkningsteknologi. Jeg har funnet ut at det er forskjellige faktorer som er med på å definere hva som regnes som privatliv og hva som er informasjon samfunnet har rett til å få vite om. Det er også veldig fascinerende hvor forskjellig bruken er i forskjellige land. Jeg har i dette underkapitlet benyttet meg av artikkelen «The global governance on automated facial recognition (AFR); ethical and legal opportunites and privacy challenges» (2021) av Qingxiu Bu (senior foreleser i korporativ lov og handelsrett ved University of Sussex). Han tar for seg retten til privatliv, og hvordan det kan bli problematisk når systemene kan gjenkjenne folk i samtid. Han tar videre for seg hvordan GDPR fungerer, men at den ikke er helt optimal enda ved at det kan være noen unntak i loven som gjør at det blir lettere å kunne misbruke teknologien. Han sammenligner også hvordan privatlivet blir sett på i forhold til USA, Kina og Europa. Også i dette underkapitlet har jeg benyttet meg av Almeida et. al (2021), som tar opp hvordan lover blir praktisert forskjellig i USA. Noe som er interessant å se på, med tanke på hvor store forskjeller som finnes i det samme landet. Hvordan skal man få til et forenelig lovverk til hele verden, når det praktiseres såpass forskjellig i bare et land? Den siste kilden jeg benyttet meg av i dette underkapitlet er Andreas Dripke (Global Chairman i Diplomatic Council) og Markus Miksch (trener og foredragsholder innenfor feltet lederskap, retorikk og økonomi) sin bok *STASI 2.0: Wie wir durch den staatlich-industriellen Digitalkomplex zu gläsernen* (2021). Disse tar for seg hvordan vår informasjon selges til tredjeparter, hvordan

overvåkningen har blitt normalisert og hvordan vi har blitt naive i forhold til hva slags informasjon som deles videre ved at det ikke er så farlig hva en tredjepart vet om oss. I det siste underkapitlet «4.1.4 Betingelser om personvern på sosiale medier» har jeg tatt utgangspunkt i hva som egentlig står i retningslinjene til henholdsvis Facebook og Snapchat, og hva disse retningslinjene sier om bruken av våre bilder og lignende på sosiale medier. Også i dette underkapitlet har jeg benyttet meg av Dripke og Miksch (2021), som tar for seg hva Facebook gjør med bilder vi har lastet opp, og hva vi egentlig godtar uten å lese betingelsene av. Dette har vært veldig interessant lesing, da det er mye informasjon der som folk flest ikke er kjent med at de har samtykket til da de godtok betingelsene uten å egentlig lese disse. De er på mange måter lagt opp til at man ikke gidder å lese dem, for å kunne benytte seg av programvaren, ved at de er lange og mye teknisk språk som man ikke gidder å sette seg inn i hva egentlig betyr.

2.2.4 Ansiktsgjenkjenningsteknologien og personvern i Norge

I store deler av underkapitlet «4.2.1 Bruken av ansiktsgjenkjenningsteknologien i Norge» har jeg benyttet meg av podkasten «Jusspodden» (2022), ledet av Marianne Reinertsen. I episoden om ansiktsgjenkjenningsteknologien, hadde hun besøk av Mona Naomi Lintvedt (stipendiat ved juridiske fakultet og tech-ekspert) som tok for seg en diskusjon rundt AGT og hvordan den benyttes i Norge. Lintvedt har forsket mye på dette feltet, og det var veldig interessant å høre på de forskjellige temaene rundt AGT som de tok opp. De mener blant annet at AGT er trygt å kunne benytte seg av i Norge, da det er mange lover og regelverk som beskytter oss og privatlivet vårt, og som igjen fører til hindringer ved forskjellige bruksområder av denne type overvåkning. De nevner også blant annet hvordan politiet har benyttet seg av programvaren Clearview AI i USA, og hvordan dette er problematisk i forhold til at de bildene som er hentet inn der aldri har blitt gitt noen form for samtykke om at de kan brukes til nettopp AGT. Dette er også noe Marcus Smith (professor i lov ved Charles Sturt University) og Seumas Miller (forsker ved Charles Sturt University) tar opp som problematisk i sin artikkel «The ethical application of biometric facial recognition technology» (2021). Begge disse har mye forskning innenfor feltet om teknologi og etikk. I teksten sin tar de for seg hvordan myndighetene har fått større makt til å innhente dataopplysninger om borgerne, spesielt etter flere terrorangrep. De sammenligner dette med hvordan det gjøres i Kina, Australia og USA. De ser også på etiske problemer som oppstår for privatlivet når det kommer til

sikkerheten for befolkningen og hvordan privatlivet individuelt og for hele samfunnet påvirker hverandre.

Det siste underkapitlet heter «4.2.2 Datatilsynets rolle». Dette tenkte jeg var hensiktsmessig å ha med, og spesielt interessant i forhold til å se på hva egentlig Datatilsynet gjør for å beskytte vårt privatliv. Det er få som tenker over denne organisasjonen, og derfor nok en grunn for å ta det med som et utgangspunkt på hvordan overvåkningen foregår i Norge. Her har jeg benyttet meg av Personvernkommisjonens rapport «Ditt personvern – vårt felles ansvar» fra 2022 som mye av grunnlaget til dette underkapitlet. Dette fordi den tar for seg mye om hva som har blitt gjort tidligere i Datatilsynet, hvilken rolle de spiller, hvordan de arbeider og hvordan mandatet er satt opp. Hensikten til Datatilsynet er å føre kontroll og påse at lover og regelverk blir fulgt av forskjellige organisasjoner og bedrifter som innhenter personlig informasjon om enkeltindivider. Dette bekreftes også på Datatilsynets sine nettsider. Jeg har også benyttet meg av «Jusspodden» som en kilde her, da de også tar opp dette med å følge opp hva slags overvåknings som er lov og ikke.

2.2.5 Etisk problematikk rundt ansiktsgjenkjenningsteknologien

Det første underkapitlet her har jeg valgt å kalle for «4.3.1 Kjølende effekter». Her tar jeg opp hvordan overvåkningen er med på å endre folks oppførsel i forhold til når de vet de blir overvåket og ikke. Nok en gang har jeg benyttet meg av Lyon (2018) som en reell kilde. Har tar opp problematikken ved bruken av AGT ved for eksempel demonstrasjoner, som i utgangspunktet er lovlig. Ved bruken av AGT, kan demonstrantene bli behandlet som kriminelle ved at de var med i demonstrasjonen. I nyhetsartikkelen «Even mask-wearers can be ID´d, China facial recognition firm says» (2020) av Martin Pollard (korrespondent i Kina for Reuters) kommer det fram ny utvikling av teknologien, som gjør det vanskeligere for vanlige folk å kunne si imot myndighetene ved å demonstrere med for eksempel en maske. Eirik Newth (astrofysiker og formidler av vitenskap og teknologi), tar opp i sin bok *Overvåkningssamfunnet* (2014) om en kjølende effekt hos blant annet journalister, ved at de sensurerer seg selv mer. Dette skjedde spesielt etter avsløringene til Snowden. En av grunnene for selvsensuren handler om at journalister ikke lenger kan garantere at samtalen mellom dem og kilden forblir mellom de to. En annen kilde jeg benyttet meg av, som tok opp dette temaet var

artikkelen «Has facial recognition technology been misused? A public perception model of facial recognition scenarios» (2021) skrevet av Xiaojun Lai (foreleser ved School of Chemical and Process Engineering ved Leeds) og Pei-Luen Patrick Rau (professor ved Department of Industrial Engineering ved Tsinghua University). Disse tar for seg hvor lett det kan være og utnyttet bilde av noens ansikt, for så å putte de inn i videoer som for eksempel deep-fake, bare for å ødelegge for vedkommende. Med AGT har dette blitt lettere å kunne utføre, spesielt med tanke på alle mulighetene som ligger i forskjellige applikasjoner.

Neste underkapittel har jeg valgt å kalle «4.3.2 Kriminalitet vs. Overvåkning». I dette underkapitlet ser jeg på om det har blitt mindre kriminalitet med masseovervåkning, eller ikke. Da et av argumentene for hvorfor vi har overvåkning går på å forhindre kriminalitet, ser jeg på dette som et vesentlig punkt å ha med i diskusjonen på problemstillingen. Den første kilden jeg har benyttet med av her er artikkelen «CCTV surveillance for crime prevention. A 40- year systematic review with meta-analysis» (2019) skrevet av Eric L. Piza (professor i kriminologi og strafferett ved College of Social Science and Humanities ved Northeastern University), Brandon C. Welsh (professor i kriminologi og strafferett ved College of Social Science and Humanities ved Northeastern University), David P. Farrington (kriminolog, rettsmedisinsk psykolog og emeritus professor i psykologisk kriminologi ved University of Cambridge) og Amanda L. Thomas (PhD kandidat i Criminal Justice ved John Jay College). De tar for seg flere områder hvor man ser at kriminaliteten har gått ned, og andre områder hvor det ikke er noen forskjell. Ved parkeringsplasser har det for eksempel blitt gjort grep for at det skal være bedre overvåket, bedre belysning og ved flere steder er det også en parkeringsvakt som patruljerer på området. Dette har hatt en forebyggende effekt. Som et supplement til deres tekst, har jeg også benyttet Mikael Priks sin artikkel «The effects of surveillance cameras on crime: Evidence from the Stockholm subway» (2015). Denne tar opp blant annet at kriminaliteten rundt narkotika ikke har gått ned, og at dette har en sammenheng med at brukerne er som regel høye da de kjøper narkotiske stoffer. Dette er en tekst Piza et. al. (2019) også referer til i sin artikkel. Ellers har jeg benyttet meg av teksten «Bak den norske overvåkningsdebatten» skrevet av Guro Flinterud (seniorforsker ved politihøgskolen i Oslo), Jon Strype (førsteamanuensis ved Oslo Nye Høyskole med emnet Pedagogisk psykologi) og Heidi Mork Lomell (professor for

institutt for kriminologi og rettssosiologi ved Universitet i Oslo og Politihøgskolen i Oslo). De tar for seg hvordan debatten om overvåkning i Norge er veldig polarisert, og at det er et stort fokus på det ene eller det andre synspunktet som er rett. De mener også at grensene for hva et privatliv er og hva som defineres som offentlig må defineres på nytt, da de senere årene grensene har flyttet på seg betraktelig. De mener også at AGT er en positiv teknologi politiet kan benytte seg av for å kunne felle de større kriminelle aktørene. Jeg har også her benyttet meg av teksten til Robins (2021) i forhold til det han skriver om å bruke algoritmer til å kunne forutse handlingene til folk er truende eller ikke. Newth (2014) tar også viktige punkter i forhold til terrorisme, ved at disse er uforutsigbare, og det blir dermed vanskelig å kunne forutse slike handlinger.

Det siste underkapitlet har jeg valgt å kalle «4.3.3 Bias i teknologien». Her har jeg benyttet meg av teksten til Robins (2021) som kilde, da han kom med mange gode statistikker rundt treffsikkerheten til AGT. Jeg benyttet meg videre av Lintvedt sine påstander om ulike bias hun tok opp i podkasten. Hun argumenterer blant annet for at selv om teknologien er testet ut på en stor gruppe mennesker i Asia, er dette en homogen gruppe, og vil dermed ikke fungere optimalt i andre land med mindre homogene grupper med mennesker. Jeg syntes det var interessant å ta med Stewart Baker (advokat) sine tanker rundt bias i sin artikkel «The Flawed Claims About Bias in Facial Recognition» (2022). Han mener at det blir feil å kalle teknologien for rasistisk, når det i bunn og grunn handler om lyssettingen på bildene må bli bedre. Han mener videre at man må bruke store nok datasett til å trene opp maskinene til å kjenne igjen folk med mørkere hudtoner. Den neste kilden jeg har benyttet meg av var Isabella Grabskis (doktorgrad student i Biostatistikk, ved Harvard University) artikkel «Fairness in Machine Learning» (2020). Hun tar opp forskjellige punkter på hvordan datasettene har blitt preget av valgene som ble tatt da man skulle lære opp maskinene. Grunnlaget vil uansett være urettferdig da en mindre gruppe alltid blir underrepresentert i datasettene. Hun mener at det viktigste steget man kan gjøre for å forhindre bias, er i første omgang å definere hva som er rettferdig, og hva som legger grunnlaget for at noe er rettferdig. Perkowitz (2021) syntes jeg var relevant å ta med, da han kommer med flere eksempler på hvor AGT har feildømt flere mørkhudede menn ved at det ble en falsk positiv match i algoritmene. Dette gjorde at mennene ble plassert på steder de ikke hadde vært, og ble deretter beskylt for kriminelle handlinger de ikke hadde begått. Han

tar videre opp forskjellige utfordringer med AGT med blant annet at treffsikkerheten ikke er god nok i forhold til flere mindre grupper. Et annet problem han tar opp er hvordan teknologien skal brukes på en god og korrekt måte i systemene som allerede er i bruk hos blant annet politi. Videre tar han opp hvordan datasettene er basert på et demografisk bias, som også har innvirkning på hvordan bias i datasettene finner resultater. Den siste kilden jeg har benyttet meg av i dette underkapitlet er Coeckelbergh (2020). Han tar opp flere eksempler i forhold til bruken av AGT til å vurdere jobbsøknader. Der viste det seg at kvinner ikke ble innkalt til intervjuer på større leder stillinger, da det lå en bias inne i systemet med å søke etter menn. Han tar videre opp problematikken for de som faller utenfor «godkjente» grupper i forhold til det å kunne få lån, jobb og nektet adgang på forskjellige steder. Dette kan føre til fatale følger for de det måtte gjelde. Han ser det også som problematisk med at en homogen gruppe jobber med datasettene, da de mindre underrepresenterte gruppene kan fort bli oversett.

3.0 Teoretisk tilnærming

I dette kapitlet vil jeg ta for meg teorigrunnlaget for å besvare problemstillingen. Dette har jeg valgt å gjøre ved å ha en underkategori med historien om overvåkning og hvordan ansiktsgjenkjenningsteknologien har endret seg i korte trekk siden 1960-tallet, og fram til dagens måter å benytte denne teknologien. Deretter vil jeg ta for meg dagens overvåkningssituasjon, hvor jeg tar for meg teorien rundt hva ansiktsgjenkjenningsteknologien, «big data», algoritmer og bias er. Dette spesielt med tanke på hvordan teknologien har utviklet seg etter terrorangrepet i USA tilbake i 2001.

3.1 Historie

Overvåkning av befolkningen er på ingen måter et nytt fenomen. Det har bare de senere årene blitt mer effektivisert ettersom teknologien har forandret seg. I utgangspunktet tenker man på videoovervåkning når man hører om overvåkning, men det er så mye mer enn det. Vi lever i et samfunn hvor man alltid er tilgjengelig på enten en mobiltelefon, eller en datamaskin. Dette har konsekvenser som har gjort det enklere for blant annet myndighetene å overvåke sin egen befolkning. Det er viktig å se tilbake på et historisk perspektiv for å kunne forstå hvorfor ting har blitt som det er nå. Eksemplene er mange når det kommer til overvåkning, kategorisering og gjenkjenning av befolkningen.

Metodene rundt å analysere og kategorisere ansikter er noe som har blitt forsket på og gjort siden tidlig 1800-tallet. Samuel Morton (1799—1851) var en amerikansk lege og naturvitenskaper, som er kjent for blant annet sin studie rundt kraniologi. I sitt arbeid samlet han inn kranier fra hele verden, som han sammenlignet med andre kranier og forsket på hvordan kraniet og rase henger sammen. Hans mål var å kunne klassifisere raser på en objektiv måte, ved å sammenligne de fysiske aspektene til de forskjellige kraniene. For å kunne klassifisere forskjellige raser, delte han folk inn i fem hovedkategorier. Disse var afrikanske, innfødte amerikanere, kaukasier, malaysisk og mongolsk. Disse kategoriene var dominert av kolonienes geopolitikk. Han bygget sin teori på at de hvite menneskene hadde større kranier, og var dermed smartere enn for eksempel mørkhudede mennesker, som han plasserte nederst på rangstigen. Noe som har kommet fram i etterprøving av teoriene hans, ser man at han hadde store feil i sin forskning. Mye kan tyde på at han var selektiv i hodeskallene, for at de skulle passe inn i hans teori. Han tok for eksempel ikke hensyn til at større personer har større hjerner. Det er nok også et politisk aspekt som lå i bakgrunnen for forskningen hans, for at man skulle kunne forsvare at man fortsatte med slaverier og slavehandel, siden de fra Afrika viste seg i hans forskning å ikke være intelligente nok i forhold til den hvite delen av befolkningen (Crawford, 2021, s. 123—127).

Under andre verdenskrig hadde for eksempel nazistene en effektiv måte med å kartlegge hvor jødene oppholdt seg i de forskjellige okkuperte landene. De kunne kartlegge hvor jødene bodde, hva de jobbet med også videre ved å bruke såkalte trykkort. Disse kortene ble benyttet som et av verdens første organiserte datasett, ved at de trykket ut punkter for religion, opprinnelsesland, morsmål og lignende. Jødene hadde flere kolonner som ble fylt ut, som ga tyskerne oversikt over hvor mange jøder med for eksempel polsk opprinnelse som bodde i Berlin. De kunne kjøre disse trykkortene igjennom en IBM-maskin, og få raskt oversikt over befolkningen med rundt 25000 kort i løpet av en time kjørt igjennom systemet (Rosenzweig, 2021). Dette var med på å kunne kartlegge hvor alle jødene var, og det ble dermed lettere å kunne organisere utkastelsen av hjemmene deres, inn til ghettoer og generelt Holocaust. Overvåkningen skjedde igjennom registreringer, folk som anga hverandre, mikrofoner og spionering. Nazistene var også eksperter på å kategorisere folk etter hvilket utseendet folk hadde. Kategoriene gikk

blant annet for jøde, homoseksuelle, kommunister og andre fiender som hadde annet syn enn hva nazistene hadde og levde etter. Hadde du for eksempel en stor nese, var du mest sannsynlig jøde. Dette gjorde at befolkningen var med på å angi andre, fordi de passet beskrivelsen til en «fiende» (United States Holocaust Memorial Museum, u.d.).

3.1.1 Tiår med utvikling

Historisk sett har overvåkning av befolkningen skjedd igjennom mange år. Etter andre verdenskrig ser man en tydelig utvikling av overvåkning av befolkningene. Dette har en tydelig sammenheng med at vi har blitt mer teknologiske i vår hverdag, og ikke minst i arbeidshverdagen. I dag er nesten ingen som ikke jobber på en eller annen type datamaskin. På slutten av 1980-tallet ble det mer vanlig med arbeid basert på bruk av datamaskiner. Med disse datamaskinene kom nye måter å kunne overvåke arbeidsprosessen til de ansatte. Staten ordnet med andre metoder for å kunne følge med på hva befolkningen holdt på med, gjennom blant annet installere videokameraer og bruke datamaskiner i seg selv for å følge sporene til befolkningen, ansatte og forbrukere. Som David Lyon (2015) skriver, har staten i flere århundre funnet forskjellige måter å telle og ha en oversikt over hva befolkningen forbruker. Lyon (2015) skriver videre at etter datamaskinen kom inn på arbeidsplassen, ble det lettere å ha en oversikt over hva som var effektivt og ikke. Det ble lettere å «styre» kundene til å kjøpe produkter bransjen ville at kundene skulle kjøpe, enda kundene selv trodde de ikke var påvirket da de handlet (Lyon 2015, s. 27-28).

På 1990-tallet var terminologien «overvåkningssamfunnet» i en mer generell daglig bruk. Dette kom av at det ble enda mer tydelig overvåkning i forhold til at det var flere synlige overvåkningskameraer. Det begynte å bli en del av hverdagen. Bankkort ble brukt mer. Det gjorde det lettere å få tall på hva og hvordan befolkningen handlet. I 1994 ble World Wide Web utviklet. Det førte til at flere fikk seg datamaskiner og flere fikk dermed en interaksjon online. Dette gjorde det nok en gang lettere for staten å kunne følge med på hva som skjedde i befolkningen (Lyon 2015, s. 28).

På 2000-tallet skjedde utviklingen i en rasende fart. Datamaskiner ble billigere, og det ble allemannseie. Utviklingen av internettet gjorde at det ble billigere for forbrukeren å benytte seg av dette, da man ikke lenger måtte bare bruke telefonlinjen for å få tilgang til

internett. På denne tiden ble sosiale medier utviklet. Sosiale medier gjorde det lettere å dele ting om livet sitt, på for eksempel Facebook, og følge med på hva andre gjorde i sitt liv. Det førte også til at overvåkningen på forbruket til befolkningen ble lettere å utføre. Overvåkningen måtte optimaliseres for de forskjellige statene etter terrorangrepene i USA 9. september 2001, og bombingen i London 7. juli 2005. Disse to hendelsene var med på hvordan sikkerhetsspørsmålet ble endret. Det ble dermed viktig å ha en effektiv og god overvåkning av fiendtlige land og områder til fienden under krigen mot terror. Samtidig som disse overvåkningsmulighetene ble utviklet, ble programvarer som ble benyttet til å overvåke befolkningen utviklet (Lyon 2015, s. 29).

3.1.2 Historien til ansiktsgjenkjenningsteknologien i korte trekk

Allerede tilbake til 1960-tallet ble det forsket på hvordan man kunne trene opp datamaskiner til å kjenne igjen en persons ansikt av forskerne Woody Bledsoe, Helen Chan Wolf og Charles Bisson. Målet var å kunne scanne en persons hårlinje, øyer og nese, for deretter å få maskinen til å finne ut hvem som matchet disse. På dette tidspunktet var ikke teknologien godt nok utviklet til at det ble vellykket (NEC, 2022). Bledsoe og kollegaene laget en maskin som kunne gjenkjenne alfa-numeriske karakterer. De prosjekterte en karakter til et rektangel på en matrise på 10 x 15 av en fotocelle. Hver fotocelle representerte et diskret element i bildet, eller pikselen, og mottok en binær 1 eller 0, avhengig om delen inneholdt deler av bildet de søkte opp eller ikke. Underveis oppstod det flere problemer da de skulle bruke denne algoritmen til å gjenkjenne ansikter. Dette på grunn av grunndataene de hadde testet ut systemet med var 2-D, mens et ansikt er i 3-D format. De måtte dermed måle opp forskjellige karakteristikker i et ansikt manuelt. Denne prosessen ble automatisert i 1973 ved hjelp av en programvare som kunne måle øyne, ører og lignende i et bilde av et ansikt. Uttestingen av systemet begynte med 400 bilder av hvite menn (Perkowitz, 2021). Allerede her kan man se at bias i teknologien begynte.

Biometrien ble videreutviklet på både 1970-, 80- og 90-tallet. Man kunne nå bruke av de tidligere innsamlede data for å forme et sett med basis av ansiktstrekk. Dette ble kjent som «Eigenface». Mye av problemet var at det fortsatt måtte kategorisere manuelt. På starten av 90-tallet kom gjennombruddet med å kunne gjenkjenne ansikter automatisk. Selv om det var et gjennombrudd innenfor teknologien, ble det nok en gang hindret av

tekniske og miljømessige faktorer. Databasen med bilder av ansikter ble derimot vedlikeholdt, da det viste seg at databasen måtte være massiv for at man skulle kunne utvikle teknologien videre (NEC, 2022).

Det var først på 2000-tallet de store gjennombruddene til ansiktsgjenkjenningsteknologien tok fart. På tidlig 2000-tall var teknologien godt utviklet, og flere myndigheter begynte å ta i bruk teknologien innenfor lovgivende makter, for å kunne gjenkjenne kriminelle. I 2006 ble teknologien nok en gang videreutviklet til å gjenkjenne ansikter gjennom bilder, 3D ansiktsbilder og irisbilder. Forskningen viste at teknologien var nå 100 ganger bedre enn hva den har vært tidligere. Når det gjelder å opprettholde en stor database, var det viktig for å få teknologien til å bli så nøyaktig som mulig. Det at Facebook gjorde det mulig tilbake i 2010 å «tagge» de forskjellige brukerne til bilder av personer som ble lastet opp har hjulpet på denne prosessen. Dette resulterte i en database på over 350 millioner bilder som ble lastet opp, og tagget til de forskjellige personene som var på bildet. Et annet gjennombrudd i ansiktsgjenkjenningsteknologien var i 2017, da Apple lanserte iPhone X, den første mobilen som kunne låse opp skjermen på mobilen ved hjelp av FaceID. Ansiktsgjenkjenningsteknologien er i stadig utvikling, og brukes nå daglig på mobiler, sosiale medier, flyplasser, tollkontroll, transport også videre (NEC, 2022).

3.2 Dagens overvåkningssituasjon

Det er ikke bare teknologien som har utviklet seg i en rasende fart, men også måter å kunne skade folk på. Etter 11. september i 2001, endret måten terrorangrep ble gjennomført på ved at terroristene styrtet flyene inn iblant annet World Trade Center. Tilbake til 2016 kom enda en måte å terrorisere befolkningen på. Dette skjedde ved at en person kjørte en lastebil inn i en folkemasse under et julemarked i Paris. Etter denne hendelsen, innførte franske myndigheter blant annet teknologien rundt ansiktsgjenkjenningsprogram, for å kunne forutse mulige kommende terrorangrep. Denne teknologien ble kjøpt fra kinesiske aktører.

I nyere tid er det heller ikke uvanlig at det dukker opp ny overvåkningsteknologi som en rekvisitt i filmer og serier. Eksemplene er mange, men man kan se overvåkningsteknologien vist fram på en god måte i filmer og serier som for eksempel:

Fast 8 (2017), Person of interest (2011—2016), Minority Report og The Capture (2019—), bare for å nevne noen. Mange er ikke klar over at mye av denne teknologien allerede er i bruk i forskjellige stater. Noen er fiktive og funnet opp av manusforfatterne, men det kan i høy grad vise hvordan teknologien har utviklet seg, og hva som egentlig er mulighetene med slik type overvåkningsteknologi.

3.2.1 Ansiktsgjenkjenningsteknologien

Ansiktsgjenkjenningsteknologien (AGT) er en biometrisk teknologi som benytter seg av algoritmer for å analysere bilder av en persons ansikt, og sammenligne dette med tidligere eksisterende bilder som er kjent i databasen. AGT er mest kjent som et verktøy for politi og andre sikkerhetsbyråer. Dette spesielt med tanke på initiativ mot anti-terrorisme. Det mange ikke tenker over, er at AGT også blir brukt i forhold til vanlige forbrukere innenfor bildenettverk og det å organisere personlige digitale bilder. Dette blir ikke sett på som noe negativt, men som praktisk og forenklet morsomhet (Lyon 2018, s. 88).

Utviklingen av AGT ble sponset og gjennomført av blant annet Department of Defense CounterDrug Technology Development Program Office, og den amerikanske hærens undersøkende laboratoriet. Denne teknologien ble i all hovedsak utviklet for å kunne få et automatisk søk på potensielle kriminelle. I starten ble bilder fra arrestasjoner, såkalte «mugshots», presentert for algoritmen, som igjen skulle finne den nærmeste matchen av enkeltpersoner fra det store bildegalleriet. Det ble også brukt for å identifisere kriminelle smuglere og terrorister igjennom tollkontroll ved flyplasser (Crawford, 2021, s. 104).
Det største vendepunktet i historien i forhold til AGT, er terrorangrepet 11. september 2001. Når det kommer til utviklingen av denne teknologien, kan man dele det opp i to epoker; før og etter terrorangrepet i USA 11. september 2001. Det ble en helt ny måte å utføre terrorangrep på, og ikke minst begynte det et kappløp om å ha den beste teknologien som kunne forutse kommende terrorhandlinger (Crawford, 2021, s. 106). Dette har igjen ført til at for eksempel personer som blir sett på som at de mest sannsynlig er muslimske, blir oftere stoppet i kontroller på flyplassen og lignende (Lyon 2018, s. 64). På tidlig 2000-tall ble sosiale medier utviklet. Facebook er et eksempel på hvordan det ble lettere å finne igjen folk, og hvordan datasettene ble forhøyet ettersom

flere folk la ut bilder av seg selv, venner og familie. Dette ble sett på som noe morsomt og spennende, spesielt da man kunne «tagge» inn enkeltpersoner. Det som de fleste ikke er klar over, er at man med alle disse opplastningene og taggingen, var med på å trene opp kunstig intelligens for å bli mer treffsikre på sine søk av personer via bruk av AGT. Det er denne databasen som er med på å forsterke effektiviteten på å gjenkjenne enkeltpersoner (Lyon 2018, s. 89).

AGT kan bli brukt på forskjellige områder. Det er spesielt tre områder man benytter seg av teknologien. Dette er innenfor verifisering, identifisering og karakterisering. I forhold til verifisering sammenlignes to bilder for å kunne avgjøre om det er den samme personen. Man er derfor avhengig av en database med bilder av vedkommende, for å få en match. Med iPhone X fikk forbrukeren muligheten til å for eksempel låse opp telefonen sin med AGT. Med sitt infrarøde kamera foran, kan den scanne 30000 punkter i ansikter, og skaper deretter en 3D-scan. Denne 3D-scannen gjør at det skal bli vanskeligere å låse opp mobilen ved bare å benytte seg av et bilde. Man kan se en videreutvikling på dette det siste året. Man kan logge inn på alt fra bankkonto til andre personlige sider med AGT. Dette er brukervennlig, da man ikke må huske på alle mulige passord og koder for å logge seg inn. I forhold til identifisering, er man avhengig av en stor database av bildet av ansiktet til enkeltpersoner. Disse blir hentet fra både bilder på sosiale medier og overvåkningsvideoer (Tennøe et.al. 2020). Det siste området handler om karakterisering. AGT har blitt trent opp med bildemateriale av befolkningen for å kunne kategorisere. Her sjekker algoritmen oppførselen, og hvordan sinnstilstanden til enkeltindividet er, for å kunne karakterisere om man for eksempel er en terrorist, eller ikke (Robins, 2021, s. 89).

Bruksområdene til ansiktsgjenkjenning varierer over store deler av verden. Argumentasjonene på hvorfor man bør fortsette å videreutvikle AGT går på at det er blant annet minsker risikoen på identitetstyveri, eller at personlig informasjon lett kan komme på avveie. Det gjør det også lettere for brukerne, da det i lengden kan bli mange passord å huske over tid. AGT er også utviklet som en hendig ting for forbrukeren (Tennøe et.al. 2020). Flere steder over hele verden har AGT blitt tatt i bruk i form av å kunne sjekke inn på flyplasser med bare ansiktet. Det er også vanlig at man kan gå igjennom passkontroll med først å scanne passet, for så at det blir verifisert med bilde av

passholderen inne i neste avlukke. Dette øker effektiviteten for kødannelsene som kan oppstå på flyplasser (Lyon 2018, s. 63). I Kina har det blitt en del av normalen at man kan betale for forskjellige tjenester ved for eksempel butikker eller kollektivtransport ved å scanne ansiktet sitt på en monitor (Tennøe et.al. 2020). Kina er ledende innenfor utviklingen av teknologien, og ligger et tiår foran resten av verden. De benytter seg av AGT for blant annet å kategorisere befolkningen i forskjellige klassesystemer. AGT ble benyttet for å kontrollere befolkningen under COVID-19, for å sjekke om de for eksempel brøt karantenen (Almeida et.al. 2021, s. 378).

3.2.2 «Big data», algoritmer og bias

«Big data» handler om hvordan man samler inn og behandler data i forhold til praksis og prosesser. Man starter med store datasett som man kategoriserer for å gjøre det enklere å søke fram det man trenger i ettertid. Under kategoriseringen er det viktig at man benytter seg av krysshenvisninger, som gjør søket i etterkant mer treffsikkert og brukervennlig. I denne prosessen er det viktig å finne forskjellige søkemønstre. På denne måten kan algoritmene vite hva du som enkeltperson vil like. Det er disse algoritmene som gjør det mulig at kunstig intelligensteknologien kan kjenne igjen hva man tidligere har søkt på. Dette er noe for eksempel Amazon.com benytter og utvikler i det daglige (Lyon 2015, s. 69).

For at teknologien skal kunne fungere, er man avhengig av innhenting av store datamaterialer som blir oppdatert kontinuerlig. Denne dataen kjøres opp mot de forskjellige algoritmene i programmene. Dette datamaterialet er det som brukes for å kunne trene opp maskinene til å fungere best mulig. Dette er med på å utvikle forskjellige datasett, som igjen er med på å forme de kunnskapsrelaterte grensene som styrer hvordan kunstig intelligens operer, og på denne måten kategorisere hva programvaren skal kunne «se» i materialene (Crawford, 2021, s. 98).

Før databasene med bilder av ansiktene til enkeltindivider ble like store som de er i dag, ble databasene laget ut ifra bildene politiet tok når de arresterte folk. Dette er bilder som blir tatt av en persons hode og ned til skuldrene, både framover og på siden. Dette for å dokumentere, og identifisere vedkommende, ved en arrestasjon. Disse bildene var med på å trene opp maskinene til å gjenkjenne folk med spesifikke trekk som er kriminelle.

Crawford (2021) tar opp noen av svakhetene med dette systemet. Hun poengterer at bildene i datasettene ble tatt ut av kontekst ved at historien, konteksten og navnet er tatt bort. En annen ting hun påpeker er at siden bildene ble tatt rett etter arrestasjon, er det heller ingen klarhet om at vedkommende ble varetektsfengslet, eller fikk en dom på det de var arrestert for. Et annet problem oppstår innenfor etikken, hvor disse personene ikke har gitt sitt samtykke til at bildet deres kan benyttes (Crawford, 2021, s. 91).

Som Coeckelbergh (2020) skriver, er maskinlæringen en statistisk prosess som ofte brukes til å finne mønster i et system. Her kommer algoritmene inn. Algoritmene kan brukes for å identifisere forskjellige mønstre eller regler i et datasett. Deretter brukes disse mønstrene, eller reglene, til å kunne forutse hvordan framtidig data vil se ut. Algoritmene kan finne mønstre og regler, som ikke er gitt av programmeren på forhånd. Et eksempel er hvordan algoritmene kan oppdage søppelpost i e-posten, og legge disse under en egen fane. Dette gjør den ved å gå igjennom tidligere e-poster og hvilke av disse mailene vi har slettet, eller lagt i spamboksen. Maskinlæringen kan foregå med tilsyn, og hvor kategorier er gitt på forhånd med enormt datagrunnlag. Dette brukes ofte i forhold til å kategorisere hvor stor sikkerhetsrisiko enkeltpersoner er. Maskinen blir lært opp til å kategorisere og deretter forutse om spesifikke enkeltpersoner vil utgjøre en samfunnsrisiko, eller ikke. Coeckelbergh (2020) skriver videre at maskinlæringen kan foregå uten tilsyn. På denne måten kan algoritmene lære seg selv hvordan den skal kategorisere elementer i forhold til de forskjellige mønstrene den oppdager. Dette er som regel mønstre ikke programmeren har tenkt som en mulighet på forhånd. Den siste læringen handler om å forsterke læringen rundt de mønstrene som blir oppdaget. I denne typen læring lærer systemet seg hva som er en bra jobb, og hva som er en dårlig jobb. Om den har kategorisert en person som lavrisiko for sikkerheten, og dette stemmer ut ifra dataene som er analysert, vil maskinen lære seg til at dette var riktig og bra gjennomført. Dette har blitt videreført til «big data» konseptet, siden den kan håndtere store mengder data, og analysere forskjellige typer data raskt (Coeckelbergh, 2020, s. 84—87).

En form for systematisk feil, blir betegnet som bias. Dette er kan ofte oppstå i algoritmen, om datagrunnlaget ikke er godt nok. Det har ført til flere saker hvor teknologien har tatt uetiske beslutninger, og diskrimineringen har vært stor for enkelte

grupper og individer. I filmen *Coded bias* (2020) kommer dette tydelig fram da MIT Media Lab forsker Joy Buolamwini oppdager at AGT ikke gjenkjenner ansiktet hennes, før hun tar på seg en hvit maske. Teknologien er ikke optimal. Den har god treffsikkerhet på hvite menn rundt 50 år, mens for eksempel mørkhudede kvinner får en langt dårligere treffprosent. Coeckelbergh (2020) tar også opp eksempler hvor algoritmene har mange feilmarginer på algoritmen. I Florida prøvde domstolen ut AGT for å gjøre domstolen mer effektiv. Systemet ble kalt for COMPAS, og skulle forutse om noen var skyldige, uskyldige og om de hadde stor sannsynlighet for å gjenta kriminelle handlinger. Det viste seg i etterkant at flere mørkhudede menn enn hvite menn som ble domfelt. Dette selv om disse i mange av tilfellene var uskyldige og det var hvite menn som hadde gjort ugjerningen. Et annet eksempel han kommer med er PredPol-produktet, som skulle hjelpe politiet til å forutse i hvilke områder det var størst sannsynlighet for kriminelle handlinger kunne oppstå. Her igjen er problemet igjen at dataene algoritmene jobber ut ifra er basert på tidligere innrapporteringer fra forskjellige områder. Dette er områder hvor befolkningen ofte består av fattige og mørkhudede folk. Dette er med på å skape en mistillit til både politiet og samfunnet (Coeckelbergh, 2020, s. 127—128).

4.0 Analyse og diskusjon

AGT er en teknologi som vokser raskt, og som blir benyttet i flere og flere land. Hittil er det rundt 64 land som benytter seg av denne teknologien. Dette gjelder for blant annet Kina, Russland, England, Tyskland og USA. Norge benytter seg også av denne teknologien. Den mest synlige bruken kommer i form av verifiseringsteknologi, som er knyttet til en enkeltpersons egen enhet som for eksempel for å låse opp mobilen, logge seg inn med bankID også videre.

Som nevnt tidligere, kan AGT i hovedsak deles inn i tre bruksområder; verifisering, identifisering og kategorisering. Det er ingen tvil om at disse tre punktene fører med seg en del etiske spørsmål, som er viktige å stille for å kunne svare på problemstillingen: *«Hva er fordelene og ulempene med å benytte ansiktsgjenkjenningsteknologien i forhold til overvåkning?».* I dette kapitlet vil jeg fokusere på følgende områder som et grunnlag for den videre refleksjonen i kapittel fem:

- Rettigheter rundt privatliv og personvern
- Åpent vs. lukket samfunn
- Datatilsynets rolle
- Kjølende effekter
- Kriminalitet vs. overvåkning
- Bias i teknologien

4.1.Retten til privatliv

Hvor ofte har man ikke hørt «vi må ha overvåkning for å beskytte befolkningen», «om du ikke har noe å skjule, har du ikke noe å frykte»? Etter 11. september 2001 ble det mer fokus på å beskytte befolkningen fra terror og annen kriminalitet. Dette terrorangrepet ble utgangspunktet for å videreutvikle overvåkningen som vi har i dag. Mange myndigheter benytter seg av forskjellige argumenter som går på «vår trygghet» for at vi skal være med på å godta at vi blir overvåket hele tiden. Det at de velger å spille på enkeltindividets frykt for at noe skal skje, er et mektig virkemiddel for at vi skal godta det som skjer rundt oss. De spiller opp mot enten må vi leve fritt uten overvåkning. Konsekvensen blir at man ikke kan forhindre grusomme ting til å skje. Ellers så må vi akseptere at vi blir overvåket for at de lettere skal kunne avverge grusomme hendelser til å skje (Lyon 2018, s. 59). Det kanskje ikke mange tenker over er at med overvåkningen og bruk av AGT, får det også en del følger for vårt dyrebare privatliv.

Privatlivet er uten tvil noe alle setter høyt. Med teknologien i utvikling har grensene for privatlivet endret seg. Tidligere ville man bare anse sitt eget hjem som privat, og enkelte offentlige steder som for eksempel garderober og toaletter. Etter at mobiltelefonen ble allemannseie, har disse grensene flyttet seg. Man kan for eksempel ha en privat telefonsamtale samtidig som man handler, med en forventning at ingen lytter til samtalen (Rössler, 2005, s. 172). Privatlivet har en vesentlig stor rolle innenfor AGT. I dette kapitlet vil jeg først definere hva privatliv er, før jeg vil diskutere videre bruken av AGT i forhold til privatliv og lover innenfor European convention of Human rights og «General Data Protection Regulation» (GDPR). Jeg vil videre diskutere hva som er utfordringene i forhold til AGT og privatlivet.

4.1.1 Hva defineres som privatliv?

Det finnes ikke noen god definisjon på hva privatliv egentlig er. Flere vil si at det handler om å ha kontroll over vår egen informasjon, hvem som vet hva og hvem som har tilgang til hva (DeCew, 2018). Om man ser tilbake på historien ble ikke retten til privatliv nevnt i tekstform før på 1960-tallet, hvor William Prosser definerte fire punkter om hvordan privatlivet blir brutt slik:

- Intrusion upon a person's seclusion or solitude, or into his private affairs
- Public disclosure of embarrassing private facts about an individual
- Publicity placing one in a false light in the public eye
- Appropriation of one's likeness for the advantage of another (DeCew, 2018)

Med disse punktene over rettigheter begynte man å se nytten av å skille privatlivet og det offentlige. I etterkant har det kommet flere retningslinjer på hvordan man kan opprettholde rettighetene til den sivile befolkningen. Et eksempel er European convention of Human rights, artikkel 8, hvor det står:

Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others (European court of human rights, 2013, s. 11).

Ifølge Stefan Strauß (2017) defineres privatlivet som at staten ikke blander seg inn i den enkeltes liv. Enkelte ganger er det nødvendig at staten overvåker enkeltindividet, men dette skal kun gjøres om det er for det som er til det beste for folket i henhold til lovverket, og for å beskytte det demokratiske samfunnet (Strauß, 2017, s. 144). Dette går mye på hvordan staten bruker teknologien for å kunne forutse for eksempel terrorangrep, og for å forhindre at dette skjer. Telefonavlytting og annen overvåkning er derfor relativt vanlig fenomen i det kriminelle miljøet. Hovedutfordringen med overvåkning er hvordan teknologien brukes til å innhente og analysere den enkeltes personlig data. En annen utfordring er at man ikke vet hva slags informasjon som blir

innhentet, hvordan dette blir oppbevart, eller til hvilken bruk og nytte er denne informasjonen tenkt. Man kan derfor på mange måter si at privatlivet og personvernet er i en utsatt posisjon, om vår informasjon ikke blir oppbevart og brukt på en riktig måte (Strauß, 2017, s. 145). Strauß referer til De Hert, som mener at for å kunne avgrense hva som er privat og offentlig, er det tre krav som må oppfylles. Dette handler om i hvilken grad dataen har legalitet, legitimitet og nødvendighet. Dette for å kunne beskytte hver enkelt persons informasjon på en god og trygg måte, og for å kunne se hva som kan deles og ikke (Strauß, 2017, s. 146). Videre referer Strauß til Clarke sine klassifikasjoner av fire hovedtyper av privatliv. Det første punktet er «bodily privacy». Dette handler om å beskytte en persons fysiske avstand og intimsone. Punkt to peker på hvordan man skal oppføre seg ute i folkemengder, og rundt enkeltpersoner. Dette går på å respektere hverandres religiøse tro, praksiser og seksuell aktivitet. Det tredje punktet handler om relasjonene man bygger opp, og operer innenfor. Det siste punktet handler om integriteten og beskyttelsen av all type sensitiv data om enkeltindividet (Strauß, 2017, s. 147). Videre referer Strauß til Finn et. al. som har videreutviklet Clarke sin liste, med punkter som: «Privacy of the person», «Privacy of behavior and action», «Privacy of communication», «Privacy of data and image», «Privacy of thoughts and feelings», «Privacy of location and space» og «Privacy of association» (Strauß, 2017, s. 147-148). Med disse punktene i bakhodet, får man et godt bilde på hvordan teknologien er med på å dytte grensene på hva som er privatliv, og i flere tilfeller bryte retten vår til privatliv. Dette med tanke på at overvåkningen har blitt en såpass vanlig del av hverdagen vår, at det blir noe man ikke tenker over lenger. Dette ser man ved for eksempel at de aller fleste har en smarttelefon, som overvåker ting du sier fordi man selv har gitt tillatelse til å bruke mikrofonen på telefonen, hvor du er, de har kameraer som gjør at det er lettere å ta bilde uten at man er klar over det (Strauß, 2017, s. 149).

Demokrati handler om å skape tillitt blant befolkningen, og ikke mistanker og frykt (Lyon 2015, s. 127). Man kan derfor på mange måter si at demokratiet er utsatt for risiko, når teknologien og staten tillater å gå inn og overvåke en sivil person. I et demokratisk land handler det om å behandle folk med verdighet. Denne verdigheten forsvinner når folk blir overvåket som om de er kriminelle. Algoritmene er stilt inn på at kriminelle ser slik og slik ut, og de som kommer innenfor disse kriteriene, blir dermed ansett som kriminelle i systemene. Dette selv om de aldri har gjort noe galt. Lyon tar opp

eksempelet om Faisal Gill, en som har hatt høy sikkerhetsklarering i militæret, og da han jobbet for Department of Homeland Security. Han jobber som advokat, og er det man kan anse som en god amerikansk borger. Ifølge avsløringene til Snowden ble blant annet hans e-poster overvåket av staten, for å se etter terrorister og mulige spioner. Alt dette bare fordi han er muslim. Dette på grunn av algoritmene har blitt satt til at muslimer kan utgjøre en fare for landet, og at de er mulige terrorister (Lyon 2015, s. 91—92). Staten bruker blant annet trygghet og sikkerhet som en begrunnelse av å ha overvåkning, men hvor er det etiske når folk blir ansett som kriminelle, bare fordi de har et stereotypisk utseende?

4.1.2 Privatliv og personvern

Privatliv og personvern er to kategorier som går inn i hverandre. De er begge beskyttet under forskjellige lovgivninger. Personvern handler om retten til å kunne være uavhengig, selvstendig ansvarlig, og ha en mulighet til å utvikle selvstendige refleksjoner. Alt dette avhenger av at man må ha en privat sfære. Selv om det er lovgitt at man har rett på et privatliv, og at private opplysninger skal bevares på en trygg måte, er det alltid noen hensyn som må tas. Dette kommer igjen ved eksempler rundt kriminelle miljøer. Man argumenterer med at skal samfunnet være trygt, må man kunne gripe inn og ta andre hensyn i forhold til de lovgitte menneskerettighetene. På denne måten kan man i større grad forutse eventuelle kriminelle hendelser, og argumentasjonen går på at dette er for den vanlige borgers frihets- og trygghetsfølelse. Tilbake i 2016 kom Europaparlaments- og rådsforordningen fram med en ny lov som gikk på behandling av personopplysninger. Denne loven blir omtalt som GDPR.

I GDPR kapittel 2, artikkel 5; Prinsipper for behandling av personopplysninger, handler om følgende punkter innenfor hvordan personopplysninger skal behandles:

- Lovlighet, rettferdighet og åpenhet
- Formålsbegrensning
- Dataminimering
- Riktighet
- Lagringsbegrensning
- Integritet og konfidensialitet

Disse punktene går på hvordan man skal innhente og behandle personopplysninger. Det må for eksempel være lovlig innhenting, og bruk, som skal skje på en rettferdig måte. Bruken av opplysningene skal være forutsigbar for den enkeltpersonen det gjelder, og hva som er hensikten med at noen trenger denne opplysningen. Loven tar videre for seg at opplysninger skal kun benyttes til angitte og legitime formål. Man skal kun innhente de nødvendige dataene, og minimere andre opplysninger som ikke er angitt som hensiktsmessige opplysninger. Videre tar loven for seg at opplysningene skal være riktige, og må oppdateres ved behov. Punktet om lagringsbegrensning er det spesifisert at opplysninger skal lagres i kort tidsperiode, og slettes på en trygg måte da opplysningene ikke er nødvendige lenger. Det siste punktet går på hvordan opplysninger vi må gi fra oss skal behandles på en korrekt måte, slik at opplysningene ikke blir misbrukt, blir ødelagt, går tapt eller blir endret. Helt til slutt i kapittel 2, artikkel 5-2 står det tydelig om hvordan de som behandler informasjonen de har tilgjengelig er ansvarlige for at punktene ovenfor blir overholdt (Datatilsynet, 2021).

4.1.3 Ansiktsgjenkjenningsteknologien og privatliv

Om man ser på hvordan forskjellige myndigheter benytter seg av AGT, vil man se på forskjellige meninger og tiltak i forhold til å sikre befolkningens rett til et privatliv, og hvordan deres data kan beskyttes på best mulig måte. Med strengere lover og regler, blir det vanskeligere å misbruke AGT. Noe av problematikken med strengere lover og regler, er at disse praktiseres forskjellig fra land til land. I land som for eksempel Kina har forskjellige selskaper tilgang til stemmer, ansikter og annet biometrisk materiale, som har vært med på å utvikle teknologien. Dette har gitt mulighet for myndighetene til å følge med på at befolkningen er lovlydige. På denne måten vil det være lettere å kunne rangere befolkningen inn i forskjellige kategorier ut ifra om de er lovlydige eller ikke (Bu, 2021).

USA er et annet eksempel på hvordan lover kan praktiseres forskjellig. Her benyttes AGT i stor grad av politiet. Per 2022 finnes det ingen tydelige lover som handler om privatlivet til befolkningen. Dette fører til at befolkningens interesser ikke blir like lett ivaretatt, og datagrunnlaget kan selges videre til tredjeparter. Et annet problem i USA er at det er forskjellige lover og regler i de forskjellige statene. Selv om det foreligger forbud mot AGT i noen få stater, er det andre lover i andre stater igjen. Dette er på

mange måter veldig problematisk, og befolkningen må ofte betale store summer for å kunne kjempe mot systemet om de mener at deres personlige data har blitt misbrukt (Almeida et.al 2021).

I Europa, og i UK, har det blitt utviklet et regelverk som skal beskytte befolkningens rettigheter i forhold til personvern. GDPR setter krav til hvordan data skal oppbevares, og at det kreves samtykke av enkeltpersoner for å kunne bruke denne dataen. Dette fører igjen til større krav til organisasjoner som samler inn data. De må gi god informasjon om hva de eventuelt skal benytte dataen de har samlet inn til (Bu, 2021, s. 116). Det finnes unntak for når myndighetene kan overstyre personvernet. Dette skjer om det er fare for sikkerheten for innbyggerne. Dette skal kun skje når det er nødvendig, og kun under spesifikke omstendigheter som må komme tydelig fram i loven til landet (Bu, 2021, s. 117). På mange måter er dette bra, og betryggende for folk flest. Men GDPR er ikke en heldekkende lovgivning i forhold til at man kan ha en sikker bruk av AGT. Noe av det som blir problematisk er blant annet at dette kun gjelder for EU. GDPR har dermed ingen lovgivende makt utenfor Europeiske land, som vil si at dataen kan fortsatt bli solgt videre til tredjeparter utenfor EU. Hva denne dataen kan bli brukt til er derfor usikkert for brukeren. Denne datadelingen er med på å skape potensielle problemer for enkeltindividet. Vi lever i dag i et samfunn hvor det aldri har vært lettere å finne informasjon om andre personer. Vi deler det meste av livet vårt på sosiale medier, som igjen er lett å søke opp for andre. Denne informasjonen blir så solgt videre til andre aktører, som benytter dataene dine til å for eksempel selge deg et produkt. Dette gjør at vi får skylapper på hva som kan skje i forhold til vår rett til privatliv. Overvåkningen har blitt normalisert, som igjen fører til at vi ikke lenger er obs på hva slags informasjon vi gir fra oss når vi tagger et bilde, eller når vi legger ut ting på sosiale medier (Dripke & Miksch, 2021, s. 57). Et annet dilemma er at loven ikke klarer å holde tritt med utviklingen av teknologien. Dette kan føre til misbruk av bilder og data i for eksempel kriminalsaker, og tilfeller man jobber for en rettferdig løsning (Bu, 2021, s. 128). AGT kan for eksempel ha en 85 % treffsikkerhet på at et enkeltindivid har befunnet seg på det stedet da den kriminelle handlingen ble begått. Men det er ikke nødvendigvis riktig person selv om det var en stor treffprosent. Det viser nødvendigheten med at loven må holde tritt med utviklingen av teknologien, og at data alltid også behandles av

mennesker, slik at vi til enhver tid vil kunne være trygge på at vi er beskyttet av loven i forhold til hvordan våre data blir lagret og benyttet.

4.1.4 Betingelser om personvern på sosiale medier

Personvern er en agenda som det har blitt mye fokus på i det siste. For at vi skal kunne benytte oss av forskjellige plattformer av sosiale medier er vi nødt til å godta betingelsene. Selv om vi godtar disse betingelsene, er ikke alltid brukeren klar over hva slags informasjonen man legger igjen på flere steder blir brukt til. Her vil jeg gå nærmere inn på Facebook og Snapchat som en plattform. Dette er bare et eksempel av mange, som benytter AGT til ting brukeren ikke er klar over.

Facebook oppdaterte sine brukerbetingelser tilbake i 2018, med en lovnad om at dette skal beskytte dataen vi legger ut på deres plattformer. Det den fortsatt gjør, er å automatisk samle inn data som brukes til å trene opp AGT. De argumenterer for dette med at man må samle inn store datasett, for å kunne beskytte folk på en best mulig måte. De skylder på at de setter privatlivet til brukeren først. Den informasjonen de lagrer om deg, selger de deretter videre til andre aktører. Brukerne er uvitende om at den uskyldige leken med å tagge folk inn i bilder, faktisk er med på å trene opp AGT. Vi gir dermed opplæring til teknologien helt gratis, og vi selv er helt uvitende om dette. Det kommer heller ikke tydelig fram i betingelsene at siden Facebook er en amerikansk bedrift, har amerikanske myndigheter tilgang til alt materiale vi laster opp (Dripke & Miksch, 2021, s. 56-57).

Om man leser betingelsene for bruken av for eksempel Facebook, ser man at de i starten sier at de ikke selger noe av din informasjon videre til andre aktører, men at de tilpasser de andres aktørenes annonsering i de kategoriene aktøren har ønsket. Som for eksempel om målgruppen er jenter 15 år, vil de få en annonse som passer til dem. Informasjonen blir videresendt i forhold til hva vi søker på. De skriver om at det er gratis å bruke for oss, mens andre aktører betaler for at Facebook skal kunne annonsere til for eksempel jente 15 år. Om man scroller litt lenger ned på betingelsene på Facebook, finner man noe som er ganske interessant. For det første er disse betingelsene noe man må godta for at man skal kunne benytte seg av tjenesten. Dessverre er de lange, med et lite brukervennlig språk. Dette fører igjen til at veldig mange faktisk ikke leser betingelsene

for å benytte plattformen. Man vil bare videre, og benytte seg av plattformen. Det man da går glipp av er blant annet at ved å godta betingelsene, gir du også Facebook lisens til å kunne benytte alt man laster opp. I de flestes tilfeller gjelder dette bilder. Med denne lisensen får Facebook lov til å bruke, lagre, kopiere og dele bildet ditt med andre (Facebook, 2023). Teknisk sett gir vi dem tillatelse til å gjøre som de selv vil med det vi legger ut.

Et annet interessant punkt i betingelsene handler om sletting av materiale. Om du sletter bildet ditt, vil det ta 90 dager før disse blir ordentlig slettet. De blir fjernet for allmenheten, når du sletter dem, men det tar tid å fjerne det fra servere osv. Ergo en estimert tid på rundt 90 dager. Selv om du sletter bildet ditt, betyr det fortsatt ikke at det blir slettet helt etter 90 dager. Gjennom lisensen vi har samtykket til, står det videre at de vil slette bildet i løpet av 90 dager, *med mindre det blir brukt av andre*. Gjennom lisensen har de andre aktørene lov til å bruke bildet, selv om du har slettet det. Det vil dermed ikke bli slettet *før* de andre aktørene også sletter det. En tredje ting jeg la merke til i betingelsene, handler om at vi samtykker til at de kan bruke navnet vårt, profilbildet vårt og informasjonen om hvilke handlinger du foretar deg og gi dette videre til andre aktører innenfor annonsering, reklame eller andre sponsede ting (Facebook, 2023). For min del er dette litt motsigende i forhold til hva de skriver i starten med at de ikke gir fra seg noe informasjon om deg. De informerer heller ikke om hva det skal brukes til, utenom aktører som skal selge produkter. Hva da med myndighetene? Hvorfor har for eksempel myndighetene i USA tilgang til alle bildene vi har lastet opp? Hva brukes de til? Hvorfor blir alle bildene vi har tagget andre inn i brukt til å trene opp AGT?

En ting jeg la merke til i vilkårene for både Facebook og Snapchat er at man ikke kan benytte seg av tjenesten om man er dømt for seksuelle forbrytelser. Da lurer jeg på hvordan de kan sjekke opp denne spesifikke informasjonen? Hvor har de tilgang til å søke opp akkurat dette punktet? Sitter de med tilgang til politiregistre over seksualforbrytere? Det står nemlig ingenting om hvordan såpass spesifikk informasjon blir innhentet. Videre skriver de om at hensikten med appen er at man skal kunne skape, laste opp, publisere, sende, motta og lagre innhold. Her er det vi som bruker som har all eierskapsrettighet, men vi gir dem tillatelse til å bruke innholdet til det de ønsker. Det kommer fram at de bruker innholdet vi laster opp til markedsføring og for å kunne

forbedre tjenestene. På et punkt nevner de at bilder vi sender/laster opp blir slettet så fort bildet har fått status som åpnet, eller at utløpstiden har utgått. De nevner at forbrukeren har ikke krav til kompensasjon hvis offentlig innhold blir brukt av selskapet i etterkant (Snapchat, 2021). For eksempel bilder, lyd og video. Da får jeg en ny undring, med hvordan kan de da bruke innholdet videre?

4.2 Ansiktsgjenkjenningsteknologien og personvern i Norge

Som mange andre land, blir AGT benyttet i Norge. Ut ifra det jeg kan se i kildene mine, brukes denne teknologien på Oslo lufthavn i forhold til overvåkning med AGT. Når man kommer til Norge fra utlandet, må man igjennom passkontroll. Om man er fra Schengenområdet, og har et biometrisk pass, kan man benytte seg av maskinene som verifiserer at informasjonen i passet ditt stemmer med deg. Dette gjøres ved at man først scanner chipen i passet, før man slippes videre inn til en sluse hvor man skal se rett inn i et kamera. Dette kameraet tar et bilde av deg, som igjen blir analysert og sjekket om det stemmer med det som står i passet du akkurat scannet inn. Stemmer det, slippes man igjennom. Dette er på mange måter mer tidseffektivt, og større sjanse for å kunne finne feil enn hva mennesker får til. Dette gjøres ved at teknologien avleser og analyserer informasjon med en bedre treffsikkerhet enn hva mennesker får til med det blotte øyet (NTB, 2012).

4.2.1 Bruken av ansiktsgjenkjenningsteknologien i Norge

Flyplassen er ikke det eneste stedet vi benytter oss av AGT. Alle som har en smarttelefon, kan benytte seg av systemet til AGT. Dette er for å kunne verifisere at det er du som skal bruke for eksempel mobilen. Det samme gjelder for PC-er. På mange måter er det tidseffektivt, og en stor fordel at man slipper å måtte huske på alle passordene til de forskjellige stedene. Utenom flyplassene er det ifølge Mona Naomi Lintvedt (stipendiat ved juridiske fakultet og tech-ekspert), som var gjest i «Jusspodden» sin podkastepisode om ansiktsgjenkjenning, kun politiet som kan benytte AGT i forhold til overvåkning. Denne bruken er strengt regulert. Her står blant annet GDPR sentralt (Reinertsen, 2022). Reinertsen og Lintvedt (2022) tar videre opp at selv om loven kan regulere flere faktorer innenfor bruken av AGT i overvåkning, er det et lite smutthull der for privatpersoner. Det er ingen reguleringer som sier noe om hver enkeltes bruk av AGT. Man kommer ikke i klemme med loven i forhold til om man vil bruke AGT kun til

personlig bruk, for å kunne identifisere for eksempel en tilfeldig forbipasserende på gata (Reinertsen, 2022).

Det er per i dag en ny Europeisk regulering i forhold til blant annet ansiktsgjenkjenning som er under utvikling, og som første utkastet er klart til. Denne tar blant annet opp et forbud for politiet å kunne benytte AGT i sanntid. Dette har blitt benyttet de senere årene iblant annet av USA. Politiet der har hatt tilgang til, og har hentet ut og sammenlignet bilder som ligger i appen Clearview AI (Smith & Miller, 2021). Selv om politiet ikke kan benytte seg av denne tjenesten, er det ingen forbud for privatpersoner å benytte denne tjenesten. Dette kan med andre ord bety at man kan finne igjen folk ved å sammenligne bilder i søkemonitoren til Clearview AI. Per i dag kan politiet i Norge kun benytte AGT i etterforskning, og ikke i sanntid. Med mindre det er en del av etterforskningen på enkeltindivider. Dette er med på å vedlikeholde tilliten i forhold til bruken av AGT hos befolkningen (Reinertsen, 2022). En grunn til at dette er problematisk er at de bildene som ligger lagret i databasen der, ikke har blitt lagret der med samtykke fra den enkelte. Det er heller ikke gitt samtykke fra plattformene som bildene er hentet ut fra til å brukes i en slik database. Hvis politiet skulle fått tillatelse til å bruke AGT i sanntid som overvåkningsmetode, er dette noe som vil påvirke oss alle. Ifølge Lintvedt (Reinertsen, 2022), vil dette skape mindre tillit hos politiet. Det blir lettere å misbruke systemet, ved at man lettere kan følge med på enkeltindivider og deres handlingsrom. AGT følger med på alle, og lagrer data om oss i en database. Dette kan igjen føre til at flere blir stoppet uten grunn, og enda flere vil bli mistenkeliggjort for noe de kanskje ikke har gjort. Bruken av AGT er regulert av forskjellige forordninger og lover som GDPR, menneskerettigheter og lignende. Det er med andre ord ikke bare å kjøre på med AGT, uten at det kan bli fulgt opp av regelverket. Det som kan være et hull i GDPR er om man skylder på at man skal kun benytte informasjonen man innhenter kun til seg selv. Lintvedt kom også med et eksempel fra Sverige for å problematisere hvordan AGT kan bli misbrukt. Her tok hun opp et eksempel med en skole, hvor de hadde benyttet AGT for å kartlegge hvilke elever som kom for sent til skolen. Hun tar fram at tanken kan være grei, men de som kommer for sent vil få konsekvenser ved at de blir på mange måter kriminalisert. Dette kan føre til at man kan begynne å benytte programvaren til å overvåke andre ting også (Reinertsen, 2022).

4.2.2 Datatilsynets rolle

Datatilsynet ble opprettet i 1980, og har siden da vært et uavhengig forvaltningsorgan. Selv om det er et selvstendig forvaltningsorgan, er det administrativt underlagt Kongen og Kommunal- og distriktsdepartementet (KDD) (Personvernkommisjonen, 2022, s. 210). Direktøren av Datatilsynet blir utnevnt av Kongen i en periode på seks år. I tillegg er det 72 ansatte. De har plikt til å avlegge en årsrapport for Kongen og KDD hvert år. Datatilsynets rolle er å føre kontroller og tilsyn i forhold til om personvernet til innbyggerne blir ivaretatt og at lover og regelverk etterleves. Dette spesielt innenfor om personopplysninger blir behandlet som de skal. Dette gjelder spesielt innenfor personopplysningsloven, politiregisterloven, helseforskningsloven og SIS-loven (Schengen informasjonssystem). En annen oppgave er å passe på at enkeltpersoner ikke blir krenket ved at deres opplysninger blir innhentet og brukt til feil formål i forskjellige situasjoner. Andre oppgaver Datatilsynet har går på veiledning, gi informasjon, aktiv deltakelse i debatter om personvern og samarbeid med nasjonale og internasjonale myndigheter (Personvernkommisjonen, 2022, s. 211).

I forhold til personvernet er regelverket vi benytter oss av i Norge regulert av personvernforordningen som er et regelverk laget av Europarådet. Som et EØS-land, er vi pliktige til å følge disse reglene, samtidig som disse går inn under andre lover og regler vi har i landet i forhold til personvern. Denne skal tolkes likt mellom medlemslandene i EU. Dette fører til at det blir et samarbeid med andre nasjonale datatilsynsmyndigheter for å sikre at lovene og reglene tolkes og etterleves likt. Dette har mange fordeler med at man kan forholde seg til en myndighet istedenfor og måtte tolke og vurdere hva som er gjeldene lokalt, nasjonalt og internasjonalt (Personvernkommisjonen, 2022, s. 212).

På Datatilsynets hjemmesider vil man kunne finne jevnlig oppdateringer i forhold til lovverk, tolkninger, veiledninger og annen informasjon når det kommer til personvern. Siden regelverket er komplisert, med vage formuleringer, er vi som enkeltpersoner, virksomheter og lignende avhengig av at veiledningen og informasjonen som legges ut er forståelig, riktig og oppdatert (Personvernkommisjonen, 2022, s. 216). Dette skaper også en tillitt til organet i forhold til at man vet at det er en informasjonskilde man kan stole på er riktig. Dette også med tanke på at den største delen av befolkningen ikke har

kunnskapen om hva som er lovlig og ikke innenfor personvern. Det er også mangel på kunnskap i forhold til hvilke rettigheter man har for innsyn, sletting av informasjon også videre (Personvernkommisjonen, 2022, s. 210). Hovedfokuset ligger på personvern, og om det blir etterlevd av de forskjellige organene og virksomhetene som skal hente ut, eller benytte seg av personlige opplysninger om enkeltindivider. Det ligger mye ansvar på de som har ansvaret for behandlingen av disse opplysningene. Her trenger man god kunnskap, og man må holde seg oppdatert på hva som er regelverket. Spesielt med nye tekniske løsninger, må de forutse og forstå hva som kan være konsekvensene for det ene og det andre (Personvernkommisjonen, 2022, s. 209). Som Lintvedt er inne på, er det en stor og krevende prosess å kunne innføre AGT som hjelp til overvåkning i Norge. Selv om man skulle tro at når AGT blir en mer normalisert del av hverdagen, må man fortsatt ta hensyn til lover og regler lokalt, nasjonalt og internasjonalt. Man skal gi samtykke til at organisasjoner kan hente ut informasjon om en, og det får man ikke gjort om man skal hele tiden bli overvåket med AGT. En annen ting er også at om man overvåker med AGT i forskjellige områder, må det markeres tydelig i forhold til skilting. Dette av den grunn for at innbyggeren er klar over hva slags overvåkning som skjer i det området (Reinertsen, 2022).

I veiledningen til Datatilsynet om hva som er lov innenfor kameraovervåkning, kommer det tydelig fram at de som setter opp overvåkningen er fullt ansvarlige og må sette seg inn i reglene og overholde disse i forhold til lagring av data også videre FØR man setter opp kameraovervåkningen. Man har for eksempel lov til å overvåke eget hus og hage, men ikke trenge inn på noens private sfære. Man kan heller ikke publisere materialet, uten at de som er på videoen har samtykket til dette. Ute i det offentlige rom (gater, parker og lignende) er det KUN myndighetene som har mulighet til å overvåke. Kameraer som kan vise opptak i sanntid, er kun tillatt å benytte ved enkelte unntak. Om det ikke er en veldig spesiell grunn for å kunne streame opptaket i sanntid, skal overvåkning uten opptak benyttes. Her kommer problematikken rundt AGT inn, da den tar opptak og gjenkjenner folk i sanntid og kan følge deres handlinger. I veilederen kommer det fram strenge krav i forhold til at man må informere om at det skjer overvåkning i området. Opptakene skal slettes etter en gitt periode, som vanligvis er på rundt syv dager. Går det utover disse syv dagene, må det være et godt dokumentert grunnlag for dette. Vi som enkeltpersoner har krav på å få innsyn i dataene som er lagret

om oss på den filmen. Det mange ikke vet er at vi da kun har mulighet til å se det filmsnuttet som vi selv er i bildet, og ikke noe annet som kommer opp i videoen. Dette må det foreligge gode rutiner på hos virksomheten og hos politiet (Datatilsynet, 2022).

4.3 Etisk problematikk rundt ansiktsgjenkjenningsteknologien

For å kunne se på fordelene og ulempene med AGT, må man se på den etiske problematikken. I dette kapitlet vil jeg ta for meg hvilke kjølende effekter AGT kan ha, om det har hatt en påvirkning i forhold til kriminaliteten og til slutt vil jeg ta for meg problematikken i forhold til bias i AGT.

4.3.1 Kjølende effekter

Et punkt som har vært gjennomgående igjennom de fleste av teorimaterialet handler om «Chilling effects»/ «kjølende effekter», og hvordan dette er med å påvirke debatten rundt overvåkning. Ikke minst i forhold til AGT. Som nevnt i kapittel 3, handler dette om at vi endrer adferd når vi vet at vi blir overvåket. Noe man har sett AGT har tatt med seg, er at folk kan unngå å uttale seg offentlig om forskjellige saker, i frykt av at de kan bli straffet. Som regel foregår denne straffen for det meste med ydmykelse, man kan bli merket som en mulig kriminell av systemene, og bli mer forfulgt og overvåket av myndighetene. Dette selv om demonstrasjonen foregikk helt lovlig som en protest på en sak man bryr seg om (Lyon 2018, s. 66). I land som ikke er et liberalt demokratisk land blir dette sett på som et strengt lovbrudd, og det vil komme følger av en slik demonstrasjon. Med AGT kan de verifisere og identifisere menneskene, selv om de er i en stor gruppe. I Kina har de for eksempel utviklet AGT til å også gjenkjenne folk, selv om de har en maske på seg. (Pollard, 2020) Til og med FaceID på iPhone, kan man sette innstillingene slik at telefonen skal gjenkjenne deg selv med maske på (Apple.com, 2023). Selv om overvåkning i store deler av historien har vært en del av vestlige demokratiske land, har det i større grad blitt et våkesamfunn. Man vet at man blir overvåket, samtidig som man våker over andre og deres handlinger og bevegelser på sosiale medier. Overvåkningen skjer på forskjellige nivåer, alt fra markedsføring til juridiske myndigheter. I de senere årene kan man se at det har blitt flere «flytende» overganger i forhold til hvordan overvåkningsteknologien blir brukt (Lyon 2018, s. 132).

Selv om overvåkning kan ha en kjølende effekt ute i det offentlige rom, så har vi aldri delt så mye om våre liv som vi gjør nå på sosiale medier. På denne måten er det lettere for alle å kunne innhente informasjon om naboen, noen man gikk i klasse til, en person man har sterke følelser for også videre. Informasjonen ligger ute, og det tar ikke lang tid før man har innhentet masse informasjon om vedkommende. Hvis man tenker på hvor lett det er for den vanlige befolkningen å innhente slik informasjon, hvor lett er det da ikke for teknologien som har blitt trent opp til dette? Eller for tredjeparter å innhente informasjon de kjøper? Dette kan også være med på å skape en kjølende effekt, ved at vi faktisk ikke vet hva slags type data som blir innhentet av oss, og vi vet ikke hva den informasjonen blir brukt til.

Rett etter avsløringene til Edward Snowden i 2013, kunne man se en økning av at folk var mer bevisste på hva man søkte etter på internett. Flere dekket til kameraene sine for at myndighetene ikke skulle kunne se hva de gjorde i sine private hjem. Avsløringene fikk en stor WOW-effekt. Dessverre ser man ofte at denne wow-effekten forsvinner når det blir normalisert (Lyon 2018, s. 89). En ting man så fikk en kjølende effekt etter disse avsløringene, var at folk selvsensurerte seg mer i forhold til hva man la ut på sosiale medier, enn hva de hadde gjort tidligere. Spesielt gjaldt dette for journalister og forfattere. De sistnevnte kunne ikke lenger garantere for at samtalen med kilden forble bare mellom de to. Dette er noe som er med på å skade ytringsfriheten (Newth, 2014, s. 50).

En annen kjølende effekt med AGT, går på hvor lett det er å manipulere bilder av folk. Man kan for eksempel legge inn bilde av en persons ansikt over det originale bildet, eller videoen, og lage for eksempel deepfake-videoer (Lai & Rau, 2021, s. 1). Dette er noe man så spesielt tydelig i oppstarten av krigen i Ukraina, hvor Voldymyr Zelenskyj ble satt inn i en film, hvor han oppfordret befolkningen til å overgi seg til de russiske styrkene. Dette var selvfølgelig ikke sant, men det er interessant å se hva teknologien kan brukes til. Noe annet som er interessant er at mulighetene til å manipulere bilder og videoer er en relativt enkel prosess, og man må være litt oppmerksom for å se at videoen, eller bildet, ikke er ekte. Mange vil la seg lure, og på denne måten kan man lett få ut for eksempel konspirasjonsteorier. Det finnes mange apper som gjør denne prosessen enkel, og man trenger derfor ikke mye kunnskap for å kunne lage slike typer filmer. Dette gir

muligheten for at man kan for eksempel sette inn ansiktet til noen over det originale, og dermed plassere dem til en hendelse de ikke har vært med på. Dette er skremmende i forhold til om kriminelle miljøer også benytter seg av denne teknologien, til å plassere andre enn dem selv til å gjennomføre en kriminell handling. Eller om ekskjæresten er irritert på at forholdet tok slutt, og putter ansiktet til ekskjæresten på hodet til en pornostjerne, som igjen kan føre til ubehageligheter og store konsekvenser i ettertid i forhold til hva som dukker opp når man gjør et søk på vedkommende. Eller i verste fall kan man havne på overvåkningslista til politiet (Foer, 2018).

4.3.2 Kriminalitet vs. overvåkning

I de siste tiårene kan man se en økning av overvåkningskameraer, spesielt i de større byene. Betyr dette at kriminaliteten har gått ned? Eller har det ikke skjedd noen stor endring, selv med mange overvåkningskameraer? Og på hvilken måte kan bruken av AGT i overvåkning være polarisert?

Ifølge Piza et.al (2019) har økningen av overvåkningskameraer fått ned kriminaliteten ved enkelte områder. Dette gjelder spesielt for offentlige steder, som gater og parkeringsplasser. Det trenger fortsatt ikke å bety at kriminaliteten har gått ned, men at den har forflyttet seg til andre steder. I hovedgatene er det oftere flere politi, vektere og andre sikkerhetsforetak som patruljerer. Områder som er ofte rapportert inn som områder som er preget av kriminalitet, blir oftere patruljert. I garasjeanlegg og ved parkeringsplasser er det ofte flere ansatte som sitter og passer på området. Det er bedre opplyst i disse områdene, og dermed lettere for kameraene å kunne fange opp om det skulle skje noe kriminelt. Det kan dermed sies at det har blitt mindre kriminalitet i disse områdene (Piza et.al, 2019, s. 26). Man kan se at det varierer i forhold til hva slags kriminell handling som utføres. Ved for eksempel ran av enkeltpersoner, er de kriminelle veldig bevisst på hvor kameraene befinner seg. Ved ran av for eksempel butikker, er dette som regel en veldig nøye planlagt prosess. En type kriminalitet man ikke ser noen effekt av med kameraovervåkning er salg av narkotiske stoffer. Priks (2017) skriver at dette nok handler om at de i flere tilfeller er nokså ruset at de ikke er legger merke til overvåkningskameraene.

Piza et.al (2019) tar opp at kriminaliteten har gått ned ved private eiendommer, da flere har fått overvåkningsutstyr installert i sine egne hjem. Men når det kommer til voldshandlinger, kan man ikke se at de hjelper med overvåkningskameraer (Piza et.al, 2019, s. 30). Man kan se en mer effektiv overvåkning over kjente kriminelle områder ved at politiet har forskjellige «hot spots» de kan gå etter, og patruljere oftere, og ved hjelp av kameraene de har montert på vesten sin. Dette har blitt et vanlig fenomen i USA og UK, men ikke noe som blir brukt med i Norge.

Ifølge Flinterud et.al (2020) er debatten rundt overvåkning polarisert i Norge. Dette i forhold til at overvåkning har blitt normalisert i vår hverdag. Vi setter spor etter oss i sanntid, som kan hentes inn igjen i ettertid. Diskusjonene rundt overvåkningen går på hvor grensene er i forhold til å kunne overvåke enkeltpersoner eller kun kriminelle. Ifølge Flinterud et.al (2020) må de klassifiserte grensene defineres på nytt, da overvåkningen har blitt mer flytende enn hva den har vært tidligere (Flinterud et.al, 2020, s. 8). De ser derimot positivt på overvåkningsteknologien som et positivt tilskudd til politiet og andre etterretningstjenester i forhold til å kunne oppklare hendelser i ettertid (Flinterud et.al, 2020, s. 14). Diskusjonene har to motstridende oppfatninger, hvor den ene siden mener at man må ha mer overvåkning for at man skal føle seg tryggere. På den andre siden er parten som sier at man må ha mindre overvåkning, for at man skal kunne få beholde frihetsbevegelsen man har i liberale vestlige demokratier.

Et av argumentene for å ha stor grad med overvåkning ligger i at man skal forutse og avverge hendelser, spesielt med tanke på terrorisme. Med overvåkningsteknologi som AGT, er mulighetene større for å kunne karakterisere hvordan folk oppfører seg, og hvilke følelser vedkommende viser. Deretter analyserer algoritmen til å analysere om personen oppfører seg truende eller ikke (Robins, 2021, s. 89). Hva skjer da om man har en dårlig dag, og ikke er smilende? Blir man også da sett på som en kriminell? Det seneste eksemplet på hvor de har benyttet seg av denne teknologien var under Pride i Sidney tidligere i år. Dette ble argumentert for som et sikkerhetsgrep slik at politiet lettere skulle kunne gripe inn om det var noen hendelser som oppstod. Over 80000 personer møtte opp til priden, og det ville dermed være vanskelig for politiet å kunne holde full oversikt over forskjellige situasjoner om de ikke hadde kunne benytte seg av AGT i dette tilfellet (Colquhoun, 2023).

Noe av problemet med å kunne forutse og avverge terrorisme, er at terrorister er sjeldne og uforutsigbare. Siden terrorangrep skjer sjeldnere enn annen type kriminalitet, er datasettene små. Dette fører igjen til at mange uskyldige blant annet kan bli nektet adgang til forskjellige land, bare fordi de blir flagget i systemet som mistenkt. De som blir rekruttert som terrorister er som regel folk som er høyt motiverte og drevet av et ideologisk og kontroversielt syn på ting. Mange er som regel høyt utdannede folk. Dette gjør at de er flinke til å kunne legge komplekse planer i forhold til terrormålet og for å kunne unngå overvåkning (Newth, 2014, s. 101). Personlig vil jeg tro at selv om INTERPOL, PST og andre etterretningsgrupper overvåker potensielle kriminelle og farer for samfunnet, er det vanskeligere med terrorister. Dette med tanke på at en terrorhandling er vanskelig å forutse, da hensikten er at det skal skje raskt og uventet. De er flinke til å rekruttere folk til å gjennomføre handlingene. Man kan se at enkeltpersoner utfører forskjellige handlinger for å få innpass i de mer ekstremistiske miljøene. Dette er for eksempel terrorhandlingen Philip Maulthaus prøvde å utføre mot moskeen i Bærum etter at han hadde drept sin adopterte søster i 2019. Terrorhandlingene de senere årene i Paris, Berlin og andre steder kan virke som at har skjedd som en impulsiv handling, uten en annen hensikt enn å skape frykt. Dette med tanke på de terrorhandlingene som har blitt utført med blant annet lastebiler. Det man kanskje som enkeltindivid selv kan gjøre i forhold til terrorisme, er å oppfatte om personer plutselig har fått ekstreme holdninger til ting. Og deretter melde dette videre, slik at myndighetene kan gjøre en analyse på om hvilket trusselsbilde vedkommende kan være.

4.3.3 Bias i teknologien

Ved de fleste tilfeller er AGT en brukervennlig og genial teknologi i forhold til å identifisere folk raskt, enkel innlogging på ting også videre. Ved det første blotte øyet kan man si at den er uproblematisk, spesielt om du er en hvit mann i 40-50 årene, eller har et asiatisk opphav. Algoritmene er best trent på akkurat disse to typene i befolkningen. Med treffsikkerhet på 99,2 % kan man si at disse to typene ikke har noen problemer med AGT. Problemene oppstår mer for kvinner, og spesielt for mørkhudede kvinner. Her dropper treffsikkerheten med 34 %. Da er det med andre ord store muligheter for at man får falske positive resultater. Dette fører til feilverifisering, og

vedkommende kan bli identifisert som en person man ikke er. Dette kan komme av manglende bilder av mørkhudede da algoritmene ble trent opp (Robins, 2021, s. 91). Siden AGT kommer fra Asia har den blitt testet på flere millioner mennesker. Man skulle derfor tro at AGT var veldig godt utviklet og testet, siden den har blitt testet ut på såpass mange. Realiteten er at den har blitt testet mot en veldig homogen gruppe. Treffsikkerheten vil dermed gå ned i andre land med andre raser (Reinertsen, 2022). Ved at det er såpass store feilmarginer i systemet, er det vanskelig å kunne forstå hvordan vi blindt kan stole på at systemet har rett.

Ifølge Stewart Baker (2022) er disse algoritmene kun et verktøy som enten stemmer, eller ikke. Han mener at teknologien alltids kan forbedres, og at man kaller teknologien rasistisk mener han er feil. For at maskinene skal kunne lære, trenger de store datasett. Desto mer data man har, desto bedre blir treffsikkerheten. Siden minoriteten er i mindretall, mener han at det er logisk at utfallene blir dårligere for dem enn for majoriteten. Baker (2022) mener at den eneste løsninga på dette problemet, er å utvide treningssettene til maskinene. Et annet problem han tar opp som har påvirkning til at det blir feil treff, handler om hvordan bildet er tatt. Hva slags lyssetting bildet er tatt i har mye å si. Han mener at hvis bildet er tatt i dårlig lys, blir det vanskeligere for algoritmene å avlese kodene og korrekturene i ansiktene til folk. Dette gjelder spesielt for mørkhudede folk. Teknologien er i frammarsj, og den har utviklet seg mye de senere årene. Baker (2022) mener at treffsikkerheten til AGT har blitt bedre, ved at man har utviklet algoritmene, og at man har blitt mer bevisst på lyssettingen. Selv om det ikke er i alle tilfeller man kan benytte bilder med god lyssetting, vil ikke dette si at algoritmene er rasistiske. Han mener videre at om man får opp et feilvarsel av AGT, så må mennesker som skal sjekke opp identiteten stille spørsmål og dobbeltsjekke informasjonen om de er i tvil. AGT er et verktøy som er i stor framvekst, og som bare blir bedre. Den blir enda bedre om man tar de grepene Baker (2022) snakker om ved å øke datasettene på minoriteten og bruke god lyssetting (Baker, 2022). Men er det virkelig så enkelt?

Isabella Grabski (2020) mener at bias oppstår da datasettene er preget av valgene som ble tatt da man skulle lære opp maskinene. Utgangspunktet for denne opplæringen av maskiner baserer seg på våre egne fordommer. Bevisste og ubevisste valg som kan føre til at en gruppe blir mindre representert. Hun mener at dataene som maskinene

opplæres av vil alltid være påvirket av eksisterende diskriminering i samfunnet vi har sett igjennom historien. Hun mener at den eneste måten man kan utbedre bias på er at man må identifisere hva som ligger i rettferdighet. Uansett hvilken side man ser det fra, vil det alltid være urettferdig for en gruppe. Det må derfor til en klarlegging i hva som ligger i rettferdighet, og når man eventuelt oppnår dette. Hun mener at det blir problematisk med bruk av AGT i forhold til at den skal bedømme om folk er sånn eller sånn. Hun tar opp det samme eksempelet som Coeckelbergh (2020) med COMPAS, som retten i USA benyttet seg av for at den skulle hvor sannsynlig det var at den tiltalte vil begå en kriminell handling igjen i framtiden. Denne har vist seg at den har dobbelt så mange feilføringer på mørkhudede enn på hvite kriminelle. Dette skaper en stor urettferdighet, og kan utgjøre store konsekvenser for den enkelte tiltalte (Grabski, 2020).

Sidney Perkowitz (2021) kommer med flere eksempler på personer som har blitt anholdt og feildømt på grunn av feil match i algoritmene. Dette gjelder blant annet for Robert Williams, Nijeer Parks og Michael Oliver. Alle mørkhudede menn som har blitt anhold og anklaget for noe de ikke har gjort, bare ved at det ble en falsk positiv match. Om man har tidligere dommer på seg, uansett hvor gamle de er, vil disse personene som blir anklaget alltid bli dømt av systemet som en kriminell. Det er derfor viktig at man sjekker opp mer rundt hendelsene og samler inn informasjon som man kan sammenligne grunnlaget med. Dette er alt i fra vitneutsagn, sammenligne rettsmedisinsk bevis fra åstedet med annen informasjon man har innhentet i de forskjellige sakene. Perkowitz (2021) tar videre opp at det er to spesifikke utfordringer vi står ovenfor med AGT. Det ene er at det må lages algoritmer som har høy treffprosent i forhold til å kunne identifisere individer uansett hvilken rase, etnisitet, kjønn og forskjellige aldersgrupper vedkommende er i. Den andre utfordringa er å innføre denne teknologien inn i den virkelige verdens teknologi og systemer, som brukes av for eksempel politi og andre myndigheter. Disse systemene er allerede preget av lengre historie med systematiske ulikheter, og det kan dermed bli en stor utfordring å få oppdatert alle systemene til å kunne gjelde for alle. Petrowitz (2021) tar videre opp at datasettene er basert på et demografisk bias. På den ene siden er det for liten datamengde av ikke-hvite i databasen, slik at systemene kan brukes på en rettferdig måte. På en annen side er det større database på bilder av mørkhudede kriminelle enn hva det er av hvite. Dette skaper

større rasistiske utfordringer. Konsekvensene kan også være store for de som blir tatt for å være en annen person enn hvem de er (Perkowitz, 2021).

Mark Coeckelbergh (2020) tar opp utfordringer som dukker opp i forhold til bias ved bruk av AGT til å analysere jobbsøknader til spesifikke jobber. Flere kvinner som søkte ble ikke tatt med til intervju, ved at det lå inne i algoritmene at det skulle være mannlige sjefer. Oftest er bias utilsiktet. Disse feilene kan komme av at man ikke forstår systemet godt nok, eller er klar over egne bias. Man tenker heller ikke alltid over hva som kan være konsekvensene når man har slått igjennom med bruk av et system (Coeckelbergh, 2020, s. 125). Konsekvensene for de som faller utenfor en gitt kategori, kan være fatale. Man kan for eksempel ikke få jobb, eller muligheten til å ta opp lån. Man kan ende opp i fengsel, eller man kan oppleve voldshandlinger mot seg selv på grunn av bias i systemene. Man kan også risikere å få høyrisikostatus i forhold til sikkerheten i et område man bor i. Coeckelbergh (2020) tar videre opp problematikken rundt politiet i USAs bruk av PredPol. Dette systemet skal forutse om det skjer en kriminell handling i et gitt område, og anbefaler ut ifra disse algoritmene hvor politiet bør patruljere. Dette er steder hvor politiet har lagt inn i systemet at det er mange hendelser, og det er som regel steder hvor majoriteten er fattige og de fleste er en minoriteters gruppe. Dette er med på å bryte ned tillitten til politiet, da man uansett blir sett på som en kriminell bare ved å bo i området (Coeckelbergh, 2020, s. 127—128). Mye av problematikken rundt bias, er at man benytter datasett som ikke er representative, og baserer seg kun på en gruppe. Disse datasettene blir fortsatt brukt til å forutse hendelser for hele befolkningen. Hvordan kan man forsvare denne bruken da det blir store feilføringer for de som ikke passer inn i den enkelte gruppen? Når det er en homogen gruppe som jobber med datasettene og algoritmene, er det deres meninger og holdninger som blir hørt i systemet. Kvinner, funksjonshemmede, eldre, fargede og personer fra utviklingsland vil dermed falle utenfor de datasettene som benyttes. Det kan oppstå en del konsekvenser for disse ved at de blir sammenlignet med en database som ikke passer for dem (Coeckelbergh, 2020, s. 129). Coeckelbergh tar opp at det er mye som kan gjøres i forhold til å minske bias, men at bias i seg selv nok aldri vil forsvinne. Dette med tanke på at vi har alle forskjellige syn og tanker på hva som er bias og ikke (Coeckelbergh, 2020, s. 131).

5.0 Avslutning og konklusjon

Det er mange fordeler og ulemper med AGT. Jeg vil i dette kapitlet reflektere rundt argumentene i det foregående kapitlet. Jeg vil også komme med en konklusjon til masteroppgavens problemstilling: «*Hva er fordelene og ulempene med ansiktsgjenkjenningsteknologien*». Først vil jeg kort oppsummere slik jeg ser fordelene og ulempene med AGT i de forskjellige emnene jeg drøftet i forrige kapittel. Jeg vil også argumentere for disse i forhold til et utilitaristisk rammeverk.

Selv om utilitarismen ikke kan kombineres med individuelle rettigheter, siden handlinger en enkeltperson gjør ikke kan ofres for det beste for fellesskapet, har rettigheter og personvern hatt en sentral rolle i drøftingen. Dette av den grunn at det i dette tilfelle kan anses som å være til det beste for samfunnet i en helhet. Man skal ikke skade andre ved at man infiltrerer med folks privatliv og deretter krenker dem med funnene. Det at hver enkelt borger har en skjermet frihet og toleranse for moralske grenser øker velferden i samfunnet. På dette grunnlaget har tematikken «privatliv og personvern» en stor rolle i denne oppgaven. GDPR er et lovverk som har en positiv kraft når det kommer til privatliv og personvern. Den stiller strenge krav og reguleringer på hva slags type informasjon som skal innhentes. Det er krav om blant annet at informasjonen må være legal, legitim og nødvendig for det enkeltes formål. Det vil si at vår informasjon er beskyttet på en god måte, da det er restriksjoner for å hente ut informasjon. Det er kun politiet som har myndighet til å innhente informasjon ved bruk av AGT. Dette gir folk mulighet til å kunne velge hva slags informasjon om seg selv de ønsker at andre skal vite om og ikke. Bruken av AGT er styrt av mange lover og regler, og det blir derfor vanskeligere å kunne misbruke teknologien.

I forhold til ulempene med AGT og privatliv/personvern, kan man se at GDPR har enkelte svakheter. Blant annet praktiseres lover og regler forskjellig fra land til land. GDPR gjelder kun i den Europeiske Unionen, og det er derfor ingen problemer for en tredjepart utenfor EU å kjøpe og selge informasjonen til enkeltpersoner som benytter seg av sosiale medier. Loven klarer ikke å holde tritt med teknologien, og da blir det vanskeligere å kunne oppbevare opplysningene på en sikker måte. GDPR har noen smutthull i forhold til at det er kun politiet som kan benytte AGT til å innhente informasjon. Det finnes ingen reguleringer på at privatpersoner ikke kan innhente

informasjon til personlig bruk. Med dette kan de blant annet identifisere en tilfeldig person de har møtt på gata.

Ut ifra det jeg kan se, har Datatilsynet positive innvirkninger på folks privatliv og personvern. De fører kontroller og tilsyn i forhold til om personvernet blir ivaretatt. De gir også ut oppdaterte veiledninger, er aktive i debatter rundt personvern, gir ut nyttig og oppdatert informasjon og samarbeider med nasjonale og internasjonale myndigheter. Dette er med på å sikre at personvernet blir ivaretatt i alle land innenfor Europarådet, og enkeltpersonene kan forholde seg til informasjonen til et land. Da slipper man å måtte sette seg inn i reglementet til andre land, siden de skal være de samme i Europa. Vi som borgere får en større tillitt til informasjonen de legger ut, da den er mer brukervennlig og oppdatert.

I forhold til kjølende effekter er det vanskelig å kunne argumentere for noen fordeler. Ulempene er det derimot flere av. Noe som har en negativ effekt er at folk unngår å uttale seg offentlig, ved at de er redde for å bli straffet. Disse straffene går ofte ut på ydmykelser, men kan også være med på å stemple folk som angivelig kriminelle. Om myndighetene følger med på oss under for eksempel demonstrasjoner, vet vi ikke hva slags informasjon de har mulighet til å innhente om oss. Selv om store avsløringer har gjort folk mer vare på det som innhentes av informasjon, er det fortsatt mange som går tilbake og blir naive da wow-effekten har lagt seg etter en stund. En annen ting er at flere driver med selvsensurering. Det at folk ikke våger å si hva de egentlig mener er med på å skade demokratiet og ikke minst ytringsfriheten. Folk er redde for å måtte oppleve hets, deepfake-videoer eller å havne på lista til politiet som en mulig kriminell.

Når det kommer til kriminalitet og overvåkning, ser man at kriminaliteten har gått ned på flere områder. Dette gjelder spesielt på offentlige steder. Man kan også se at kriminaliteten i private hjem har gått ned de stedene overvåkningskameraer har blitt montert opp. Politiet har hatt mange fordeler ved å benytte seg av teknologien for å oppklare hendelser i ettertid. Med teknologi som kan karakterisere folks oppførsel og følelser er med på å avverge enkelte kriminelle handlinger. Ulempene med kriminalitet og overvåkning går på at i flere områder har det ikke blitt mindre kriminalitet, men at den har forflyttet seg. Man kan se at de kriminelle har blitt mer kreative i sine

handlinger, og at de planlegger bedre. Det blir mer utfordrende å kunne avverge mulige handlinger. Siden de også har blitt mer bevisste på hvor kameraene står, kan det bli vanskelig å kunne identifisere den kriminelle i politiets etterarbeid. Selv med mange overvåkningskameraer, har ikke dette hatt noen innvirkning på voldshandlinger. Det er også vanskelig å kunne forutse eventuelle terrorhandlinger, da de er sjeldne og uforutsigbare. Flere har opplevd at de har blitt markert som en mulig mistenkt.

Når det kommer til bias, ligger det i navnet at det ikke er mange fordeler innenfor dette området. Feil og mangler er et stort problem når det kommer til å benytte AGT. Man kan for eksempel få 34% dårligere treffprosent på mørkhudede kvinner, enn hva man kan få på en hvit middelaldrende mann. Selv om majoriteten av befolkningen ikke har noe problem med teknologien, og at algoritmene kan trenes opp til å få bedre treffprosent, er fortsatt datasettene preget av valgene som ble tatt da maskinene skulle læres opp. Historisk sett har disse valgene blitt basert på egne bevisste eller bevisste fordommer mot spesielt mørkhudede folk. Dette er med på å skape mer diskriminering ved at en gruppe blir mindre representert enn andre. Falske-positive resultater har ført til at flere har blitt arrestert for en handling, som det viser seg at de ikke har begått. Alt dette bare fordi det var en tilnærmet lik match. Et annet problem er demografiske bias. Datamengden for ikke-hvite er relativt små, men det er en større database på mørkhudede som kriminelle. Denne databasen går ikke kun på lovbrudd, men også arrestasjoner. Politiet registrerer arrestasjonene inn i systemene, og områdene disse arrestasjonene skjer blir merket av som et område man må være ekstra på vakt ved. Bare det faktum at man bor i området, gjør at man er ekstra var på om vedkommende kan være en angivelig kriminell. Dette er mye av den underliggende problematikken ved å benytte slike systemer. Mye av hovedproblemet ved bias går på at det ikke er representative datasett, når datasettene kun baserer seg på en homogen gruppe. På mange måter kan man si at bias aldri vil forsvinne, da det er forskjellige syn og tanker på hva bias er.

Teknologien har kommet for å bli, og er under en stadig utvikling. Det er det ingen tvil om. Mange diskuterer i dag om man bør forby AGT. Personlig tenker jeg at fordelene med å benytte teknologien veier høyere enn hva ulempene er. Det handler på mange måter om hvordan man benytter seg av denne teknologien og hvem som kan benytte

den. Ved et eventuelt totalforbud, ser jeg for meg at vi vil miste mange tekniske løsninger og muligheter vi har blitt avhengige av i hverdagen vår. Mye av dette allerede har blitt en såpass vanlig del av hverdagen vår at vi ikke lenger tenker over den. Jeg tenker at lover og regler må være oppdaterte i forhold til utviklingen av teknologien, og at det ikke kan være fritt vilt å bruke den. Det må være klare retningslinjer som beskytter både personvernet vårt og samfunnet i en helhet. Noe av hovedproblemet er at loven ikke klarer å holde tritt med utviklinga av teknologien. Det kan få større følger i ettertid, om de tekniske løsningene går utover det lovverket forteller. En annen ting jeg tenker på som en viktig del av utviklingen av AGT, er at informasjonen algoritmene innhenter, må alltid bli verifisert av mennesker. Dette for å sikre at det stemmer 100 %, og at man på denne måten slipper de eksemplene hvor feil person har blitt anholdt for en kriminell handling.

De største ulempene går på dette med bias og kjølende effekter. For at bruken av AGT skal være optimal, må det skje en stor utbedring av disse. Når det kommer til bias, er det fortsatt en lang vei å gå når det gjelder å utbedre teknologien og trene opp maskinene på nytt til å få en bedre treffprosent på alle typer hudfarger. Til nå har det vært en relativt homogen gruppe som har jobbet med opplæringsmaterialene til maskinene, og dette skaper forskjeller. For å fange opp disse utelatte gruppene er det viktig at man har nok materiale for alle grupper å trene opp maskinene og algoritmene med, men det er også viktig at disse gruppene er representert blant de som jobber med denne opptreningen. På denne måten kan jeg tenke meg at bias vil bli mindre, for det er flere grupper av mennesker som ser hva som eventuelt mangler. Vi har et historisk perspektiv som vi må lære av, for at vi skal kunne forbedre oss i framtiden og for at diskrimineringen av minoritetsgruppene i kategoriseringen ikke får så stor plass innenfor teknologien. I forhold til de kjølende effektene som dukker opp ved bruk av denne teknologien, er det viktig at det arbeides for at folks ytringsfrihet ikke står på spill. Man skal ikke bli straffet fordi man har demonstrert lovlig og ytret sine meninger. Med AGT kan man misbruke informasjonen som blir innhentet, og demonstrantene kan for eksempel bli stemplet som farlige kriminelle. For vestlige liberale demokratier har det vært en viktig sak at man ikke skal bli som Kina, og deres overvåkningsregime. Veien kan bli kort dit, om man begynner å misbruke teknologien til å stoppe ytringene til befolkningen. I et utilitaristisk rammeverk handler det om å ikke straffe hardere enn nødvendig. Straff er smerte og bør

unngås. Samfunnet er bygget opp på dette aspektet at hvis noen gjør noe ulovlig skal straffen være streng nok til at man ikke vil gjenta den ulovlige handlingen. Straffen kan også være et virkemiddel for at folk velger den beste handlinga som ikke er ulovlig. Dette ser man igjen i straffeloven i Norge. Man skal styre atferd inn i fremtiden. Man skal handle ut ifra det som er det beste for alle, og som gir mest mulig velferd. Da kan man ikke ha en heksejakt av folk som ytrer sine meninger, ved å bruke teknologien imot dem. Det er bare fantasien som kan sette en stopper på hvordan man kan utvikle teknologien i årene framover. Men jeg tror det er nødvendig at folk setter seg inn i hva teknologien faktisk gjør, og at man fortsetter å forske på feltet på hva som egentlig er konsekvensene med bruken av teknologien, og hva som kan skje når den blir misbrukt. For folk flest handler det om å kunne bruke sunn fornuft på hva som bør deles på sosiale medier og kanskje lese seg litt opp på hva de forskjellige sosiale mediene egentlig innebærer, og hva man faktisk godtar med deres gitte vilkår.

Kilder

Alexandrie, G. (2017). Surveillance cameras and crime: A review of randomized an natural ecperiments. Hentet 09.03.23 fra *Säkerhet för Näringsliv och Samhälle*: https://www.securityuser.com/snos/pdf/Surveillance_cameras_and_crime_Authors_accepted_manuscript.pdf

Almeida, D., Shmarko , K., & Lomas, E. (2021). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*, 377-387. Hentet 23.01.23 fra *Springer link:* https://link.springer.com/article/10.1007/s43681-021-00077-w

Alnes, J. H. (2020). Hermeneutik. Hentet 03.02.23 fra *Store norske leksikon*: https://snl.no/hermeneutikk

Apple.com. (2023). Support. Hentet 05.04.23 fra apple.com: https://support.apple.com/en-us/HT213062

Baker, S. (2022, Februar 02). The Flawed Claims About Bias in Facial Recognition. Hentet 15.01.23 fra *Lawfare*: https://www.lawfareblog.com/flawed-claims-about-bias-facial-recognition

Bu, Q. (2021, april 07). The global governance on automated facial recognition (AFR): ethical and legal opportunities and privacy challenges. Hentet 06.01.23 fra *SpringerLink-International Cybersecurity Law Review*: https://link.springer.com/article/10.1365/s43439-021-00022-x

Carson, S. G., & Kosberg, N. (2022). *Etikk - teori og praksis.* Oslo: Cappelen Damm.

Coeckelbergh, M. (2020). *AI Ethics.* Cambridge, London: The MIT press.

Colquhoun, L. (2023, februar 28). Crowd Surveillance Poses a Data Dilemma. Hentet 28.03.23 fra *CDOtrends Digital & Data insight for Business Leaders*: https://www.cdotrends.com/story/17893/crowd-surveillance-poses-data-dilemma?refresh=auto

Crawford, K. (2021). *Atlas of AI.* London: Yale university press.

Datatilsynet. (2021). Datatilsynets strategi - hva er personvern. Hentet 05.04.23 fra *Datatilsynet*: https://www.datatilsynet.no/om-datatilsynet/planer/datatilsynets-strategi/hva-er-personvern/

Datatilsynet. (2022, Januar 19). Kameraovervåkning - hva er lov? Hentet 28.01.23 fra *Datatilsynet.no*: https://www.datatilsynet.no/personvern-pa-ulike-omrader/overvaking-og-sporing/kameraovervaking/

DeCew, J. (2018, januar 18). Privacy. Hentet 15.01.23 fra *Stanford Encyclopedia of Philosophy Archive:* https://plato.stanford.edu/archives/spr2018/entries/privacy/

Difference between. (2012). Difference Between Consequentialism and Utilitarianism. Hentet 03.03.23 fra *Differencebetween.com*: https://www.differencebetween.com/difference-between-consequentialism-and-vs-utilitarianism/#:~:text=Utilitarianism%20combines%20the%20aspects%20of%20hedonism%20and%20consequentialism.&text=While%20the%20greatest%20good%20alone,the%20greatest%20number%20o

Dripke, A., & Miksch, M. (2021). *STASI 2.0: Wie wir durch den staatlich-industriellen Digitalkomplex zu gläsernen Bürgern werden und was das für unsere Zukunft bedeutet .* Norderstedt: Diplomatic council publishing.

European court of human rights. (2013). European Convention on Human Rights. Hentet 21.01.23 fra European court of human rights: https://www.echr.coe.int/documents/convention_eng.pdf

European Parliament . (2021, September). Regulating facial recognition in the EU. Hentet 21.01.23 fra *European Parlamentary Research Service*: https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf

Facebook. (2023). Terms of Service. Hentet 10.04.23 fra *Facebook*: https://www.facebook.com/legal/terms

Feldstein, S. (2021, september). The Global Expansion of AI Surveillance. Hentet 15.01.23 fra *Carnegie - Endowment for international peace*: https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf

Flinterud, G., Strype, J., & Lomell, H. M. (2020). Bak den norske overvåkningsdebatten. *Norsk statsvitenskapelig tidsskrift*, pp. 4-21.

Foer, F. (2018, mai). The Era of Fake Video Begins. Hentet 04.04.23 fra *The Atlantic:* https://www.theatlantic.com/magazine/archive/2018/05/realitys-end/556877/

Gieseke, J. (2011). *Die Stasi - 1945-1989.* München: Pantheon.

Grabski, I. (2020, januar 28). Fairness in Machine Learning. Hentet 20.03.23 fra *Harvard University:* https://sitn.hms.harvard.edu/uncategorized/2020/fairness-machine-learning/

Greenwald, G. (2014). *Edward Snowden, NSA og overvåkningsstaten.* Oslo: Cappelen Damm.

Hansson, S. O. (2017). Theories and Methods for the Ethics of Technology. I S. O. Hansson, *The Ethics of Technology - Methods and Approaches* (pp. 1-14). London: Rowman & Littlefield International, Ltd.

Harding, L. (2014). *Snowden-filene: historien om verdens mest ettersøkte mann.* Oslo: Forlaget press.

Hartzog, W. (2018, august 02). Facial Recognition Is the Perfect Tool for Oppression. Hentet 17.01.23 fra *Medium.com*: https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66

Kantayya, S. (Director). (2020). *Coded Bias* [Film].

Lai, X., & Rau, P.-L. P. (2021, mai 07). Has facial recognition technology been misused? A public perception model of facial recognition scenarios. Hentet 29.01.23 fra *ScienceDirect - Computers in Human Behavior:* https://www.sciencedirect.com/science/article/abs/pii/S074756322100217X

Louvet, S. (Director). (2018). *The World Under Surveillance* [Film].

Lyon, D. (2015). *Surveillance after Snowden.* Cambridge: Polity.

Lyon, D. (2018). *the Culture of Surveillance: Watching as a Way of life.* Cambridge: Polity.

Macnish, K. (2018). *The etichs of surveillance - an introduction.* New York: Routledge.

Najibi, A. (2020, oktober 24). Racial Discrimination in Face Recognition Technology. Hentet 05.02.23 fra *Harvard University*: https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

NEC. (2022). A brief history of Facial Recognition. Hentet 03.02.23 fra *NEC - Orchestrating a brighter world*: https://www.nec.co.nz/market-leadership/publications-media/a-brief-history-of-facial-recognition/

Newth, E. (2014). *Overvåkningssamfunnet.* Oslo: Humanist forlag.

NTB. (2012, desember 15). Tilbyr selvbetjent passkontroll. Hentet 20.01.23 fra *E24*: https://e24.no/naeringsliv/i/bK194g/tilbyr-selvbetjent-passkontroll

Nyreng, F. (1999). *Etiske teorier - en systematisk fremstilling av syv etiske teoriretninger.* Bergen: Fagbokforlaget.

Orlowski, J. (Director). (2020). *The Social Dilemma* [Film].

Perkowitz, S. (2021, februar 06). The Bias in the Machine: Facial Recognition Technology and Racial Disparties. Hentet 10.01.23 *MIT Schwarzman College of Computing*: https://mit-serc.pubpub.org/pub/bias-in-machine/release/1

Personopplysningsloven. (2016, april 27). *Lov om behandling av personopplysninger (2016/679)*. Retrieved from Lovdata: https://lovdata.no/lov/2018-06-15-38/gdpr/a5

Personvernkommisjonen. (2022). Ditt personvern - vårt felles ansvar. Tid for en personvernpolitikk. Hentet 23.03.23 fra *Regjeringen.no*: - https://www.regjeringen.no/contentassets/e4c60a6c51b147628b2c2e55db7e08e3/no/pdfs/nou202220220011000dddpdfs.pdf

Piza, E. L., Welsh, B. C., Farrington, D. P., & Thomas, A. L. (2019). CCTV surveillance for crime prevention. A 40-year systematic review with meta-analysis. Hentet 15.03.23 fra *City University of New York Academic Works*: https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1275&context=jj_pubs

Pollard, M. (2020, mars 09). Even mask-wearers can be ID´d, China facial recognition firm says. Hentet 06.04.23 fra *Reuters:* https://www.reuters.com/article/us-health-coronavirus-facial-recognition-idUSKBN20W0WL

Priks, M. (2015). The effects of surveillance cameras on crime: Evidence from the Stockholm subway. *Economic Journal*, pp. 289-305.

Raab, C. D. (2013, oktober 11). Privacy as a Security Value. Hentet 14.01.23 fra *SSRN:* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3057433

Rauenzahn, B., Chung, J., & Kaufman, A. (2021, mars 20). Facing Bias in Facial Recognition Technology. Hentet 07.02.23 fra *The Regulatory Review*: https://www.theregreview.org/2021/03/20/saturday-seminar-facing-bias-in-facial-recognition-technology/

Rössler, B. (2005). *The value of privacy.* Malden: Polity press.

Reinertsen, M. (2022, mars 23). §91 Ansiktsgjenkjenning. Hentet 06.03.23 fra [Audio-podkast-episode 91] *Jusspodden*: https://pod.space/erdetlov/91-ansiktsgjenkjenning

Robins, S. (2021). Facial Recognition for Counter-Terrorism: Neither a Ban Nor a free-for-all. In A. Henschke, A. Reed, S. Robbins, & S. Miller, *Counter-Terrorism, Ethics and Technology-Emerging Challanges at the Frontiers of Counter-Terrorism* (pp. 89-104). Cham, Sveits: Springer.

Rosenzweig, P. (2021, februar 24). Germany´s Surveillance System in the Nazi Era. Hentet 28.03.23 fra *Wondrium Daily*: https://www.wondriumdaily.com/germanys-surveillance-system-in-the-nazi-era/

Sagdahl, M. S. (2021, juli 01). *Utilitarismen*. Hentet 29.04.23 fra *Store norske leksikon*: https://snl.no/utilitarisme

Sarabdeen, J. (2022, mars 08). Protection of the rights of the individual when using facial recognition technology. Hentet 18.02.23 fra *ScienceDirect - Heliyon Volume 8*: https://www.sciencedirect.com/science/article/pii/S2405844022003747

Saugstad, J. (2005). Normativ etikk. In P. Ariansen, I. Bostad, S. Mathisen, & Ø. Rabbås, *Exphil 2, Tekster i etikk* (pp. 39-42). Oslo: Universitetet i Oslo.

Selinger, E., & Hartzog, W. (2020, mars 19). The Inconsentability of Facial Surveillance. Hentet 24.01.23 fra *SSRN*: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3557508

Selinger, E., & Leong, B. (2021, februar 07). The Ethics of Facial Recognition Technology. Hentet 24.01.23 fra *SSRN*: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3762185

Smith, M., & Miller, S. (2021, april 13). The ethical application of biometric facial recognition technology. Hentet 22.01.23 fra *SpringerLink - AI & Society 37, s167-175*: https://link.springer.com/article/10.1007/s00146-021-01199-9

Snapchat. (2021). Snap Inc. Tjenestevilkår. Hentet 10.04.23 fra Snap.com: https://snap.com/nb-NO/terms

Snowden, E. J. (2019). *Permanent Record.* London: Henry Holt and Company.

Strauß, S. (2017). Privacy Analysis - Privacy Impact Assesment. I S. O. Hansson, *The Ethics of Technology - Methods and Approaches* (pp. 143-156). London: Rowman & Littlefield international.

Tennøe, T., Johannessen, A. F., & Barland, M. (2020). Ansiktsgjenkjenning og personvern. Hentet 23.04.23 fra *Teknologirådet*: https://cdn.innocode.digital/teknologiradet/uploads/2020/02/RTT-ansiktsgjenkjenning_m-lenker-mars.pdf

Thales. (n.d.). Facial recognition history. Hentet 10.02.23 fra *Thales - Building a future we can all trust*: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/history-of-facial-recognition#:~:text=Facial%20recognition%20is%20more%20than,computer%20was%20to%20find%20matches

Thierer, A. (2019, mai 17). The Great Facial Recognition Technopanic of 2019. Hentet 24.01.23 fra *Mercatus Center:* https://www.mercatus.org/economic-insights/expert-commentary/great-facial-recognition-technopanic-2019

United States Holocaus Memorial Museum. (n.d.). Holocaust Encyclopedia. Hentet 01.05.23 fra *United States Holocaus Memorial Museum*: https://encyclopedia.ushmm.org/content/en/article/nazi-racism-an-overview

Verbeek, P.-P. (2011). *Moralizing Technology- Understanding and Designing the Morality of Things.* Chicago/London: The University of Chigago.

Wang, M., & Chen, W. (2022, desember 02). Regulating the use of facial recognition technology across borders: A comparative case analysis of the European Union, the United States, and China. Hentet 24.02.23 fra *ScienceDirect - Telecommunications Policy Volume 47, Issue 2:* https://www.sciencedirect.com/science/article/abs/pii/S0308596122001847