Politiets bruk av ansiktsgjenkjenningsteknologi i kriminalitetsbekjempende virksomhet

Lovhjemmel og forholdsmessighet

Kandidatnummer: 134

Antall ord: 13944

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

20. desember 2020

Innholdsfortegnelse

Innholdsfortegnelse 2
1 Innledning 4
1.1 Tema 4
1.2 En ny teknologi? 5
1.3 Problemstillinger og aktualitet 8
1.4 Avgrensninger 9
1.5 Rettskildebildet og metodiske utfordringer 10
1.6 Oppgavens videre gang 11
2 Retten til «privatliv» etter Grunnloven § 102 og EMK artikkel 8 12
2.1 Innledning 12
2.2 Er bruk av ansiktsgjenkjenningsteknologi et «inngrep» i privatlivet? 12
2.3 Vilkår ved inngrep i privatlivet 15
2.3.1 Lovhjemmelskravet 15
2.3.2 Formålskravet 15
2.3.3 Forholdsmessighetskravet 16
3 Politiets fotoregister som referansegrunnlag 17
4 Rettsgrunnlaget for bruk av ansiktsgjenkjenning 21
4.1 Innhenting etter politiloven § 6 a 21
4.2 Forbehandling av opplysningene etter politiregisterloven § 8 22
4.3 Treff (matching) 24
4.3.1 Innledning 24
4.3.2 Formålskravet i politiregisterloven § 4 25
4.3.3 Nødvendighetskravet i politiregisterloven §§ 5 og 7 26
4.3.4 Kvalitetskravet i politiregisterloven § 6 29
4.4 Konklusjon 33
5 Er ansiktsgjenkjenning etter dagens lovregler forholdsmessig i lys av Grunnloven § 102 og EMK artikkel 8? 34
5.1 Innledning 34
5.2 Er lovgivers vurderinger «relevante og tilstrekkelige»? 35
5.3 Gir reglene «effektiv beskyttelse mot misbruk av opplysningene»? 36
5.4 Lagringsreglenes forholdsmessighet 39
5.4.1 EMDs vurderinger i *Gaughran mot Storbritannia* 39
5.4.2 Er de norske lagringsreglene forholdsmessige i lys av kravene i Grunnloven § 102 og EMK artikkel 8? 40

5.4.3 Lagringsadgangens forhold til formålskravet – uttalelser i *Gaughran mot Storbritannia* 43
6 Oppsummering 45
Litteraturliste 46

1 Innledning

1.1 Tema

«Kunstig intelligens» defineres av *Store norske leksikon* som «informasjonsteknologi som justerer sin egen aktivitet og derfor tilsynelatende fremstår som intelligent».[1] Kunstig intelligens har blant annet muliggjort automatisk ansiktsgjenkjenning. Denne teknologiformen har utviklet seg raskt, særlig de siste ti årene. Teknologien kan brukes til flere formål, for eksempel for å låse opp mobiltelefoner, som betalingsmiddel[2] og i passkontroller. Den brukes også i politiets kriminalitetsbekjempelse, og i politiarbeid i stadig flere land. Politiets bruk av ansiktsgjenkjenningsteknologi er delvis kontroversiell og gjenstand for utprøving og grensedragning. I denne oppgaven skal jeg ta opp spørsmål knyttet til politiets bruk av ansiktsgjenkjenningsteknologi i kriminalitetsbekjempelsen. Teknologien muliggjør identifikasjon av personer ved bruk av personers ansiktstrekk, algoritmer og et sammenligningsgrunnlag som består av fotografier.[3]

Så vidt jeg har kunnet bringe på det rene, er det i norsk politiarbeid i dag bare Kripos som bruker ansiktsgjenkjenningsteknologi. Bruken er begrenset til utelukkende å gjelde identifikasjon av personer som er registrert i sporregisteret. Sporregisteret er en del av fotoregisteret, og gir politiet anledning til å registrere opplysninger om personer med «ukjent identitet» når opplysningene «antas å ha tilknytning til uoppklart straffesak», se politiregisterforskriften § 46-5 fjerde ledd.[4] Kripos kan bruke foto som er sikret i forbindelse med etterforskning som grunnlag for sammenligning med foto som finnes sporregisteret. Bildet som skal sammenlignes med sporregisteret, kalles «sporfoto». Ved treff i systemet vil eksperter på ansiktssammenligning sammenlikne fotoene og vurdere kvaliteten på den automatiske gjenkjenningen.[5] Ansiktsgjenkjenning kan utnytte både stillbilder og video. Dette innebærer at politiet rent teknologisk har muligheten til å bruke bilder fra forskjellige kilder og sammenlikne dem med personer som finnes i sporregisteret.

[1] Tidemann (2020).
[2] Giske (2019).
[3] Se Fussey og Murray (2019) s. 19 – og Nätt (2019).
[4] Forskrift 20. september 2013 nr. 1097 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterforskriften).
[5] En stor del av informasjonen i dette avsnittet baserer seg på e-post-korrespondanse med Kathrine Moe, ved Kripos' retts- og påtaleavdeling, personvernseksjonen, 2.-6. november. Gjengitt med samtykke.

1.2 En ny teknologi?

Jeg har fått opplyst at Kripos' bruk av ansiktsgjenkjenning skjer ved ettertidsbehandling.[6] Det innebærer at politiet bruker ansiktsgjenkjenningsteknologi en stund *etter* at opptaket ble gjort eller fotografiet ble tatt. Ettertidsbehandling skiller seg fra sanntidsbehandling, som innebærer at bildeanalysen skjer samtidig eller nært i tid med videoopptaket eller fotograferingen, noe som gjør fortløpende identifikasjon mulig.

Teknologien som anvendes for ansiktsgjenkjenning, er i dag så god at det er mulig å benytte intelligent videoanalyse, som innebærer at teknologien fanger opp kamerafotografier av personer, analyserer disse og varsler dersom en person i referansematerialet blir fanget opp av overvåkningskameraet. Dette gir politiet nye muligheter i kriminalitetsbekjempelsen, blant annet at ansiktsgjenkjenning kan skje i nær sanntid med opptaket. Dermed kan politiet få opp automatiske varsler og reagere raskt, for eksempel ved å bli varslet om at en ettersøkt person er blitt fanget opp av overvåkningskameraet.

Ansiktsgjenkjenning kan anvendes for verifikasjon og identifikasjon. Ved *verifikasjon* sammenliknes et bilde med et annet for å avgjøre om et individ *er* den det synes å være.[7] Denne formen anvendes for eksempel ved automatisk passkontroll. *Identifikasjon* skjer når en ønsker å finne én bestemt person blant et ubestemt antall.[8] I slike tilfeller sammenliknes bildet med en på forhånd definert liste av bilder.[9] Metoden kan også brukes for å avdekke om personer som er registrert i fotoregisteret, befinner seg på et visst sted. Det er særlig ansiktsgjenkjenning ved identifikasjon som er aktuell i denne oppgaven.

Ansiktsgjenkjenning ved bruk av intelligent videoanalyse skjer ved anvendelse av såkalt *dyp læring*. Dette innebærer at «dype kunstige nevrale nettverk»[10] trenes opp til å kunne trekke ut ansiktskjennetegn og sammenlikne dem. Systemene læres først opp fra datasystemer, hvor maskinen kjenner innholdet i bildene. På bakgrunn av dette trenes det opp en klassifikator som kan skille ulike gjenstander (i dette tilfellet ansikter og ansiktstrekk) fra hverandre, og

[6] *Ibid*.
[7] Tennøe, Johannessen og Barland (2020) s. 1-2.
[8] *Ibid*.
[9] *Ibid*. s. 2.
[10] Tidemann (2017).

gjenkjenne innholdet i bildene. Teknologiens treffsikkerhet avhenger av treningssettets omfang.[11]

Teknologien analyserer altså ansiktstrekk. I tråd med politiregisterloven § 2 nr. 16[12] må bruk av teknologien derfor anses for å være «en særskilt teknisk behandling knyttet til en fysisk persons fysiske […] egenskaper» som «muliggjør eller bekrefter» en «entydig identifikasjon», og derfor en «biometrisk opplysning». At teknologien fremskaffer en «biometrisk opplysning», har betydning for politiets behandlingsadgang, fordi det gjelder enkelte særregler for behandling av slike opplysninger. Jeg kommer inn på disse underveis i oppgaven (se særlig underkapittel 4.3.3).

Et sentralt spørsmål er om det reelt sett er forskjell på ansiktsgjenkjenningsteknologi og fotografiteknologi. Ansiktsgjenkjenning er et teknisk hjelpemiddel for analyse av foto og video. Spørsmålet er om det gjør teknologien til noe annet enn en automatisk og forbedret metode for sammenlikning av fotografier som polititjenestepersonell lenge har foretatt manuelt, slik at den kan anses som en ny teknologiform. Spørsmålet kan illustreres med et eksempel fra DNA-teknologien. Metoden for og kunnskapen om analysering av DNA-spor har utviklet seg mye de siste årene. Dette øker muligheten for å identifisere ukjente gjerningspersoner og oppklare straffesaker hvor etterforskningen har stoppet opp grunnet mangel på bevis. Gjerningspersonen kan ikke påberope seg manglende hjemmel og forutberegnelighet fordi den teknologiske utviklingen gjør at straffbare handlinger som ble begått for noen år siden, nå kan oppklares. Lovhjemmelen er den samme selv om teknologien har utviklet seg. Gjelder det samme argumentet for ansiktsgjenkjenningsteknologi?

Ansiktsgjenkjenningsteknologi gir økte muligheter for automatisk identitetsgjenkjennelse, for eksempel ved å identifisere flere personer samtidig og få opp fortløpende varsler. Som nevnt gir dette politiet nye muligheter i kriminalitetsbekjempelsen, for eksempel til å finne ettersøkte personer. Teknologiformen gjør ikke bare det kriminalitetsbekjempende arbeidet mer effektivt, det muliggjør også identifikasjoner som politiet mest sannsynlig ellers ikke ville kunnet foreta. Omfanget av myndighetenes muligheter for kontroll og overvåkning vil dermed øke. Kanskje kan slike forbedringer medføre at kvantitet slår over i kvalitet, at en

[11] Avsnittet baserer seg på foredraget til Eikvil (2020), minutt 5-6. Gjengitt med samtykke.
[12] Lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven).

gradsforbedring også vil innebære en vesensforskjell. Ansiktsgjenkjenningsteknologi kan i så fall ikke bare anses et hjelpemiddel for allerede regulerte metoder, men må betraktes som en ny og egen teknologiform.

Ny teknologi må være legitimt begrunnet og må brukes på en etisk forsvarlig måte. I *S. og Marper mot Storbritannia* formulerer Den europeiske menneskerettighetsdomstol (heretter forkortet til EMD) dette som at medlemsstatene plikter å sørge for rett balanse mellom motstridende rettigheter ved anvendelse av ny teknologi.[13] Dommen gjaldt spørsmål om brudd på retten til «privatliv» etter Den europeiske menneskerettighetskonvensjon (heretter EMK) artikkel 8[14] fordi myndighetene hadde fortsatt å oppbevare fingeravtrykk, celleprøver og DNA-profiler av to personer etter at straffesaken mot dem hadde medført frifinnelse for den ene og var avviklet for den andre. Anvendelse av kunstig intelligens i kriminalitetsbekjempelsen medfører moralske problemstillinger knyttet til om, og i så fall hvordan, teknologien bør benyttes.

Når politiet tar i bruk nye virkemidler, er det sentrale etiske spørsmålet hva som skjer «when LFR [Live Facial Recognition] is used for a purpose, whether by the police or anyone else». Implikasjonene av teknologiens kvalitet kan være store.[15] Da London Metropolitan Police mellom 2016 og 2019 testet ut teknologien, var antallet feiltreff høyt, og «the lack of information on who is on the watchlists due to the absence of legislation or guidance» ble også kritisert.[16] Bruk av ansiktsgjenkjenningsteknologi krever altså utvetydig lovtekst og må foregå innenfor avgrensede rammer. Også åpenhet rundt bruken er viktig.

I 2019 satte Europakommisjonen ned en ekspertgruppe for utarbeidelse av etiske retningslinjer «for etisk og ansvarlig utvikling av kunstig intelligens».[17] Utarbeidelsen baserer seg på generell menneskerettighetslovgivning og EUs pakt om grunnleggende rettigheter.[18] Blant hensyn som ble vektlagt, er menneskets selvbestemmelsesrett og kontroll, personvern,

[13] *S. og Marper mot Storbritannia* [GC] no. 30562/04 og 30566/04 avsnitt 112.
[14] Convention for the Protection of Human Rights and Fundamental Freedoms, Roma, 4. november 1950. (Den europeiske menneskerettighetskonvensjonen).
[15] London Policing Ethics Panel (2018) s. 12.
[16] European Union Agency For Fundamental Rights (2019) s. 12.
[17] Kommunal- og moderniseringsdepartementet (2020) s. 58.
[18] *Ibid*.

åpenhet, likebehandling og nytte for samfunn og miljø.[19] Enkelte forventer et midlertidig forbud mot slik teknologibruk frem til eventuell lovregulering er på plass.[20]

1.3 Problemstillinger og aktualitet

Oppgavens tema er altså politiets bruk av ansiktsgjenkjenningsteknologi i kriminalitetsbekjempelsen. Den overordnede problemstillingen gjelder hvorvidt dagens regelverk gir adgang til å benytte åpen overvåkning med fastmontert politikamera på offentlig sted, i en ettertids- eller sanntidsanalyse, hvor videostrømmen fra kameraet matches mot politiets fotoregister. Det forutsettes at analysen utføres ved hjelp av kunstig intelligens, det vil si ved bruk av teknologi for automatisk ansiktsgjenkjenning. Problemstillingen drøftes på grunnlag av politiloven § 6 a[21] og politiregisterlovgivningen. Tolkningen av regelverket må skje i lys av begrensningene som følger av Grunnloven § 102, jf. § 113[22] og EMK artikkel 8.

Lovgivningen hjemler adgang både til å ha politikamera på offentlig sted, jf. politiloven § 6 a, og til å ha et fotoregister, jf. politiregisterloven § 13 og politiregisterforskriften kapittel 46. Grunnen til at problemstillingen likevel reises, er at analysemulighetene som ligger i ansiktsgjenkjenningsteknologien neppe ble vurdert av lovgiver da bestemmelsene ble til. Det er først de senere år at teknologien er blitt god og effektiv nok for slik bruk. Dette gir nye muligheter for politiet til å identifisere og lokalisere personer. Samtidig har politiets bruk av ansiktsgjenkjenning skapt debatt i mange land. Anvendelse av teknologien til å overvåke borgerne er velkjent fra Kina.[23] I USA varierer bruken mellom ulike stater: Mens statlig bruk av ansiktsgjenkjenning er forbudt i San Fransisco,[24] har politiet i New York City brukt ansiktsgjenkjenning over 8000 ganger det siste året. Det hevdes blant annet at teknologien ble brukt av politiet under Black Lifes Matter-demonstrasjoner våren 2020.[25] Også flere europeiske stater tester ut muligheten for teknologibruken. Dette gjelder for eksempel tyske myndigheter som tester teknologien ut ved å overvåke jernbanestasjoner,[26] og i England har London-politiet varslet at det vil bruke ansiktsgjenkjenning på enkelte offentlige områder.[27]

---

[19] *Ibid*. s. 59-60.
[20] Tennøe, Johannessen og Barland (2020) s. 4.
[21] Lov 4. august 1995 nr. 53 om politiet (politiloven).
[22] Lov 17. mai 1814 Kongeriket Norges Grunnlov (Grunnloven).
[23] Almås (2019).
[24] Tennøe, Johannessen og Barland (2020) s. 4.
[25] Selinger og Cahn (2020).
[26] European Union Agency for Fundamental Rights (2019) s. 12.
[27] Tennøe, Johannessen og Barland (2020) s. 2.

Nye muligheter aktualiserer spørsmålet om politiet kan ta teknologien i bruk etter gjeldende lovverk, og reiser viktige problemstillinger knyttet til rekkevidden av bruken etter dagens lovregler, samt forholdsmessigheten ved fremgangsmåten. Problemfeltet presiseres i denne oppgaven til hvorvidt regelverket tillater automatisk kobling mellom politikameraet og politiets fotoregister, en kobling som med ansiktsgjenkjenningsteknologi gir mulighet for å identifisere og lokalisere personer som politiet ønsker opplysninger om, og reiser derfor følgende problemstillinger:

1. Gir dagens regelverk hjemmel for automatisk matching av videostrømmen fra politikameraet mot fotoregisteret?
2. Forutsatt at hjemmel foreligger, er spørsmålet om dagens regelverk ut fra en forholdsmessighetsvurdering oppstiller tilstrekkelige vilkår og sikkerhetsforanstaltninger som kan forhindre vilkårlighet og misbruk.

1.4 Avgrensninger

Jeg skal fokusere på politiets kriminalitetsbekjempelse, og avgrenser mot norsk spesialpoliti som for eksempel Politiets Sikkerhetstjeneste (PST). For slikt spesialpoliti gjelder det særskilte regler for blant annet deres hovedoppgaver og behandlingsvilkår.[28] Oppgaven avgrenser seg også mot politiets administrative arbeid etter politiregisterloven § 2 nr. 13 bokstav b). Av hensyn til oppgavens lengde tar jeg bare opp spørsmål knyttet til gjenkjenning av personer og identitetsfastsettelse. Det avgrenses derfor mot annen bruk av teknologien, for eksempel bruk som avdekker en persons følelser og humør.[29]

Jeg begrenser meg videre til kun å bruke politiets fotoregister som referansemateriale. For å skille klart mellom fotografiene i politiets fotoregister og bildene som kommer inn gjennom overvåkningskamera, vil jeg, der det er tjenlig, benytte begrepet «kamerafotografi» for bildene som stammer fra overvåkningskamera satt ut i medhold av politiloven § 6 a. For bildene som hentes inn i forbindelse med registerfotografering etter politiregisterloven § 13, jf. straffeprosessloven § 160[30], bruker jeg begrepet «registerfotografi».

[28] Se f.eks. Auglend og Mæland (2016) s. 1123.
[29] Se f.eks. Crawford og Paglen (2020).
[30] Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (Straffeprosessloven).

Oppgaven gjelder politiets overvåkningsmulighet, hvor videokameraet fanger opp et ubestemt antall personer, og avgrenser seg derfor mot spørsmål knyttet til en-til-en-bruk av teknologien, som for eksempel ved automatisk passkontroll. Oppgaven avgrenses også til å gjelde fastmonterte, skiltede kameraer satt ut av politiet i tråd med politiloven § 6 a. Bruk av mobile overvåkningskameraer og skjult kameraovervåkning etter straffeprosessloven § 202 a behandles derfor ikke. Selv om politiet har hjemmel i straffeprosessloven kapittel 16 til å innhente overvåkningsmateriale fra private aktører, avgrenser jeg også mot dette.

1.5 Rettskildebildet og metodiske utfordringer

Informasjonsbehandling er en sentral del av politiets kriminalitetsbekjempelse. Teknologiutvikling gir stadig nye måter å behandle informasjon på, og gjelder uavhengig av om politiet driver etterforskning, forebygging eller etterretning. Reguleringen av politiets adgang til å behandle opplysninger, særlig politiregisterloven og -forskriften, er derfor av stor betydning for politiets mulighet til å løse sine oppgaver.

Ansiktsgjenkjenning er en fersk teknologi, og det er få (om noen) rettskilder som eksplisitt gjelder politiets bruk av den. Politiregisterloven kapittel to inneholder imidlertid generelle bestemmelser for krav til politiets behandling av opplysninger. Nærmere regler for behandling av fotografi-opplysninger spesielt finnes i politiregisterforskriften. Mangel på rettskilder skaper tolkningsproblemer. Politiregisterforskriften fra 2013 har for eksempel ikke tilgjengelige forarbeider som kan si noe om hva lovgiver har ment på lovgivningstidspunktet. Politiregisterloven fra 2010 har derimot forarbeider. Disse nevner imidlertid ikke ansiktsgjenkjenningsteknologi. Etter det jeg har fått opplyst, fikk Kripos teknologi for ansiktsgjenkjenning først i 2017.[31] Det er derfor usannsynlig at lovgiver har tenkt på ansiktsgjenkjenning ved utarbeidelsen av loven eller forskriften.

Siden teknologien er såpass fersk, er også mangel på rettspraksis en utfordring, men det finnes noen dommer fra Høyesterett og EMD som kan bidra i argumentasjonen. Dommene er særlig relevante for problemstillingen som gjelder lovreglenes forhold til forholdsmessighetskravet i EMK artikkel 8, og vil derfor bli omtalt i kapittel 5.

[31] E-post-korrespondanse med Kathrine Moe, ved Kripos' retts- og påtaleavdeling, personvernseksjonen, 2.-6. november. Gjengitt med samtykke.

Mangel på rettskilder medfører at det må legges særlig vekt på andre tilgjengelige rettskilder. Siden ordlyden er det naturlige utgangspunktet for lovgivers vilje, blir denne sentral. Mange har imidlertid kritisert loven og forskriften for å være komplisert og fragmentert.[32] Siden forskriftsbestemmelser utfyller den tilhørende loven, er hensynet til sammenheng mellom de enkelte bestemmelser spesielt og lov og forskrift generelt viktige momenter. Dessuten er regelverkets formål sentralt.[33] Politiregisterloven § 1 og -forskriften § 1-1 første ledd bestemmer at lovens formål er å bidra til «effektiv løsning av politiets og påtalemyndighetens oppgaver», «beskyttelse av personvernet» og «forutberegnelighet for den enkelte ved behandlingen av opplysninger». Formålene viser at forutberegnelighet og personvern er legitime hensyn i vurderingen. Politiregisterforskriften § 1-1 andre ledd bestemmer i tillegg at når behandling av opplysninger nødvendiggjør «en avveining mellom hensynet til personvern og hensynet til kriminalitetsbekjempelsen, skal det ved avveiningen foretas en forholdsmessighetsvurdering». Bestemmelsen viser til § 4-2 første ledd, som inneholder momenter i forholdsmessighetsvurderingen. Av bestemmelsen følger det at det blant annet skal legges vekt på «formålet med behandlingen», «hvilke opplysninger som skal behandles», «om behandlingen gjelder alvorlig eller mindre alvorlig kriminalitet» og «antallet personer som får tilgang til opplysningene». Som nevnt har forholdsmessighetsvurderingen en kobling til oppgavens kapittel 5.

1.6 Oppgavens videre gang

Kapittel 2 omhandler Grunnloven § 102 og EMK artikkel 8. Dette er grunnleggende bestemmelser som setter grenser for politiets inngrep i personvernet. I kapittel 3 redegjør jeg for vilkårene for registrering i fotoregisteret, det vil si registeret som inneholder referansemateriale for ansiktsgjenkjenning. I kapittel 4 vurderer jeg hvorvidt dagens lovverk gir hjemmel for bruk av ansiktsgjenkjenningsteknologi slik jeg har beskrevet den. Kapittel 5 omhandler hvorvidt dagens regelverk oppstiller tilstrekkelige vilkår og sikkerhetsforanstaltninger mot vilkårlighet og misbruk, slik at teknologibruken kan fungere forholdsmessig. Kapittel 6 inneholder en kort oppsummering og konklusjoner på diskusjonen av oppgavens problemstillinger.

[32] Se f.eks. Politidirektoratet (2018) s. 7.
[33] Bergo (2019) s. 184-185.

2 Retten til «privatliv» etter Grunnloven § 102 og EMK artikkel 8

2.1 Innledning

Grunnloven § 102 første ledd slår fast at «[e]nhver» har rett til respekt for sitt «privatliv». Ordlyden «[e]nhver» betyr at rettigheten gjelder for alle. Rent språklig forstås «privatliv» som en rett til frihet fra innblanding og forstyrrelse fra omverdenen. Ifølge menneskerettighetsutvalget omfatter begrepet personvernet «i vid forstand». Dette sikres best gjennom «ivaretakelse av den personlige integritet, herunder ivaretakelse av den enkeltes mulighet for privatliv, selvbestemmelse og selvutfoldelse».[34]

Forarbeidene sier videre at «Grunnlovens menneskerettighetsbestemmelser [skal] tolkes i lys av de internasjonale menneskerettighetskonvensjonene og praksis knyttet til disse».[35] Dette ble også lagt til grunn i HR-2016-2554-P, avsnitt 81. Bestemmelsene begrenser lovgivers frihet til å danne nye lovregler, ettersom disse må holde seg innenfor de grenser som trekkes opp av Grunnloven og EMK.[36] Enkeltmenneskets rett til respekt for sitt «privatliv» følger av EMK artikkel 8 nr. 1. Dersom staten handler på en måte som griper inn i privatlivet, har det skjedd et «inngrep», se EMK artikkel 8 nr. 2. Uttrykket «inngrep» er vidt, og kan ikke defineres på én bestemt måte. Et inngrep kan også være av ulik styrke.[37] Det kan være ulike former for ileggelse av tyngende plikter fra myndighetenes side, enten det er i form av en strafferettslig sanksjon, et påbud eller forbud, et avslag på rettsgoder eller andre former for innblanding. Artikkel 8 nr. 2 oppstiller tre vilkår for når myndighetene kan gjøre inngrep i rettigheten: Inngrepet må være «i samsvar med loven», være «nødvendig i et demokratisk samfunn» og oppfylle ett av bestemmelsens hensyn. Dersom ett eller flere av vilkårene ikke er oppfylt, foreligger det en krenkelse av retten til privatliv.

2.2 Er bruk av ansiktsgjenkjenningsteknologi et «inngrep» i privatlivet?

Før jeg går inn på inngrepsvurderingen, finner jeg det nødvendig å presisere hva jeg mener med «bruk av ansiktsgjenkjenningsteknologi». Med uttrykket «bruk» sikter jeg til «behandling». Hva som nærmere ligger i begrepet, skal vurderes i kapittel 3. Spørsmålet i

[34] Dok. nr. 16 (2011 – 2012) s. 177.
[35] *Ibid*. s. 90.
[36] Prop. 131 L (2018 – 2019) s. 12.
[37] Se Aall (2018) s. 119-122.

dette underkapittelet er om «behandling» av fotografi med ansiktsgjenkjenningsteknologi er et inngrep i privatlivet etter EMK artikkel 8.

Det finnes ingen entydig definisjon av begrepet «privatliv».[38] Derfor er heller ikke inngrep i rettigheten definert. En definisjon er vanskelig å gi, og upraktisk: Den store variasjonen i avgjørelser fra EMD viser kompleksiteten i og mangfoldet av situasjoner som angår spørsmål om inngrep i privatlivet. For oppgavens formål vil det føre for langt å foreta en generell utgreiing av hva som ligger i begrepet. Det vil derfor fokuseres på det relevante for mine problemstillinger, altså spørsmål knyttet til inngrep i privatlivet ved bruk av kameraovervåkning, som muliggjør den analysen som følger av ansiktsgjenkjenningsteknologi, og registrering i fotoregisteret.

I *S. og Marper mot Storbritannia* la EMD til grunn at inngrep i privatlivet etter EMK artikkel 8 må vurderes ut fra «the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained» (avsnitt 67). Jeg vil først vurdere om den formen for kameraovervåkning som politiet anvender ved bruk av ansiktsgjenkjenningsteknologi, er et inngrep i privatlivet etter EMK artikkel 8. EMD har i gjentatte dommer lagt til grunn at alminnelig kameraovervåkning på offentlig sted *ikke* er et inngrep i privatlivet. I *Peck mot Storbritannia* (avsnitt 59) uttaler for eksempel EMD at «[t]he monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life». Filming uten lagring av kameraopptaket er altså ikke å anse som et inngrep i privatlivet. Registrering og lagring av personopplysninger er derimot omfattet av begrepet «privatliv», se *Leander mot Sverige*.[39] Det samme er lagt til grunn i *Amann mot Sveits*[40] og i *S. og Marper mot Storbritannia* (avsnitt 67). For ansiktsgjenkjenning vil dette angå privatlivet til den som får registrert informasjon om seg på grunn av treff i systemet.

Uttrykket «personopplysning» er definert i politiregisterloven § 2 nr. 1 som en «opplysning og vurdering som kan knyttes til fysisk person som kan identifiseres direkte eller indirekte». Forarbeidene slår fast at også «[a]videntifiserte opplysninger» er personopplysninger. Dette

[38] *Peck mot Storbritannia* [J] 2003 no. 44647/98 avsnitt 57. Se også Christensen (2020) s. 129.
[39] *Leander mot Sverige* [J] no. 9248/81 avsnitt 48.
[40] *Amann mot Sveits* [GC] no. 27798/95 avsnitt 65.

gjelder også anonymiserte opplysninger – «dersom de[n] knytter seg til en så liten gruppe at tilhørigheten røpes».[41] Liknende definisjoner finnes også i politiregisterforskriften § 1-2 nr. 1. Det er ikke tvilsomt at bruk av ansiktsgjenkjenningsteknologi på et fotografi er en opplysning som kan medføre identifikasjon av en bestemt person, og altså en «personopplysning».[42] Bruk av ansiktsgjenkjenning på et kamerafotografi innhentet i medhold av politiloven § 6 a er et inngrep i «privatlivet» etter EMK artikkel 8 nr. 1.

Det vurderes så om det å fotografere anholdte personer utgjør et inngrep i privatlivet etter EMK artikkel 8. I *Gaughran mot Storbritannia*[43] (avsnitt 65) legger EMD til grunn at i utgangspunktet er verken lagring eller bruk av fotografier tatt av anholdte personer (norsk rett straffeprosessloven § 160) et inngrep i privatlivet. I avsnitt 66 følger det imidlertid at det å ta registerfotografi kan være et inngrep i enkelte tilfeller, og at dette må vurderes ut fra «the specific context […]». EMD legger her (i avsnitt 70) vekt på den lange lagringstiden (lagring på ubestemt tid) og at den stadige teknologiske utvikling gjør at registerfotografiene kan anvendes til stadig flere formål, inkludert ansiktsgjenkjenning. Domstolen mente at dette uten tvil gjorde at det å ta og oppbevare registerfotografi er et inngrep i privatlivet. (Denne dommen blir videre drøftet i oppgavens kapittel 5.)

De norske reglene som hjemler at anholdte personer kan fotograferes, følger av politiregisterloven § 13 og straffeprosessloven § 160. Bestemmelsene vil bli nærmere redegjort for i kapittel 3. I denne sammenheng er det tilstrekkelig å slå fast at registerfotografiene, ut fra EMDs praksis, i utgangspunktet ikke utgjør et inngrep i privatlivet. Spørsmålet er imidlertid om muligheten til å bruke fotoregisteret som referansedatabase for ansiktsgjenkjenning medfører at bruk og lagring av registerfotografiene likevel *er* et inngrep. Som lagt til grunn i *Gaughran mot Storbritannia*, må inngrepsspørsmålet vurderes ut fra den spesifikke konteksten. Også i Norge vil teknologiutviklingen medføre at registerfotografiene kan anvendes til stadig flere formål, herunder ansiktsgjenkjenning. Videre er lagringstiden for disse registerbildene svært lang (se underkapittel 5.4.2). Jeg legger altså til grunn at fotografering av anholdte personer for lagring i fotoregisteret er et inngrep i deres «privatliv» etter EMK artikkel 8.

[41] Ot.prp. nr. 108 (2008 – 2009) s. 291.
[42] Dette støttes av *S. og Marper mot Storbritannia*, hvor EMD i avsnitt 68 la til grunn at fingeravtrykk, DNA-profiler og celleprøver inneholder «personal data […] as they relate to identified or identifiable individuals».
[43] *Gaughran mot Storbritannia* [J] no. 45245/15.

2.3 Vilkår ved inngrep i privatlivet

Inngrep i privatlivet kan, som allerede nevnt, skje dersom vilkårene i EMK artikkel 8 nr. 2 er oppfylt. Begrunnelsen for dette er at det kan «ligge tyngre lodd i den annen vektskål, enten dette er hensynet til samfunnet (som rikets sikkerhet) eller private (som å sikre blodprøve i en farskapssak)».[44] I det følgende skal jeg gjennomgå vilkårene som oppstilles i EMK artikkel 8 nr. 2.

2.3.1 Lovhjemmelskravet

EMK artikkel 8 nr. 2 hjemler for det første at inngrep i privatlivet må være «i samsvar med loven». Ordlyden oppstiller et krav om hjemmel i nasjonal lov. I norsk rett oppstiller Grunnloven § 113 et krav om at myndighetenes «inngrep» overfor den enkelte må ha «grunnlag i lov». Ordlyden oppstiller et krav om at myndighetene kun kan gjøre inngrep i de grunnlovfestede rettighetene, herunder i retten til privatliv, dersom det er hjemlet i skreven og vedtatt lov eller forskrift. I Rt. 2014 s. 1105 (avsnitt 24) tolkes hjemmelskravet strengt: Inngrep kan bare skje dersom «og utelukkende i den utstrekning» det er hjemmel i lov eller forskrift.

EMDs lovkrav er videre enn det som følger av Grunnloven § 113. I *The Sunday Times mot Storbritannia* sies det at uttrykket «law» i EMK artikkel 8 nr. 2 «covers not only statute but also unwritten law».[45] Dommen gjelder ytringsfrihetsbestemmelsen (EMK artikkel 10). I avsnitt 48 slår EMD fast at uttalelsene likevel er sentrale for EMK artikkel 8 fordi uttrykket «law» skal tolkes likt. EMDs hjemmelskrav omfatter altså skreven lov, men også ulovfestet nasjonal rett kan være tilstrekkelig dersom kvalitetskrav knyttet til tilgjengelighet og forutberegnelighet innfris.[46] Bakgrunnen for dette vide lovbegrepet er at medlemsstatene har noe ulik praksis knyttet til hva som godtas som lov. Med krav om hjemmel i skreven lov oppstiller Grunnloven § 113 et mer formelt hjemmelskrav enn EMK, og det er dette kravet som legges til grunn i denne oppgaven.

2.3.2 Formålskravet

[44] Aall (2018) s. 115.
[45] *Sunday Times mot Storbritannia* [P] no. 6538/74 avsnitt 47.
[46] Aall (2018) s. 124.

EMK artikkel 8 nr. 2 hjemler inngrep i enkeltpersoners privatliv for en rekke opplistete formål. Formålene er vidt utformet og er tolket tilsvarende vidt.[47] Poenget er at formålene skal begrense statens inngrepsmulighet og sørge for at inngrepene er akseptable.[48] Bruk av ansiktsgjenkjenningsteknologi i kriminalitetsbekjempelsen kan sørge å «forebygge uorden eller kriminalitet», og tjener derfor et legitimt formål etter EMK artikkel 8 nr. 2.

2.3.3 Forholdsmessighetskravet

At inngrepet er «nødvendig i et demokratisk samfunn» oppstiller etter ordlyden et forholdsmessighetskrav. Det er lagt til grunn i sikker EMD-praksis at vilkåret forutsetter et presserende samfunnsbehov. Dermed er det ikke tilstrekkelig at inngrepet er ønskelig eller hensiktsmessig.[49] Uttrykket krever en forholdsmessighetsvurdering hvor formålet med inngrepet må være så viktig at det veier opp for ulempene det har for den det gjelder.

Ved bruk av inngripende teknologi i kriminalitetsbekjempelsen står hensynet til politiets arbeid mot hensynet til den enkeltes privatliv. Vurderingen av forholdsmessighetskravet kan falle ut forskjellig avhengig av omstendigheter som inngrepets styrke og viktigheten av formålet med inngrepet. Også de aktuelle lovreglenes utforming kan ha betydning for forholdsmessighetsvurderingen. Forholdsmessighetskravet henger dermed sammen med lovhjemmelskravet. Jeg kommer, som nevnt, tilbake til sider ved forholdsmessigheten i oppgavens kapittel 5, hvor jeg vurderer om dagens regelverk oppstiller tilstrekkelige vilkår og sikkerhetsforanstaltninger som kan forhindre vilkårlighet, misbruk og uheldig formålsutglidning.

[47] Kvam (2013) s. 313.
[48] Aall (2018) s. 150.
[49] *Ibid*. s. 153.

3 Politiets fotoregister som referansegrunnlag

Siden bruk av ansiktsgjenkjenningsteknologi i kriminalitetsbekjempelsen forutsetter bruk av identiteter i politiets fotoregister, vil hvem som kan registreres ha betydning for omfanget av teknologibruken. Omfanget er relevant å vurdere fordi det kan ha betydning for formåls- og forholdsmessighetsvurderingen av inngrepet. Politiregisterloven § 13 første ledd pålegger politiet å føre et fotoregister som er «innhentet i samsvar med straffeprosessloven § 160» og «bestemmelsene i påtaleinstruksen». Påtaleinstruksen § 11-2[50] viser til straffeprosessloven § 160 og politiregisterloven § 13, jf. politiregisterforskriften § 46-5. Dermed er det relevant å vurdere straffeprosessloven § 160.

Straffeprosessloven § 160 første ledd første punktum gir politiet anledning til å fotografere personer som «mistenkes eller er dømt for en handling som etter loven kan medføre frihetsstraff». Ordlyden «mistenkes» betyr at politiet mener det er en reell mulighet for at den registrerte har begått en kriminell handling, og dermed får rettslig status som mistenkt. Det er imidlertid ikke krav om sannsynlighetsovervekt. Straffeprosessloven gir ikke «nærmere retningslinjer om når en person får status som mistenkt», og vurderingen må «bygge på rettspraksis, teori og reelle hensyn».[51] For mistenkt-begrepet er det for eksempel tilstrekkelig at politiet betrakter en person som mistenkt.[52] Ordlyden «dømt for en handling som etter loven kan medføre frihetsstraff» tilsier at en person har fått en rettskraftig dom og er ilagt straff for en lovovertredelse med en strafferamme som kan medføre fengselsstraff. Det kvalifiserer altså ikke til registrering i fotoregisteret dersom handlingen har en strafferamme som kun kan medføre bot, men bestemmelsen oppstiller ikke et krav om at frihetsstraff faktisk er idømt. (Andre punktum hjemler at det også kan registreres fotografi av en person som er «utvist eller utlevert til fremmed stat».)

Nærmere regler for «behandling» av fotografiopplysninger finnes i politiregisterforskriften kapittel 46. Ifølge politiregisterforskriften § 46-1 første ledd første punktum skal det føres et «register for foto» som er «innhentet i medhold av straffeprosessloven § 160» eller i henhold

[50] Forskrift 28. juni 1985 nr. 1679 om ordningen av påtalemyndigheten (Påtaleinstruksen).
[51] Øyen (2019) s. 99.
[52] *Ibid*.

til samtykke. Andre punktum bestemmer at fotoregisteret består av et identitetsregister, et etterforskningsregister og et sporregister. Registrene er «gjensidig søkbare», jf. § 46-7 første ledd første punktum. Jeg redegjør for forskjellene mellom disse registrene senere i dette kapitlet. Politiregisterforskriften § 46-4 regulerer hvilke opplysninger som kan registreres i fotoregisteret, og det følger her at det blant annet er anledning til å registrere «foto» og «video» (nr. 3) og «tilhørende personalia» (nr. 4).

Formålet med fotoregisteret følger særlig av § 46-1 første ledd tredje punktum, hvor det heter at «[o]pplysningene» kan «behandles» for å bidra til «sammenligning, gjenkjennelse og identifikasjon» av personer, herunder også til «verifisering av identitet», for «politimessige formål». Begrepet «behandles» relaterer seg til «[o]pplysningene». Ifølge politiregisterloven § 2 nr. 2 skal «behandling» forstås som «enhver elektronisk eller manuell bruk av opplysninger». Dette eksemplifiseres med en rekke alternativer, hvor uttrykket «for eksempel» brukes. Dette viser at opplistingen ikke er uttømmende. Eksempelvis regnes «innsamling», «registrering», «oppbevaring», «sammenlikning» og «sammenstilling» som «behandling». Behandlingsbegrepet er altså vidt og dynamisk. Hva som menes med begrepet vil variere med teknologiform, hvilke opplysninger som anvendes og hvilket steg i prosessen det dreier seg om. Et dynamisk behandlingsbegrep gir rettsanvender et visst handlings- og tolkningsrom. Den teknologiske koplingen av de innhentede biometriske opplysningene fra registerbildene og bildet fra overvåkningskameraet vil være en form for «sammenstilling» eller «sammenligning» av opplysninger. I tråd med politiregisterloven § 2 nr. 2 er bruk av ansiktsgjenkjenningsteknologi altså «behandling av opplysninger». Det er viktig å understreke at en slik kopling ikke øker fotoregisteret med materiale fra videostrømmen. Den nye informasjonen som hentes inn gjennom eventuell sammenligning og gjenkjenning, blir lagret på de respektive sakene, og ikke i registrene.

I det følgende redegjør jeg for fotoregisterets tre deler: identitets-, etterforsknings- og sporregisteret. Politiregisterforskriften § 46-5 første til fjerde ledd inneholder nærmere reguleringer for hvem som skal eller kan registreres i fotoregisteret. Første og andre ledd regulerer registrering i *identitetsregisteret*. Første ledd inneholder kategorier av personer som det «skal» registreres opplysninger om. Ordlyden «skal» tilsier at politiet plikter å registrere opplysningene. Dette gjelder personer som er idømt «ubetinget fengselsstraff eller forvaring»

(nr. 1), som «begjæres varetekstfengslet» (nr. 2), som «overføres til tvungent psykisk helsevern eller tvungen omsorg» (nr. 3) og som «er besluttet utvist» (nr. 4).

Andre ledd lister opp persongrupper som det i identitetsregisteret «kan» registreres opplysninger om. Ordlyden «kan» tilsier at politiet selv avgjør om registrering skal foretas. Etter nr. 1 første punktum kan det registreres opplysninger om en person som er dømt til en strafferettslig reaksjon som nevnt i § 44-4 «for en handling som etter loven kan medføre frihetsstraff». Det kan også registreres fotografi av personer som er dømt strafferettslig utilregnelig etter straffeloven § 20 (nr. 2), personer som er ilagt en straff i tråd med straffeloven § 29 i utlandet (nr. 3), personer som «er siktet for lovbrudd i Norge og forholdet overføres en annen stat for straffeforfølgning» (nr. 4), dersom personen «begjærer det av grunner som finnes fyllestgjørende» (nr. 5), eller dersom vedkommende er «besluttet utlevert til annen stat» (nr. 6).

Tredje ledd bestemmer at det i *etterforskningsregisteret* «kan» registreres opplysninger av personer som er «mistenkt eller siktet for en handling som kan medføre frihetsstraff». Ordlyden «mistenkt eller siktet» gjelder rettslige posisjoner. Begrepet «mistenkt» og uttrykket «en handling som kan medføre frihetsstraff» tolkes likt med utrykkene i straffeprosessloven § 160. Straffeprosessloven § 82 første ledd fastslår hvem som anses som «siktet». Det følger at mistenkte får status som «siktet» når «påtalemyndigheten har erklært ham for siktet», «når forfølgning mot ham er innledet ved retten», eller når «det er besluttet eller foretatt pågripelse, ransaking, beslag eller liknende forholdsregler rettet mot ham».

Politiregisterforskriften § 46-5 fjerde ledd regulerer politiets adgang til registrering av opplysninger i *sporregisteret*. Her kan det registreres foto av «personer med ukjent identitet» når opplysningene «antas å ha tilknytning til uoppklart straffesak». Ordlyden «personer med ukjent identitet» betyr at politiet ikke vet hvem personen er. Ordlyden «antas å ha tilknytning til uoppklart straffesak» tilsier at politiet har grunn til å tro at vedkommende har forbindelse med en straffesak som ikke er oppklart. Bestemmelsen gjelder den etterforskende virksomhet, men oppstiller ikke et krav om at den registrerte antas å ha begått den kriminelle handlingen. Det må likevel være visse holdepunkter for at vedkommende er av interesse for etterforskningen. Foto som registreres i sporregisteret kan komme fra ulike kilder, for

eksempel private overvåkningskameraer fra butikker, men også fra politiets egne overvåkningskameraer.

Adgangen til å registrere personer i fotoregisteret er altså begrenset til å gjelde straffedømte, mistenkte og siktede, og personer med ukjent identitet som antas å ha tilknytning til en uoppklart straffesak. For det siste tilfellet vil altså personer som kan ha betydning for politiets etterforskning kunne registreres, selv om det ikke er holdepunkter for at personen har begått kriminelle handlinger. Det må imidlertid være holdepunkter for at vedkommende kan ha betydning for etterforskningen. Dette medfører at politiet ikke kan registrere personer som ikke antas å ha forbindelse med en kriminell handling eller oppfyller kriteriene for registrering i sporregisteret. For slike personer har politiet dermed ikke et sammenlikningsgrunnlag, og teknologien vil ved anvendelse ikke kunne gi treff. I det videre skal jeg vurdere hvor langt dagens lovbestemmelser rekker for behandling av opplysninger innhentet ved bruk av ansiktsgjenkjenningsteknologi med bruk av politiets fotoregister som referansegrunnlag.

4 Rettsgrunnlaget for bruk av ansiktsgjenkjenning

4.1 Innhenting etter politiloven § 6 a

Bruk av ansiktsgjenkjenningsteknologi forutsetter innhenting av opplysninger i form av fotografi og videoopptak. Innhentingen kan skje på flere måter. Oppgaven er, som nevnt i underkapittel 1.4, begrenset til innhenting av foto fra politiets egne overvåkningskameraer etter politiloven § 6 a. Politiloven § 6 a første ledd første punktum gir politiet rett til å «benytte kameraovervåking dersom det er nødvendig for å gjennomføre oppgaver som nevnt i § 2 nr. 1 til 4». Ordlyden «benytte kameraovervåking» gir altså politiet anledning til å ta i bruk kameraovervåkning. Slik overvåkning kan anvendes for å beskytte person, eiendom og andre fellesgoder, og for å sikre den offentlige orden og sikkerhet (nr. 1), i kriminalitetsforebyggende arbeid og for å motvirke andre krenkelser av den offentlige orden og sikkerhet (nr. 2), for avdekking og stansing av kriminell virksomhet og forfølgelse av straffbare forhold (nr. 3) og for ytelse av hjelp og tjenester til borgerne når dette er nødvendig (nr. 4).

Paragraf 6 a gir politiet anledning til å drive vedvarende og systematisk kameraovervåkning i kriminalitetsbekjempende hensikt. Andre ledd første punktum uttrykker at kameraovervåkning bare kan benyttes «dersom de hensyn som tilsier overvåking, overstiger hensynet til den registrertes personvern». Ordlyden åpner for en forholdsmessighetsvurdering, hvor formålet med politiets overvåkning etter første ledd, må være viktigere enn den registrertes personvern. Andre punktum uttrykker at det særlig skal legges vekt på «hvordan overvåkingen skal skje» og «hva slags område som skal overvåkes». Forarbeidene legger til grunn at det må «legges vesentlig vekt på om overvåkingen vil omfatte steder der en begrenset krets av personer ferdes jevnlig, eller om overvåkingen gjelder parker, strender og lignende rekreasjonsområder som er tilgjengelig for allmennheten».[53]
Overvåkningskameraene vil ofte være plassert på offentlige områder med mye ferdsel, som for eksempel på jernbanestasjoner, flyplasser og kjøpesentre. For den videre drøftelsen forutsettes det at de oppsatte overvåkningskameraene er satt ut i tråd med forholdsmessighetskravet i andre ledd.

[53] Prop. 56 LS (2017 – 2018) s. 224.

Ansiktsgjenkjenningsteknologi ved bruk av politiets egne oppsatte kameraer og med fotoregisteret som referansegrunnlag er et hjelpemiddel i politiets etterforskende og forebyggende arbeid. Bruken vil samsvare med politiets oppgaver slik de er nevnt politiloven § 2 nr. 1 til 4 gjennom «sammenligning» mellom registerfotografiene og overvåkningsmaterialet, jf. politiregisterforskriften § 46-1 første ledd tredje punktum.

Politiregisterloven oppstiller tre grunnvilkår for at politiet kan behandle opplysningene som er hentet inn i tråd med politiloven § 6 a.[54] Politiregisterloven § 4 oppstiller et krav om formålsbestemthet. Videre inneholder § 5 et nødvendighetskrav «som generelt begrenser behandlingen til det som er påkrevd ut fra formålet».[55] Endelig oppstiller § 6 et kvalitetskrav.[56] I underkapittel 4.3 skal jeg vurdere hvilken betydning bestemmelsene har for politiets bruk av ansiktsgjenkjenningsteknologi, som redegjort for i forrige avsnitt, både for etterforskende og forebyggende arbeid, og ved ettertids- og sanntidsbehandling. Først skal jeg imidlertid se på politiregisterloven § 8, fordi denne gir politiet rett til å forbehandle opplysninger.

4.2 Forbehandling av opplysningene etter politiregisterloven § 8

Som Henry John Mæland skriver, har politiet ofte «behov for å kunne innhente opplysninger som man på innhentingstidspunktet vet lite om betydningen av, men som det er et behov for å kunne sjekke ut».[57] Bruk av overvåkningskameraer medfører en strøm av data til politiet, og det vites sjelden nøyaktig hvilke bilder som er relevante å samle inn og lagre, før behandling har skjedd.

Politiregisterloven § 8 hjemler politiets rett til forbehandling av opplysninger for å avgjøre om politiregisterloven og -forskriftens krav til videre eller fortsatt behandling er oppfylt. Første ledd åpner for at opplysninger «uansett [kan] behandles» i «4 måneder» dersom «det er nødvendig for å avklare om kravene i § 4, § 5 nr. 1 og 2 og § 6 første ledd nr. 1 er oppfylt». Forarbeidene uttrykker at første ledd gjelder behandling av opplysninger «utenfor

[54] Auglend og Mæland (2016) s. 393.
[55] *Ibid*.
[56] *Ibid*.
[57] *Ibid*. s. 1125.

straffesaksbehandling».[58] Bestemmelsen regulerer altså politiets forebyggende virksomhet. Ordlyden «uansett» gir politiet anledning til forbehandling av opplysninger for å avgjøre om videre behandling skal skje. Som nevnt i kapittel 3, må behandlingsbegrepet i politiregisterloven § 2 nr. 2 tolkes vidt, og fristen løper derfor fra første bruk av opplysningene. Slik forstås også forarbeidene, som uttrykker at bestemmelsen åpner for politiets behandling av «opplysninger for å avklare om de lovpålagte kravene til formålsbestemthet, nødvendighet og relevans er oppfylt».[59] Bestemmelsen gir altså mulighet for å filtrere vekk øvrige identiteter som fanges opp av kameraet, men som ikke finnes i fotoregisteret, og som politiet derfor verken har behov for eller anledning til å innhente opplysninger om. Bestemmelsen åpner også for å dobbeltsjekke (som regel ved en menneskelig vurdering) at et treff mot fotoregisteret er pålitelig og gir grunnlag for handling fra politiets side.

Tredje ledd bestemmer at «[t]idsbegrensningen» i første ledd ikke gjelder «behandling av opplysninger i den enkelte straffesak». Ordlyden «den enkelte straffesak» forstås som politiets etterforskende virksomhet. Forarbeidene bekrefter ordlydsforståelsen, og begrunner regelen med at «straffesaker preges av at politiet vil kunne motta store mengder opplysninger uten at det er sikkert om disse er nødvendige eller relevante for å oppklare den konkrete saken», og at «tidsfrister vil kunne få en uheldig innvirkning» på etterforskningen.[60] I etterforskende virksomhet kan altså politiet oppbevare kamerafotografi så lenge det har behov for det for å avgjøre om opplysningene oppfyller vilkårene i de nevnte lovbestemmelsene for videre behandling. Opplysningene kan imidlertid ikke lagres «lenger enn nødvendig», jf. politiregisterloven § 6 første ledd nr. 3.

Politiregisterloven § 8 gir altså politiet anledning til å hente inn og behandle opplysninger for å avgjøre om det har behov for opplysningene. Forbehandling gjelder midlertidig både for forebyggende og etterforskende virksomhet. Forskjellen er at det er en konkret og fastsatt tidsbegrensning for forebyggende virksomhet («4 måneder»), som for etterforskning ikke finnes. Her har lovgiver funnet at hensynet til etterforskningen veier tyngre enn personvernhensyn, slik at forbehandlingen kan vare så lenge politiet har behov for opplysningene. I den forbindelse kan det spørres om bruk av ansiktsgjenkjenning i urimelig

[58] Ot.prp. nr. 108 (2008 – 2009) s. 298.
[59] *Ibid*.
[60] *Ibid*.

grad går på bekostning av personvernet til personer som ikke er i fotoregisteret, men som fanges opp av kameraet, selv om teknologien ikke gir treff. Et spørsmål som kan reises i denne sammenheng, er om regelverket burde vært presisert slik at det i ethvert tilfelle kreves en begrunnelse for bruk av ansiktsgjenkjenning. I så fall måtte politiet på forhånd velge ut de personer i registeret som det ønsker å fange opp av kameraet, og derigjennom gjenkjenne. I denne sammenheng er det rimelig å anta at fotoregisteret brukes dynamisk, ved at politiet «flagger» personer i fotoregisteret (identifiserte og uidentifiserte) som det er behov for å fange opp med overvåkningskameraet. Det kan for eksempel dreie seg om en gruppe kriminelle personer med ukjent identitet, en etterlyst kriminell person som det er holdepunkter for at oppholder seg i et visst område, eller en person som er straffedømt flere ganger, og som av den grunn har forbud mot å oppsøke visse områder. I slike tilfeller vil bruk av ansiktsgjenkjenning opp mot aktuelle personer i fotoregisteret være i tråd med formålskravet i politiregisterloven § 4 og -forskriften § 46-1 første ledd tredje punktum, og forhindre at ansiktsgjenkjenning leder til ubegrunnet overvåkning. På den annen side vil det ikke alltid være mulig for politiet på forhånd å avgjøre hvem det ønsker opplysninger om. Slik sett vil et altfor rigid utformet lovverk kanskje innebære at politiets arbeid blir unødig vanskeliggjort. For slike spørsmål må lovgiver foreta avveininger og tenke nøye gjennom konsekvensene det omtalte behovet for presiseringer kan medføre.

4.3 Treff (matching)

4.3.1 Innledning

Før politiet setter ut overvåkningskamera, må formålet med behandlingen av fotoene være klart (jf. politiregisterloven § 4). Ved behandlingen, og dermed ved vurderingen av om kamerafotografiene gir treff, blir bildene omgjort til en mal. Teknologirådet betegner dette som «en digital avbildning av de biometriske kjennetegnene».[61] Ettersom registerbildene anvendes som sammenlikningsgrunnlag, vil alle ansikter som fanges opp av kameraet behandles i søket etter treff. Dette er som allerede nevnt i tråd med politiregisterloven § 8. For fortsatt oppbevaring og videre behandling må treffene oppfylle vilkårene i § 5, og behandlingen må være «strengt nødvendig» etter § 7. Opplysningene må også oppfylle kvalitetskravene i § 6. Dette må kontrolleres manuelt av polititjenestepersonell, som et

[61] Teknologirådet (2007) s. 26.

element av menneskelig vurdering før man handler på grunnlag av teknologiens resultater, et naturlig moment i behandlingen som i senere tid er formulert som et krav.[62]

4.3.2 Formålskravet i politiregisterloven § 4

Effektiv kriminalitetsbekjempelse er viktig for rettshåndhevelsen og gagner samfunnet som helhet. Bruk av ansiktsgjenkjenningsteknologi er selvsagt et godt virkemiddel for dette, særlig dersom politiet kan gjenkjenne personer det ønsker kontakt med eller opplysninger om. Som nevnt, er denne oppgaven avgrenset til at det er personer i politiets fotoregister som kan gjenkjennes.

Politiregisterloven § 4 hjemler behandling av opplysninger for «det formålet de er innhentet for», eller til andre «politimessige formål», med mindre annet er bestemt i eller i medhold av lov. Ordlyden «det formålet de er innhentet for» åpner for at politiet alltid kan behandle opplysningene ut fra begrunnelsen for innhentingen. Men vilkåret begrenser behandling av opplysninger til ett eller flere konkrete og på forhånd bestemte formål. Dermed vil formålet i politiregisterforskriften § 46-1 være relevant å vurdere. Som nevnt følger det av § 46-1 første ledd tredje punktum at opplysningene i fotoregisteret kan behandles «for å bidra til sammenligning, gjenkjennelse og identifikasjon» av personer for «politimessige formål», herunder til «verifisering av identitet».

Ordlyden «politimessige formål» i politiregisterloven § 4 og -forskriften § 46-1 første ledd tredje punktum er vid og forstås som ethvert formål som ligger innenfor politiets oppgaver og legitime hensyn. Begrepet skal ifølge forarbeidene tolkes i lys av definisjonen i § 2 nr. 13.[63] Her defineres begrepet som «politiets kriminalitetsbekjempende virksomhet», herunder «etterforskning, forebyggende arbeid og ordenstjeneste» (bokstav a)). Oppgaven avgrenser seg som nevnt mot «politiets service- og bistandsfunksjon» og «føring av vaktjournaler» i bokstav b). Bruk av ansiktsgjenkjenningsteknologi i kriminalitetsbekjempelsen er innenfor «politimessige formål». Videre er formålet ved å knytte bruken opp mot fotoregisteret nettopp å kunne drive «sammenligning», «gjenkjennelse og identifikasjon» og «verifisering av identitet», jf. politiregisterforskriften § 46-1 første ledd tredje punktum. Dette vil også være i

[62] Krav om manuell kontroll finnes i Europaparlamentets og Rådets direktiv (EU) 2016/680 om personvern for politi og påtalemyndighet mv. artikkel 11. Direktivet er nyere enn politiregisterloven, men er like fullt gjeldende for dagens krav.
[63] Ot.prp. nr. 108 (2008 – 2009) s. 294.

tråd med politiets adgang til å drive kameraovervåkning etter politiloven § 6 a, som må ligge innenfor oppgavene i politiloven § 2 nr. 1 til 4, hvor særlig nr. 1 til 3 omhandler kriminalitetsbekjempelse.

4.3.3 Nødvendighetskravet i politiregisterloven §§ 5 og 7

Politiregisterloven §§ 5 og 7 oppstiller videre krav til behandling av overvåkningsmaterialet som er innhentet. I dette underkapittelet skal jeg vurdere hva disse bestemmelsene åpner for ved bruk av ansiktsgjenkjenning med fotoregisteret som referansegrunnlag.

Politiregisterloven § 5 oppstiller overordnede regler for hvem politiet kan behandle opplysninger om, og når slik behandling kan skje. Første punktum oppstiller en formålsbegrensning, hvor behandlingen avgrenses til «når det er nødvendig ut fra formål som nevnt i § 4». Andre punktum gir ytterligere begrensninger som varierer ut fra om politiet driver etterforskende eller forebyggende arbeid (nr. 1 og 2). Nr. 3 omhandler politiets service- og bistandsfunksjon etter politiregisterloven § 2 nr. 13 bokstav b). Oppgaven avgrenser som nevnt mot denne delen av politiets arbeid.

Nr. 1 omhandler behandling av opplysninger i «den enkelte straffesak». Ordlyden viser til politiets etterforskende virksomhet. Denne forståelsen støttes av forarbeidene.[64] Behandling av opplysninger for dette formål skal skje i samsvar med «reglene i straffeprosessloven». Av hensyn til temaet i dette kapittelet, som er lovhjemmelens rekkevidde ved bruk av fotoregisteret som referansegrunnlag, går jeg ikke nærmere inn på reglene i straffeprosessloven.

I etterforskende virksomhet kan kamerafotografi sammenlignes med bilder i sporregisteret, fordi det der er registrert fotografier av personer med «ukjent identitet» som «antas å ha tilknytning til uoppklart straffesak». Dette kan bidra til at politiet kan få informasjon om personer det ønsker å komme i kontakt med eller ønsker informasjon om. Ved bruk av sanntidsgjenkjenning kan personen identifiseres ved at politiet kan rykke ut og slik avklare viktige opplysninger. Ved bruk av ettertidsgjenkjenning kan politiet få annen informasjon som kan være relevant for den videre etterforskningen, for eksempel viktige bevis.

[64] *Ibid.*

Som nevnt i kapittel 3, kan sporregisteret inneholde bilder av flere identiteter enn dem som har, eller er mistenkt for å ha, begått et lovbrudd. Ordlyden «antas å ha tilknytning til en uoppklart straffesak» i politiregisterforskriften § 46-5 fjerde ledd, tilsier at også andre personer som kan gi opplysninger til saken, kan registreres. Dette kan for eksempel være personer som er blitt utsatt for en kriminell handling, eller vitner. Dersom politiet antar at en person som er avbildet på et kamerafotografi i forbindelse med en kriminell handling, har tilknytning til saken, kan politiet legge bildet inn i fotoregisteret og bruke ansiktsgjenkjenning for å forsøke å få treff på personen på et senere tidspunkt. Dette er altså en nyttig metode som kan anvendes av politiet i deres arbeid med å få kontakt med personer det antas er relevante for etterforskningen.

Også personer som er «mistenkt» eller «siktet» for en handling som kan medføre frihetsstraff, og derfor er i etterforskningsregisteret, kan gjenkjennes ved teknologibruken (se politiregisterforskriften § 46-5 tredje ledd). Teknologien kan for eksempel brukes for å finne en person som har unndratt seg straff. Ved bruk av ansiktsgjenkjenning i ettertid, kan politiet få oversikt over hvor personen befinner seg (for eksempel hvilket område eller hvilken by), og slik ha en viss kontroll på vedkommendes bevegelser. Ved bruk av sanntidsgjenkjenning vil teknologien kunne medføre at politiet kan reagere raskt og rykke ut og pågripe vedkommende.

Videre kan personer som tidligere har vært straffedømt, og som dermed finnes i identitetsregisteret, gjenkjennes ved bruk av ansiktsgjenkjenningsteknologi med politiets fotoregister som referansegrunnlag. Dette kan av og til være problematisk, fordi informasjonen verken er nødvendig etter § 5 eller relevant etter § 6 (se avsnitt 4.3.4 nedenfor) fordi politiet ikke nødvendigvis har behov for å gjenkjenne vedkommende (for eksempel fordi det ikke er større fare for at den registrerte vil begå lovbrudd, enn det er fare for at andre gjør det). I slike tilfeller har politiet hjemmel i politiregisterloven § 8 tredje ledd til å innhente opplysningene og lagre dem så lenge det trengs for å avgjøre relevansen av dem. Kanskje bør lovgiver vurdere å vedta et individuelt begrunnelseskrav for enhver person det ønsker å gjenkjenne, slik at politiet må «flagge» de personene det er aktuelt å gjenkjenne.

Politiregisterloven § 5 andre punktum nr. 2 begrenser politiets adgang til å behandle opplysninger for «kriminalitetsbekjempelsen utenfor den enkelte straffesak». Ordlyden viser

til politiets kriminalitetsforebyggende arbeid. Forarbeidene bekrefter forståelsen, og tilføyer at bestemmelsen gir «anvisning på hvilke personer det kan behandles opplysninger om og hvilke omstendigheter som må foreligge for at slik behandling kan skje».[65] Bestemmelsen lister opp en rekke persongrupper som kan gjenkjennes i politiets forebyggende arbeid. For mitt formål, som er å drøfte politiets anledning til å gjenkjenne personer i politiets fotoregister, er det kun tidligere straffedømte (forskriften § 46-5 første og andre ledd), mistenkte eller siktede (tredje ledd) og ukjente personer med antatt tilknytning til et straffbart forhold (fjerde ledd) som det er relevant å drøfte gjenkjennelsen av. Derfor vil ikke alle alternativene være relevante her.

Bokstav a) første punktum uttrykker at det kan behandles opplysninger om en person som «er knyttet til et miljø hvor en vesentlig del av virksomheten består i å begå lovbrudd, eller ut fra andre objektive holdepunkter kan antas å begå slike». Ordlyden gir anledning til å behandle opplysninger om personer som politiet antar er en del av et kriminelt miljø. Av forarbeidene følger det at det i utgangspunktet ikke er tilstrekkelig at «en person tidligere er dømt for å ha begått kriminelle handlinger».[66] Dette innebærer både et krav om gjentakelsesfare og et forholdsmessighetskrav: Jo mer alvorlig et antatt lovbrudd er, jo lavere terskel for registrering.[67]

Paragraf 5 nr. 2 bokstav a) åpner derfor ikke nødvendigvis for at enhver person i politiets identitetsregister kan gjenkjennes. Gjenkjennelse bør særlig dreie seg om personer som gjentatte ganger har begått kriminalitet, eller som har begått svært alvorlige lovbrudd. Det er noe uklart hvor terskelen for behandling etter denne bestemmelsen videre går. Dette bør lovgiver avklare dersom ansiktsgjenkjenningsteknologi skal kunne anvendes i større utstrekning enn den allerede blir i dag.

Det kan tenkes at bokstav a) gir politiet anledning til å anvende teknologien for å gjenkjenne personer som det anser kan være en fare for allmennhetens sikkerhet. Situasjonen kan for eksempel være overvåkning på en konsert. Bruk av ansiktsgjenkjenning i sanntid kan gi politiet varsler ved treff på personer i identitetsregisteret dersom kravene i politiregisterloven § 5 nr. 2 bokstav a) er oppfylt, for eksempel fordi vedkommende ved gjentatte anledninger er dømt for et lovbrudd. Det er også grunn til å mene at en person som er dømt for et svært

[65] *Ibid*.
[66] *Ibid*. s. 295.
[67] *Ibid*. s. 294-295.

alvorlig lovbrudd, for eksempel terrorvirksomhet, i slike tilfeller vil kunne gjenkjennes. Ved treff kan politiet rykke ut og forebygge eventuelle alvorlige hendelser.

Politiregisterloven § 5 andre punktum nr. 2 oppstiller også en rekke andre persongrupper som det kan «behandles» opplysninger om i forebyggende arbeid, for eksempel en person som «er blitt […] utsatt for et lovbrudd» (bokstav c) og en person som «er informant» (bokstav d). I enkelte tilfeller vil slike persongrupper finnes i sporregisteret (fordi de oppfyller de respektive vilkårene i politiregisterforskriften § 46-5 fjerde ledd), og disse vil i så fall kunne gjenkjennes også i den forebyggende virksomhet. Dette kan virke noe urimelig, ettersom en «informant» ikke alltid vil ha betydning for politiets forebyggende arbeid. Her synes det å være behov for mer spesifikke lovregler for hvem politiet kan gjenkjenne i forebyggende virksomhet. Ansiktsgjenkjenning gir politiet adgang til automatisk å bruke hele fotoregisteret (alle tre typene) i alle slags saker, noe som noen ganger kan medføre problemer.

Fordi ansiktsgjenkjenningsteknologi medfører behandling av biometriske personopplysninger, må politiets bruk av kamerafotografiene med det formål «entydig å identifisere en fysisk person» være «strengt nødvendig ut fra formålet med behandlingen», jf. politiregisterloven § 7. Dette gjelder uavhengig av om behandlingsformålet er etterforskende eller forebyggende. Ordlyden «strengt nødvendig» skjerper forholdsmessighetskravet, og betyr at behandlingen må være avgjørende. Forarbeidene forklarer vilkåret noe omstendelig: De aktuelle opplysningene må være «av vesentlig betydning for formålet», og det må «være en klar sammenheng mellom den sensitive opplysningen og formålet med behandlingen, eller at unnlatelsen av å behandle opplysningen kunne føre til at man forpurrer eller hindrer formålet med behandlingen».[68] Politiregisterforskriften § 4-3 er klarere, og der fremgår det at vilkåret innebærer at behandlingen av opplysningene kan skje «dersom dette er den eneste muligheten til å oppnå formålet med behandlingen». Ved politiets bruk av ansiktsgjenkjenningsteknologi må det antas at politiet allerede har avklart formålet med beslutningen om å koble videostrømmen mot fotoregisteret.

4.3.4 Kvalitetskravet i politiregisterloven § 6

Politiregisterloven § 6 oppstiller krav til kvaliteten på overvåkningsfotografiene politiet vil behandle. I denne sammenheng er det tilstrekkelig å vurdere første ledd nr. 1 og 2. Nr. 3, som

[68] *Ibid*. s. 297.

omhandler lagringsadgangen, vil vurderes i underkapittel 5.4. Bakgrunnen for kvalitetskravet er særlig rettssikkerhetshensyn. Vilkåret skal sørge for at politiet ikke bygger saker på opplysninger som kan gi et uriktig bilde av virkeligheten.

Opplysningene som behandles etter § 6 første ledd nr. 1 skal «være tilstrekkelige og relevante for formålet med behandlingen». Ordlyden «tilstrekkelige» tilsier at opplysningene gir nok informasjon til ikke å kunne misforstås eller mistolkes ut fra hensikten med behandlingen. Kravet er ifølge forarbeidene relativt, og innebærer at opplysningene er fullstendige, «det vil si utfyllende og detaljerte». Kravet «hindrer at opplysningene gir et misvisende eller uriktig bilde av en person eller en situasjon».[69] Det samme følger av politiregisterforskriften § 5-1 første ledd.

Tilstrekkelighetskravet innebærer at opplysningene skal gi en dekkende oppfatning av saken. Særlig mengden opplysninger er sentralt. Det er forskjell på en situasjon hvor overvåkningskameraet kun har resultert i ett eller noen få bilder, og en situasjon hvor det finnes flere bilder av den registrerte personen fra flere vinkler og med ulik avstand. Et høyt antall fotografier kan være nødvendig for å få et tilfredsstillende sammenligningsgrunnlag. Vilkåret er særlig aktuelt ved den siste manuelle kvalitetssjekken.

Ordlyden «relevante» tilsier at opplysningene kan være av interesse for politiets formål og virksomhet. Kravet innebærer at opplysningene «har en tilknytning til formålet og er nødvendige for behandlingen på det konkrete tidspunkt».[70] Politiet kan ikke behandle opplysningene dersom «formålet kan oppnås ved at det behandles færre opplysninger eller mindre sensitive opplysninger».[71] En slik forståelse følger også av politiregisterforskriften § 5-1 andre ledd. Ifølge forarbeidene vil kravet variere: Tidlig i etterforskningen kan det være større behov for å behandle flere typer opplysninger, fordi politiet ennå ikke vet hvilken informasjon det har behov for. Senere kan innsamlingskravene bli strengere.[72] Ifølge Mæland handler relevanskravet om «hvor mange opplysninger det er nødvendig å ha om de personer man behandler opplysninger om».[73] Dette medfører at politiet i tråd med politiregisterloven §

[69] *Ibid*. s. 296.
[70] *Ibid*.
[71] *Ibid*.
[72] *Ibid*.
[73] Auglend og Mæland (2016) s. 1124.

8 første og tredje ledd må slette unødvendig informasjon etterhvert som det forstår hvilke opplysninger som er overflødige for formålet.

Vilkåret om at opplysningene må være «tilstrekkelige» og «relevante» i politiregisterloven § 6 første ledd nr. 1 medfører også at det ikke kan behandles opplysninger om personer som ikke er av relevans for politiets formål. Situasjonen kan for eksempel være at politiet i forebyggende virksomhet ønsker kontroll med et stort idrettsarrangement med flere tusen deltakere. Ved bruk av sanntidsgjenkjenning har politiet som nevnt fire måneder på seg til å avgjøre relevansen av opplysningene som kommer inn gjennom videostrømmen, se politiregisterloven § 8 første ledd. Alle opplysninger som ikke er relevante innen utløpet av firemånedersfristen, må altså slettes.

Politiregisterloven § 6 nr. 2 krever at opplysningene som behandles, er «korrekte og oppdaterte». Ordlyden tilsier at opplysningene må være riktige, nøyaktige og gjeldende på behandlingstidspunktet. Ifølge forarbeidene er kravet situasjonsbetinget. I situasjoner hvor det finnes ett korrekt svar, «kan kravet til korrekthet likestilles med hva som er riktig eller sant». Ved beskrivelse av hendelser «er opplysninger korrekte dersom de beskriver det som faktisk har skjedd».[74] Vilkåret skal ifølge politiregisterforskriften § 5-2 første ledd første punktum forstås som at «opplysningene fremstår som riktige på grunnlag av de opplysningene som foreligger». Begrepet «oppdaterte» gir anvisning om at opplysningene som skal behandles, er ferske. Ifølge politiregisterforskriften § 5-2 andre ledd må opplysningene være «fullstendige». Kravene til at opplysningene er korrekte og oppdaterte, henger tett sammen og vil derfor behandles samlet.

Kravene om at fotografiene må være korrekte og oppdaterte, kan medføre at register- og kamerafotografiene er for uklare til at det kan være grunnlag for å stole på den automatiske ansiktsgjenkjenningen. Selv om bildet i seg selv er korrekt, i den forstand at det er troverdig og gjenspeiler virkeligheten, kan de innhentede opplysningene ha en slik kvalitet at det kan være vanskelig å fastslå om opplysningene som kan leses ut av bildet, er korrekte. Videre behandling av opplysninger kan derfor være problematisk ut fra rettssikkerhetsbetraktninger. Det er uklart hvor strenge krav som bør stilles i slike situasjoner, og kravene vil nødvendigvis variere. I vurderingen kan faktorer som personenes avstand fra og vinkel til

[74] Ot.prp. nr. 108 (2008 – 2009) s. 296.

overvåkningskameraet, lys og mørke, værforhold og bekledning ha betydning. Siden slike faktorer ofte er vanskelig å gjøre noe med, kan kvaliteten på kamerafotografiene ofte være problematisk.[75]

Paragraf 6 andre ledd sier at det er anledning til å behandle «[i]kke-verifiserte opplysninger» hvis «det er nødvendig ut fra formålet med behandlingen». Ordlyden gir anledning til å behandle opplysninger selv om det ikke er sikkert at opplysningene er korrekte, dersom det er nødvendig ut fra formålet med behandlingen. Denne forståelsen støttes av forarbeidene, hvor det følger at ikke-verifiserte opplysninger ikke nødvendigvis er «sammenfallende med ikke korrekte opplysninger».[76] Videre er det til tider vanskelig å avgjøre om opplysningene som gjenkjennes, er korrekte og oppdaterte før det er foretatt en manuell vurdering. Bestemmelsen gir altså politiet anledning til å anvende både ettertids- og sanntidsgjenkjenning, fordi det kan hente inn og behandle informasjon fra kamerafotografiene, før det vet om opplysningene er «korrekte og oppdaterte».

Kvalitetskravet stiller også krav til kvaliteten på *teknologien* og hvordan den virker i forhold til referansegrunnlaget. Dette er viktig for å hindre altfor mange feiltreff, for eksempel i form av «falske positive» treff, det vil si uriktige matcher, eller at gjenkjenningen er så usikker at opplysningene ikke kan tjene som bevis i en eventuell straffesak. Siden ansiktsgjenkjenningssystemer er trent opp på basis av et visst bildemateriale, kan dette materialet ha betydning for gjenkjenningens kvalitet.

London Metropolitan Police gjennomførte i årsskiftet 2018/2019 flere forsøk med bruk av ansiktsgjenkjenning i sanntid. Referansematerialet besto av personer som har unndratt seg arrest, individer som man trodde mest sannsynlig ville begå voldskriminalitet, og personer som politiet mente kunne utgjøre en trussel mot den offentlige trygghet.[77] Undersøkelsen ble gjennomført ved at personer som ga treff i det på forhånd bestemte registeret, ble stoppet av en polititjenesteperson, som undersøkte om identiteten stemte overens med treffet.

Forsøket medførte en rekke falske positive treff. Ved en test i Soho, London, 17. og 18. desember 2018, var for eksempel 11 av de til sammen 14 personene som systemet mente

[75] European Union Agency For Fundamental Rights (2019) s. 10.
[76] Ot.prp. nr. 108 (2008 – 2009) s. 297.
[77] European Union Agency For Fundamental Rights (2019) s. 12.

«matchet» mot registeret, falske positive treff, eller så usikre at nærmere etterforskingsskritt ikke ble igangsatt.[78] Det samme gjelder testen som ble gjennomført i Romford, London, 14. februar 2019, hvor 13 av 16 resultater var falske positive eller for usikre til å fortsette behandlingen.[79] Forsøket bør være en viktig lærdom, siden det viser at teknologien må ha så høy kvalitet at den ikke gir for mange feiltreff. For mange falske positive treff medfører en rettssikkerhetsfare fordi det kan medføre behandling av informasjon på feilaktig grunnlag, noe som i verste fall kan resultere i uriktige domfellelser.

4.4 Konklusjon

Som påvist, gir bestemmelsene i politiregisterloven og -forskriften hjemmel for automatisk matching av videostrømmen fra politikameraet mot politiets fotoregister, både i ettertid og i sanntid. Det er også kommet frem at politiets mulighet for behandling av treffene, er noe forskjellig for etterforskende og forebyggende arbeid. Videre synes bruk av politiets fotoregister som referansegrunnlag å være en legitim og rimelig avgrensning for bruken av ansiktsgjenkjenningsteknologi, ettersom bruk av dette registeret forhindrer unødige inngrep i øvrige personers privatliv, samtidig som det gjerne er de registrerte personene som er av særlig interesse for politiet.

Gjennomgangen i dette kapitlet viser imidlertid at det ikke er noen lovbestemmelser som positivt hjemler politiets bruk av ansiktsgjenkjenning. Dette gjør det noe uklart hva lovreglene egentlig innebærer, noe som *kan* åpne for vilkårlighet og formålsutglidninger. Disse forhold gjør det rimelig å reise noen spørsmål knyttet til forholdsmessigheten ved slik teknologibruk.

[78] Fussey og Murray (2019) s. 111-112.
[79] *Ibid*. s. 114-115.

5 Er ansiktsgjenkjenning etter dagens lovregler forholdsmessig i lys av Grunnloven § 102 og EMK artikkel 8?

5.1 Innledning

I HR-2019-1226-A (avsnitt 94) ble forholdsmessighetsvurderingen uttrykt som om de norske reglene «oppfyller de [forholdsmessighets]krav som er oppstilt i EMDs praksis». Dommen gjelder spørsmål om forholdsmessighet ved registrering av DNA-profilen til en person som var dømt til 18 måneders fengsel for skattesvik. I forholdsmessighetsvurderingen viser retten i avsnitt 57 til *S. og Marper mot Storbritannia* (avsnitt 101) og uttaler at det må ses hen til «[b]ehovet for inngrepet» og om «lovgivers vurderinger er relevante og tilstrekkelige». Høyesterett viser videre til avsnitt 103 i samme dom, hvor det fremheves at de nasjonale lovbestemmelsene «må gi garantier – «appropriate safeguards» – mot bruk av personopplysninger som er uforenlig med artikkel 8». I den forbindelse må lovgivningen «sikre at lagringen av slike opplysninger er «relevant and not excessive in relation to the purposes for which they are stored»», og «gi[r] effektiv beskyttelse mot misbruk av opplysningene».

Siden dommen omhandler spørsmål om hvorvidt et konkret tilfelle er i tråd med EMDs krav til registrering av DNA-profiler etter EMK artikkel 8, viser Høyesterett til en rekke momenter som ifølge EMD er relevante i forholdsmessighetsvurderingen. Blant momentene er spørsmålet om registreringen gjelder en person som er domfelt (avsnitt 65), om lovbruddet er tilstrekkelig alvorlig (avsnitt 67), om reglene for slettingsadgang er tilstrekkelig differensierte (avsnitt 71), intensiteten i inngrepet (avsnitt 75), og lovgivers vurderinger og avveininger ved utformingen av lovreglene (avsnitt 77 flg.).

Forholdsmessighetsvurderingen er altså en bred vurdering, og det vil føre for langt å foreta en fullstendig utgreiing av den. Dessuten er ikke alle momentene relevante for min problemstilling. Problemstillingen i dette kapitlet er hvorvidt dagens regelverk ut fra en forholdsmessighetsvurdering oppstiller tilstrekkelige vilkår og sikkerhetsforanstaltninger som kan forhindre vilkårlighet og misbruk. Dette omtaler EMD (og Høyesterett – som sitert ovenfor) ofte som «appropriate safeguards». Dette blir generelt vurdert i underkapittel 5.3, og i underkapittel 5.4 skal jeg vurdere dette konkret opp mot reglene for lagringsadgang i

politiregisterforskriften § 46-15. For å underbygge denne drøftelsen, skal jeg først vurdere momentet knyttet til hvorvidt lovgivers vurderinger og avveininger ved utformingen av lovreglene er «relevante og tilstrekkelige» ut fra en forholdsmessighetsvurdering (underkapittel 5.2). Dette gjør jeg fordi lovgivers vurderinger og utforming av reglene henger nøye sammen med sikring mot vilkårlighet og misbruk: At hjemmelsgrunnlaget ikke er spesifikt utformet for denne nye teknologien, kan medføre fare for bruks- og formålsutglidning, som igjen øker faren for vilkårlighet og misbruk. EMDs forholdsmessighetskrav retter seg altså både mot lovgiver, og oppstiller krav til utforming av reglene, og mot domstoler og påtalemyndighet, og oppstiller begrensninger for tolkning og anvendelse av reglene. Ved vurderingen av i hvilken grad lovbestemmelsene sikrer mot vilkårlighet og misbruk, er det særlig domstolenes tilnærming til spørsmålet som skal vektlegges. For norsk rett er det dermed Høyesteretts tilnærming til spørsmålet som må legges til grunn. Temaet er fremdeles politiets bruk av ansiktsgjenkjenning på overvåkningsfotografier fra politiets egne overvåkningskameraer og med politiets fotoregister som referansegrunnlag.

5.2 Er lovgivers vurderinger «relevante og tilstrekkelige»?

I HR-2019-1226-A legger Høyesterett til grunn at de vurderinger lovgiver foretar i forbindelse med lovvedtakelsen er et viktig moment i vurderingen av lovens forholdsmessighet (se avsnitt 78 og 85). Dette skjer gjerne ved presisereringer i forarbeidene. Høyesterett viser til en rekke forarbeidsuttalelser og konkluderer i avsnitt 85 med at lovgiver «har foretatt grundige vurderinger av forholdsmessigheten av DNA-registreringen», særlig siden relevante hensyn er avveid.

Selv om også fotoregisteret er vurdert i lovforarbeidene, står det ingenting om bruk av ansiktsgjenkjenningsteknologi. Siden lovgiver sannsynligvis ikke har vurdert teknologibruken ved vedtakelsen av politiregisterloven og -forskriften, kan det spørres om det å hjemle teknologien i disse lovbestemmelsene er problematisk ut fra forholdsmessighetsbetraktninger. Dette skyldes særlig lovbestemmelsenes tilgjengelighet: Anvendelse av de gjennomgåtte bestemmelsene i politiregisterloven og -forskriften som regulerer bruk av ansiktsgjenkjenningsteknologi, kan virke noe komplisert, også for en jurist. Selv om bestemmelsene gir fullgode lovhjemler for teknologibruken, er det at reglene er vanskelig tilgjengelige, uheldig ut fra forutberegnelighetshensyn. Lovhjemlene er heller ikke

tilstrekkelig klart avgrenset hva gjelder bruksområde. Siden ansiktsgjenkjenningsteknologi er en ny teknologi, burde lovgiver kanskje vurdere å oppstille egne lovregler for anvendelsen, slik det i politiregisterforskriften er gjort for DNA-, fingeravtrykks- og fotografiteknologien. Dette kan for eksempel løses med et eget kapittel som regulerer behandling av opplysninger med ansiktsgjenkjenningsteknologi. Eksplisitte lovregler for bruk av denne teknologien kan utgjøre et viktig rettssikkerhetsaspekt som sørger for klare lovregler, åpenhet rundt bruken og forutberegnelighet for borgerne.

Lovgivertaushet kan medføre uklarhet knyttet til hvordan lovteksten skal forstås: Hvordan skal rettsanvender forholde seg til at lovgiver ikke eksplisitt har tatt stilling til hva lovteksten innebærer? Særlig problematisk er dette ved tolkning av forskrifter, fordi det sjelden finnes tilgjengelige forarbeider til disse. Rettsanvender bør være varsom med å tolke lovteksten vidt i slike tilfeller. Grunnen til dette er rettssikkerhetsbetraktninger og at sammenstilling av flere lovtekster for tilpasning i enkelttilfeller, kan medføre vilkårlighet og formålsutglidninger. Dette kan tilsi at lovgivers vurderinger ikke er «relevante og tilstrekkelige» for anvendelse på ansiktsgjenkjenningsteknologi. Ut fra dette blir det naturlig å føre vurderingen over i et spørsmål om anvendelse av ansiktsgjenkjenningsteknologi med hjemmel i den aktuelle lovgivningen i tilstrekkelig grad sikrer mot vilkårlighet og misbruk.

5.3 Gir reglene «effektiv beskyttelse mot misbruk av opplysningene»?

Formålsutglidning har allerede skjedd på DNA-rettens område. I HR-2018-2241-U vurderte Høyesterett formålsbegrensingens rekkevidde «[i] mangel av uttrykk for en klar lovgivervilje» (se avsnitt 20). Høyesterett tolket politiregisterloven § 12 sjette ledd første punktum, som sier at DNA-opplysninger kun skal brukes i «strafferettspleien», utvidende, til å kunne benyttes som bevis for et sivilt formål, nærmere bestemt fastsettelse av farskap. Det er naturlig at lovgiver ikke kan liste opp ethvert tilfelle som opplysningene *ikke* skal anvendes på (dette er jo potensielt en uendelig rekke tilfeller). Mangel på presiseringer, eksempelvis i lovforarbeidene, skaper likevel usikkerhet og dermed også mulighet for formålsutglidninger. I nevnte dom tolker flertallet tilfellet på tvers av klar lovtekst, fordi det mener dette gir det beste resultatet i den konkrete saken. At formålsutglidning er en utfordring, støttes av HR-2020-1776-A, hvor Høyesterett i vurderingen av om vevsprøver fra en avdød person kunne utleveres til påtalemyndigheten i forbindelse med en straffesak, vektla at «utlevering i

enkelttilfeller uten klar forankring i helseforskningsloven § 27 [kan] åpne for formålsutglidning […]» (se avsnitt 39).

Når formålsutglidning skjer på et område hvor det av lovteksten fremgår klart for hvilke formål opplysningene kan anvendes (som i HR-2018-2241-U), er formålsutglidningen tydelig. Formålsutglidning på et område hvor det i utgangspunktet ikke finnes spesifikke lovregler for den aktuelle teknologibruken, som for ansiktsgjenkjenning, vil være vanskeligere å oppdage fordi det ikke nødvendigvis fremgår eksplisitt. Dersom politiet skulle bruke teknologien til annet enn «sammenligning», «gjenkjennelse og identifikasjon» og «verifisering av identitet» (jf. politiregisterforskriften § 46-1 første ledd tredje punktum), ville vi stå for overfor noe slikt. Slik «skjult» formålsutglidning kan være uheldig. Kravet til lovhjemlenes presisjon, og betydningen av om lovgiver har sett for seg teknologianvendelsen på lovgivningstidspunktet eller ikke, må ses i lys av de mulighetene teknologien gir politiet, og intensiteten i inngrepet teknologibruken medfører.

I HR-2019-1226-A avsnitt 89 argumenterer Høyesteretts flertall for at registrering av en persons DNA-profil ikke utgjør en stor fare for misbruk, fordi opplysningene ikke sier «noe om […] utseende eller kroppsbygning». Slik skiller DNA-teknologien seg fra ansiktsgjenkjenningsteknologi, som nettopp registrerer viktige trekk ved en persons utseende. Høyesterett argumenterer også for at regelen for destruering av biologiske opplysninger i politiregisterforskriften § 45-18 sikrer «en garanti mot senere misbruk og spredning av sensitive opplysninger». Jeg kan ikke se at det finnes en liknende regel for destruering av fotografiopplysninger. Mangel på differensierte lovregler på dette punktet tilsier at muligheten for at de biometriske personopplysningene fra ansiktsgjenkjenningsteknologien kan komme på avveie, og åpner slik for misbruk.

Som argumentert for i underkapittel 1.2, åpner ansiktsgjenkjenningsteknologi for nye muligheter som skiller seg fra andre former for biometrisk teknologi. En forskjell gjelder antallet personer som berøres av teknologibruken. Ved DNA- og fingeravtrykksteknologi må politiet aktivt avgjøre hvilken DNA-profil eller hvilket fingeravtrykk som skal analyseres. Ved bruk av ansiktsgjenkjenning vil derimot et uvisst antall personer som beveger seg over et område kunne filmes og potensielt gjenkjennes, selv om politiet kun har behov for én konkret gjenkjenning. Dette vil gjelde for både ettertids- og sanntidsgjenkjenning. Dermed vil også

andre personer enn de politiet har behov for gjenkjennes, dersom de finnes i fotoregisteret. Selv om politiregisterloven § 8 gir anledning til behandling i slike tilfeller, kan slik overvåkning virke nokså inngripende, fordi politiet på denne måten kan få en rolle som samfunnsvokter og gis en overvåkningsmulighet politiet ikke tidligere har hatt. Regler for å trygge rettssikkerheten til de øvrige personene, for eksempel ved å flagge enkeltpersoner som det ønskes treff på, og gode regler for fortløpende sletting, vil kanskje kunne bøte på problemet (jf. underkapittel 4.2). Mangel på differensierte regler på dette punktet tilsier at reglene ikke er presist nok utformet for bruk på ny teknologi.

Dagens kritikk av ansiktsgjenkjenningsteknologi går særlig på teknologibrukens konsekvenser. Bruken gir for eksempel muligheter til å skyve på grensene for hva myndighetene kan finne ut om oss. Datatilsynet frykter at teknologibruken kan gå på bekostning av individets frihet. Særlig utsatt er ytringsfriheten (Grunnloven § 100 og EMK artikkel 10). Datatilsynets omtaler dette som en «nedkjølingseffekt», hvor teknologien kan innebære en fare for «nedkjøling i et åpent, demokratisk samfunn» og dermed «en svekkelse av den reelle ytringsfriheten».[80] Også teknologirådet har reist innvendinger mot bruken. De sterkeste innvendingene gjelder teknologiens adgang til å drive masseovervåkning og kontroll.[81] Lovreglenes generelle utforming kan altså gjøre misbruk enklere. Dermed kan vi måtte spørre slik den romerske dikteren Juvenal (55-135) gjorde allerede for nærmere 2000 år siden: Hvem vokter vokterne?[82] Hvem skal sørge for at politiet ikke går utover sine avgrensede rammer og derigjennom misbruker sin makt? I den grad dette kan kontrolleres, er det lovgivers oppgave: For å hindre slike konsekvenser og frykt for misbruk, kan lovgiver oppstille egne lovbestemmelser som eksplisitt begrenser teknologibruken. Her har også domstolene en viktig oppgave i å være varsom med å tilpasse en generell lovtekst til enkelttilfeller. Utover dette vil bruken i stor grad måtte bygge på tillit.

Det kan se ut til at lovgiver er oppmerksom på de raske teknologiske endringene på fotografiteknologiens område, og at lovtekstene ikke er presise. Fotoregisterbestemmelsen i politiregisterloven § 13 er i år til vurdering i et høringsnotat fra Justis- og beredskapsdepartementet, hvor det foreslås å presisere § 13 til eksplisitt å nevne sporregisteret. Bakgrunnen for dette er ifølge departementet at «det for politiets arbeid med

[80] Datatilsynet (2020) s. 28.
[81] Tennøe (2020).
[82] Paulsen (2019) 23-24.

straffesaker er et klart behov for å kunne registrere foto […] av personer med ukjent identitet som antas å ha tilknytning til uoppklart straffesak».[83] Dette gjøres for å unngå «tvil om adgangen til å registrere [foto]opplysninger».[84] Arbeidet vil kunne medføre klarere lovtekst hva gjelder lovens virkeområde, og vil gjøre bestemmelsen mer i samsvar med de krav til forholdsmessighetsvurderingen som oppstilles av EMD.

5.4 Lagringsreglenes forholdsmessighet

5.4.1 EMDs vurderinger i *Gaughran mot Storbritannia*

Et sentralt moment i forholdsmessighetsvurderingen er, som allerede nevnt, om reglene sikrer at lagringen av personopplysninger er «relevant and not excessive in relation to the purposes for which they are stored» (se for eksempel HR-2019-1226-A avsnitt 57). Hvorvidt lagringen er «excessive», vil henge sammen med spørsmålet om lagringens nødvendighet. Det er derfor relevant å vurdere om de norske lagringsreglene i politiregisterloven § 46-15 er forholdsmessige i lys av Grunnloven § 102 og EMK artikkel 8.

Gaughran mot Storbritannia gjaldt lagring av biometrisk informasjon fra en tolv år gammel arrestasjon for promillekjøring. Ifølge engelsk rett kunne informasjon fra mistenktes DNA-profil, fingeravtrykk og fotografi oppbevares i politiets registre på ubestemt tid. Klageren mente dette var et brudd på retten til «privatliv» etter EMK artikkel 8.

En vesentlig del av forholdsmessighetsvurderingen i *Gaughran mot Storbritannia* gjelder direkte fastleggelse av statens skjønnsmargin i den konkrete saken. I avsnitt 85 fremgår det at dersom den nasjonale domstolen har foretatt en adekvat forholdsmessighetsvurdering ved avveiningen mellom klagerens personlige interesser og generelle offentlige interesser i saken, overprøver EMD bare forholdsmessigheten dersom det er «compelling reasons for doing so». I avsnitt 86 uttaler EMD at den mener tvingende grunner foreligger i denne saken. Det legges vekt på at det skjer en stadig utvikling på teknologifronten, noe som skaper en risiko for vilkårlighet, «especially where the technology available is continually becoming more sophisticated». I denne vurderingen bygger EMD på *Catt mot Storbritannia*.[85] I *Gaughran mot Storbritannia* (avsnitt 94) legger EMD til grunn at lagringsregler på ubestemt tid krever å at «certain safeguards [is] present and effective for the applicant».

[83] Justis- og beredskapsdepartementet (2020) s. 29.
[84] *Ibid*.
[85] Catt mot Storbritannia [J] no. 43514/15 avsnitt 114.

I den konkrete forholdsmessighetsvurderingen viser domstolen til at det i engelsk rett ikke er noen lovbestemmelse som gir klageren anledning til å søke om å få «the data concerning him deleted if conserving the data no longer appeared necessary in view of the nature of the offence, the age of the person concerned, the length of time that has elapsed and the person's current personality» (se avsnitt 94). Mangel på differensierte slettingsregler utgjorde et brudd på EMK artikkel 8.

5.4.2 Er de norske lagringsreglene forholdsmessige i lys av kravene i Grunnloven § 102 og EMK artikkel 8?

Den omtalte kritikken av bruk av ansiktsgjenkjenningsteknologi (jf. underkapittel 5.3) og vurderingene i *Gaughran mot Storbritannia* gjør det rimelig å spørre om de norske lagringsreglene for registerfotografi er forholdsmessige etter kravene i Grunnloven § 102 og EMK artikkel 8. Høyesteretts tilnærming til EMDs skjønnsmargin er omtalt av Stig H. Solheim i *Juridisk metode og tenkemåte*, hvor det fremgår at «[i]stedenfor å vise til skjønnsmarginen kan en nasjonal dommer vektlegge de samme argumentene for å definere terskelen for proporsjonalitet i sin konkrete sak. Dette inkluderer også momentet om hvorvidt lovgiver har foretatt en spesifikk vurdering av hvordan inngrepet vil ramme de ulike berørte interesser, og om denne avveiningen er funnet fair». Slik «kan norske domstoler […] komme frem til at lovgiver har et visst handlingsrom det ikke er naturlig for en dommer å prøve fullt ut».[86] For en nasjonal domstol er altså momentene i *Gaughran mot Storbritannia* direkte relevante for forholdsmessighetsvurderingen, og det er dette utgangspunktet jeg tar for den videre vurderingen. EMDs signal om betenkeligheter for personvernet ved teknologiutviklingen tilsier at lovgivningen er underlagt en aktiv domstolskontroll.

Politiregisterloven § 6 første ledd nr. 3 hjemler at opplysninger ikke skal «lagres lenger enn nødvendig ut fra formålet med behandlingen». Ifølge ordlyden plikter politiet å slette opplysningene når det ikke lenger er behov for å lagre dem ut fra behandlingens begrunnelse. Bestemmelsen skal ifølge forarbeidene leses i lys av forskrift om sletting.[87] Politiregisterforskriften § 46-15 første ledd første punktum pålegger en sletteplikt av foto i identitetsregisteret dersom den registrerte «rettskraftig frifinnes». Politiet plikter ifølge

[86] Solheim (2019) s. 384.
[87] Ot.prp. nr. 108 (2008 – 2009) s. 296-297.

ordlyden å slette foto av personer som i en rettskraftig dom frifinnes for de straffbare handlingene. I slike tilfeller har ikke politiet lenger behov for å lagre registerfotografiet ut fra formålet det i utgangspunktet ble samlet inn for.

Paragraf 46-15 første ledd andre punktum hjemler at sletting i identitetsregisteret ellers skal skje «senest 5 år etter at vedkommende er død» eller tidligere «dersom fortsatt registrering åpenbart ikke lenger vil være hensiktsmessig». Ordlyden «åpenbart ikke lenger vil være hensiktsmessig» oppstiller en unntaksregel og en ganske snever sletteplikt, og samsvarer med forbudet mot lagring lenger enn nødvendig i politiregisterloven § 6 nr. 3. Spørsmålet er når denne unntaksregelen kommer til anvendelse, og om dette er i tråd EMK artikkel 8.

Flertallet i HR-2019-1226-A uttaler at det må foretas en individuell vurdering av hvert enkelt tilfelle, men at politiets sletteplikt er restriktiv og skal forstås som en sikkerhetsventil (avsnitt 97). Selv om dommen gjelder politiets registrering av DNA-profil, var lagringsreglene et moment i vurderingen av om registreringen var uforholdsmessig. For DNA følger dette av § 45-17. Ordlyden i § 45-17 første ledd andre punktum og § 46-15 første ledd andre punktum er lik. Dette tyder på at bestemmelsene bør tolkes likt, og dommen synes derfor å ha overføringsverdi til dette kapittelets vurderinger.

Ved vurderingen av slettingsadgangens samsvar med EMD, erkjenner flertallet at lagringsadgangen i utgangspunktet er tidsubestemt og at slettingsadgangen er snever, men mener dette må gjelde uavhengig av lovbruddets alvorlighetsgrad, så lenge lovbruddet etter lovbestemmelsen kan medføre frihetsstraff (avsnitt 95 og 96). Spørsmålet er om den snevre slettingsregelen i andre punktum er tilstrekkelig differensiert ut fra de krav som oppstilles i EMDs praksis på dette punktet.

Det finnes ikke eksplisitte lovbestemmelser som gjør det enklere å få foto av seg slettet på grunnlag av handlingens alvorlighetsgrad, hvor lang tid det har gått, og den registrertes nåværende situasjon. Mangel på dette synes ikke å være helt på linje med uttalelsene i *Gaughran mot Storbritannia* avsnitt 94. Flertallet i Høyesterett mener dette har mindre betydning, fordi den snevre slettingsadgangen i politiregisterforskriften § 45-17 første ledd andre punktum (se avsnitt 97 i HR-2019-1226-A) oppfyller EMDs krav. Mindretallet mener derimot at vilkåret om at opplysningene i DNA-registeret skal slettes senest 5 år etter

vedkommendes død, «langt på vei vil fungere «as a norm rather than a maximum»», og at unntaksbestemmelsen i annet punktum nærmest aldri vil anvendes (avsnitt 121).

Flertallet og mindretallet er altså uenige om hvordan lagringsreglene skal tolkes: Kan en regel som hjemler lagring på ubestemt tid uten differensierte vurderinger, godtas fordi det er tatt inn en snever slettingsregel som nærmest aldri vil bli anvendt? På bakgrunn av disse betraktningene kan det spørres om flertallets vurdering av de norske reglene om lagringsadgang i HR-2019-1226-A vil stå seg i EMD.

Ifølge *Gaughran mot Storbritannia* (avsnitt 57) er det bare fem andre land i Europa som, slik som Norge, har «administrative or other similar specialised review of the necessity of the data detention».[88] Det kan likevel spørres om slettingsadgangen er så snever at den ikke vil tas i bruk. I motsetning til 19 andre europeiske stater har Norge ikke mulighet for «judicial review» av registreringen av biometriske opplysninger: Det følger av politiregisterloven § 55 annet ledd, jf. første ledd nr. 3, at det er «[r]iksadvokaten» som avgjør klager omhandlende sletting.[89]

Selv om Høyesterett har lagt til grunn at de norske reglene for sletting av DNA-opplysninger er forenlig med EMDs praksis, viser gjennomgangen at dette er usikkert. Dommens dissens svekker rettskildevekten. I tillegg er flertallets premisser blitt kritisert. Blant andre har Ragna Aarli argumentert for at slettingsmuligheten i det norske registeret ikke er reell.[90] Uavhengig av konklusjon synes jeg flertallets argumentasjon er noe svak. Staten prosederer på at enhver sak vil få en individuell vurdering, men flertallet stiller ikke spørsmål ved hva slik vurdering innebærer, og hvor sannsynlig det er at sletting foretas (avsnitt 97).[91]

[88] Kolsrud (2020).
[89] *Ibid*.
[90] Aarli (2019).
[91] Få dager før innlevering avsa Høyesterett en dom (HR-2020-2372-A) omhandlende forholdsmessighetsvurderingen i EMK artikkel 8 ved registrering av DNA-profil til en person dømt til 18 dagers fengsel og en bot på 40 000 kroner for forsøk på promillekjøring. Høyesterett mente slettingsadgangen for registrering av en persons DNA-profil var i tråd med EMDs praksis på området, men uttalte at Kripos i større grad ta i bruk den snevre slettingsadgangen i politiregisterforskriften § 45-17 i større grad, noe som det siste året også har skjedd (se avsnitt 48). Høyesterett synes å opprettholde den lave registreringsterskelen fra HR-2019-1226-A, og uttaler at «desto viktigere blir de øvrige trekk ved ordningen i forholdsmessighetsvurderingen» (avsnitt 43). Dette synes å underbygge relevansen av mine drøftelser i dette kapitlet.

5.4.3 Lagringsadgangens forhold til formålskravet – uttalelser i *Gaughran mot Storbritannia*

Avslutningsvis vil jeg si noe om EMDs bemerkninger hva gjelder formålet med lagring av informasjon. I både HR-2019-1226-A og *Gaughran mot Storbritannia* forstås formålet «å forebygge uorden eller kriminalitet» vidt: Hele formålet med lagring er kriminalitetsbekjempelse. I *Gaughran mot Storbritannia* legger EMD til grunn at lagringen av bildet hadde et langt bredere formål i å «assisting in the identification of persons who may offend in the future» (se avsnitt 75). Spørsmålet er imidlertid om man kan komme til et punkt hvor opplysningene har vært lagret så lenge at de ikke lenger kan begrunnes i kriminalitetsbekjempelse, slik at lagringen til slutt vil måtte begrunnes i andre formål. Den teknologiske utviklingen kan over tid gi informasjonen et annet potensial. I enkelte tilfeller vil man kunne tale om ny teknologibruk som igjen kan anvendes på stadig nye måter. Mer konkret er derfor spørsmålet om det skal godtas at opplysninger som lagres på ubestemt tid med et kriminalitetsbekjempende formål, skal kunne anvendes for eksempel 30 år senere og dermed kanskje for et annet formål enn opprinnelig tiltenkt, fordi teknologien muliggjør bruk som ikke fantes på det opprinnelige lagringstidspunktet.

Selv om lagring er en del av det kriminalitetsbekjempende arbeidet, og derfor ikke i seg selv kan anses å medføre en formålsutglidning, kan lang lagringstid medføre at det opprinnelige formålet bak lagringen ikke lenger er sentralt. Dette vil kunne skyve på forholdsmessighetsvurderingen. Situasjonen kan for eksempel være at en person for mange år siden har vært dømt for en straffbar handling som kan medføre frihetsberøvelse, og hvor fotografi av vedkommende derfor er lagret i identitetsregisteret etter politiregisterforskriften § 46-5 første ledd. Selv om det ikke lenger er mer sannsynlig at vedkommende i større grad enn andre vil begå et nytt lovbrudd, vil vedkommende som følge av lagringsreglene i politiregisterforskriften § 46-15, fremdeles finnes i fotoregisteret. Personen vil derfor kunne fanges opp av overvåkningskamera og gjenkjennes når vedkommende befinner seg på et område hvor det drives ansiktsgjenkjenning. I utgangspunktet er dette en legitim bruk etter dagens lovregler: Politiregisterloven § 8 gir politiet adgang til å behandle opplysninger for å finne ut om vilkårene for videre behandling er oppfylt. I et slikt tilfelle vil politiet ikke kunne legitimere videre behandling ut fra nødvendighetskravet i § 5, og opplysningene må derfor slettes. Det å bli gjenkjent ved bruk av ansiktsgjenkjenningsteknologi vil uansett være problematisk, fordi det gir politiet opplysninger om at en person befinner seg i et område og

på hvilket tidspunkt. Dette vil kunne gi en overvåkningsfølelse og kan virke stigmatiserende. Dette taler for at det er behov for mer presise regler for adgang til sletting. Den snevre regelen som hjemler adgang til sletting i dag, synes ikke å være helt adekvat.

6 Oppsummering

Norsk rett har altså ikke regler som eksplisitt hjemler bruk av ansiktsgjenkjenning, men som påvist i kapittel 4 stenger lovgivningen heller ikke for slik teknologibruk. Grunnen til dette er at reglene for behandling av opplysninger i politiregisterloven og -forskriften ikke er spesifikke hva gjelder anvendelsesmuligheter. Dette gir rettsanvender et visst handlings- og tolkningsrom. Dermed hjemler dagens regelverk automatisk matching av videostrømmen fra politikameraet mot fotoregisteret. Visse problemer oppstår imidlertid når teknologien utvikler seg med en slik hastighet at anvendelse av lovbestemmelsene på tilfeller som lovgiver ikke har tenkt på, blir mulig, slik det er ved bruk av ansiktsgjenkjenningsteknologi.

Kapittel 5 redegjør for betenkeligheter ut fra et rettssikkerhetsperspektiv, og diskuterer visse aspekter ved forholdsmessighetsvurderingen knyttet til teknologibruken ut fra dagens lovverk. Reglene for lagring av registerfotografier i politiregisterloven § 46-15 kan for eksempel anses for å være mer inngripende ved bruk av ansiktsgjenkjenning. Mangel på klart uttrykt lovgivervilje gjør det vanskelig å vite hva lovgiver har ment å omfatte med de aktuelle lovbestemmelsene. Vurderingen av forholdsmessighet ved bruk av intelligent videoanalyse blir dermed aktualisert. Derfor kan dagens lovverk neppe sies å oppstille tilstrekkelige vilkår og sikkerhetsforanstaltninger som kan forhindre vilkårlighet og misbruk, og det er kanskje best i en forholdsmessighetsvurdering å tolke reglene innskrenkende, inntil lovgiver mer eksplisitt har tatt stilling til bruk av ansiktsgjenkjenningsteknologi og utformer egne lovregler som gjør faren for vilkårlighet og formålsutglidninger mindre. Slik kan lovgiver sørge for et regelverk som ikke bryter med de menneskerettslige kravene i EMK artikkel 8.

Denne oppgaven tar opp bare en liten bit av et felt som i fremtiden ganske sikkert kommer til å få større betydning og økt oppmerksomhet. Juridiske (og etiske) problemer knyttet til kunstig intelligens og myndighetenes anvendelse av stadig mer høyteknologiske hjelpemidler vil nok øke. Den konklusjonen på oppgaven som peker fremover, er derfor at det er ønskelig at lovverket tilpasses og holder tritt med den hurtige teknologiske utviklingen.

Litteraturliste

Lover, forskrifter og direktiver

Lov 17. mai 1814 Kongeriket Norges Grunnlov (Grunnloven).

Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (Straffeprosessloven).

Forskrift 28. juni 1985 nr. 1679 om ordningen av påtalemyndigheten (Påtaleinstruksen).

Lov 4. august 1995 nr. 53 om politiet (politiloven).

Lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven).

Forskrift 20. september 2013 nr. 1097 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterforskriften).

Europaparlamentets og Rådets direktiv nr. 680/2016 av 27. april 2016 om beskyttelse av fysiske personer ved behandling av personopplysninger for å forebygge, etterforske, avdekke eller straffeforfølge lovbrudd eller gjennomføring av straffereaksjoner, og om fri utveksling av slike opplysninger og opphevelse av rådets rammebeslutning.

Internasjonale rettskilder

Convention for the Protection of Human Rights and Fundamental Freedoms, Roma, 4. November 1950. (Den europeiske menneskerettighetskonvensjonen).

Forarbeider

Ot.prp. nr. 108 (2008 – 2009) Om lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven).

Dok. nr. 16 (2011 – 2012) Rapport fra Menneskerettighetsutvalget om menneskerettigheter i Grunnloven.

Prop. 56 LS (2017 – 2018) Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om

innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordningen) i EØS-avtalen.

Prop. 131 L (2018 – 2019) Lov om informasjonstilgang m.m. for Partnerdrapsutvalget.

Avgjørelser fra EMD

Sunday Times mot Storbritannia [P], no. 6538/74 [1979] Series A no 30.

Leander mot Sverige [J], no. 9248/81 [1987] Series A no 116.

Amann mot Sveits [GC], no. 27798/95, ECHR 2000-II.

Peck mot Storbritannia [J], no. 44647/98, ECHR 2003-I.

S. og Marper mot Storbritannia [GC], no. 30562/04 og 30566/04, ECHR 2008.

Catt mot Storbritannia [J], no. 43514/15, 24. januar 2020.

Gaughran mot Storbritannia [J], no. 45245/15, 13. februar 2020.

Avgjørelser fra Høyesterett

Rt. 2014 s. 1105

HR-2016-2554-P

HR-2018-2441-U

HR-2019-1226-A

HR-2020-1776-A

HR-2020-2372-A

Litteratur

Aall, Jørgen, *Rettsstat og menneskerettigheter: en innføring i vernet om individets sivile og politiske rettigheter etter den norske forfatning og etter den europeiske menneskerettighetskonvensjon*, 5. utg., Bergen, Fagbokforlaget 2018.

Aarli, Ragna, «Kommentar til Høyesteretts dom om DNA-registrering», *Rett 24*, 9. august 2019, https://juridika.no/innsikt/kommentar-til-høyesteretts-dom-om-dna-registrering, (lest 16. september 2020).

Auglend, Ragnar L. og Mæland, Henry John, *Politirett*, 3. utg., Oslo, Gyldendal juridisk, 2016.

Bergo, Knut, «Tolking og anvendelse av lov, forskrift og forarbeider», i *Juridisk metode og tenkemåte*, Alf Petter Høgberg og Jørn Øyrehagen Sunde (red.), Universitetsforlaget 2019, s. 175-238.

Christensen, Tanja Kammersgaard, *De retlige rammer for politiets digitale overvågning*, Det Samfundsvidenskabelige Fakultet, Aalborg Universitet, Aalborg, 2. mars 2020.

Crawford, Kate og Paglen, Trevor, «Excavating AI The Politics of Images in Machine Learing Training Sets», 19. september 2019, https://www.excavating.ai, (lest 2. oktober 2020).

Datatilsynet, «Personvernundersøkelsen 2019/2020: Om befolkningens holdninger til personvern og kjennskap til det nye personvernregelverket», 2020, https://www.datatilsynet.no/contentassets/f33d4e1b374c4b5eba839a782ea833b9/personvernundersokelsen-2019-2020.pdf, (lest 21. september 2020).

Eikvil, Line, *Introduksjon til ansiktsgjenkjenningsteknologi*, nettseminar om ansiktsgjenkjenning Juristforbundets Tech Forum og Tekna Big Data, 27. oktober 2020, https://www.tekna.no/fag-og-nettverk/IKT/ikt-bloggen/se-direkte-ansiktsgjenkjenning/, (sett 27. oktober 2020).

E-post-korrespondanse med Kathrine Moe, ved Kripos' retts- og påtaleavdeling, personvernseksjonen, 2. til 6. november. Gjengitt med samtykke.

European Union Agency For Fundamental Rights, «Facial recognition technology: Fundamental rights considerations in the context of law enforcement», Wien 2019, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf, (lest 3. november 2020).

Fussey, Pete og Murray, Daragh, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognitoin Technology,* Economic & sosial research counsil 2019, https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf, (lest 27. august 2020).

Justis- og beredskapsdepartementet, *Høring – endringer i politiregisterloven og -forskriften – sletting av opplysninger i politiets registre mv*, Oslo 2020, https://www.regjeringen.no/contentassets/4195fe060d144757a1fa9fa26c65a8fe/horingsnotat---forslag-til-endringer-i-politiregisterloven-og-politiregisterforskriften.pdf, (lest 25. november 2020).

Kolsrud, Kjetil, «England felt for å lagre DNA-profil i promillesak», *Rett24*, 14. februar 2020, https://rett24.no/articles/england-felt-for-a-lagre-dna-profil-i-promillesak, (lest 16. september 2020).

Kommunal- og moderniseringsdepartementet, *Nasjonal strategi for kunstig intelligens*, Oslo 2020, https://www.regjeringen.no/contentassets/1febbbb2c4fd4b7d92c67ddd353b6ae8/no/pdfs/ki-strategi.pdf, (lest 20. november 2020).

Kvam, Bjarne, *Politiets persondatarett: En studie av hjemmels- og formålskrav ved politiets utlevering av personopplysninger til utlandet*, Det juridiske fakultet, Universitetet i Bergen, Bergen, 28. juni 2013.

London Policing Ethics Panel, «Interim report on live facial recognition», 2018, http://www.policingethicspanel.london/uploads/4/4/0/7/44076193/lpep_report_-_live_facial_recognition.pdf, (lest 4. november 2020).

Nätt, Tom Heine, «biometrisk identifisering» Store norske leksikon, 16. desember 2019, https://snl.no/biometrisk_identifisering, (lest 7. september 2020).

Paulsen, Jens Erik, «Holdninger til høyteknologi», i *Det digitale er et hurtigtog! Vitenskapelige perspektiver på politiarbeid, digitalisering og teknologi*, Sunde, Inger Marie og Sunde, Nina (red.), Fagbokforlaget 2019, s. 23-49.

Politidirektoratet, «Høringssvar – personvernkommisjon – innspill til mandat», 2018. Hentet fra https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/02-horinger-og-svar/personvernkommisjonen--innspill-til-mandat/politidirektoratets-horingssvar---personvernkommisjonen---innspill-til-mandat-.pdf, (lest 4. desember 2020).

Solheim, Stig H, «Rettsanvendelsesprosessen på EMK-rettens område», i *Juridisk metode og tenkemåte*, Alf Petter Høgberg og Jørn Øyrehagen Sunde (red.), Universitetsforlaget 2019, s. 360-385.

Teknologirådet, «Oversikt over sikkerhetsteknologier», Oslo 2007, https://teknologiradet.no/wp-content/uploads/sites/105/2018/06/Rapport-Oversikt-over-sikkerhetsteknologier.pdf, (lest 3. september 2020).

Tennøe, Tore, «Når kunstig intelligens går på trynet», 18. februar 2020, https://teknologiradet.no/ansiktsgjenkjenning-bor-forbys/, (lest. 15. november 2020).

Tennøe, Tore, Johannessen, Adele og Barland, Marianne, «Ansiktsgjenkjenning og personvern» *Fra rådet til tinget* 2020, https://teknologiradet.no/wp-content/uploads/sites/105/2020/02/RTT-ansiktsgjenkjenning_m-lenker.pdf, (lest 27. august 2020).

Tidemann, Axel, «dyp læring» Store norske leksikon, 28. november 2017, https://snl.no/dyp_læring, (lest 27. november 2020).

Tidemann, Axel, «kunstig intelligens» Store norske leksikon, 8. januar 2020, https://snl.no/kunstig_intelligens, (lest 20. november 2020).

Øyen, Ørnulf, *Straffeprosess*, 2. utg., Fagbokforlaget 2019.

Avisartikler

Almås, Gry Blekastad, «Digitalt diktatur: Kina planlegger sosialt poensystem», *NRK*, 5. februar 2019, https://www.nrk.no/urix/kinas-digitale-diktatur_-gar-du-pa-rodt-lys_-blir-du-uthengt-pa-storskjerm-1.14369439, (lest 22. november 2020).

Giske, Marit Elisabeth, «Blunk! så har du betalt», *DNB Nyheter*, 1. juli 2019, https://www.dnb.no/dnbnyheter/no/din-okonomi/blunk-sa-har-du-betalt, (lest 27. august 2020).

Selinger, Evan og Cahn, Albert Fox, «Did you protest recently? Your face might be in a database», *The Guardian*, 17. juli 2020, https://www.theguardian.com/commentisfree/2020/jul/17/protest-black-lives-matter-database, (lest 6. november 2020).