



AALBORG UNIVERSITET

DE RETLIGE RAMMER FOR POLITIETS BRUG AF ANSIGTSGENKENDELSE I EFTERFORSKNINGEN

Specialeafhandling

Juridisk Institut, AAU

*Udarbejdet af Caroline Egelund Christensen
15. maj 2025*

Titelblad

Studieretning: Jura

Vejleder: Lene Wachter Lentz

Emne: Straffeprocess

Titel: De retlige rammer for politiets brug af ansigtsgenkendelse i efterforskningen

English title: The legal framework regarding the use of facial recognition technology in law enforcement

Afleveringsdato: 15. maj 2025

Anslag: 143.865

Udarbejdet af: Caroline Egelund Christensen 2020 2938

Sider 73

Ord 19.719

Tegn (uden mellemrum) 124.247

Tegn (med mellemrum) 143.865

Afsnit 190

Linjer 2.057

☐ Medtag fodnoter og slutnoter

1. Abstract

The purpose of this paper is to examine the regulatory framework regarding the use of facial recognition technology in law enforcement, and to assess whether this legal framework is sufficient and appropriate from a legal policy perspective. The first part of this examination thus entails an analysis of various legal sources to create an overview of the legal framework in the area from a broad perspective. It is then addressed whether the legal framework is sufficient in relation to the need for regulation in an area of law enforcement technology which develops at a fast pace.

The formulation of the problem is split in two parts, and answering the first part of the statement requires an application of the legal dogmatic method, while the legal policy method is applied to address the second part. The first part, I will conduct an analysis of the legal framework regarding the use of facial recognition technology in law enforcement by analyzing different relevant sources of law – both the national Danish regulation regarding the police's investigative resources, regulation from the EU regarding law enforcement authorities and article 8 of the European Convention of Human Rights. All these sources contribute to the legal framework around the use of facial recognition technology in law enforcement in various ways. From this analysis, it can be concluded that the regulatory framework is fragmented, imprecise and arbitrary. The regulation in national Danish law almost only accounts for the collection of data, and the requirement for the collection differs greatly in the different scenarios. The regulation regarding the use of facial recognition itself is primarily based on an implemented EU-directive, but the implementation lacks precision and thoroughness. There are requirements in article 8 of the ECHR on the use of facial recognition technology, but these are attached to the specific case at hand, and therefore cannot be relied on by itself. Based on this analysis, I discuss what the reason is behind the nature of the regulation on the area, whether the framework is sufficient and finally give a recommendation from a legal policy standpoint on how the regulation should be handled. In conclusion, the fragmentation of the regulation is due to multiple factors, for example the fact that facial recognition does not live up to the definition in national law of when to regulate the police's investigative resources. There is a need for improved legislation regarding the use of facial recognition technology, and this paper recommends that the legislation should contain clear and precise requirements for the different ways of using facial recognition technology.

Indholdsfortegnelse

1. ABSTRACT	1
2. INTRODUKTIONSAFSNIT	5
2.1. INDLEDNING	5
2.2. PROBLEMFORMULERING OG SPECIALETS OPBYGNING	6
2.3. AFGRÆNSNING	7
2.4. METODEAFSNIT	8
2.4.1. Metode.....	8
2.4.2. Retskilder	9
2.4.2.1. National ret	9
2.4.2.2. EU-ret	10
2.4.2.3. EMRK	13
2.4.3. Litteratur	14
3. ANSIGTSGENKENDELSE.....	17
3.1. ANSIGTSGENKENDELSE SOM TEKNOLOGI	17
3.1.1. Fremgangsmåden	18
3.1.1.1. Dataindsamling	18
3.1.1.2. Databehandling.....	18
3.1.1.3. Sammenligning.....	19
3.1.2. Typer af ansigtsgenkendelse	19
3.1.2.1. Verifikation og identifikation.....	19
3.1.2.2. Retrospektivt og realtid.....	20
3.1.3. Definition	21
4. RETLIGE RAMMER FOR POLITIETS BRUG AF ANSIGTSGENKENDELSE	23
4.1. NATIONAL RET	23
4.1.1. Generelt om politiets efterforskningsmidler.....	24
4.1.2. Retsplejeloven	24
4.1.2.1. Observation	25
4.1.2.1.1. Observation på ikke frit tilgængeligt sted (§ 791 a)	25
4.1.2.1.2. Observation på frit tilgængeligt sted	25
4.1.2.1.3. Teleobservation (§ 791 a, stk. 5)	26
4.1.2.2. Legemsbesigtigelse.....	27
4.1.2.2.1. Personfotografier med henblik på senere identifikation (§ 792 b)	28
4.1.2.2.2. Opbevaring og sletning af personfotografier (§ 792 f)	30
4.1.2.3. Overtagelse af TV-overvågning (§ 791 e)	31
4.1.3. Politiloven.....	33
4.1.3.1. Politilovens § 2 a.....	33
4.1.4. Delkonklusion.....	35
4.2. EU-RETLIGE RAMMER FOR POLITIETS ANVENDELSE AF ANSIGTSGENKENDELSE	39

4.2.1.	<i>AI-forordningen</i>	39
4.2.2.	<i>Retshåndhævelsesdirektivet og retshåndhævelsesloven</i>	40
4.2.2.1.	Anvendelsesområde.....	40
4.2.2.2.	Generelle bestemmelser.....	42
4.2.2.3.	Kategorier af personoplysninger	42
4.2.2.3.1.	Biometrisk data.....	43
4.2.2.4.	Behandling af almindelige personoplysninger.....	44
4.2.2.5.	Behandling af følsomme personoplysninger, herunder biometriske data	45
4.2.3.	<i>Delkonklusion</i>	50
4.3.	EMRK'S RAMMER FOR POLITIETS ANVENDELSE AF ANSIGTSGENKENDELSE	52
4.3.1.	<i>Artikel 8 – retten til respekt for privatliv</i>	52
4.3.1.1.	Retshåndhævende myndigheders indsamling, behandling og opbevaring af fotos og biometriske data	53
4.3.1.2.	Ansigtsgenkendelse	56
4.3.2.	<i>Delkonklusion</i>	57
4.4.	KONKLUSION	60
5.	DISKUSSION AF DE RETLIGE RAMMER FOR ANSIGTSGENKENDELSE	64
5.1.	ÅRSAGEN TIL UDFORMNINGEN AF DE RETLIGE RAMMER	64
5.1.1.	<i>Regulering af politiets efterforskningsmidler</i>	64
5.1.2.	<i>International regulering</i>	67
5.2.	VURDERING AF REGULERINGEN	67
5.2.1.	<i>Nuværende brug af ansigtsgenkendelse i praksis</i>	68
5.2.2.	<i>Menneskeretlige overvejelser</i>	69
5.2.3.	<i>Straffeprocessuelle overvejelser</i>	70
5.3.	RETSPOLITISKE OVERVEJELSER	73
5.3.1.	<i>Regulering af ansigtsgenkendelse som straffeprocessuelt tvangsindgreb</i>	73
5.3.2.	<i>Andre muligheder for regulering på området</i>	74
6.	LITTERATURLISTE	76

KAPITEL 1

INTRODUKTIONSAFSNIT: Indledning, problemformulering, afgrænsning og metode

2. Introduktionsafsnit

2.1. Indledning

I takt med den hastige teknologiske udvikling muliggøres nye efterforskningsmidler, som skaber nye muligheder og øger effektiviteten i politiets efterforskning af straffesager. Det er ikke nyt, at politiet har adgang til at anvende ansigtsgenkendelsesteknologi i efterforskningen, idet ansigtsgenkendelsesteknologi anvendes som hjælpeværktøj til identifikation af ofre i sager om seksuelt misbrug.¹ Debatten blussede igen op i forbindelse med en række banderelaterede sager, hvor svenske unge blev rekrutteret til at udføre kriminalitet i Danmark.² Politiet ønskede at kunne anvende ansigtsgenkendelse til automatisering af gennemgang af videomateriale frem for at gøre dette manuelt ved brug af store mængder personaleressourcer. Ønsket herom har resulteret i, at Københavns Politi i en forsøgsordning har fået grønt lys fra Justitsministeriet til at anvende retrospektiv ansigtsgenkendelse til gennemgang af billede- og lydmateriale under visse betingelser i efterforskningen af straffesager.

At ansigtsgenkendelse nu på forsøgsbasis ligger i værktøjskassen hos Københavns Politi – og på sigt måske hos alle landets politikredse – krævede ifølge Justitsministeriet ikke umiddelbart ændringer i den nuværende lovgivning, og opfattelsen må således være, at de nuværende retlige rammer er tilstrækkelige.³ Anvendelse af nye teknologiske muligheder er ikke uden grundlæggende retssikkerhedsmæssige betænkeligheder. Danmark er et af de lande i verden med mest overvågning pr. indbygger,⁴ og potentialet i ansigtsgenkendelsesteknologien er derfor stort. Både for så vidt angår betydning for en efterforskning, men også hvad angår betydningen for borgernes grundlæggende rettigheder. Justitsministeren har på tidspunktet, hvor ansigtsgenkendelse kun blev anvendt i ordningen med digital offergenkendelse, udtalt, at en udvidelse af brug af ansigtsgenkendelse ville kræve grundige overvejelser af juridisk, praktisk og principiel karakter. Her blev lagt særlig vægt på, at ansigtsgenkendelse er en indgribende teknologi, og at politiets anvendelse heraf må leve op til nogle strenge retlige krav. Da politiets mulighed for at anvende ansigtsgenkendelse til strafforfølgningsformål på forsøgsbasis blev en realitet, er dette ønske om en grundig debat vedrørende de principielle

¹ Justitsministeriets orientering til Retsudvalget af 21. juni 2024

² Ifølge DR er der tale om mindst 25 episoder mellem april og august 2024. Se Politiet vil skifte mennesker ud med computere i jagten på svenske kriminelle i Danmark, Mathilde Faurby (9. august 2024)

³ Justitsministeriet: "Politiet får grønt lys til ansigtsgenkendelse", 5. september 2024

⁴ Så meget videoovervågning er der i Danmark, Emilie Foxil (9. oktober 2019)

spørgsmål og retlige rammer udeblevet. Justitsministeren anså det nemlig ikke for nødvendigt at ændre i lovgivningen, for at forsøgsordningen med ansigtsgenkendelse ved Københavns Politi kunne iværksættes.⁵ Man er således af den opfattelse, at de nuværende lovgivningsmæssige rammer er tilstrækkelige.⁶

Dette speciale afstedkommes af en undren over, at en så indgribende teknologi kan anvendes af politiet til efterforskning i straffesager uden lovændringer. Skyldes det, at lovgivningen allerede imødeser og kan rumme anvendelsen af nye teknologier? Denne undren giver anledning til at undersøge de lovgivningsmæssige rammer for politiets anvendelse af ansigtsgenkendelse i efterforskningen – både de nationale, EU-retlige og menneskeretlige – samt hvorvidt reguleringen af politiets efterforskningsmidler er tidssvarende, eller om nye teknologier udfordrer definitionen i så høj grad, at der aktualiseres et behov for nytænkning for at undgå en uhensigtsmæssig og tilfældighedspræget retstilstand.

2.2. Problemformulering og specialets opbygning

Specialets problemformuleringen er følgende:

Hvad er de retlige rammer for politiets anvendelse af ansigtsgenkendelse i efterforskningen, og hvilke retspolitiske overvejelser giver dette anledning til?

Nærværende speciale er i besvarelsen af denne problemformulering opdelt i en række kapitler, som er opdelt på følgende måde. **Kapitel 1** indeholder projektets indledning, problemformulering, afgrænsning og metodeafsnit, hvor emnet introduceres og problematiseres, og hvor de relevante retskilder for besvarelse af problemformulering gennemgås. **Kapitel 2** indebærer en gennemgang af ansigtsgenkendelse fra et teknologisk perspektiv, fordi det er nødvendigt at forstå teknologien, før de retlige rammer for denne kan behandles meningsfuldt. **Kapitel 3** indeholder den retsdogmatiske analyse af den lovgivning, der danner grundlag for politiets anvendelse af ansigtsgenkendelse i efterforskningen, hvilket både omfatter national lovgivning, men også internationale rammer for ansigtsgenkendelse, herunder EU-retten og den Europæiske Menneskerettighedskonvention. Den retsdogmatiske

⁵ Retsudvalgets spørgsmål nr. 1344 stillet den 13/8 2024, besvaret af justitsministeren den 8/11 2024.

⁶ Pressemeldelse, Justitsministeriet: "Politiet får grønt lys til ansigtsgenkendelse", 5. september 2024

analyse sker ved en udvælgelse, analyse og systematisering af de regler, som kan have en betydning for alle stadier af ansigtsgenkendelsesteknologien, herunder dataindsamling og -behandling i et bredere perspektiv. I **kapitel 4** konkluderes den retsdogmatiske del af specialets problemformulering vedrørende de retlige rammer for brug af ansigtsgenkendelse. Med afsæt i overblikket over de retlige rammer for ansigtsgenkendelse vil det i **kapitel 5** blive diskuteret, om den danske retstilstand er hensigtsmæssig – bl.a. hvorvidt den danske tradition for regulering af politiets efterforskning, herunder straffeprocessuelle indgreb, er hensigtsmæssig. I denne forbindelse følger nogle retspolitiske overvejelser om, hvordan reguleringen i stedet kunne gribes an.

2.3. Afgrænsning

Ansigtsgenkendelse anvendes i mange sammenhænge, både i Danmark og internationalt. Teknologien anvendes eksempelvis i danske lufthavne og på fodboldstadions, som sikkerhedsmekanisme på personlig elektronik mm. I dette speciale er fokus på retshåndhævende myndigheders anvendelse af ansigtsgenkendelse, fordi dette adskiller sig fra øvrig anvendelse, idet private aktørers anvendelse af teknologien i høj grad hviler på samtykke fra den registrerede, hvilket ikke er tilfældet for retshåndhævende myndigheder. Det er dog ikke al anvendelse af ansigtsgenkendelse hos retshåndhævende myndigheder, som undersøges i dette speciale. Det er ikke nyt, at dansk politi kan anvende ansigtsgenkendelse i forbindelse med efterforskning af straffesager. Det har således været muligt for politiet at benytte ansigtsgenkendelse til eksempelvis identificering af ofre i sager vedrørende seksuelt materiale. En mere generel adgang til anvendelse af ansigtsgenkendelse i efterforskning rejser imidlertid nogle andre retssikkerhedsmæssige spørgsmål end til den blotte identificering af forurettede, og specialet er derfor afgrænset til at omhandle rammerne for brug af ansigtsgenkendelse vedrørende mistænkte personer til formål for strafforfølgning, idet denne anvendelse i langt højere grad er byrdefuld og indgribende for borgeren. Dette skyldes, at ansigtsgenkendelsen ikke anvendes til fordel for den registrerede, hvilket rejser nogle mere principielle spørgsmål. Specialet vil behandle de retlige rammer for både ansigtsgenkendelse i realtid og retrospektiv ansigtsgenkendelse. Endvidere er specialet afgrænset til at behandle de retlige rammer for visse typer af ansigtsgenkendelse. Ansigtsgenkendelse kan anvendes med forskellige formål (verifikation og identifikation),⁷ og dette speciale afgrænses til at behandle de retlige rammer

⁷ Der henvises til afsnit 3.1.2.1. for gennemgang af denne sondring.

for politiets brug af ansigtsgenkendelse til brug for identifikation, fordi denne brug af ansigtsgenkendelse er mere indgribende.

2.4. Metodeafsnit

I dette afsnit gennemgås de metodiske overvejelser, som ligger til grund for besvarelsen af specialets problemformulering. Som følge af emnets karakter inddrages både retskilder fra dansk ret, EU-retten og folkeretten, hvorfor disse gennemgås hver for sig med særligt fokus på de anvendte retskilder. Slutteligt følger en række overvejelser vedrørende samspillet mellem særligt EU-retten og folkeretten.

2.4.1. Metode

I dette afsnit foretages en gennemgang af de metodiske tilgange, som anvendes til besvarelsen af specialets problemformulering. I besvarelsen af den første del af specialets problemformulering anvendes retsdogmatisk metode. I dansk ret foretages en opdeling mellem den juridiske metode og den retsdogmatiske metode, idet førstnævnte bruges til den praktiske løsning af et konkret juridisk problem, mens sidstnævnte metode anvendes i den retsvidenskabelige undersøgelse, eksempelvis af en problemformulering.⁸ Det er således sidstnævnte metode, som primært anvendes i nærværende speciale. Ved hjælp af den retsdogmatiske metode er det muligt at analysere og beskrive gældende ret,⁹ og metoden anvendes således i den del af specialets problemformulering, som angår undersøgelsen af de retlige rammer for politiets anvendelse af ansigtsgenkendelse til retshåndhævende formål. Den retsdogmatiske metode bidrager til at kunne foretage en systematisering af retsreglerne inden for det udvalgte område og derved skabe et overblik over retstilstanden, herunder om der er en usikkerhed forbundet hermed, hvilket er en central del af den retsdogmatiske metode.¹⁰

I besvarelsen af problemformuleringen indgår ud over retsdogmatisk metode et retspolitisk element. Den første del af problemformuleringen søger at afklare de retlige rammer for ansigtsgenkendelse, imens den anden del indebærer en behandling af, hvorfor de retlige rammer er udformet, som de er og hvorvidt denne udformning er hensigtsmæssig. I besvarelsen af denne del af problemformuleringen indgår nogle generelle overvejelser vedrørende

⁸ Munk-Hansen: Retsvidenskabsteori (2018), 2. udgave, DJØF Forlag, s. 193

⁹ Ibid., s. 204

¹⁰ Ibid., s. 204

hensynsafvejninger. Den retspolitiske metode adskiller sig fra den retsdogmatiske, idet retspolitisk metode ikke søger at afklare gældende ret, men derimod rejse spørgsmål herom.¹¹

2.4.2. Retskilder

Reguleringen på området for retshåndhævende myndigheders brug af ansigtsgenkendelse sker både i retskilder fra national ret, EU-retten og EMRK. I analysen inddrages således forskellige retskilder herfra, herunder lovgivning og praksis. Et særligt opmærksomhedspunkt i undersøgelsen er som følge af de spredte retskilder at holde det indbyrdes samspil for øje. De metodiske overvejelser vedrørende de anvendte retskilder gennemgås nedenfor.

2.4.2.1. National ret

Til besvarelse af specialets problemformulering anvendes national ret. I dette afsnit foretages en gennemgang af de anvendte kilder fra national ret samt deres retskildeværdi. Retskilderne i national ret er loven, retspraksis, sædvane og forholdets natur.¹² Det er relevant at inddrage loven som retskilde i besvarelsen af problemformuleringen. I besvarelsen heraf inddrages nærmere bestemt retsplejeloven¹³ og politiloven.¹⁴ Derudover inddrages retshåndhævelsesloven, men idet denne lov implementerer et EU-direktiv, henvises til afsnittet om de EU-retlige kilder nedenfor for en gennemgang heraf. For at kunne beskrive, analysere og systematisere gældende ret er der behov for at fortolke den lovgivning, der inddrages. Loven kan fortolkes således, at anvendelsesområdet indskrænkes eller udvides relativt til ordlyden, eller at anvendelsesområdet nærmere præciseres inden for den naturlige sproglige forståelse af ordlyden.¹⁵ Disse typer af fortolkning kan ske med udgangspunkt i bestemmelsens ordlyd, hvilket læner sig op ad den sædvanlige sproglige forståelse. Såfremt ordlyden ikke giver tilstrækkelig klarhed, kan en subjektiv formålsfortolkning med inddragelse af lovens forarbejder anvendes som et fortolkningsbidrag.¹⁶ Lovforarbejder består både af bl.a. ministeriets bemærkninger og betænkninger.¹⁷ Det er imidlertid ikke givet, at lovforarbejderne kan afklare tvivlen om forståelse af bestemmelsen i den kontekst, der undersøges. I et sådant

¹¹ Munk-Hansen: Retsvidenskabsteori (2018), 2. udgave, DJØF Forlag, s. 74

¹² Ibid., s. 195

¹³ Lovbekendtgørelse nr. 1160 05/11/2024 af retsplejeloven

¹⁴ Lovbekendtgørelse nr. 1270 af 29/11/2019 om politiets virksomhed (politiloven)

¹⁵ Munk-Hansen: Retsvidenskabsteori (2018), 2. udgave, DJØF Forlag, s. 296

¹⁶ Ibid., s. 298

¹⁷ Ibid., s. 259

tilfælde kan der ske en objektiv formålsfortolkning, som søger at afklare formålet uden brug af forarbejderne.¹⁸ I besvarelsen af specialets problemformulering er der i analysen inddraget lovbemærkninger fra samtlige love, imens der ved analyse af retsplejelovens bestemmelser tillige er inddraget de betænkninger, som ligger til grund for udarbejdelsen af den generelle systematik og de nærmere overvejelser vedr. bestemmelserne i loven. I sidstnævnte tilfælde spiller den juridiske litteratur, som ikke er en retskilde, en særegen rolle, fordi retsplejelovens systematisk i høj grad er baseret på Hans Gammeltoft-Hansens definition og overvejelser herom. Gammeltoft-Hansens litteratur på området kan således tjene som supplement til fortolkning af retsplejeloven.

2.4.2.2. EU-ret

EU-retten inddrages for at afklare de retlige rammer for politiets anvendelse af ansigtsgenkendelse. Det er således nødvendigt at afklare, hvorledes EU-retten har gyldighed og virkning for så vidt angår den nationale retsstilling. EU-rettens grundlag udgøres af traktater, som Danmark har tiltrådt, og således har EU-retten grundlæggende samme udgangspunkt som folkeretten.¹⁹ EU-retten adskiller sig dog herfra, idet medlemsstaterne, ved tiltrædelse af traktaterne, delvist har opgivet lovgivningskompetence. Det betyder, at EU har en supranational retsdannelse, idet der skabes ret i EU's institutioner med udgangspunkt i traktaterne.²⁰ Retskilderne er rangeret i et internt hierarki med primærretten øverst. Primærretten består af traktaterne, herunder TEU, TEUF²¹ og Chartret om grundlæggende rettigheder²², hvilket betyder, at al underordnet EU-ret skal have hjemmel i traktaterne og ikke må stride derimod.²³ Sekundærreguleringen består af forordninger, direktiver mm. Længere nede i hierarkiet findes praksis fra EU-Domstolen.

Primærretten

Som nævnt ovenfor udgør traktaterne grundlaget for EU-retten. De behandles ikke nærmere her. Danmark har imidlertid forbehold for dele af traktaterne, hvorved EU-regulering på disse

¹⁸ Munk-Hansen: Retsvidenskabsteori (2018), 2. udgave, DJØF Forlag, s. 80 f.

¹⁹ Ibid., s. 276

²⁰ Ibid., s. 276

²¹ Traktat om den Europæiske Unions Funktionsmåde

²² Chartret er udviklet med udgangspunkt i medlemsstaternes forfatningssikrede grundrettigheder og internationale forpligtelser, herunder EMRK.

²³ Neergaard & Nielsen: EU-ret (2020), 8. udgave, Karnov Group, s. 121

områder ikke er bindende for Danmark. Heriblandt findes retsforbeholdet, som vedrører samarbejde om retlige og indre anliggender,²⁴ hvilket omfatter det retlige samarbejde i straffesager og politisamarbejdet.²⁵ Nærværende speciale omhandler politiets anvendelse af ansigtsgenkendelse til retshåndhævende formål, og derfor medfører retsforbeholdet, at retsakter vedtaget i EU på dette område som udgangspunkt ikke gælder for Danmark. Chartret om grundlæggende rettigheder har samme rang som traktaterne, jf. art. 6, stk. 1 TEU²⁶ og har kun retsvirkning for national ret på områder, som er reguleret af EU.²⁷ Chartret inddrages ikke særskilt i besvarelsen af problemformuleringen, fordi rettighederne er udarbejdet med stærk inspiration fra EMRK. Chartret har således kun selvstændig betydning i det omfang, det yder en stærkere beskyttelse end EMRK, hvilket ikke behandles her.²⁸

Sekundærregulering

Som nævnt ovenfor består sekundærreguleringen af forordninger, direktiver mm., jf. art. 288 TEUF. Forordninger er karakteriseret ved at være direkte bindende²⁹ og skal ikke implementeres i national ret.³⁰ Direktiver er bindende for medlemsstaterne, men det overlades til medlemsstaterne selv at implementere dem,³¹ hvilket betyder, at borgere i medlemsstaterne ikke kan støtte direkte ret på et direktiv, men derimod på den nationale ret, som gennemfører direktivet.³² Direktivet har dog selvstændig betydning, fordi fortolkning af den nationale regulering på et direktivreguleret område vil påvirkes af direktivet og EU-retten i bredere forstand.³³ Såfremt en lov er vedtaget på baggrund af et direktiv, skal fortolkningen af loven ske i overensstemmelse med direktivet ud fra princippet om direktivkonform fortolkning.³⁴ I en sådan situation vil direktivets ordlyd og formål have mere vægt end ordlyden i de nationale lovbestemmelser, såfremt disse ikke er i overensstemmelse med direktivet.

²⁴ Dette betyder, at Danmark ikke bindes af EU-regulering i henhold til tredje del, afsnit V TEUF, som omhandler regler vedrørende frihed, sikkerhed og retfærdighed.

²⁵ Neergaard & Nielsen: EU-ret (2020), 8. udgave, Karnov Group, s. 43

²⁶ Ibid., s. 171

²⁷ Ibid., s. 187

²⁸ Chartrets art. 52(3)

²⁹ Art. 288, stk. 2 TEUF

³⁰ Neergaard & Nielsen: Retsvidenskabsteori (2018), 2. udgave, DJØF Forlag, s. 277

³¹ Art. 288, stk. 3 TEUF

³² Munk-Hansen: Retsvidenskabsteori (2018), 2. udgave, DJØF Forlag, s. 278

³³ Ibid., s. 278

³⁴ Ibid., s. 278

I nærværende speciale inddrages en række forskellige retskilder fra EU-retten, særligt sekundærregulering og vejledninger fra European Data Protection Board.

*AI-forordningen*³⁵

Det fremgår af AI-forordningen, at Danmark som følge af retsforbeholdet er undtaget fra AI-forordningens artikel 5, stk. 1, litra g, d og h, stk. 2-6 samt artikel 26, stk. 10.³⁶ De nævnte artikler regulerer retshåndhævende myndigheder, og Danmark er således undtaget fra disse. Det betyder, at AI-forordningen ikke udgør en del af den retlige ramme for politiets anvendelse af ansigtsgenkendelse i Danmark. Som følge af retsforbeholdet vil AI-forordningens øvrige bestemmelser om ansigtsgenkendelse formentligt ikke være gældende regulering for så vidt angår dansk politi.

Retshåndhævelsesdirektivet

Databeskyttelsesforordningen³⁷ sætter rammerne for medlemsstaternes behandling af personoplysninger. Databeskyttelsesforordningen undtager imidlertid behandling af personoplysninger, “som foretages af kompetente myndigheder med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed.”³⁸ Databeskyttelsesforordningen er således ikke inddrages i besvarelsen af specialets problemformulering, fordi den ikke finder anvendelse på området for retshåndhævende myndigheders behandling af personoplysninger, som derimod reguleres ved retshåndhævelsesdirektivet.³⁹ Danmark er som udgangspunkt ikke omfattet af retshåndhævelsesdirektivet, da regulering af retshåndhævende myndigheder er omfattet af det

³⁵ Europa-Parlamentets og Rådets forordning (EU) 2024/1689 af 13. juni 2024 om harmoniserede regler for kunstig intelligens og om ændring af forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 og (EU) 2019/2144 samt direktiv 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (forordningen om kunstig intelligens)

³⁶ AI-forordningen, præambel 41

³⁷ Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)

³⁸ Databeskyttelsesforordningen, artikel 2(2)(d)

³⁹ Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA

danske forbehold vedrørende retlige og indre anliggender.⁴⁰ Man valgte imidlertid at implementere direktivet, da dette var en forudsætning for indgåelse af en samarbejdsaftale mellem Danmark og Europol.⁴¹ Direktivets implementering i dansk ret ved retshåndhævelsesloven⁴² betyder derfor, at disse retskilder er relevante for analysen af de retlige rammer for dansk politis anvendelse af ansigtsgenkendelse. Retshåndhævelsesloven er således en national regulering, der implementerer et direktiv, hvorfor loven behandles under afsnittet vedrørende de EU-retlige rammer. Idet direktiver ikke har direkte retsvirkning i et medlemsland, tager analysen udgangspunkt i retshåndhævelsesloven. Denne fortolkes imidlertid direktivkonformt, og direktivet anvendes derfor som et fortolkningsbidrag. Som fortolkningsbidrag inddrages endvidere vejledninger vedrørende retshåndhævende myndigheders anvendelse af ansigtsgenkendelse udstedt af European Data Protection Board (EDPB).⁴³ EDPB udsteder vejledninger på området for databeskyttelse, herunder databeskyttelsesforordningen og retshåndhævelsesdirektivet. Disse har til formål at bidrage til en fælles forståelse af reglerne på området samt komme med en nærmere beskrivelse heraf.⁴⁴ Vejledningerne karakteriseres som soft law og er derfor ikke bindende for medlemsstaterne, men EDPB har kompetence til at bidrage til fortolkningen af de regler, som medlemsstaterne er bundet af.⁴⁵

2.4.2.3. EMRK

I dette afsnit foretages en gennemgang af de metodiske overvejelser vedrørende den Europæiske Menneskerettighedskonvention, idet EMRK inddrages i besvarelsen af specialets problemformulering. EMRK blev ved lov inkorporeret i dansk ret i 1992.⁴⁶ Dette betyder, at EMRK har en anderledes retskildeværdi end øvrige folkeretlige konventioner, idet den har en “stærkere gennemslagskraft end øvrige ikke-inkorporerede konventioner.”⁴⁷ På grund af inkorporering finder EMRK direkte anvendelse i national ret. EMRK har retsvirkning ved, at lovgiver sikrer overensstemmelse med EMRK’s rettigheder, og at domstolenes afgørelser

⁴⁰ L 168 Forslag til lov om retshåndhævende myndigheders behandling af personoplysninger, s. 13

⁴¹ Ibid., s. 14

⁴² Lov nr. 410 af 27/04/2017 om retshåndhævende myndigheders behandling af personoplysninger

⁴³ EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement

⁴⁴ EDPB’s hjemmeside

⁴⁵ Eurofound: European Industrial Relations Dictionary: Soft Law

⁴⁶ Lov nr. 285 af 29/04/1992 om den Europæiske Menneskerettighedskonvention

⁴⁷ Rytter: Individets grundlæggende rettigheder (2021), 4. udgave, Karnov Group, s. 61

træffes i overensstemmelse hermed.⁴⁸ EMRK består af en række grundlæggende rettigheder og forpligtelser, som de ratificerende stater er forpligtede til at overholde. I fortolkningen af konventionen har praksis fra EMD væsentlig betydning, idet formålet, ud over at behandle de enkelte sager, er at “belyse, sikre og videreudvikle”⁴⁹ rettighederne. EMD inddrager tidligere afgørelser i sin fortolkning af konventionen, selvom de ikke formelt set er bundet heraf,⁵⁰ fordi udviklingen i samfundet kan begrunde en ny retning.⁵¹ Netop denne udvikling af retstilstanden, som skal afspejle den generelle samfundsudvikling, er kernen i EMD’s dynamiske fortolkningsstil. I fravær af praksis på et område sker fortolkningen ud fra ordlyd, sammenhæng, genstand og formål, samt ud fra konventionens præambler.⁵² På grund af inkorporeringen og den direkte anvendelse af EMRK skal konventionen ved danske domstole fortolkes i overensstemmelse med den fortolkning, der lægges til grund af Den Europæiske Menneskerettighedsdomstol (herefter “EMD”).⁵³ Danske domstole skal således afgøre sager i overensstemmelse hermed, hvilket betyder, at afgørelser afsagt af EMD har retskildeværdi i national kontekst.

Afgørelser udgør som nævnt en vigtig retskilde i fortolkningen af indholdet af konventionens artikler. I besvarelsen af specialets problemformulering analyseres derfor nogle udvalgte afgørelser, som omhandler artikel 8 om retten til privatliv i relation til politiets brug af ansigtsgenkendelse. På grund af den måde, EMD fungerer på, hvor der gennem praksis etableres principper, som der anvendes og bygges videre på i nyere praksis, er udvælgelsen foretaget med udgangspunkt i den seneste dom på området. I denne dom refererer EMD til og bygger videre på tidligere afgørelser, som derfor tillige må være af relevans for området. Ud fra disse betragtninger er der foretaget en analyse og systematisering af Glukhin mod Rusland (2023), Gaughran mod Storbritannien (2020) samt S. og Marper mod Storbritannien (2008).

2.4.3. Litteratur

⁴⁸ Rytter: Individets grundlæggende rettigheder (2021), 4. udgave, Karnov Group, s. 59

⁴⁹ Kjølbro: Den Europæiske Menneskerettighedskonvention for praktikere (2020), 5. udgave, Jurist- og Økonomiforbundets Forlag, s. 15

⁵⁰ Ibid., s. 15-16

⁵¹ Ibid., s. 16

⁵² Ibid., s. 20

⁵³ Munk-Hansen: Retsvidenskabsteori (2018), 2. udgave, DJØF Forlag, s. 204

Ud over retskilderne er der tillige inddraget juridisk litteratur i besvarelsen af problemformuleringen. Det skal bemærkes, at litteratur ikke er en retskilde.⁵⁴ Litteraturen er inddraget i besvarelsen med dette in mente, og fungerer derfor udelukkende som et supplement til forståelsen af de pågældende områder.

⁵⁴ Munk-Hansen: Retsvidenskabsteori (2018), 2. udgave, DJØF Forlag, s. 304

KAPITEL 2

GENERELT OM ANSIGTSGENKENDELSE: Ansigtsgenkendelse som teknologi

3. Ansigtsgenkendelse

Før der kan foretages en gennemgang af det retlige grundlag for politiets anvendelse af ansigtsgenkendelse i Danmark, er det nødvendigt at beskrive ansigtsgenkendelse som teknologi nærmere. I følgende afsnit klarlægges, hvad ansigtsgenkendelse indebærer som teknologi – både hvordan teknologien defineres, hvad teknologien konkret indebærer og hvilke typer af ansigtsgenkendelse, der findes. Formålet med afsnittet er at give en overflyvning over selve teknologien samt foretage nogle inddelinger, som har betydning for specialets afgrænsning af emnet, men som også danner grundlaget for strukturen af den senere analyse.

3.1. Ansigtsgenkendelse som teknologi

Dataetisk Råd definerer ansigtsgenkendelse som “en computersoftware, som kan analysere billeder for at opdage, evaluere og identificere ansigter.”⁵⁵ Ansigtsgenkendelse er således en teknologi, som muliggør automatisk genkendelse af individer på baggrund af deres ansigter – eksempelvis i billede- og videomateriale.⁵⁶ Ansigtsgenkendelsesteknologi vil ofte være baseret på og udviklet med kunstig intelligens, også kaldet AI.⁵⁷ Kunstig intelligens defineres i AI-forordningen som “et maskinbaseret system, som er udformet med henblik på at fungere med en varierende grad af autonomi, og som efter idriftsættelsen kan udvise en tilpasningsevne, og som til eksplicite eller implicite mål af det input, det modtager, udleder, hvordan det kan generere output såsom forudsigelser, indhold, anbefalinger eller beslutninger, som kan påvirke fysiske eller virtuelle miljøer.”⁵⁸ Netop ved hjælp af kunstig intelligens muliggøres anvendelse af ansigtsgenkendelse på større skala og med højere effektivitet, men samtidigt rejser det nogle problemstillinger. Teknologiens algoritme træffer sine beslutninger på baggrund af en vidensbase⁵⁹ – karakteren og kvaliteten af dette input har derfor stor betydning for, om algoritmen kan anvendes med nøjagtighed til forskellige formål. Det er vigtigt at være bevidst om, at denne vidensbase har stor betydning for algoritmens beslutninger og resultater, og at algoritmen kommer frem til de mest retvisende resultater, jo mere det materiale, der ønskes behandlet, ligner vidensbasens materiale.⁶⁰ Det har også betydning, at algoritmen har en vis autonomi, hvor det kan være svært at få gennemsigtighed i beslutningsprocesserne. Desuden

⁵⁵ Dataetisk Råd: “Hvad er ansigtsgenkendelse?”, 2022

⁵⁶ EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, s. 9

⁵⁷ Ibid., s. 8

⁵⁸ AI-forordningens art. 3(1)

⁵⁹ Akbari, Ali: Facial Recognition 101 – Technical Insights, 2024, s. 31

⁶⁰ Ibid., s. 34

udvikler kunstig intelligens sig selv, og at den performer godt på ét tidspunkt betyder ikke, at den fortsætter med det. Derfor kræves regelmæssig vedligeholdelse.⁶¹

3.1.1. Fremgangsmåden

Ansigtsgenkendelsesteknologien består af flere stadier, og nedenstående gennemgang heraf sker med udgangspunkt i en bred opfattelse af teknologien. Det er for snævert kun at anse ansigtsgenkendelse for at indebære genkendelse af et ansigts i et givet billede- eller videomateriale, idet der tillige må tages højde for de øvrige ”stadier” i teknologiens fremgangsmåde – eksempelvis dataindsamling og en eventuelt efterfølgende identifikation af den pågældende. Et bredt perspektiv må således anlægges for at få et fyldestgørende billede af ansigtsgenkendelse som teknologi.

3.1.1.1. Dataindsamling

Dataindsamling dækker over indsamlingen af det materiale, der skal behandles af ansigtsgenkendelsesteknologien, hvilket ofte vil være billede- eller videomateriale. Typen og kvaliteten af indsamlede data har betydning for, med hvor stor nøjagtighed teknologien kan foretage ansigtsgenkendelse. Det kan have stor betydning, hvis et billede er sløret, dårlig kvalitet, dårligt belyst eller vinklet el.lign.⁶²

3.1.1.2. Databehandling

Efter der er foretaget en dataindsamling af materiale, er næste skridt at foretage en databehandling heraf. Databehandlingen består både af ansigtsopdagelse og en biometrisk analyse. Det første skridt i databehandlingen består af, at teknologien ‘opdager’ ansigter i det anvendte materiale.⁶³ Teknologien kan lokalisere ansigter på et billede eller en videooptagelse ved at finde strukturer, som normalt kendetegner et menneskeansigt.⁶⁴ Herved sker en afgrænsning af de steder i materialet, hvor der formentligt findes ansigter. Dette kan for eksempel være ansigtsfokus på digitale kameraer, som ved hjælp af teknologien kan fokusere på ansigter ved at lokalisere dem.⁶⁵ Ud fra strukturerne i et lokaliseret ansigt, dvs. øjne, næse,

⁶¹ Akbari, Ali: Facial Recognition 101 – Technical Insights, 2024, s. 31

⁶² EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, s. 13

⁶³ Akbari, Ali: Facial Recognition 101 – Technical Insights, 2024, s. 29

⁶⁴ Dataetisk Råd: “Hvad er ansigtsgenkendelse?”, 2022

⁶⁵ Eksemplet fremgår af Dataetisk Råd: “Hvad er ansigtsgenkendelse?”, 2022

mund mm. samt disses nærmere karakteristika, herunder afstand til hinanden, vil teknologien fastsætte en række punkter i ansigtet. Ud fra disse punkter laver teknologien et datasæt, som også kaldes en 'skabelon'.⁶⁶ Skabelonen kan entydigt identificere en person, fordi den er særegen for individet. Der sker således en ny dannelse af data, når den biometriske ansigtsskabelon dannes.⁶⁷

3.1.1.3. Sammenligning

Databehandlingen resulterer i en genereret skabelon af det lokaliserede ansigt, og på baggrund heraf har teknologien til sidst mulighed for at genkende personen på eksempelvis et andet billede eller en video.⁶⁸ Sammenligningen er ikke eksakt – den baserer sig på et estimeret match mellem skabeloner genereret på baggrund af det anvendte materiale og en database. Der er således tale om en sandsynlighedsberegning, hvorfor udvikleren eller brugeren af programmet må fastsætte en nedre grænse for, hvornår en vis sandsynlighed er tilstrækkelig for at fastslå et match.⁶⁹

3.1.2. Typer af ansigtsgenkendelse

I det følgende afsnit foretages en gennemgang af forskellige typer af ansigtsgenkendelsesteknologi. Ansigtsgenkendelsesteknologien kan både anvendes til varierende formål og omfang. Desuden har anvendelsens tidsperspektiv betydning, herunder om ansigtsgenkendelsen bruges i realtid eller retrospektivt.

3.1.2.1. Verifikation og identifikation

Der skelnes mellem ansigtsgenkendelse til brug for verifikation og identifikation.⁷⁰ Verifikation indebærer, at ansigtsgenkendelsesteknologien foretager en sammenligning af, hvorvidt et ansigts biometriske skabelon matcher en allerede kendt skabelon.⁷¹ Verifikation kendes bl.a. fra FaceID-funktionen på telefoner, men den anvendes også i visse danske lufthavne, hvor der foretages en bekræftelse af en rejsendes identitet.⁷² Verifikation kaldes også

⁶⁶ EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, s. 9

⁶⁷ Se også databeskyttelsesforordningens præambel 51

⁶⁸ Akbari, Ali: Facial Recognition 101 – Technical Insights, 2024, s. 29

⁶⁹ EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, s. 10

⁷⁰ Se AI-forordningens præambel 17

⁷¹ Facial Recognition Technology – Key Issues and Emerging Concerns (Selwyn et. al.), 2024, s. 11

⁷² Retsudvalgets spørgsmål nr. 1344 stillet den 13/8 2024, besvaret af justitsministeren den 8/11 2024.

én-til-én sammenligning, fordi der kun dannes en biometrisk skabelon af én person, som sammenlignes med én bestemt skabelon, der er kendt på forhånd. Ved brug af FaceID-funktionen på en telefon foretager teknologien eksempelvis ikke yderligere identifikation af den person, der forsøger at låse en telefon op – den vurderer kun, hvorvidt denne person matcher kriterierne for oplåsning.⁷³ Identifikation kaldes også én til mange sammenligning. Denne form for ansigtsgenkendelse fungerer ved, at den skaber en biometrisk skabelon af et ansigt, som derefter kan sammenlignes med en database af biometriske skabeloner. Formålet er således ultimativt at identificere personen.⁷⁴ Én-til-mange sammenligningen er i stand til at identificere en person blandt en menneskemængde, og netop dette giver teknologien vidtgående rækkevidde, hvad angår muligheden for masseovervågning.⁷⁵ En teknologi, der er velegnet til verifikationsformål, egner sig ikke nødvendigvis til anvendelse med henblik på identifikation.⁷⁶

3.1.2.2. Retrospektivt og realtid

Ansigtsgenkendelsen kan foretages i realtid eller retrospektivt. Ansigtsgenkendelse i realtid indebærer, at ansigtsgenkendelsen sker ‘live’. Teknologiens integration i eksempelvis overvågningskameraer vil muliggøre en næsten straksidentifikation af personer, som måtte fremgå af den database, overvågningsmaterialet holdes op imod.⁷⁷ Med andre ord sker dataindsamlingen, databehandlingen og sammenligningen⁷⁸ tidsmæssigt meget tæt på hinanden, og ansigtsgenkendelsen er derfor i praksis tæt på automatiseret. En sådan teknologi vil være meget effektiv, eksempelvis til brug ved en ‘man-hunt’, hvor hurtig identificering og lokalisering af en person er afgørende. Ansigtsgenkendelse i realtid vil imidlertid også resultere i, at almindelige menneskers ansigtsbiometri behandles i langt højere grad end ved retrospektiv ansigtsgenkendelse. Retrospektiv ansigtsgenkendelse er derimod kendetegnet ved, at ansigtsgenkendelsesteknologien tidsmæssigt anvendes senere, end dataindsamlingen er foretaget. Der er en væsentlig forsinkelse sammenlignet med ansigtsgenkendelse i realtid.⁷⁹

⁷³ Selwyn m.fl.: Facial Recognition Technology – Key Issues and Emerging Concerns, 2024, s. 11

⁷⁴ EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, s. 10

⁷⁵ Selwyn m.fl.: Facial Recognition Technology – Key Issues and Emerging Concerns, 2024, s. 11–12

⁷⁶ Akbari, Ali: Facial Recognition 101 – Technical Insights, 2024, s. 34

⁷⁷ Se AI-forordningen, præambel (17)

⁷⁸ Se afsnit 3.1.1. ovenfor for gennemgang heraf

⁷⁹ Se AI-forordningen, præambel (17)

Retrospektiv ansigtsgenkendelse er mindre indgribende, fordi anvendelsen heraf vil basere sig på en vis forudgående mistanke.⁸⁰

3.1.3. Definition

Teknologien har mange forskellige anvendelsesområder, og disse områder har betydning for, hvor indgribende anvendelsen af teknologien kan være. Af denne årsag er det ikke muligt at finde en entydig definition på ansigtsgenkendelse, som der kan tages udgangspunkt i. Med inspiration fra AI-forordningens definition af systemer til biometrisk fjernidentifikation kan den form for ansigtsgenkendelse, der i nærværende speciale tages udgangspunkt i, formuleres som *et AI-system, der ud fra et indsamlet materiale kan foretage ansigtsopdagelse, biometrisk analyse og sammenligning, og ud fra dette er i stand til at identificere fysiske personer, uanset om den fysiske persons identitet reelt bekræftes.*

⁸⁰ Simmler, Monika og Canova, Giulia: Facial recognition technology in law enforcement – Regulating data analysis of another kind, 2025

KAPITEL 3

RETSDOGMATISK ANALYSE: De nationale, EU-retlige og menneskeretlige rammer for brug af ansigtsgenkendelse

4. Retlige rammer for politiets brug af ansigtsgenkendelse

I nærværende speciale søges følgende problemformulering besvaret: ”Hvad er de retlige rammer for politiets anvendelse af ansigtsgenkendelse i efterforskningen, og hvilket retspolitiske overvejelser giver dette anledning til?”. I det følgende afsnit besvares den første del af problemformuleringen, idet der i afsnittet foretages en analyse af de retlige rammer for politiets anvendelse af ansigtsgenkendelse i efterforskningen af straffesager. De retlige rammer analyseres ud fra et bredt perspektiv på ansigtsgenkendelsesteknologi, hvor der inddrages reguleringen med relevans for både dataindsamling, databehandling og sammenligning. Afsnittet er opdelt således, at der først foretages en analyse af de nationale retlige rammer med særligt fokus på retsplejeloven og politiloven. Derefter analyseres EU-rettens rammer, hvor AI-forordningen og retshåndhævelsesloven og retshåndhævelsesdirektivet inddrages. Slutteligt foretages en gennemgang af de menneskeretlige rammer med særligt fokus på artikel 8 om retten til privatliv.

4.1. National ret

I dette afsnit undersøges, hvilke rammer der i nationale lovgivning sættes for politiets anvendelse af ansigtsgenkendelse i efterforskningen med udgangspunkt i retsplejeloven og politiloven. Som nævnt består ansigtsgenkendelsesteknologien af flere dele, som hver især muliggør processen, herunder dataindsamlingen, databehandling og en efterfølgende sammenligning. I dette afsnit fokuseres særligt på dataindsamlingen og de bestemmelser, der regulerer politiets mulighed for at komme i besiddelse af fotografier og videomateriale. Overvågningsmateriale er oplagt at benytte i denne sammenhæng og vil også i høj grad være det, man ønsker at bruge ansigtsgenkendelse på, særligt ved indsamling af store mængder materiale.⁸¹ Herudover er rammerne for politiets mulighed for at optage fotografier relevant, da der på baggrund af disse kan dannes biometriske skabeloner af ansigter, men også fordi fotografier kan opbevares i databaser, som kan anvendes som et sammenligningsgrundlag til brug for identifikation af personer. Der foretages indledende en overordnet gennemgang af rammerne for politiets efterforskning. Derefter behandles de konkrete bestemmelser i retsplejeloven og politiloven, som kan tænkes at have betydning for de retlige rammer for ansigtsgenkendelse.

⁸¹ Der henvises til indledningen samt afsnit 5.2.1. *Nuværende brug af ansigtsgenkendelse*, hvor Justitsministerens og politiets bemærkninger vedrørende dansk politis adgang til at bruge ansigtsgenkendelse er gengivet.

4.1.1. Generelt om politiets efterforskningsmidler

Dansk politi er ved lov pålagt at varetage forskellige opgaver, herunder “at bringe strafbar virksomhed til ophør samt efterforske og forfølge strafbare forhold”,⁸² hvilket nærmere reguleres i retsplejeloven. Formålet med en efterforskning er flerdelt. Politiet skal afklare, om betingelserne for at pålægge strafansvar er til stede, tilvejebringe oplysninger til brug for sagens afgørelse og forberede sagens behandling i retten, jf. retsplejelovens § 743. Efterforskningen danner således grundlag for sagsoplysningen i en straffesag,⁸³ og politiet har til formålet adgang til forskellige efterforskningsmidler. Efterforskningen kan ske ved almindelige efterforskningsskridt som afhøringer, observation og øvrige foretagender, som ikke er forbudt for nogen; politiet kan tilsvarende foretage en sådan efterforskning uden en udtrykkelig hjemmel.⁸⁴ Til brug for efterforskningen har politiet endvidere hjemmel til at foretage indgreb i borgernes rettigheder i visse tilfælde og under iagttagelse af en række betingelser. Disse særlige efterforskningsskridt kaldes straffeprocessuelle tvangsindgreb og er reguleret i retsplejelovens kap. 68-75 b. I Strafferetsplejerådets arbejde med modernisering af retsplejeloven tog man udgangspunkt i Hans Gammeltoft-Hansens definition af straffeprocessuelle tvangsindgreb:⁸⁵ “en foranstaltning, der efter sit almindelige formål udføres som led i en strafforfølgning, og hvorved der realiseres en strafbar gerningsbeskrivelse rettet mod legeme, frihed, fred, ære eller privat ejendom.”⁸⁶ Reguleringen af udvalgte straffeprocessuelle tvangsindgreb med betydning brugen af ansigtsgenkendelse gennemgås i det følgende afsnit.

4.1.2. Retsplejeloven

I dette afsnit sker en gennemgang af de konkrete efterforskningsskridt, som kan tænkes at have relevans for politiets anvendelse af ansigtsgenkendelse. Det er som nævnt en forudsætning for at kunne anvende ansigtsgenkendelse, at der er indsamlet materiale. Selvom de straffeprocessuelle tvangsindgreb i retsplejeloven ikke direkte regulerer politiets mulighed for at anvende ansigtsgenkendelse, udgør de således stadig i bred forstand en retlig ramme herfor.

⁸² Se politilovens § 2, stk. 1, nr. 3

⁸³ Bet. 622/1971 om efterforskning i straffesager, s. 8

⁸⁴ Vestergaard: Straffeproses – grundtræk af dansk strafferetspleje (2017), 1. udgave, Gjellerup Forlag, s. 51

⁸⁵ Betænkning 1023/1984 om politiets indgreb i meddelelshemmeligheden og anvendelse af agenter, s. 12

⁸⁶ Gammeltoft-Hansen, Hans: U.1979B.1 (Om afgrænsningen af straffeprocessuelle tvangsindgreb), s. 8

Konkret vedrører de udvalgte bestemmelser politiets muligheder for optagelse og anvendelse af fotografier og videomateriale, herunder fotografering, legemsbesigtigelse og optagelse af fotografi i denne forbindelse samt optagelse af personfotografi. Desuden gennemgås adgangen til teleobservation og regulering vedrørende TV-overvågning. Gennemgangen fokuserer på de aspekter ved indgrebet, som kan have betydning for ansigtsgenkendelse, imens der ses bort fra det øvrige indhold.

4.1.2.1. Observation

4.1.2.1.1. Observation på ikke frit tilgængeligt sted (§ 791 a)

Politiets adgang til at fotografere og videooptage til brug for en efterforskning er reguleret i retsplejelovens § 791 a. Bestemmelsen omhandler primært observation på et ikke frit tilgængeligt sted, hvis denne observation foretages ved brug af hjælpemidler. Bestemmelsen er opdelt i kategorier, hvor kravene til indgrebet skærpes i takt med karakteren af indgrebet, herunder lokaliteten samt typen og placering af apparat.⁸⁷ Der er således større krav til at opsætte automatisk virkende overvågningskamera i en bolig,⁸⁸ end der er til iagttagelse ved hjælp af kikkert af en person, der befinder sig i sin have.⁸⁹ Fælles for indgrebene er, at der ikke skal opfyldes et mistankekrav, hvilket skyldes, at indgrebet ikke nødvendigvis vil være rettet mod en mistænkt. Der skal blot være mistanke om, at en forbrydelse er begået.⁹⁰ Politiet har kompetence til at iværksætte indgreb efter stk. 1 (de kvalificerede indgreb), mens kompetencen til at træffe bestemmelse om stk. 2 (de mere kvalificerede indgreb) og stk. 3 (de særligt kvalificerede indgreb) ligger hos retten.⁹¹

4.1.2.1.2. Observation på frit tilgængeligt sted

Modsætningsvist kræver politiets fotografering og TV-overvågning af personer på et frit tilgængeligt sted ikke en særlig hjemmel i retsplejeloven, idet der som følge af, at der ikke realiseres et strafbart gerningsindhold, ikke er tale om et straffeprocessuelt indgreb.⁹² Strafferetsplejeudvalget overvejede, om der på trods heraf var behov for regulering på området

⁸⁷ Folketingstidende 1998-99, tillæg A, sp. 862

⁸⁸ Se § 791 a, stk. 3

⁸⁹ Se § 791 a, stk. 1 samt Bet. 1298/1995 om fotoforevisning, konfrontation, efterlysning og observation, s. 90-91

⁹⁰ Folketingstidende 1998-99, tillæg A, sp. 863

⁹¹ Bet. 1298/1995 om fotoforevisning, konfrontation, efterlysning og observation, s. 99

⁹² Ibid., s. 80

med særligt fokus på politiets mulighed for at foretage skjult TV-overvågning, fordi denne form for observation i visse tilfælde kan være meget indgribende.⁹³ En generel modvilje mod skjult efterforskning og dets associationer til et “overvågningssamfund”, samt den omstændighed, at indgrebet kan ramme mange personer, som ikke har forbindelse til en forbrydelse, talte for at foretage en regulering.⁹⁴ På den anden side blev bemærket, at der ikke var tale om et straffeprocessuelt tvangsindgreb, samt at færden på frit tilgængelige områder må indebære en vis accept af, at man iagttages. Desuden anførte man, at “beskyttelsesinteressen [...] måske i højere grad er knyttet til den brug, politiet gør af de optagne billeder, end til selve optagelserne.”⁹⁵ Man konstaterede, at en generel modvilje mod et overvågningssamfund, den politiske kontrol af politiets virksomhed og ressourcemæssige begrænsninger samlet set ville være tilstrækkeligt til at “modvirke eventuelle tendenser i retning af en mere udbredt TV-overvågning af befolkningen.”⁹⁶ Politiets adgang til fotografering og TV-overvågning på frit tilgængelige steder er ikke reguleret andetsteds. Eksempelvis er politiet ikke omfattet af TV-overvågningsloven.⁹⁷ Politiets adgang til dette er således kun reguleret af almindelige forvaltningsretlige principper.

4.1.2.1.3. Teleobservation (§ 791 a, stk. 5)

Udover ovennævnte regulering af politiets adgang til at foretage “fysisk” observation i en efterforskning, regulerer bestemmelsen tillige teleobservation i stk. 5. Efter RPL § 791 a, stk. 5, nr. 2 kan politiet foretage teleobservation ved “på anden måde ved hjælp af en GPS eller et andet lignende apparat at registrere en mistænks færden”, såfremt noget indikerer, at indgrebet må antages at være af væsentlig betydning for efterforskningen, og hvis kriminalitetskravet på minimum 1 år og 6 måneder er opfyldt.

Teleobservation ved hjælp af GPS eller andre apparater blev indført i 2018, hvor uberettiget registrering af en persons færden ved hjælp af en GPS eller et andet lignende apparat blev kriminaliseret i straffeloven,⁹⁸ hvilket skabte behov for at hjemle politiets muligheder for at

⁹³ Bet. 1298/1995 om fotoforevisning, konfrontation, efterlysning og observation, s. 123

⁹⁴ Ibid., s. 124

⁹⁵ Ibid., s. 125

⁹⁶ Ibid., s. 125

⁹⁷ Lovbekendtgørelse 2023-02-24 nr. 182 om TV-overvågning (TV-overvågningsloven) – se lovens § 1

⁹⁸ Lovforslag nr. L20, s. 15

foretage et tilsvarende straffeprocessuelt tvangsindgreb.⁹⁹ Kriminaliseringen i straffeloven skete både som følge af EU-regulering på databeskyttelsesområdet¹⁰⁰ samt generelle overvejelser vedrørende den teknologiske udvikling, som har skabt nye muligheder for krænkelse af privatlivets fred.¹⁰¹ RPL § 791 a, stk. 5, nr. 2 regulerer politiets muligheder for anvendelse af GPS eller andet lignende apparat, som kan bruges til at registrere en bestemt persons færden på en måde, så det er muligt løbende eller efterfølgende at følge denne uden selv at være fysisk til stede. Bestemmelsen omfatter således overvågning ved andre apparater end GPS, herunder ved hjælp af et videokamera, der kan vise en persons færden.¹⁰² Som følge heraf kan der være et vis sammenfald mellem RPL § 791 a, stk. 1-3 og stk. 5. Det er kun, hvis indgrebet omfattes af både stk. 3 og stk. 5, at de strengere krav i stk. 3 tillige skal opfyldes, da kravene efter stk. 1-2 og stk. 5 ligner hinanden.¹⁰³ Teleobservation kræver en retskendelse, jf. RPL § 791 a, stk. 8, 2. pkt. Desuden skal der beskikkes en indgrebsadvokat, og der skal gives efterfølgende underretning til den person, hvis færden politiet har registreret.¹⁰⁴

4.1.2.2. Legemsbesigtigelse

Legemsindgreb er reguleret i retsplejelovens kapitel 72, hvori nogle af bestemmelserne udgør en del af de retlige rammer for politiets anvendelse af ansigtsgenkendelse, idet bestemmelserne regulerer politiets muligheder for at optage fotografier (dataindsamling) samt regler vedrørende opbevaring og sletning. I dette afsnit gennemgås de relevante regler med særligt fokus på retsplejelovens §§ 792, 792 a, 792 b og 792 f.

Retsplejelovens regulering af legemsindgreb er baseret på Strafferetsplejeudvalgets betænkning,¹⁰⁵ som man valgte at følge i det fremsatte lovforslag.¹⁰⁶ Legemsindgreb defineres som "de straffeprocessuelle tvangsindgreb, hvorved der tilvejebringes og fastholdes oplysninger om et levende menneskeligt legeme eller dele heraf eller oplysninger om, hvorvidt

⁹⁹ Lovforslag nr. L20, s. 15

¹⁰⁰ Ibid., s. 14

¹⁰¹ Straffelovrådet var af den opfattelse, at "en overvågning af en persons geografiske placering, der finder sted på afstand ved hjælp af en gps eller et andet lignende apparat, i almindelighed er udtryk for en krænkelse af en sådan grovhed, at der er grundlag for at overveje en kriminalisering i straffeloven." Se Lovforslag nr. L20, s. 14

¹⁰² Lovforslag nr. L20, s. 69

¹⁰³ Ibid., s. 70

¹⁰⁴ Ibid., s. 70-71

¹⁰⁵ Bet. 1104/1987 om legemsindgreb under efterforskningen

¹⁰⁶ Folketingstidende 1988-89 Tillæg A, sp. 2233

genstande er anbragt på legemet eller i legemets hulrum."¹⁰⁷ Man ønskede ud fra denne definition at lave en "samlet og systematiseret regulering"¹⁰⁸ på området.

Legemsindgrebene inddeles i RPL § 792, stk. 1 i legemsbesigtigelse (nr. 1) og legemsundersøgelse (nr. 2). Opdelingen mellem legemsbesigtigelse og legemsundersøgelse er først og fremmest foretaget ud fra betragtningen af, hvad der vil være mest indgribende for personens integritet i øjeblikket og i mindre grad ud fra overvejelser om, hvad man efterfølgende kan bruge de indsamlede oplysninger til.¹⁰⁹ Det følger af RPL § 792, stk. 1, nr. 1, at optagelse af fotografier er legemsbesigtigelse. Optagelse af fotografier er omfattet af definitionen på legemsindgreb, fordi der herved sker en fastholdelse af oplysninger – eksempelvis fotos af skader og slagmærker.¹¹⁰ Betingelserne for indgrebet fremgår af § 792 a, hvorefter den pågældende med rimelig grund skal være mistænkt for en lovovertrædelse, der er undergivet offentlig påtale, og hvor indgrebet må antages at være af væsentlig betydning for efterforskningen. Det er forudsat, at legemsindgreb efter § 792 a kun kan foretages over for en sigtet person.¹¹¹

4.1.2.2.1. Personfotografier med henblik på senere identifikation (§ 792 b)

Optagelse af personfotografier til brug for senere identifikation er ikke omfattet af hverken definitionen af straffeprocessuelle tvangsindgreb eller legemsindgreb, men på trods heraf har man truffet et valg om at sidestille dette indgreb med legemsbesigtigelse.¹¹² Dette valg begrundes ud fra en betragtning om, at en regulering af optagelse af personfotografier i retsplejeloven ville være mest praktisk og hensigtsmæssigt.¹¹³ Personfotografier indebærer optagelse af fotografier "til indsættelse i politiets samling med henblik på senere identificering af de pågældende."¹¹⁴ På trods af at fotograferingen ikke nødvendiggøres som følge af en konkret efterforskning, men derimod sker med henblik på en senere identifikation af

¹⁰⁷ Bet. 1104/1987 om legemsindgreb under efterforskningen, s. 11

¹⁰⁸ Ibid., s. 36

¹⁰⁹ Ibid., s. 41

¹¹⁰ Ibid., s. 44

¹¹¹ Ibid., s. 53

¹¹² Folketingstidende 1988-89 Tillæg A, sp. 2235

¹¹³ Bet. 1104/1987 om legemsindgreb under efterforskningen, s. 44

¹¹⁴ Ibid., s. 27

personen,¹¹⁵ er optagelse af personfotografier kategoriseret som legemsbesigtigelse. Med inddragelsen af optagelse af personfotografi med henblik på senere identifikation som et legemsindgreb øges politiets muligheder for at kunne optage personfotografier i forhold til adgangen i § 792 a.¹¹⁶

Både Strafferetsplejeudvalget og Justitsministeriet anså det for nødvendigt, at politiet har mulighed for at optage billeder af en sigtet person til brug for senere identifikation.¹¹⁷ Selvom optagelse af personfotografier til eventuel identifikation i fremtiden karakteriseres som “værende af meget lidt indgribende karakter”,¹¹⁸ anerkendes det samtidigt, at “der knytter sig alligevel betydelig interesse til emnet, da det tilvejebragte materiale kan udgøre et vigtigt bevismiddel, og da det kan systematiseres, registreres og opbevares og dermed få betydning for andre sager end netop den, hvortil det indhentes.”¹¹⁹ Det er således ikke selve optagelsen af personfotografiet, der opleves som indgribende, men derimod den efterfølgende mulige anvendelse i andre sager. Optagelse af personfotografi med henblik på senere identifikation reguleres i RPL § 792 b. Der er ikke noget indikationskrav efter § 792 b. Det betyder, at der ikke er krav om, at optagelsen af fotografiet skal være af betydning for den konkrete efterforskning, hvilket skal ses i sammenhæng med formålet om, at fotografiet optages til brug for eventuel senere identifikation. Det manglende indikationskrav modsvarer med et skærpet kriminalitetskrav.¹²⁰ Efterforskningen skal vedrøre en forbrydelse med en strafferamme på mindst 1 år og 6 måneder, og den pågældende skal med rimelig grund være mistænkt.¹²¹ Kompetencen til at træffe afgørelse om, at en legemsbesigtigelse efter både §§ 792 a og 792 b er tillagt politiet, jf. RPL § 792 c,¹²² hvilket ansås for at være “ubetænkeligt”¹²³ ud fra den betragtning, at optagelsen af et fotografi kun er “forbundet med ringe eller ingen ubehag eller

¹¹⁵ Bet. 1104/1987 om legemsindgreb under efterforskningen, s. 13

¹¹⁶ Folketingstidende 1988-89 Tillæg A, sp. 2246

¹¹⁷ Folketingstidende 1988-89 Tillæg A, sp. 2236–2237

¹¹⁸ Bet. 1104/1987 om legemsindgreb under efterforskningen, s. 25

¹¹⁹ Ibid., s. 25

¹²⁰ Bet. 1104/1987 om legemsindgreb under efterforskningen, s. 53, Folketingstidende 1988–89 Tillæg A, sp. 2237

¹²¹ Ibid.

¹²² Se også Folketingstidende 1988-89 Tillæg A, sp. 2247

¹²³ Bet. 1104/1987 om legemsindgreb under efterforskningen, s. 55

ulejlighed”,¹²⁴ og at politiets kompetence blev modsvaret med den samtidige indførelse af regler om opbevaring og sletning af de optagne fotografier.¹²⁵

4.1.2.2.2. Opbevaring og sletning af personfotografier (§ 792 f)

I retsplejelovens § 792 f reguleres politiets opbevaring og sletning af personfotografier og andet materiale, som man er kommet i besiddelse af ved legemsindgreb.¹²⁶ Behovet for reguleringen af politiets opbevaring af oplysninger tilvejebragt ved legemsindgreb skyldes bl.a., at særligt fingeraftryk og personfotografier ofte indføres og systematiseres i registre,¹²⁷ hvilket gør dem let tilgængelige gennem søgefunktioner. Systematiseringen i registre giver desuden mulighed for inddragelse i efterforskningen af senere sager.¹²⁸ Bestemmelsen omfatter både opbevaring i et register og lign. samt på den enkelte sag.¹²⁹ Man forsøgte ved bestemmelsen at finde en balance mellem hensynet til borgerens retssikkerhed på den ene side, som nødvendiggør en klarhed vedrørende politiets beføjelser, og på den anden side politiets mulighed for at anvende bl.a. personfotografier og fingeraftryk som arbejdsredskaber.¹³⁰ Desuden var man af den opfattelse, at politiets registre formentligt ville blive endnu vigtigere arbejdsredskaber i takt med den teknologiske udvikling, som kunne muliggøre lagring af andre typer af oplysninger i registre.¹³¹ Bestemmelsen skelner mellem opbevaring af personfotografier optaget efter § 792 b¹³² og andet materiale, eksempelvis fingeraftryk. Selvom opbevaringen af registrerede fingeraftryk og fotografier har “visse lighedspunkter”,¹³³ begrundes denne opdeling ud fra, at personfotografier i sagens natur har en tilknyttet “indlysende genkendelsesmulighed for udenforstående.”¹³⁴ Det gælder for politiets opbevaring af personfotografier optaget med henblik på senere identifikation, at politiet ikke må “opbevare personfotografier med henblik på senere identifikation af personer, der ikke har været sigtet, eller som er frifundet, eller mod hvem påtale er opgivet.” Det betyder, at opbevaring af personfotografier optaget efter § 792 b

¹²⁴ Bet. 1104/1987 om legemsindgreb under efterforskningen, s. 55

¹²⁵ Reguleret i RPL § 792 f, gennemgået straks nedenfor (afsnit 4.1.2.2.2.)

¹²⁶ Folketingstidende 1988-89 Tillæg A, sp. 2252

¹²⁷ Bet. 1104/1987 om legemsindgreb under efterforskningen, s. 85

¹²⁸ Ibid., s. 87

¹²⁹ Ibid., s. 88

¹³⁰ Ibid., s. 87

¹³¹ Ibid., s. 85

¹³² Fotografier optaget efter RPL § 792 a samt fotografier optaget som led i skygning hører således under “andet materiale”. Se hertil Bet. 1104/1987 om legemsindgreb under efterforskningen, s. 89

¹³³ Bet. 1104/1987 om legemsindgreb under efterforskningen, s. 44

¹³⁴ Ibid., s. 89

kun må opbevares, såfremt en person i øjeblikket er sigtet eller dømt. Såfremt en sigtelse opgives, eller denne person frifindes,¹³⁵ skal personfotografiet destrueres.¹³⁶

4.1.2.3. Overtagelse af TV-overvågning (§ 791 e)

Retsplejelovens § 791 e regulerer politiets mulighed for overtagelse af TV-overvågning fra andre myndigheder og private.¹³⁷ Bestemmelsen indebærer som nævnt ovenfor, at politiet fra andre myndigheder og private har mulighed for at overtage TV-overvågning i et område. Det har derfor betydning for bestemmelsens rækkevidde, hvilke rammer der er for myndigheder og private personer og virksomheders TV-overvågning, og bestemmelsen skal derfor ses i sammenhæng med TV-overvågningsloven.¹³⁸ Det følger heraf, at der som udgangspunkt er forbud mod, at private kan foretage overvågning af områder, som benyttes til almindelig færdsel, jf. lovens § 1. Der er dog en række undtagelser for så vidt angår eksempelvis tankstationer, indkøbscentre, pengeinstitutter, almindelige butikker og boligorganisationer.¹³⁹ Undtagelserne betyder, at private i mange situationer kan foretage TV-overvågning af områder, som benyttes til almindelig færdsel. Politiet har et register over TV-overvågning opsat efter TV-overvågningsloven, hvori myndigheder og private er forpligtet til at lade deres overvågning registrere.¹⁴⁰ Overtagelse af overvågning efter RPL § 791 e er ikke begrænset til overvågning omfattet af TV-overvågningsloven – også overvågning opsat i eksempelvis baglokaler i butikker kan overtages.¹⁴¹ Med overtagelse menes, at politiet efter bestemmelsen får rådighed over allerede optaget TV-overvågningsmateriale, men også at der er adgang til at overtage et overvågningskamera i realtid – eventuelt med fjernadgang. Det er netop behovet herfor, som betyder, at retsplejelovens regulering vedrørende eksempelvis beslaglæggelse og edition, hvorefter politiet kan få udleveret optagelser, ikke er tilstrækkelige.¹⁴² Denne overtagelse kan

¹³⁵ Frifindes personen i det forhold, der under efterforskningen begrundede optagelsen efter § 792 b, kan fotografiet kun fortsat opbevares, såfremt personen er blevet dømt i et andet forhold, der i sig selv kunne begrunde optagelse af fotografi efter § 792 b. Se hertil Folketingstidende 1988–89 Tillæg A, sp. 2252.

¹³⁶ Folketingstidende 1988-89 Tillæg A, sp. 2252

¹³⁷ Dog er private hjem undtaget, jf. § 791 e, stk. 1, 2. pkt.

¹³⁸ Lovbekendtgørelse 2023-02-24 nr. 182 om TV-overvågning (TV-overvågningsloven)

¹³⁹ Se TV-overvågningslovens § 2

¹⁴⁰ Se TV-overvågningslovens § 2 e

¹⁴¹ Lovforslag nr. L103, s. 11

¹⁴² Ibid., s. 10-11

ske i “forholdsvis store områder, eksempelvis en hel bydel” på én gang, og indgrebet kan således berøre flere TV-overvågninger og mange mennesker.¹⁴³

Formålet med overtagelsen af TV-overvågning som beskrevet ovenfor kan efter bestemmelsen både være med henblik på at forebygge kriminalitet, men også for at efterforske kriminalitet, som allerede er begået. Fælles for begge tilfælde er, at man anser TV-overvågning for at være et særdeles brugbart og relevant redskab for at kunne danne sig et overblik over en mulig gerningspersons færden.¹⁴⁴ Det kan derfor være relevant at foretage indgrebet i situationer, hvor det af forskellige årsager er særligt vigtigt at kunne identificere og lokalisere en gerningsmand hurtigt, eksempelvis ved et igangværende eller nært forestående angreb.¹⁴⁵ Desuden kan det være relevant i forbindelse med efterforskning af allerede begået kriminalitet i situationer, hvor det har afgørende betydning at lokalisere både gerningsmand og vidner hurtigt.¹⁴⁶ Det er særligt brugbart i situationer, hvor en gerningsmand opholder sig i en menneskemængde eller et andet sted, som gør det svært at opspore vedkommende. Her kan videoovervågningen gøre det muligt at overskue situationen hurtigere.¹⁴⁷

Kravene til overtagelse af TV-overvågning efter RPL § 791 e indebærer, at der skal være afgørende grunde til overtagelsen med henblik på at forebygge eller efterforske en forbrydelse. Desuden er kriminalitetskravet, at det skal vedrøre en lovovertrædelse med en strafferamme på mindst 6 år, eller som er omfattet af straffelovens kap. 12 og 13, og som kan medføre eller har medført fare for menneskers liv eller velfærd eller for betydelige samfundsværdier. Bestemmelsen er indført med særligt fokus på politiets håndtering af terrortrusler, men indgrebet kan også anvendes til forebyggelse og opklaring af andet kriminalitet, herunder bandekriminalitet.¹⁴⁸ Kriminalitetskravet afspejler, at der er tale om et intenst indgreb, både hvad angår den, der får overtaget sin TV-overvågning, men også hvad angår de overvågede. Såfremt indgrebet vil være uforholdsmæssigt, kan det ikke foretages, jf. stk. 2. Kompetencen til at træffe afgørelse om at foretage indgrebet er henlagt til retten, og det kræver således en

¹⁴³ Lovforslag nr. L103, s. 10-11

¹⁴⁴ Ibid., s. 2-3

¹⁴⁵ Ibid., s. 10

¹⁴⁶ Ibid., s. 10

¹⁴⁷ Ibid., s. 10

¹⁴⁸ Ibid., s. 14

kendelse, jf. stk. 3.¹⁴⁹ En indgrebsadvokat repræsenterer her de modstående interesser, det vil sige både den, hvis TV-overvågning overtages samt de overvågedes interesser.¹⁵⁰ Samlet set er der strenge krav til politiets overtagelse af TV-overvågning. Når politiet har overtaget TV-overvågning, har de valgfrihed ift. i hvilket omfang, udstyret anvendes. Politiet kan således vælge blot at se med, men de kan også vælge at optage billeder mm. Når politiet har fået råderet over optagelser foretaget af de overtagne overvågningskameraer, er det op til politiet, hvad disse optagelser anvendes til efterfølgende.¹⁵¹ De oplysninger, som indsamles fra den overtagne overvågning, kan anvendes til yderligere efterforskning og som bevis i straffesager.¹⁵² Politiet må kun opbevare optagelserne, såfremt de har dannet grundlag for en sigtelse, eller hvis de er af fortsat efterforskningsmæssig betydning – i modsat fald er der krav om tilintetgørelse, jf. RPL § 791.¹⁵³ I bemærkningerne til lovforslaget fremgår de overvejelser, som ligger til grund for indførelsen af bestemmelsen i retsplejeloven. En del af disse er gennemgået ovenfor. Den teoretiske definition af straffeprocessuelle tvangsindgreb ses imidlertid ikke inddraget i lovbemærkningerne. Her inddrages udelukkende overvejelser vedrørende de øvrige straffeprocessuelle tvangsindgreb, som kan give politiet lignende handlemuligheder, og hvorvidt disse muligheder var tilstrækkelige for at imødegå politiets behov.

4.1.3. Politiloven

Politoloven regulerer politiets virksomhed – herunder opgaver, beføjelser mm. Loven opsætter i mindre grad visse rammer for politiets indsamling og behandling af personoplysninger, idet dette er reguleret i en enkelt bestemmelse; politilovens § 2 a.

4.1.3.1. Politilovens § 2 a

Politolovens § 2 a regulerer i stk. 1 politiets mulighed for at foretage tværgående informationsanalyser. I stk. 2 reguleres indsamling og behandling af oplysninger fra offentligt tilgængelige kilder. Sidstnævnte kan være relevant for de nationale rammer for politiets anvendelse af ansigtsgenkendelse, fordi det er en måde, hvorpå politiet kan indsamle billede- og videomateriale.

¹⁴⁹ Lovforslag nr. L103, s. 15

¹⁵⁰ Ibid., s. 17

¹⁵¹ Ibid., s. 14

¹⁵² Ibid., s. 17

¹⁵³ Ibid., s. 17

Stk. 1 – tværgående informationsanalyse

Politilovens § 2 a, stk. 1, lyder: “Politiet foretager tværgående informationsanalyser på grundlag af de oplysninger, politiet behandler, når det er nødvendigt af hensyn til udførelsen af politiets opgaver”. Formålet med bestemmelsen er at give politiet en klar hjemmel til i bred forstand at udnytte de oplysninger, politiet ad anden vej lovligt har indsamlet.¹⁵⁴ Bestemmelsen hjemler derfor bl.a., at politiet kan videreanvende og behandle data “til andre formål end dem, de i snæver forstand er indsamlet til”.¹⁵⁵ Tværgående informationsanalyse skal forstås bredt som samkøring af oplysninger fra forskellige datakilder.¹⁵⁶ Kriteriet om nødvendighed indebærer, at behandlingen af dataene skal være nødvendig for at varetage de opgaver, politiet er pålagt efter politilovens § 2, herunder i forbindelse med opklaring af strafbare forhold. Nødvendigheden vurderes ud fra et politifagligt skøn.¹⁵⁷

Stk. 2 – open source intelligence

Det følger af politilovens § 2 a, stk. 2, at politiet kan indsamle og behandle oplysninger fra offentligt tilgængelige kilder, når det er nødvendigt af hensyn til udførelsen af politiets opgaver – herunder efterforskning og forfølgning af strafbare forhold. Ved indførelsen af bestemmelsen var formålet ikke at give politiet flere beføjelser vedrørende indsamling og behandling af oplysninger, men derimod at give politiet et “klart retligt grundlag for indsamlingen og behandlingen af offentligt tilgængelige oplysninger.”¹⁵⁸ Indtil indførelsen af bestemmelsen fandtes ikke en udtrykkelig hjemmel for indsamlingen.¹⁵⁹ Bestemmelsen giver politiet hjemmel til at indsamle offentligt tilgængelige oplysninger – i praksis omtalt som “open source”. Disse oplysninger anvendes til at “understøtte og supplere igangværende efterforskning.”¹⁶⁰ Offentligt tilgængelige kilder beskrives som i bred forstand at omfatte alle elektroniske og ikke-elektroniske informationskilder, “som inden for rammerne af gældende ret og uden

¹⁵⁴ Dette indebærer både oplysninger indsamlet gennem straffeprocessuelle tvangsindgreb og almindelige efterforskningsskridt, som ikke kræver særlig hjemmel.

¹⁵⁵ Lovforslag nr. L171, s. 17

¹⁵⁶ Ibid., s. 18

¹⁵⁷ Ibid., s. 17

¹⁵⁸ Ibid., s. 3

¹⁵⁹ Det anføres i bemærkningerne, at indsamling af offentligt tilgængelige oplysninger er omfattet af EMRK art. 8 om retten til privatliv, hvorfor det må leve op til kravet vedrørende hjemmelsgrundlaget. Se Lovforslag nr. L171, s. 10

¹⁶⁰ Lovforslag nr. L171, s. 6

gennemførelsen af et straffeprocessuelt indgreb kan tilgås i det offentlige rum,” herunder særligt internettet. Det er også omfattet af begrebet, hvis det er muligt at få adgang til oplysningerne gennem en betalingstjeneste.¹⁶¹ Der er krav om, at indsamlingen og behandlingen skal være “nødvendig” for udførelsen af politiets opgaver, som fremgår af PL § 2. Vurdering vedrørende indsamlingen og behandlingens nødvendighed skal være konkret.¹⁶²

Stk. 3 – hjemmel til udstedelse af bekendtgørelser

Det følger af politilovens § 2 a, stk. 3, at Justitsministeren fastsætter nærmere regler vedr. indsamling og behandling af oplysninger efter bestemmelsens stk. 2 og 3, herunder formål med behandling, sletning af oplysninger og tekniske og organisatoriske foranstaltninger. Det er anført i lovbemærkningerne, at fastsættelse af sådanne regler på bekendtgørelsesniveau med mere konkrete rammer er en forudsætning for brug af stk. 1 og 2. Det anføres, at sådanne rammer eksempelvis kunne indebære fastsættelse af krav til karakteren af strafbare forhold, som kan danne grundlag for tværgående informationsanalyser, jf. stk. 2.¹⁶³ På nuværende tidspunkt ses imidlertid ikke at være fastsat sådanne regler af relevans.

4.1.4. Delkonklusion

I ovenstående afsnit er der foretages en analyse af de nationale retlige rammer for politiets brug af ansigtsgenkendelse i efterforskningen. Det kan konkluderes, at der ikke i national ret findes en direkte lovregulering af politiets mulighed for at anvende ansigtsgenkendelse. Det betyder imidlertid, at der ikke er nogen retlige rammer for brugen af ansigtsgenkendelse i national ret. Ud fra analysen konkluderes, at en række bestemmelser i retsplejeloven og politiloven udgør en indirekte regulering af adgangen til brug af ansigtsgenkendelse gennem visse straffeprocessuelle tvangsindgreb og andre efterforskningsskridt, som opstiller betingelserne for eksempelvis indsamling af billede- og videomateriale. Indledningsvis kan det konstateres, at politiet ikke er underlagt nogle begrænsninger vedrørende fotografering og TV-overvågning af personer på frit tilgængelige steder ud over almindelige forvaltningsretlige principper. Politiet er således ikke umiddelbart i national ret begrænset af nogen rammer på dette område, såfremt indsamlingen sker på et frit tilgængeligt sted, og sådanne fotografier kan derfor frit kan indsamles og anvendes i efterforskningen – også til brug for ansigtsgenkendelse. Indsamling

¹⁶¹ Lovforslag nr. L171, s. 10–11

¹⁶² Ibid., s. 18

¹⁶³ Ibid., s. 19

af foto- og videomateriale på et ikke frit tilgængeligt sted er derimod underlagt begrænsninger. Dette reguleres i RPL § 791 a. Bestemmelsen vurderes dog at være af mindre betydning som følge af, at fotograferingen og TV-overvågningen skal ske på et ikke frit tilgængeligt sted, før det er omfattet. Formålet med at anvende dette indgreb vil formentlig ikke være at indsamle et billede af en mistænkt som sådan, men derimod at foretage en dokumentation af pågældendes adfærd. Det virker derfor ikke oplagt, at indgrebet i praksis vil udgøre en oplagt hjemmel til indsamling af materiale, som senere kan anvendes til ansigtsgenkendelse.

Politiets mulighed for at overtage TV-overvågning fra myndigheder og private efter RPL § 791 e er endnu en måde, hvorpå politiet kan komme i besiddelse af videomateriale. Af denne årsag er bestemmelsen indirekte med til at sætte rammerne for politiets anvendelse af ansigtsgenkendelse til efterforskningsbrug. Bestemmelsen har betydning, både hvad angår retrospektiv ansigtsgenkendelse og realtid. Politiet gives mulighed for at indsamle materiale, som kan anvendes i efterforskning af en allerede begået forbrydelse samt overtagelse af TV-overvågning i et større område. I begge tilfælde vil anvendelse af ansigtsgenkendelse i høj grad effektivisere politiets brug af indgrebet, fordi det indsamlede materiale vil være et endnu mere effektivt efterforskningsværktøj, såfremt man knytter ansigtsgenkendelse til. Det fremgår af bemærkningerne, at en stor del af årsagen til behovet for indgrebet er opsporing og identifikation af en gerningsmand, og her må ansigtsgenkendelse siges at være særligt egnet. Politiet vil således med indgrebet ikke være begrænset til at bruge ansigtsgenkendelse på egne kameraer og disses optagelser. Det er dog værd at fremhæve, at der stilles høje krav til anvendelse af indgrebet, hvorfor politiets adgang til at overtage TV-overvågning er begrænset til alvorlige tilfælde.

Der er desuden foretaget en gennemgang af rammerne for politiets optagelse af fotografier i forbindelse med legemsbesigtigelse, jf. RPL §§ 792 og 792 b. Sondringen mellem de to bestemmelser vil i praksis ske på baggrund af det formål, hvormed fotografiet optages. Idet optagelse af fotografier efter § 792 a kun kan foretages, såfremt det er af væsentlig betydning for efterforskningen, vil dette ofte være tilfælde, hvor der er behov for dokumentation af eventuelle skader osv. Bestemmelsen vil derfor have meget lidt relevans i forhold til indsamling af fotografier, som kan anvendes til brug for ansigtsgenkendelsesteknologi. Derimod vil § 792 b om optagelse af personfotografier være relevant, idet fotografierne optages og opbevares med henblik på senere identifikation, ofte i et register. Indgrebet vil have særlig relevans for rammerne for ansigtsgenkendelse, når det kommer til opbygning af en database

hos politiet, som et indsamlet materiale kan holdes op imod for at foretage sammenligning og identifikation. Desuden vil bestemmelsen regulere optagelse af et fotografi, som vil kunne sammenholdes med indholdet i en sådan database. Betingelserne for opbevaring af disse personfotografier fremgår af RPL § 792 f. Bestemmelsen er således relevant for politiets brug af ansigtsgenkendelse, fordi politiets muligheder for at opbevare personfotografier i en database begrænses. Det er kun personfotografier af en sigtet eller dømt person, som må indgå i en sådan database. De retlige rammer for en sådan database har betydning for brugen af ansigtsgenkendelse, fordi brug af dette i nogle tilfælde vil kræve et sammenligningsgrundlag – eksempelvis ved brug af database til identifikation af en person på samme måde, som man gør med fingeraftryk.

Teleobservation er reguleret i RPL § 791 a, stk. 5, og her etableres formentligt visse indirekte rammer for politiets adgang til at anvende ansigtsgenkendelse i efterforskningen. Indgrebet omfatter anvendelse af videokamera til at vise en persons færden, hvilket kan forstås således, at politiet eksempelvis ved hjælp af et videokamera monteret på en bil kan modtage direkte billeder fra videokameraet, hvorved det er muligt at følge en persons færden. Det kan derimod også forstås sådan, at det vil være omfattet af bestemmelsen, hvis politiet anvender allerede opsatte videokameraer til at overvåge en person ved at følge dennes færden. Her vil brug af ansigtsgenkendelse både retrospektivt og i realtid muliggøre overvågning af en bestemt persons nuværende eller tidligere geografiske placering fra afstand. Iværksættelse af dette kan således vær omfattet af kravene i RPL § 791 a, stk. 5, men bestemmelsen vil formentligt ikke anvendes i denne situation, da det ikke har været formålet med den.

Indsamling af oplysninger fra offentligt tilgængelige kilder samt adgang til tværgående informationsanalyse er desuden reguleret af politilovens § 2 a, der blot opstiller krav om, at denne indsamling og behandling er nødvendig i varetagelsen af politiets opgaver. Politiet kan således med få begrænsninger indsamle eksempelvis billede- og videomateriale frit tilgængeligt på internettet, såfremt dette er “nødvendigt” – eksempelvis til brug for en efterforskning. De kan endvidere i vidt omfang sammenkøre alle indsamlede oplysninger i tværgående informationsanalyser, såfremt dette er nødvendigt i den specifikke sag. Adgangen til tværgående informationsanalyse kan formentligt hjemle sammenligningen af en biometrisk ansigtsskabelon med en database af personfotografier for gennem et match at fastslå vedkommendes identitet, såfremt denne persons biometriske ansigtsskabelon findes i et register. Det bemærkes dog, at dette formentligt vil kræve udstedelse af en bekendtgørelse med

de nærmere betingelser, jf. PL § 2 a, stk. 3. Det vurderes derimod, at bestemmelsen ikke hjemler en generel adgang til at foretage ansigtsgenkendelse som sådan. Det er først, når der sker en sammenligning mellem to biometriske ansigtsskabeloner,¹⁶⁴ at der kan være tale om en ‘tværgående informationsanalyse’.

¹⁶⁴ Der henvises til ”trin 3” af teknologiens fremgangsmåde som opdelt i afsnit 3.1.1.

4.2. EU-retlige rammer for politiets anvendelse af ansigtsgenkendelse

Til brug for besvarelsen af specialets problemformulering, som vedrører de retlige rammer for politiets brug af ansigtsgenkendelse, er det nødvendigt at inddrage EU-regulering for at få et fyldestgørende billede. I det følgende afsnit analyseres AI-forordningen og retshåndhævelseslovens (og -direktivets) rammer for anvendelse af ansigtsgenkendelse.

4.2.1. AI-forordningen

I dette afsnit undersøges AI-forordningen og dennes rammer for politiets anvendelse af ansigtsgenkendelse. På trods af at Danmark som følge af forbeholdet er undtaget fra regulering, som angår retshåndhævende myndigheder,¹⁶⁵ foretages alligevel en kort gennemgang af forordningens relevante bestemmelser. Forordningen er på området for retshåndhævende myndigheder ikke er gældende ret i Danmark, men reguleringen inddrages igen senere i specialets diskussion.

I AI-forordningen sondres mellem flere kategorier af AI-systemer. Disse opdeles ud fra den risiko, de indebærer for grundlæggende rettigheder og personers sikkerhed. AI-systemerne med den højeste risiko forbydes, jf. art. 5, stk. 1. Eksempler på disse AI-systemer er anvendelse af ansigtsgenkendelse til risikovurdering af, hvorvidt en person vil begå en strafbar handling baseret på profilering af personlighedstræk eller personlige egenskaber (litra d) samt biometrisk kategorisering, hvorfra kan udledes følsomme personoplysninger såsom race eller seksuel orientering (litra g). Desuden fastsættes et forbud mod "anvendelse af systemer til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse." (litra h). Ansigtsgenkendelse i realtid kan undtagelsesvist tillades, hvis det er strengt nødvendigt, og hvis formålet enten er at lave en målrettet eftersøgning af eksempelvis forsvundne personer, at forebygge en overhængende fare mod fysiske personers liv og sikkerhed. Det kan eksempelvis være ved terrorangreb, eller når ansigtsgenkendelse anvendes for at lokalisere eller identificere en person, der er mistænkt for en oplistet forbrydelse, som i medlemsstaten kan straffes med mindst 4 års fængsel. Efter stk. 2 er der endvidere krav om, at der tages en række hensyn og gøres nogle overvejelser vedrørende situationens karakter vejet op imod konsekvenserne for de berørte personers rettigheder. Vurderingen af nødvendigheden af brugen af

¹⁶⁵ Se AI-forordningens præambel 41: Danmark som følge af retsforbeholdet er undtaget fra AI-forordningens artikel 5, stk. 1, litra g, d og h, stk. 2-6 samt artikel 26, stk. 10.

ansigtsgenkendelsen vedrører bl.a. tidsperioden samt omfanget af det geografiske og personmæssige anvendelsesområde – det skal derfor kun iværksættes i det omfang, der er indikation på, at det er nødvendigt. Der sættes i stk. 3 krav om, at iværksættelsen af brugen betinges af “en forudgående tilladelse, der er udstedt af en judiciel myndighed”, eksempelvis en kendelse. Kravet om en retskendelse kan dog undgås, såfremt medlemsstaten vedtager lovgivning, som giver retshåndhævende myndigheder tilladelse til denne brug af ansigtsgenkendelse. En sådan lovgivning skal holde sig inden for rammerne af ovennævnte betingelser. AI-forordningens art. 6 klassificerer højrisko-AI-systemer, som bl.a. omfatter systemer til biometrisk fjernidentifikation,¹⁶⁶ herunder retrospektivt brug af ansigtsgenkendelse. Reglerne for anvendelse af disse systemer følger af direktivets afsnit 2, og de indebærer krav om risikostyring,¹⁶⁷ registrering af logfiler,¹⁶⁸ gennemsigtighed¹⁶⁹ og menneskeligt tilsyn¹⁷⁰ m.fl.

4.2.2. Retshåndhævelsesdirektivet og retshåndhævelsesloven

Retshåndhævelsesdirektivet er EU-retlig regulering på det databeskyttelsesretlige område, som regulerer retshåndhævende myndigheders behandling af personoplysninger. Direktivet er implementeret i national ret ved retshåndhævelsesloven.¹⁷¹ Indledende behandles retshåndhævelseslovens anvendelsesområde for at skabe et overblik over, hvornår loven regulerer politiets behandling af personoplysninger og i hvilket omfang. Desuden gennemgås lovens mulige databehandlingsgrundlag, herunder hvordan disse regulerer ansigtsgenkendelse konkret.

4.2.2.1. Anvendelsesområde

Indledningsvis foretages en gennemgang af hvilke betingelser, der skal opfyldes, for at retshåndhævelsesloven finder anvendelse. Den første betingelse vedrører den behandlende myndighed. Det følger af retshåndhævelseslovens § 1, at loven gælder for navngivne kompetente myndigheders behandling af personoplysninger, hvilket omfatter politiet, anklagemyndigheden, herunder den militære anklagemyndighed, kriminalforsorgen, Den

¹⁶⁶ Se art. 6, stk. 2, som henviser til bilag III

¹⁶⁷ AI-forordningen, art. 9

¹⁶⁸ Ibid., art. 12

¹⁶⁹ Ibid., art. 13

¹⁷⁰ Ibid., art. 14

¹⁷¹ Der henvises til afsnit 2.4.2.2. for de nærmere metodemæssige overvejelser.

Uafhængige Politiklagemyndighed og domstolene. Den anden betingelse er, at der sker en behandling af personoplysninger, som er omfattet af loven. Disse vedrører behandling, som ”helt eller delvist foretages ved hjælp af automatisk databehandling, og for anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.”¹⁷² Behandling er defineret i lovens § 3, nr. 2 som “enhver aktivitet eller række af aktiviteter med eller uden brug af automatisk behandling, som personoplysninger eller en samling af personoplysninger gøres til genstand for.” Behandling omfatter derfor bl.a. indsamling, registrering, organisering, systematisering og opbevaring.¹⁷³ Automatisk databehandling skal forstås i overensstemmelse med begrebet “elektronisk databehandling”, som blev anvendt i persondatalovens § 1, stk. 1.¹⁷⁴ Det betyder, at al databehandling ved brug af teknologi vil være omfattet, imens manuel databehandling, eksempelvis af fysiske papirsager, kun vil blive omfattet, hvis oplysninger vil blive indeholdt i et register.

Der er krav om, at denne behandling af personoplysninger sker ud fra et bestemt formål. Behandling skal således ske ”med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod eller forebygge trusler mod den offentlige sikkerhed.”¹⁷⁵ Ikke alle de nævnte myndigheders behandling af persondata vil således falde inden for lovens anvendelsesområde.¹⁷⁶ I dansk kontekst kommer dette til udtryk ved, at behandling af personoplysninger inden for strafferetsplejen i sagens natur vil falde inden for anvendelsesområdet, fordi forseelser, der kan føre til bøde eller fængselsstraf, vil udgøre “strafbare handlinger” i lovens forstand.¹⁷⁷ Desuden finder loven anvendelse på de kompetente myndigheders behandling vedrørende aktiviteter, som ikke nødvendigvis kan rummes inden for den danske strafferetspleje. Her kan eksempelvis nævnes politiaktiviteter, der retter sig mod potentielle strafbare forhold, eksempelvis opgaver vedrørende opretholdelse af lov og orden,¹⁷⁸ der typisk henføres under politiets

¹⁷² Retshåndhævelsesdirektivet art. 2, stk. 2 og retshåndhævelseslovens § 1, stk. 1.

¹⁷³ Retshåndhævelsesdirektivets art. 3, nr. 2

¹⁷⁴ Lovforslag nr. L168, s. 58

¹⁷⁵ Retshåndhævelsesdirektivets art. 2, stk. 1, jf. art. 1, stk. 1 og retshåndhævelseslovens § 1, stk. 1.

¹⁷⁶ Som nævnt i direktivets præambel 12 er det nemlig muligt for de kompetente myndigheder at varetage opgaver, der ikke nødvendigvis har retshåndhævende karakter. Denne behandling vil være omfattet af databeskyttelsesforordningen.

¹⁷⁷ Lovforslag nr. L168, s. 19

¹⁷⁸ Retshåndhævelsesdirektivet præambel 12

ordenshåndhævelsesbeføjelser og således uden for strafferetsplejen.¹⁷⁹ Retshåndhævelseslovens anvendelsesområde afspejler derfor ikke den klassiske opdeling mellem inden for og uden for strafferetsplejen, som der er tradition for i dansk ret.

4.2.2.2. Generelle bestemmelser

Al behandling af personoplysninger, som er omfattet af retshåndhævelsesloven, skal overholde en række generelle regler. Det følger af lovens § 4, at oplysningerne skal behandles i overensstemmelse med god databehandlingsskik, hvilket både omfatter, at der skal tages hensyn til oplysningernes karakter i behandlingen, men også at oplysningerne skal være relevante, tilstrækkelige og at de ikke må omfatte mere, end der kræves for at opfylde formålet. Oplysningerne skal være korrekte, og forkerte oplysninger skal slettes eller berigtiges. Retshåndhævende myndigheder skal således tage højde for kvaliteten af den data, de behandler. Hvad angår ansigtsgenkendelse har dette betydning derved, at billeder af lav kvalitet skal behandles mere påpasseligt end billeder af høj kvalitet, fordi der er større risiko for et fejlagtigt resultat. Det følger desuden af retshåndhævelseslovens § 6, at den dataansvarlige så vidt muligt skal sondre mellem personoplysninger om forskellige kategorier af registrerede, når det er relevant. Disse forskellige kategorier indebærer mistænkte personer, dømte, forurettede og andre personer. En sådan sontring kan foretages ved at opstille forskellige regler for behandling af personoplysninger i de forskellige grupper.¹⁸⁰ Idet sontringen kun skal foretages “så vidt muligt”, vil der i de fleste sammenhænge ikke være krav om “en forskellig behandling af oplysninger om forskellige kategorier af registrerede i den samme konkrete straffesag.”¹⁸¹ Det vil desuden ikke være relevant at sondre, når der sker behandling af personoplysninger, som varetager tungtvejende hensyn, eksempelvis forebyggelse af alvorlig kriminalitet.¹⁸² Kravet vil derfor have mindre betydning i praksis.

4.2.2.3. Kategorier af personoplysninger

Retshåndhævelsesloven regulerer, på hvilket grundlag politiet kan behandle personoplysninger som led i retshåndhævelsen. Det er nødvendigt at sondre mellem almindelige og følsomme personoplysninger for at afgøre, hvilke betingelser der stilles til behandling af disse.

¹⁷⁹ Lovforslag nr. L168, s. 19

¹⁸⁰ Ibid., s. 68

¹⁸¹ Ibid., s. 68

¹⁸² Ibid., s. 68

Grundlaget for behandling af almindelige personoplysninger findes i retshåndhævelseslovens § 9. Såfremt der er tale om behandling af særligt følsomme personoplysninger, findes grundlaget for behandlingen i § 10. Denne bestemmelse regulerer behandling af oplysninger vedrørende bl.a. race, seksuel orientering men også behandling af biometriske data med formål om entydigt at identificere en fysisk person. Såfremt personoplysningen hører under denne kategori, følger det af retshåndhævelseslovens § 10, stk. 1, at der som udgangspunkt er forbud mod behandling heraf. Det skal ses i sammenhæng med, at følsomme personoplysninger anses som særligt beskyttelsesværdige, og at udgangspunktet er, at oplysningerne så vidt muligt ikke bør behandles. På trods af forbuddet er det muligt at behandle oplysningerne under iagttagelse af kravene i § 10, stk. 2, hvilket behandles nedenfor. Som eksempel kan nævnes behandlingen af et fotografi af en identificerbar fysisk person. Udgangspunktet er, at dette vil være omfattet af § 9, medmindre det ud fra fotografiet er muligt at udlede oplysninger, der omfattes af § 10. Det har således betydning for kravene til politiets behandling af personoplysninger, om oplysningen er følsom eller ej, da oplysningens karakter er afgørende for valg af behandlingsgrundlag. Der er strengere krav til behandling af følsomme personoplysninger.

4.2.2.3.1. Biometrisk data

Biometriske data med formål om entydigt at identificere en fysisk person er omfattet af retshåndhævelseslovens § 10. Spørgsmålet er, hvad dette nærmere indebærer, herunder om al behandling af biometrisk data er omfattet. Biometrisk data defineres i retshåndhævelseslovens § 3, nr. 12 som "Personoplysninger, der som følge af specifik teknisk behandling vedrørende en fysisk persons fysiske, fysiologiske eller adfærdsmæssige karakteristika muliggør eller bekræfter en entydig identifikation af vedkommende, f.eks. ansigtsbillede eller fingeraftryksoplysninger."¹⁸³ Før personoplysninger kan karakteriseres som biometriske data, skal der foretages en specifik teknisk behandling. 'Behandling' er defineret ovenfor. At behandlingen skal være teknisk indebærer, at der anvendes en form for teknologi, hvilket eksempelvis kan være ansigtsgenkendelse, hvor der dannes en biometrisk ansigtsskabelon. Der må således ikke være tale om manuel behandling. Desuden skal behandlingen vedrøre fysiologiske eller adfærdsmæssige karakteristika ved en fysisk person, hvilket kan være et ansigtsbillede, men også en persons gang, fingeraftryk eller andre karakteristika. Afgørende for, om der er tale om biometriske data efter retshåndhævelsesloven er, at den tekniske

¹⁸³ Ordlyden er overensstemmende med direktivets art. 3, nr. 13.

behandling af den udvalgte karakteristika kan medføre “entydig identifikation” af den fysiske person. Det er netop kernen af biometriske data, at fysiologiske eller adfærdsmæssige karakteristika kan anvendes til at identificere en person ved dannelsen af en biometrisk ansigtsskabelon, som er unik for den fysiske person. Definitionen opstiller imidlertid ikke krav om, at en identitet herved faktisk kan fastslås – muligheden for at kunne foretage identifikationen er tilstrækkeligt. Hertil anfører EDPB tillige i en vejledning, at entydig identifikation ikke kræver, at man kan fastlægge en persons identitet, men at man har identificeret vedkommende således, at det er muligt entydigt at genkende denne person ud fra den biometriske skabelon, som er dannet.¹⁸⁴ Denne vurdering stemmer overens med den almindelige definition af ansigtsgenkendelse med identifikationsformål – modsat verifikation.¹⁸⁵ Ræsonnementet hænger desuden sammen med, at databeskyttelsen i bredere forstand kun gælder for en identificeret eller identificerbar fysisk person.¹⁸⁶ I vurderingen af, om en person er identificerbar, inddrages alle midler, der “med rimelighed kan tænkes bragt i anvendelse af den dataansvarlige eller en anden person til direkte eller indirekte at identificere, herunder udpege, den pågældende.” Hvorvidt midler med rimelighed kan tænkes anvendt, afhænger af objektive forhold, herunder hvor mange omkostninger identifikationen er forbundet med, og hvor meget tid, det er nødvendigt at bruge “under hensyntagen til den tilgængelige teknologi på behandlings-tidspunktet og den teknologiske udvikling.”¹⁸⁷ Der foretages således en konkret vurdering ud fra de midler, som den retshåndhævende myndighed har til rådighed. Et eksempel herpå kunne være en database med personfotografier, som gør det nemmere at foretage identifikation.

4.2.2.4. Behandling af almindelige personoplysninger

Behandling af almindelige personoplysninger reguleres af retshåndhævelseslovens § 9, hvorefter behandling kan ske, hvis det er ‘nødvendigt’ af hensyn til formålene nævnt i § 1, stk. 1. Bestemmelsen overlader et stort skøn til databehandleren, som i dette tilfælde er de retshåndhævende myndigheder; såfremt det vurderes, at den pågældende behandling er nødvendig for at varetage myndighedens opgaver, kan behandlingen foretages. Det kan have betydning for vurderingen, om den registrerede har givet samtykke til behandlingen, men der

¹⁸⁴ EDPB Guidelines 3/2019 on processing of personal data through video devices, s. 16-17

¹⁸⁵ Se afsnit 3.1.2.1

¹⁸⁶ Modsat anonymiserede oplysninger, der således ikke omfattes af beskyttelsen, jf. præambel 21

¹⁸⁷ Se retshåndhævelsesdirektivets præambel 21

er ikke krav om samtykke.¹⁸⁸ Behandlingen bør imidlertid kun foretages, hvis formålet hermed ikke kan opfyldes på anden vis. Kravet om nødvendighed er således en samlet proportionalitetsafvejning, hvor der skal foretages en afvejning mellem nødvendighed og forholdsmæssighed af behandlingen i et demokratisk samfund på den ene side og på den anden side hensynet til “den berørte fysiske persons legitime interesser.”¹⁸⁹

Grundlaget for politiets indsamling af eksempelvis video- og billedmateriale findes således i retshåndhævelseslovens § 9, da der blot er tale om almindelige personoplysninger. Som nævnt er kravet til dette blot, at behandlingen er nødvendig for, at politiet kan opfylde sine opgaver. Såfremt det indsamlede materiale behandles ved hjælp af ansigtsgenkendesteknologi, vil dette resultere i skabelsen af en biometrisk data i form af en biometrisk ansigtsskabelon. Behandlingen vil, såfremt den biometriske data dannes med henblik på identifikation, skulle finde sit grundlag i retshåndhævelseslovens § 10.

4.2.2.5. Behandling af følsomme personoplysninger, herunder biometriske data

Behandlingen af særligt følsomme personoplysninger skal ske i overensstemmelse med kravene i retshåndhævelseslovens § 10, hvilket inkluderer behandling af biometriske data med formål om entydigt at identificere en person. Som nævnt ovenfor er behandlingen af følsomme personoplysninger som udgangspunkt forbudt, jf. § 10, stk. 1, men denne behandling kan alligevel foretages, såfremt en række betingelser er opfyldt, jf. § 10, stk. 2:

“Under overholdelse af betingelserne i denne lov kan der dog foretages behandling af oplysninger omfattet af stk. 1, når det er strengt nødvendigt og sker af hensyn til de formål, der er nævnt i § 1, stk. 1, herunder for at beskytte den registreredes eller en anden fysisk persons vitale interesser, eller hvis behandlingen vedrører oplysninger, som tydeligvis er offentliggjort af den registrerede.”

¹⁸⁸ Lovforslag nr. L168, s. 28

¹⁸⁹ Retshåndhævelsesdirektivet, præambel 26

Ordlyds- og formålsfortolkning

Ved en ordlydsfortolkning af bestemmelsen kan udledes, at kravene til behandling af følsomme personoplysninger er 1) at behandlingen skal foretages inden for de rammer, der sættes for behandling af personoplysninger i retshåndhævelsesloven, herunder god databehandlingsskik,¹⁹⁰ 2) at behandlingen er 'strengt nødvendig' og 3) at behandlingen foretages med henblik på formålene nævnt i lovens § 1, stk. 1, herunder ud fra to eksplicitte formål. Kravet om, at behandlingen skal være 'strengt nødvendig', er en skærpelse af behandlingsgrundlaget i forhold til almindelige personoplysninger,¹⁹¹ hvor der kun stilles krav om, at behandlingen skal være 'nødvendig'. Af lovbemærkningerne fremgår imidlertid, at det næppe er muligt at sondre mellem disse krav.¹⁹² Den tredje betingelse vedrørende behandlingens formål må forstås således, at behandling af følsomme personoplysninger kan foretages, hvis formålet med behandlingen er at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder for at beskytte mod eller forebygge trusler mod den offentlige sikkerhed. Desuden nævnes to eksplicitte formål, behandlingen kan foretages på baggrund af, men på grund af brugen af 'herunder' inden disse nævnes, forstås disse blot som eksempler på situationer, som hører under de nævnte formål. Af lovbemærkningerne fremgår blot, at disse eksempler er medtaget for at sikre, at der ikke kan rejses tvivl om en korrekt implementering af retshåndhævelsesdirektivet.¹⁹³ Det virker overflødigt at medtage betingelsen om, at behandlingen af oplysninger nævnt i § 10, stk. 1 kan ske ud fra de nævnte formål, fordi dette i forvejen er en forudsætning for, at behandlingen overhovedet er reguleret af retshåndhævelsesloven.¹⁹⁴ Der opstilles således ikke herved skærpede krav til behandlingen, hvilket efterlader betingelsen om 'streng nødvendighed' som det eneste, der adskiller grundlaget for behandling af almindelige og følsomme personoplysninger. Sammenholdt med, at det i bemærkningerne anføres, at betingelsen om 'streng nødvendighed' næppe kan sondres fra kravet om 'nødvendighed' efter § 9, vil der i praksis ikke være forskel på adgangen til at behandle almindelige og følsomme personoplysninger. Der er således behov for tillige at fortolke RHL § 10 i lyset af direktivets art. 10.

¹⁹⁰ Der henvises til afsnit 4.2.2.2. *Generelle bestemmelser* for en gennemgang heraf.

¹⁹¹ Retshåndhævelsesdirektivets art. 8 og retshåndhævelseslovens § 9

¹⁹² Lovforslag nr. L168, s. 68

¹⁹³ Ibid., s. 68

¹⁹⁴ Der henvises til afsnit 4.2.2.1. *Anvendelsesområde*

Direktivkonform fortolkning

Det kan konstateres, at der er uoverensstemmelser mellem direktivets art. 10 og lovens § 10 på trods af, at en korrekt implementering af retshåndhævelsesdirektivet har været et opmærksomhedspunkt.¹⁹⁵ Selvom direktivet ikke har direkte retsvirkning i Danmark, skal retshåndhævelsesloven fortolkes direktivkonformt, fordi loven implementerer et EU-direktiv. Der foretages således i det følgende en gennemgang af direktivets art. 10, hvorefter behandling af følsomme personoplysninger kun tillades, når det er strengt nødvendigt, og under forudsætning af, at behandlingen er omfattet af de fornødne garantier for den registreredes rettigheder og frihedsrettigheder. Derudover er der efter art. 10 krav om, at behandlingen enten a) er hjemlet i EU-retten eller i medlemsstatens nationale ret, b) sker for at beskytte registreredes eller en anden fysisk persons vitale interesser eller c) hvis behandlingen vedrører oplysninger, som tydeligvis er offentliggjort af den registrerede.

Direktivet fastsætter således samme betingelse om, at behandlingen skal være ‘strengt nødvendig’. I direktivet uddybes ikke, hvad dette krav om streng nødvendighed nærmere indebærer. EDPB anfører hertil, at kravet om streng nødvendighed betyder, at myndighedens skønsmargin for nødvendigheden er på et absolut minimum, og at der bør være fastlagt objektive kriterier for behandlingen for at undgå en generel eller systematisk behandling.¹⁹⁶ Sådanne objektive kriterier kan vedrøre “arten og grovheden af den overtrædelse, som den registrerede [...] mistænkte for at have begået, eller andre relevante forhold.”¹⁹⁷ Det bemærkes, at brug af ansigtsgenkendelse i realtid uden en særlig begrundelse herfor må have en generel og systematisk karakter, hvilket gør det uforeneligt med kravet om streng nødvendighed. Det må derfor udelukke brug heraf, medmindre iværksættelsen sker for at varetage et nærmere afgrænset formål. I vejledningen bemærkes endvidere, at kravet om streng nødvendighed betyder, at politiet ikke må foretage såkaldt ‘scraping’ af materiale, herunder billeder som kan findes online, til brug for udarbejdelse af en database med biometriske ansigtsskabeloner. En sådan fremgangsmåde vil derfor aldrig kunne leve op til kravet om streng nødvendighed i § 10, stk. 2.¹⁹⁸ Det må samlet set konstateres, at retshåndhævelsesdirektivets art. 10 utvetydig stiller krav om, at der er skærpede krav til nødvendigheden af at foretage behandling efter

¹⁹⁵ Lovforslag nr. L168, s. 14

¹⁹⁶ EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, s. 21

¹⁹⁷ Se hertil C-205/21, præmis 133

¹⁹⁸ EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, s. 29

retshåndhævelseslovens § 10, uanset at indholdet af nødvendighedskravet er vanskeligt at fastlægge i praksis.

Derudover skal behandlingen være omfattet af garantier for den registreredes rettigheder og frihedsrettigheder. I direktivets præambel 37 uddybes, at følsomme oplysninger ikke bør behandles, ”medmindre behandling er omfattet af de fornødne garantier for den registreredes rettigheder og frihedsrettigheder, der er fastsat ved lov, og er tilladt i tilfælde hjemlet ved lov.” Det betyder, at behandlingen af de følsomme oplysninger nævnt i § 10 skal være i overensstemmelse med den registreredes rettigheder efter retshåndhævelsesdirektivet og -loven, men også med rettighederne efter EMRK og Chartet. De fornødne garantier for den registreredes rettigheder og frihedsrettigheder kan eksempelvis angå nærmere regulering vedrørende indsamlingen, personalets adgang til oplysninger og forbud mod videregivelse.

Behandlingen kan foretages på ét af tre forskellige grundlag. En hjemmel i national ret kan således ligge til grund for behandlingen af følsomme personoplysninger. Såfremt adgangen ikke er hjemlet ved lov, kan behandlingen kun ske, hvis det er med henblik på beskyttelse af en fysisk persons interesser eller hvis oplysningerne tydeligvis er offentliggjort af den registrerede. Vedrørende det første mulige behandlingsgrundlag er det uklart, om man er af den opfattelse, at retshåndhævelseslovens § 10 i sig selv udgør en lovhjemmel i national ret til behandling af følsomme personoplysninger og derved giver det lovgrundlag for behandling, som art. 10 stiller krav om.¹⁹⁹ Artikel 10 har imidlertid karakter af at være en form for generalklausul,²⁰⁰ som opstiller betingelser for behandling af følsomme personoplysninger, herunder at det kan ske ved hjemmel i national ret. Kravet til denne hjemmel omtales i præambel 33. Der er ikke nødvendigvis krav om vedtagelse af en lov, men grundlaget bør “være klart og præcist, og anvendelse heraf bør være forudsigelig for de personer, der er omfattet af dets anvendelsesområde.” Hjemlen skal således angive målet og formålet med behandlingen samt de specifikke personoplysninger, der skal behandles. Desuden skal risikoen for misbrug og vilkårlighed imødegås i et lovgrundlag, hvorfor “procedurerne for sikring af personoplysningernes integritet og fortrolighed samt procedurerne for deres tilintetgørelse”²⁰¹

¹⁹⁹ I et svar på et spørgsmål stillet af Retsudvalget, hvor der foretages en gennemgang af de retlige rammer for behandling af biometrisk data, nævnes der ikke andre lovhjemler som behandlingsgrundlag. Der henvises til Retsudvalgets spørgsmål nr. 1344 stillet den 13/8 2024, besvaret af justitsministeren den 8/11 2024.

²⁰⁰ EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, s. 21

²⁰¹ Retshåndhævelsesdirektivet, præambel 33

tillige skal være klart og præcist angivet. Hvorvidt retshåndhævelseslovens § 10 kan udgøre et sådant lovgrundlag i national ret, afhænger derfor bl.a. af, hvilken type personoplysninger, der skal behandles, idet bestemmelsen udgør et behandlingsgrundlag for mange typer af oplysninger, hvor der må stilles varierende krav til hjemlen. EDPB bemærker i den forbindelse, at den blotte implementering af retshåndhævelsesdirektivets art. 10 ikke udgør en tilstrækkelig hjemmel til politiets anvendelse af ansigtsgenkendelsesteknologi.²⁰² Art. 10 omhandler behandling af mange forskellige former for følsomme personoplysninger, og politiets behandling af biometriske data ved hjælp af ansigtsgenkendelse har særligt vidtrækkende konsekvenser. I EDPB's vejledning bemærkes vedrørende ansigtsgenkendelse, at teknologiens iboende sammenhæng med behandling af biometrisk data betyder, at der herved naturligt er en særlig risiko for indgreb i grundlæggende rettigheder.²⁰³ Behandling af biometriske data bør nyde specifik beskyttelse som følge af de "betydelige risici for grundlæggende rettigheder og frihedsrettigheder."²⁰⁴ Den blotte implementering af art. 10 giver derfor ikke tilstrækkelig hjemmel til anvendelse af ansigtsgenkendelse i sig selv. En yderligere national regulering heraf er således påkrævet, for at anvendelsen af ansigtsgenkendelse er i overensstemmelse med EU-retten,²⁰⁵ hvor der skal opstilles konkrete betingelser for at danne og behandle biometriske data. Slutteligt bemærkes, at direktivet søger at harmonisere reglerne på området, og at medlemsstaternes implementering ikke bør medføre en forringelse af den beskyttelse af personoplysninger, som bestemmelserne i direktivet indeholder. Medlemsstaterne er imidlertid ikke forhindret "i at fastsætte højere standarder end dem, der er indeholdt i dette direktiv, for beskyttelse af den registreredes rettigheder og frihedsrettigheder med hensyn til kompetente myndigheders behandling af personoplysninger."²⁰⁶

Det er således tvivlsomt, om retshåndhævelseslovens § 10, stk. 2 udgør en tilstrækkelig hjemmel til anvendelse af ansigtsgenkendelse ud over de tilfælde, der eksplicit er nævnt i både retshåndhævelsesdirektivets art. 10 og retshåndhævelseslovens § 10. Det første eksplicit nævnte tilfælde giver et behandlingsgrundlag, når politiet anvender ansigtsgenkendelse i tilfælde, hvor den registrerede er forurettet, hvor brugen af ansigtsgenkendelse kan siges at

²⁰² EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, s. 21

²⁰³ Ibid., s. 13

²⁰⁴ Retshåndhævelsesdirektivet, præambel 37

²⁰⁵ EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, s. 21

²⁰⁶ Retshåndhævelsesdirektivet, præambel 15

beskytte den registreredes vitale interesser. Et eksempel herpå kan være den digitale offergenkendelse, som politiet anvender for at identificere den forurettede. I en situation, hvor en mistænkt eller sigtet person derimod er den registrerede, vil dette behandlingsgrundlag kunne anvendes, såfremt brugen af ansigtsgenkendelse sker af hensyn til en anden fysisk persons vitale interesser. Det kan være i tilfælde, hvor der er fare for tab af menneskeliv, eksempelvis i en “man-hunt”. Det er uklart, om der skal være tale om en bestemt fysisk person, og hvad vitale interesser indebærer. Der må imidlertid være tale om, at interessen skal være af en vis styrke og betydning. Den anden situation, hvor der er grundlag for behandling af biometriske data, er, hvor den registrerede selv har offentliggjort personoplysninger. Her bemærkes, at dette ikke giver et grundlag for at danne biometriske data ud fra offentliggjorte billeder. Det skal derimod være selve den biometriske ansigtsskabelon, som er offentliggjort, såfremt dette skal være grundlag for behandling af biometrisk data.²⁰⁷

4.2.3. Delkonklusion

I ovenstående afsnit er der foretages en analyse af de EU-retlige rammer for politiets brug af ansigtsgenkendelse i efterforskningen, hvilket udgøres af retshåndhævelsesdirektivet, som er implementeret i dansk ret ved retshåndhævelsesloven. Direktivet udspringer af et behov for at imødekomme nye udfordringer for beskyttelsen af personoplysninger, som opstår i takt med en teknologisk udvikling i høj fart. Disse udfordringer består både ved, at der behandles personoplysninger i stigende grad, men også at teknologien giver nye muligheder for, hvordan personoplysningerne kan behandles og anvendes i retshåndhævende arbejde.²⁰⁸ Dette modsvarer af et behov for øget beskyttelse af personoplysninger i form af “en stærk og mere sammenhængende ramme for beskyttelse af personoplysninger i Unionen.”²⁰⁹ Det kan ud fra analysen konkluderes, at næsten al politiets behandling af personoplysninger vil være omfattet af retshåndhævelsesloven, fordi den finder anvendelse på politiets løsning af opgaver både inden for og uden for strafferetsplejen, hvor også de ordensmæssige opgaver omfattes. Flere bestemmelser i retshåndhævelsesloven er relevante for politiets anvendelse af ansigtsgenkendelse. Som nævnt tidligere forudsætter brug af ansigtsgenkendelsesteknologi, at der indsamles billede- og videomateriale. Indsamling og anden behandling af materiale vil skulle opfylde betingelserne i lovens § 9, som blot opstiller et krav om nødvendighed. Såfremt

²⁰⁷ EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, s. 21

²⁰⁸ Retshåndhævelsesdirektivet, præambel 3

²⁰⁹ Ibid., præambel 4

politiet ønsker at behandle materialet med ansigtsgenkendelsesteknologi, hvorved der dannes biometriske data, skal betingelserne i lovens § 10, stk. 2 opfyldes. En fortolkning af retshåndhævelseslovens § 10 ud fra bestemmelsens ordlyd og bemærkninger vil umiddelbart resultere i, at den registrerede er stillet dårligere end efter direktivets regler. Derfor må direktivets art. 10 tillægges betydelig vægt i fortolkningen. Ud fra en direktivkonform fortolkning kan konkluderes, at anvendelse af ansigtsgenkendelse kan ske på tre måder. Enten skal der være lovhjemmel, hvor typen af personoplysninger (biometriske data), formålet og målet med behandlingen angives klart. Lovens § 10 lever ikke op til disse krav i sig selv, og det er derfor tvivlsomt, om politiet har adgang til at anvende ansigtsgenkendelse i andre tilfælde end de eksplicit nævnte. De nævnte tilfælde indebærer anvendelse af ansigtsgenkendelse for at beskytte den registreredes eller en anden fysisk persons vitale interesser eller hvis behandlingen vedrører oplysninger, som tydeligvis er offentliggjort af den registrerede. I alle tilfælde er det en betingelse, at behandlingen skal være strengt nødvendig, og at formålet ikke kan opnås på anden og mindre indgribende vis. Betingelsen om streng nødvendighed indebærer et krav om, at behandlingen underlægges objektive kriterier for at undgå en generel og systematisk behandling af følsomme personoplysninger. Dermed udelukkes brug af ansigtsgenkendelse i realtid, som foretages generelt og systematisk uden fastsættelse af kriterier for, hvornår iværksættelse heraf er nødvendig. Sådanne kriterier kan eksempelvis være et kriminalitetskrav, hvor grovhed og karakter af lovovertrædelsen indgår i afvejningen. Derudover indebærer betingelsen om streng nødvendighed, at politiet ikke kan oprette et register til brug for sammenligning af ansigtsskabeloner, hvis dette oprettes med materiale indsamlet generelt og systematisk fra online kilder.

4.3. EMRK's rammer for politiets anvendelse af ansigtsgenkendelse

Til brug for besvarelsen af specialets problemformulering, som vedrører de retlige rammer for politiets brug af ansigtsgenkendelse, er det tillige nødvendigt at analysere rammerne herfor i EMRK. I dette afsnit foretages således en analyse af, hvilke rammer EMRK sætter for politiets anvendelse af ansigtsgenkendelse. Indledende gennemgås EMRK art. 8 om retten til respekt for privatlivet og dens anvendelsesområde, herunder hvordan dette relaterer sig til ansigtsgenkendelse. Herefter analyseres relevant praksis fra EMD vedrørende indsamling og opbevaring af materialebrug samt brug af ansigtsgenkendelse.

4.3.1. Artikel 8 – retten til respekt for privatliv

Det følger af EMRK art. 8, at "Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance.". Hvad privatliv indebærer kan ikke præcist defineres, men EMD har udtalt, at begrebet skal fortolkes bredt.²¹⁰ Der er dog krav om, at indgrebet skal være af en vis intensitet for at være omfattet.²¹¹ Retten til respekt for privatliv omfatter retten til et "privat socialt liv", hvor det enkelte individ har mulighed for at kunne udvikle sin personlighed, relationer til andre mennesker og omverdenen uden uønsket indblanding, hvilket indebærer temaer vedr. identitet og personlig integritet i bred forstand.²¹² Idet retten til at forme relationer til andre mennesker og omverdenen er omfattet, er det ikke kun privatsfæren, der nyder beskyttelse. Der er således en vis ret til at leve privat og uden uønsket opmærksomhed i et vist omfang, også i det offentlige.²¹³ Niveauet af beskyttelse og tilsvarende krav til indgreb har dog sammenhæng med, hvad man berettiget kan forvente det pågældende sted. Beskyttelsen af privatlivet er derfor større i hjemmet end i det offentlige rum,²¹⁴ og overvågning af det offentlige rum udgør som følge heraf ikke som udgangspunkt et indgreb i retten til privatliv.²¹⁵

²¹⁰ Kjølbros: Den Europæiske Menneskerettighedskonvention for praktikere (2020), 5. udgave, Jurist- og Økonomforbundets Forlag, s. 958

²¹¹ Ibid., s. 859

²¹² Ibid.

²¹³ Ibid.

²¹⁴ Rytter: Individets grundlæggende rettigheder (2021), s. 214

²¹⁵ Kjølbros: Den Europæiske Menneskerettighedskonvention for praktikere (2020), 5. udgave, Jurist- og Økonomforbundets Forlag, s. 869

Retten til respekt for privatliv er ikke en absolut rettighed, idet der kan foretages indgreb i rettigheden under visse betingelser, som fremgår af art. 8, stk. 2.²¹⁶ Ingen offentlig myndighed må herefter gøre indgreb i retten til privatliv, medmindre det sker i overensstemmelse med loven og er nødvendigt i et demokratisk samfund af hensyn til et legitimt formål. Dette indebærer 1) et krav om lovgrundlag, 2) et legitimt formål og at indgrebet er 3) nødvendigt i et demokratisk samfund. Krav om lovgrundlag er et legalitetskrav, hvorefter der i national ret skal være en hjemmel til indgrebet. Legalitetskravet er ikke formelt, hvilket vil sige, at der ikke er krav om, at hjemlen findes i loven. Det kan tillige være gennem praksis eller uskrevne retsregler, at kravet opfyldes.²¹⁷ Desuden stilles der efter denne betingelse visse kvalitative krav til hjemlen,²¹⁸ og denne skal være tilgængelig og medføre en forudsigelig retstilstand.²¹⁹ Kravet om legitimt formål indebærer, at indgrebet skal ske for at varetage et af de i art. 8, stk. 2 nævnte formål, herunder den nationale sikkerhed, offentlige tryghed eller for at forebygge uro eller forbrydelse. Kravet om nødvendighed i et demokratisk samfund indebærer, at indgrebet skal varetage et presserende socialt behov. Desuden er kravet udtryk for, at der skal foretages en generel vurdering af, om indgrebet er proportionalt med det forfulgte formål.²²⁰

4.3.1.1. Retshåndhævende myndigheders indsamling, behandling og opbevaring af fotos og biometriske data

I dette afsnit analyseres to afgørelser, som vurderes at være særligt relevante vedr. retten til privatlivets betydning for politiets indsamling og opbevaring af fotografier og biometriske data; i afgørelsen *S. og Marper mod Storbritannien* foretager EMD en vurdering af, hvorvidt indsamling og opbevaring af DNA-profiler, vævsprøver og fingeraftryk udgør et indgreb i retten til privatliv, og under hvilke betingelser dette indgreb er berettiget. I afgørelsen *Gaughran mod Storbritannien* anvender EMD disse principper på indsamling og opbevaring af fotografier og biometriske data, herunder i relation til potentielt brug af ansigtsgenkendelse. Der foretages således en samlet analyse af afgørelserne, fordi *Gaughran* bygger videre på principper fastlagt i *S. og Marper*.

²¹⁶ Kjølbros: Den Europæiske Menneskerettighedskonvention for praktikere (2020), 5. udgave, Jurist- og Økonomiforbundets Forlag, s. 837

²¹⁷ Ibid., s. 838

²¹⁸ Ibid., s. 837

²¹⁹ Ibid., s. 839

²²⁰ Ibid., s. 851

S. og Marper mod Storbritannien

I *S. og Marper* udtaler EMD sig generelt om personlige oplysninger i forhold til retten til privatliv. Indsamling og opbevaring af oplysninger er et indgreb i individets ret til privatliv, såfremt oplysningerne kan siges at vedrøre individets privatliv. Vurderingen afhænger af de konkrete omstændigheder for indsamling og opbevaring, karakteren af oplysningerne, den efterfølgende brug og behandling samt hvad denne brug eller behandling kan resultere i.²²¹ Den konkrete type af oplysninger, der indsamles, behandles og opbevares, skal således vurderes ud fra disse kriterier i forhold til, om det udgør et indgreb i retten til privatliv. I *S. og Marper* drejede sagen sig om indsamling og opbevaring af DNA-profiler, vævsprøver og fingeraftryk, som alle udgør et indgreb i art. 8 efter disse kriterier.²²² EMD udtaler sig i *S. og Marper* om vurderingen af, hvorvidt indgreb i art. 8 vedrørende personlige oplysninger er berettiget. Det bemærkes, at kravene til lovgrundlagets klarhed og præcision, det legitime formål og nødvendigheden i et demokratisk samfund skal foretages samlet, fordi kravene til indgrebets lovgrundlag og formålet afhænger af indgrebets intensitet. Der foretages derfor en samlet vurdering af proportionaliteten.²²³ Det har bl.a. indflydelse på intensiteten, at indsamlingen sker af retshåndhævende myndigheder og til dertilhørende formål, samt at oplysningerne udsættes for automatisk behandling. I denne forbindelse bemærker EMD, at et mere intenst indgreb skal modsvares af et klarere og mere præcist lovgrundlag med stærkere retssikkerhedsgarantier og kontrolmekanismer.²²⁴ I *S. og Marper* konkluderer EMD, at der er sket krænkelse af art. 8. Opbevaringen af DNA-profilerne, vævsprøverne og fingeraftrykkene var ikke proportional,²²⁵ hvilket skyldes den systematiske og generelle indsamling, som hverken stillede krav til grovhed eller karakter af lovovertrædelse. Der blev tillige lagt vægt på den tidsubestemte opbevaring, som ikke differentierede mellem sigtede, dømte og frifundne personer. Desuden havde den manglende domstolskontrol betydning for vurderingen.²²⁶ I afgørelsen slår EMD således fast, at man, for at leve op til proportionalitetskravet, skal sikre sig et klart, præcist og detaljeret lovgrundlag for indsamling og behandling af personlige oplysninger.²²⁷

²²¹ *S. and Marper mod Storbritannien* (2008), § 67

²²² Det konkluderes, at indsamlingen og opbevaringen af både DNA-profiler, vævsprøver og fingeraftryk udgjorde et indgreb i retten til privatliv. Se hertil *S. and Marper mod Storbritannien* (2008), §§ 77 og 86

²²³ *S. and Marper mod Storbritannien* (2008), § 103

²²⁴ *Ibid.*, § 103

²²⁵ *Ibid.*, § 125

²²⁶ *Ibid.*, § 119

²²⁷ *Ibid.*, § 99

Gaughran mod Storbritannien

EMD tager i *Gaughran mod Storbritannien* stilling til, om optagelse og opbevaring af fotografier udgør et indgreb i privatlivet.²²⁸ Retten til privatliv inkluderer retten til ens eget billede. Førend optagelse og opbevaring af et fotografi kan udgøre et indgreb i retten til privatliv, skal det imidlertid indeholde oplysninger vedrørende individets privatliv. Vurderingen foretages ud fra den fastlagte fremgangsmåde i *S. og Marper* som gennemgået ovenfor.²²⁹ EMD lægger i denne vurdering stor vægt på de momenter, som vedrører omstændighederne vedrørende indsamlingen, den efterfølgende brug og behandling samt hvad denne brug eller behandling kan resultere i. EMD fremhæver i denne sammenhæng to ting; for det første, at fotografiet er indsamlet af politiet og skal opbevares uden tidsbegrænsning i en database. For det andet har det betydning, om der er mulighed for, at fotografiet senere behandles med ansigtsgenkendelsesteknologi.²³⁰ I den konkrete sag kunne det ikke udelukkes, at fotografiet kunne blive uploadet i en database, hvor der var mulighed for at bruge ansigtsgenkendelse.²³¹ På grund af den manglende tidsbegrænsning og muligheden for brug af ansigtsgenkendelse konkluderer EMD, at optagelse og opbevaring af fotografier i det konkrete tilfælde udgør et indgreb i art. 8.²³² EMD vurderer herefter, om opbevaring af biometriske data og fotografier af en dømt person er berettiget.²³³ Formålene med indsamlingen og opbevaringen af fotografier er legitime, da dette sker for at opdage og forebygge kriminalitet. Indsamlingens formål er at forbinde en person til en bestemt sag, imens opbevaringen sker til brug for identifikation af overtrædere i fremtidige sager.²³⁴ EMD udtrykker tvivl om, hvorvidt lovgrundlaget var for bredt og upræcist,²³⁵ men som følge af, at kravene til lovgrundlaget skal afspejle indgrebets intensitet, sker en samlet proportionalitetsvurdering i stedet. Fremgangsmåden som er fastlagt i *S. og Marper*, hvor der sker en samlet vurdering af lovgrundlag, legitimt formål og proportionalitet, følges således i *Gaughran*.²³⁶ Det konkluderes, at en tidsbegrænsede opbevaring ikke automatisk kan medføre, at indgrebet er uproportionalt.

²²⁸ *S. and Marper mod Storbritannien* (2008), § 66

²²⁹ *Gaughran mod Storbritannien* (2020), § 66

²³⁰ *Ibid.*, § 67

²³¹ *Ibid.*, § 69

²³² *Ibid.*, § 70

²³³ *Ibid.*, § 76

²³⁴ *Ibid.*, § 75

²³⁵ *Ibid.*, § 74

²³⁶ *Ibid.*, § 73

Det betyder derimod, at indgrebet skal modsvares af stærke kontrolmekanismer og garantier, og at disse bliver afgørende for udfaldet.²³⁷ Der var ikke sådanne kontrolmekanismer til stede; indsamlingen og opbevaringen blev foretaget uden at holde karakteren og grovheden af lovovertrædelsen for øje, og uden at forholde sig til det konkrete behov for fortsat opbevaring.²³⁸ EMD konkluderer, at den vilkårlige opbevaring af biometriske data og fotografier, som kunne foretages uden krav og uden nogen sikkerhedsmekanismer, udgjorde en krænkelse af art. 8.

4.3.1.2. Ansigtsgenkendelse

EMD har taget stilling til retshåndhævende myndigheders brug af ansigtsgenkendelse i en afgørelse mod Rusland.²³⁹ Sagen drejer sig om en borgers afholdelse af en ulovlig demonstration, hvor russisk politi anvendte ansigtsgenkendelse, først til at identificere borgeren på et billede, hvor han var i færd med at demonstrere, hvilket politiet var kommet i besiddelse af fra en Telegram-kanal. Der er således tale om brug af retrospektiv ansigtsgenkendelse til identifikationsformål. Herefter lokaliserede politiet den pågældende borger ved brug af ansigtsgenkendelse i realtid.²⁴⁰ Indledende foretager EMD en vurdering af, hvorvidt brugen af ansigtsgenkendelse på den pågældende måde udgør et indgreb i retten til privatliv, jf. EMRK art. 8. EMD anfører hertil, at behandling af klagerens personlige oplysninger med ansigtsgenkendelse for både at identificere og lokalisere ham udgjorde et indgreb i klagerens ret til privatliv.²⁴¹ I denne vurdering inddrager EMD principperne fastlagt i *Gaughran mod Storbritannien* (2020), hvor indsamling og opbevaring af fotografier sammenholdt med muligheden for at anvende ansigtsgenkendelsesteknologi herpå, udgjorde et indgreb i retten til privatliv. EMD vurderer herefter, hvorvidt indgrebet har været berettiget. EMD udtaler sig først generelt om de krav, der kan stilles til et lovgrundlag, som tillader brug af ansigtsgenkendelse. Her bemærkes, at et sådant lovgrundlag bør indeholde detaljerede anvisninger vedrørende omfang og anvendelse samt indeholde stærke retssikkerhedsgarantier, som skal modvirke misbrug og en tilfældighedspræget anvendelse. Det bemærkes samtidigt, at kravet til sikkerheds- og kontrolmekanismer skærpes, for så vidt angår brug af

²³⁷ *Gaughran mod Storbritannien* (2020), § 88

²³⁸ *Ibid.*, § 94

²³⁹ *Glukhin mod Rusland* (2023)

²⁴⁰ *Ibid.*, § 68

²⁴¹ *Ibid.*, § 73

ansigtsgenkendelse i realtid, fordi dette er mere indgribende.²⁴² EMD udtaler, at der er tvivl om, hvorvidt lovgrundlaget er formuleret for bredt, fordi ansigtsgenkendelse vil kunne anvendes til bredt afgrænsede formål, alle grupper af personer og til alle typer af sager, ligesom der ikke var nogen retssikkerhedsgarantier eller kontrolmekanismer.²⁴³ Det konkluderes imidlertid ikke, om kravet om tilstrækkeligt lovgrundlag er opfyldt eller ej, fordi vurderingen af betingelserne for indgrebs berettigelse efter art. 8, stk. 2 foretages samlet. Vurderingen af lovgrundlaget og det legitime formål hænger sammen med vurderingen af, hvorvidt indgrebet var nødvendigt i et demokratisk samfund.²⁴⁴ EMD bemærker dog, at indgrebet varetager et legitimt formål i form af forebyggelse af kriminalitet.²⁴⁵ I vurderingen af indgrebs proportionalitet inddrages indgrebs intensitet.²⁴⁶ EMD anser brug af ansigtsgenkendelse til både identifikation og lokalisering af klager “særligt indgribende”, imens det gentages, at dette især gælder for brug af ansigtsgenkendelse i realtid. Det betyder, at der tilsvarende må stilles større krav til, hvornår et sådant indgreb er berettiget.²⁴⁷ ²⁴⁸ Karakteren og grovheden af den overtrædelse, der efterforskes, skal inddrages i denne afvejning,²⁴⁹ og det har også betydning, at behandlingen foretages af politiet og om behandlingen foretages automatisk.²⁵⁰ EMD konkluderer, at hverken brug af ansigtsgenkendelse retrospektivt eller i realtid var proportionalt, fordi der ikke kunne godtgøres et “presserende socialt behov” for indgrebet, og fordi det ikke var “nødvendigt i et demokratisk samfund”. Det har formentlig afgørende betydning for vurderingen, at der kun var tale om overtrædelse af en administrativ forskrift, som kunne straffes med bøde, samtidig med at der er udtrykt tvivl om lovgrundlagets klarhed og præcision.

4.3.2. Delkonklusion

²⁴² Glukhin mod Rusland (2023), § 82

²⁴³ Ibid., § 83

²⁴⁴ Ibid., § 78

²⁴⁵ Ibid., § 84

²⁴⁶ Ibid., § 86

²⁴⁷ Ibid., § 86

²⁴⁸ Her bemærkes dog, at der grundet de konkrete omstændigheder stilles endnu større krav i nærværende sag, fordi billederne af klageren afslører oplysninger om hans politiske overbevisning, hvilket er særligt følsomt.

²⁴⁹ Glukhin mod Rusland (2023), § 87

²⁵⁰ Ibid., § 75

EMRK art. 8 opstiller nogle retlige rammer for politiets brug af ansigtsgenkendelse for så vidt angår 1) retshåndhævende myndigheders indsamling og opbevaring af fotografier, som kan behandles med ansigtsgenkendelse og 2) konkret brug af ansigtsgenkendelse. I begge tilfælde er der tale om indgreb i retten til privatliv, fordi muligheden for brug eller brugen af ansigtsgenkendelse udgør et indgreb. Ved vurderingen af indgrebets berettigelse vil kravene til lovgrundlaget, det legitime formål og nødvendigheden i et demokratisk samfund blive inddraget i en samlet proportionalitetsvurdering. Årsagen hertil er, at indgrebets intensitet sætter højere krav til lovgrundlagets klarhed og præcision samt nødvendigheden. Det kan således konkluderes, at indsamling og opbevaring af fotografier, der kan blive brugt til ansigtsgenkendelse, udgør et indgreb i EMRK art. 8. Lovgrundlaget, som muliggør opbevaring af fotografierne, skal opstille krav som retfærdiggør, at opbevaringen er relevant og nødvendig. Der skal endvidere tages højde for kontrolmekanismer. Jo bredere grundlag, der er for indsamling og opbevaring, des større krav stilles der til kontrolmekanismerne, hvilket sikrer, at indgrebet er proportionalt. Det er interessant, at EMD i vurderingen ikke kun forholder sig til selve indsamlingen og opbevaringen af fotografierne, men tilsvarende hvordan en eventuel behandling, herunder brug af ansigtsgenkendelse, kan have betydning for indgrebets intensitet. EMD foretager således en samlet vurdering af alle omstændigheder, som kan have betydning for individets ret til privatliv, hvor indsamlingen og opbevaringen ikke kan adskilles fra den efterfølgende brug. Vedrørende anvendelse af ansigtsgenkendelse kan det konkluderes, at dette udgør et indgreb i retten til privatliv. Indgrebets intensitet afhænger bl.a. af, om ansigtsgenkendelsen er retrospektiv eller i realtid, men også af mængden af personer, hvis oplysninger behandles og hvorvidt behandlingen sker automatisk som ved realtidsansigtsgenkendelse. Desuden har det betydning, at indgrebet foretages af politiet. Samlet set stilles der krav om præcision og klarhed i lovgrundlaget, som tillige skal indeholde stærke processuelle garantier mod misbrug mm. I vurderingen af, hvorvidt brug af ansigtsgenkendelse er proportionalt, foretages en afvejning mellem indgrebets intensitet samt karakteren og grovheden af den lovovertrædelse, der efterforskes. EMD bemærker, at teknologiens muligheder for udnyttelse af oplysninger, eksempelvis ved ansigtsgenkendelse, nødvendiggør stærke retssikkerhedsgarantier, såfremt retten til privatliv ikke skal udhules. En teknologi som ansigtsgenkendelse bør således ikke anvendes uden krav hertil og uden at foretage en afvejning mellem dets indgribende karakter og retten til privatliv generelt.²⁵¹

²⁵¹ Glukhin mod Rusland (2023), § 75

KAPITEL 4

KONKLUSION: Konklusion på den retsdogmatiske analyse

4.4. Konklusion

Nærværende speciale har haft til formål at afklare, hvad de retlige rammer er for politiets brug af ansigtsgenkendelse i efterforskningen. Problemformuleringen er besvaret ved en retsdogmatisk analyse af relevant regulering i national ret, herunder retsplejeloven og politiloven, EU-retten og EMRK, som regulerer ansigtsgenkendelse på varierende måde og i varierende grad. Analysen af de retlige rammer for ansigtsgenkendelse er foretaget med udgangspunkt i et bredt perspektiv, idet der både inddrages regulering af dataindsamling, databehandling og muligheden for at foretage sammenligning i en database. Vedrørende reguleringen af dataindsamling kan det ud fra analysen konkluderes, at der i national ret er der forskellige muligheder for, at politiet kan indsamle fotografier og videoovervågning. Der er stor variation i kravene til at foretage disse indgreb og de processuelle garantier forbundet hermed – eksempelvis er politiets overvågning af offentligt tilgængelige steder stort set ureguleret, imens der er høje krav til politiets overtagelse af privates TV-overvågning samt stærke processuelle garantier forbundet hermed. I EU-retten stilles krav om, at indsamling af materiale er nødvendigt, og samme krav stilles for at politiet kan indsamle offentligt tilgængeligt materiale efter politiloven. Endvidere viser analysen af EMRK art. 8, at indsamling af fotografier, hvorpå der senere kan anvendes ansigtsgenkendelse udgør et indgreb i retten til privatliv og skal derfor opfylde kravene i art. 8, stk. 2 vedrørende et klart og præcist lovgrundlag, legitimt formål og nødvendighed i et demokratisk samfund. Det kan konkluderes, at der er stor variation i kravene til at foretage disse indgreb og de processuelle garantier forbundet hermed – i visse tilfælde er dataindsamling stort set ureguleret, imens der i andre tilfælde er høje krav og stærke processuelle garantier forbundet hermed, selvom retshåndhævelsesloven stiller et underliggende krav om nødvendighed ved al dataindsamling. De retlige rammer for dataindsamling til brug for ansigtsgenkendelse ender derfor med at resultere i en vilkårlig retstilstand, hvor det er tilfældigt, om det pågældende materiale er indsamlet ud fra høje krav og retssikkerhedsgarantier, eller om materialet kan indsamles uden at leve op til nogen krav. Samlet set afspejler de retlige rammer for dataindsamling, at det primært er hensynet til, hvor indgribende selve indsamlingen er for individet, frem for hvad det indsamlede materiale kan bruges til. Det er uhensigtsmæssigt, at det bliver vilkårligt, om der stilles høje eller ingen krav dataindsamlingen til brug for ansigtsgenkendelse.

Selve brugen af ansigtsgenkendelsesteknologien på det indsamlede materiale kaldes i dette speciale 'databehandling'. Det kan konkluderes ud fra den retsdogmatiske analyse, at national ret i mindre grad regulerer dette. Retsplejelovens regler om teleobservation kan efter sin ordlyd

og forarbejder omfatte brugen af ansigtsgenkendelse, hvis formålet hermed er at følge en bestemt persons færden. Bestemmelsen vurderes imidlertid at være af mindre betydning som retlige ramme for brug af ansigtsgenkendelse. Selvom ordlyden og formålet kan rumme brugen af ansigtsgenkendelse, er dette ikke en del af bestemmelsens kerneformål. Den vurderes derfor ikke at blive tillagt betydning i praksis. Hvad angår EU-regulering viser analysen, at selve brugen af ansigtsgenkendelse reguleres af retshåndhævelsesloven, fordi den medfører dannelse af biometriske data. Retshåndhævelseslovens rammer for brug af ansigtsgenkendelse er uklare. Dette skyldes både den måde, loven implementerer direktivet, fordi der er en række uoverensstemmelser herimellem. Det skyldes også den brede ordlyd, idet bestemmelsen regulerer al behandling af følsomme personoplysninger. Ud fra analysen kan det konkluderes, at implementeringen medfører tvivl om, hvorvidt der i retshåndhævelsesloven er selvstændig hjemmel til at gøre brug af ansigtsgenkendelse. Det er tvivlsomt, om ansigtsgenkendelse vil kunne anvendes for at forfølge andre formål end dem, der udtrykkeligt er nævnt i bestemmelsen. Disse formål omfatter 1) hvis det sker af hensyn til den registrerede eller en anden fysisk persons vitale interesser eller 2) hvis materialet er offentliggjort af den registrerede selv. Det kan dog konkluderes, at retshåndhævelsesloven stiller krav om, at behandling af biometriske data kun sker, hvis det er strengt nødvendigt. Kriteriet efterlader et minimalt skøn og et krav om, at behandling af følsomme oplysninger underlægges objektive kriterier. Det kan eksempelvis være betingelser om karakteren og grovheden af kriminaliteten, og at dette skal være proportionalt med anvendelsen af den bestemte type af ansigtsgenkendelse. Kravet om streng nødvendighed er i praksis uforeneligt med generelt og systematisk brug af ansigtsgenkendelse i realtid, hvis der ikke opstilles konkrete betingelser for iværksættelsen. Vurderingen af kriteriet ligner proportionalitetsafvejningen efter EMRK art. 8. Efter denne er der krav om, at lovgrundlaget, som brugen af ansigtsgenkendelse sker på baggrund af, skal være klart og præcist, hvilket indebærer, at der bør opstilles klare retningslinjer for anvendelsen, herunder stærke processuelle garantier. Kravene til lovgrundlagets klarhed og præcision afhænger af, hvor indgribende den anvendte type af ansigtsgenkendelse er – der stilles eksempelvis højere krav til brug af ansigtsgenkendelse i realtid end til retrospektiv ansigtsgenkendelse. Lovgrundlaget skal uanset typen af ansigtsgenkendelse afspejle en afvejning af indgrebets intensitet og nødvendighed. En sådan afvejning kan ske ved, at der tages højde for kriminalitetens grovhed og karakter, men også at der altid bør opstilles klare retningslinjer for anvendelsen, herunder stærke processuelle garantier. Hvad angår de retlige rammer for opbevaring af personfotografier, herunder til brug for databaser, kan det konkluderes, at dette er reguleret af både national ret, EU-retten og

EMRK art. 8. I retsplejeloven opstilles betingelser for opbevaring af personfotografier, bl.a. at det kun kan ske, hvis den pågældende er sigtet eller dømt. Efter EMRK art. 8 er der ved en sådan opbevaring tale om et indgreb i retten til privatliv, og det spiller en rolle i denne vurdering, at der kan blive anvendt ansigtsgenkendelse på billederne. Opbevaring af personfotografier er desuden reguleret af retshåndhævelsesloven og skal være nødvendigt, imens opbevaring af biometriske data skal opfylde kravene for behandling af følsomme personoplysninger. Det må herudover formodes, at politilovens hjemmel til at foretage tværgående informationsanalyser grundet sin brede ordlyd kan hjemle en mulighed for at foretage sammenligning mellem indsamlet materiale og et opbygget register med fotografier eller biometriske data. Politiloven giver desuden mulighed for at indsamle materiale fra online kilder, men dette materiale må ikke generelt og systematisk uden krav hertil anvendes til opbygning af et register, der skal anvendes til ansigtsgenkendelsesformål (såkaldt 'scraping'), fordi det vil være uforeneligt med kravet om streng nødvendighed ved behandling af biometriske data i retshåndhævelsesloven. Slutteligt bemærkes, at sammenligning også er en form for databehandling, hvorfor de ovennævnte rammer for databehandlingen også gælder for sammenligning. Det kan samlet set konkluderes, at rammerne for politiets brug af ansigtsgenkendelse i bred forstand er fragmenterede. Selvom der findes visse retlige rammer, er disse ikke udarbejdet specifikt med henblik på at regulere brugen af ansigtsgenkendelse. Det kan derfor konkluderes, at der på dette område er et vist tomrum og uklarhed i retstilstanden.

KAPITEL 5

**DISKUSSION: Diskussion af de retlige rammer for ansigtsgenkendelse samt
retspolitiske overvejelser vedr. reguleringen**

5. Diskussion af de retlige rammer for ansigtsgenkendelse

Problemformuleringen i nærværende speciale vedrører en analyse af de retlige rammer for politiets brug af ansigtsgenkendelse i forbindelse med efterforskningen. Denne første del af problemformuleringen er besvaret i konklusionen ovenfor. I dette afsnit behandles anden del af specialets problemformulering, som omhandler hvorvidt de retlige rammer giver anledning til retspolitiske overvejelser. Indledningsvist diskuteres det ud fra et retsdogmatisk perspektiv, hvorfor rammerne er udformet, som de er, og om de retlige rammer udgør en hensigtsmæssig og tilstrækkelig regulering af politiets anvendelse af ansigtsgenkendelse. Slutteligt følger nogle retspolitiske forslag til, hvordan reguleringen af brugen af ansigtsgenkendelse i stedet kunne gribes an.

5.1. Årsagen til udformningen af de retlige rammer

Som gennemgået i afsnittet ovenfor er de retlige rammer på området for politiets anvendelse af ansigtsgenkendelse usammenhængende og uklar. Reguleringen af de retlige rammer kommer fra både national ret, EU-retten og EMRK. I dette afsnit diskuteres årsagerne bag udformningen af de retlige rammer. Indledningsvist diskuteres systematikken for reguleringen af politiets efterforskningsvirksomhed generelt og hvordan dette har betydning for udformningen af de retlige rammer for ansigtsgenkendelse i national ret. Efterfølgende behandles reguleringen af retshåndhævende myndigheders behandling af personoplysninger, og til sidst inddrages EMRK.

5.1.1. Regulering af politiets efterforskningsmidler

I dette afsnit diskuteres den generelle tilgang til regulering af politiets efterforskningsmidler. Som tidligere nævnt er udgangspunktet for reguleringen af politiets efterforskningsmidler, at politiets efterforskning enten 1) ikke kræver hjemmel eller 2) at efterforskningsmidlerne reguleres som straffeprocessuelle tvangsindgreb. Politiets brug af ansigtsgenkendelse er ikke reguleret som et straffeprocessuelt tvangsindgreb, og årsagen hertil diskuteres i dette afsnit. Da politiets efterforskningsmidler som hovedregel kun reguleres, når der er tale om et straffeprocessuelt tvangsindgreb, er det nødvendigt først at fastlægge definitionen heraf. Reguleringen af de straffeprocessuelle tvangsindgreb i retsplejeloven bygger i hovedsagen²⁵²

²⁵² Se eksempelvis Bet. 1023/1984 – Politiets indgreb i meddelelseshemmeligheden og anvendelse af agenter, s. 12, hvor man tilslutter sig Hans Gammeltoft-Hansens definition

på Hans Gammeltoft-Hansens definition.²⁵³ Behovet for en sondring mellem almindelige efterforskningsskridt og straffeprocessuelle tvangsindgreb begrundes ud fra legalitetsprincippet. Tvangsindgrebene griber ind i ellers beskyttede goder, og indgrebets karakter og intensitet nødvendiggør derfor et særligt klart hjemmelsgrundlag. Hjemmelsgrundlaget er en forudsætning for, at politiet overhovedet kan foretage indgrebet. Andre efterforskningsmidler, der ikke karakteriseres som straffeprocessuelle tvangsindgreb, kan også lovreguleres, men dette vil i så fald være med formål om at begrænse anvendelsen – ikke for at tillade efterforskningsmidlet.²⁵⁴ Indgrebenes karakter, hvorefter de gør indgreb i grundlæggende frihedsrettigheder, og deres intensitet, hvormed de gør indgreb i disse, modsvarer af lovfæstede krav til anvendelsen af dem. Det lovfæstede krav indebærer et mistanke-, indikations- og kriminalitetskrav, hvilket sikrer, at der opfyldes en række betingelser, før politiet har adgang til at foretage indgrebene. Det varierer indgrebene imellem, om kompetencen til at afgøre, hvorvidt betingelserne er opfyldt, ligger hos politiet selv eller hos retten. Fordelen ved at regulere et efterforskningsmiddel som et straffeprocessuelt tvangsindgreb er således, at et klart og præcist lovgrundlag samt processuelle garantier sikres. Et straffeprocessuelt tvangsindgreb defineres som “en foranstaltning, der efter sit almindelige formål udføres som led i en strafforfølgning, og hvorved der realiseres en strafbar gerningsbeskrivelse rettet mod legeme, frihed, fred, ære eller privat ejendom.”²⁵⁵ Særligt betingelsen, som stiller krav om realisering af en strafbar gerningsbeskrivelse, er interessant. Rationalet bag dette kriterium er, at det er realiseringen af en strafbar gerningsbeskrivelse, som i første omgang begrunder behovet for en hjemmel. De straffeprocessuelle tvangsindgreb har således den funktion, at politiet har mulighed for at foretage efterforskningsskridt, som ellers ville være ulovlige.²⁵⁶ Det fremhæves, at netop denne sondring er afgørende for sondringen mellem almindelige efterforskningsmidler og straffeprocessuelle tvangsindgreb. Heri ligger en iboende antagelse om, at kriminalisering af en adfærd i straffeloven afspejler samfundets opfattelse af, at beskyttelse mod en sådan adfærd er særligt påkrævet. På denne måde bliver retsplejelovens regulering af straffeprocessuelle tvangsindgreb en afspejling af straffelovens bestemmelser og beskyttelseshensyn. Den sidste betingelse vedrører, at “den krænkede

²⁵³ Se hertil Hans Gammeltoft-Hansen: *Straffeprocessuelle tvangsindgreb – retspolitiske studier* (1981) (Juristforbundets forlag) og Hans Gammeltoft-Hansen i U.1979B.1 (Om afgrænsningen af straffeprocessuelle tvangsindgreb)

²⁵⁴ U.1979B.1, s. 2

²⁵⁵ *Ibid.*, s. 8

²⁵⁶ *Ibid.*, s. 5

beskyttelsesinteresse skal være af personlig karakter.”²⁵⁷ Nærmere bestemt skal der ske en krænkelse af “legeme, frihed, fred, ære eller privat ejendom”. Denne opstilling afspejler grundlovens frihedsrettigheder, samt de grundlæggende beskyttelseshensyn i straffeloven.²⁵⁸

Spørgsmålet er herefter, om ansigtsgenkendelse er et straffeprocessuelt tvangsindgreb. Det kan lægges til grund, at politiets brug af ansigtsgenkendelse i en efterforskning vil være en foranstaltning, som efter sit almindelige formål udføres som led i en strafforfølgning. Spørgsmålet er dog, hvorvidt brug af ansigtsgenkendelse realiserer en strafbar gerningsbeskrivelse. Betingelsen om realisering af en strafbar gerningsbeskrivelse kræver, at brugen af ansigtsgenkendelse er kriminaliseret i straffeloven, hvilket ikke er tilfældet. Det kan formentligt forklares ud fra, at den almindelige borger ikke har adgang til brug af denne teknologi, hvorfor der ikke er et behov for kriminalisering. Som følge af, at politiet som myndighed ved brug af ansigtsgenkendelse kan gøre indgreb i borgerens liv på et helt andet niveau i forhold til, hvad en almindelig borger kan, vil der ikke være det samme behov for beskyttelse mod borgeres brug af ansigtsgenkendelse og mod politiets brug heraf. Det er således problematisk blot at læne sig op ad straffelovens beskyttelseshensyn, fordi formålet hermed er beskyttelse af borgerne mod uønsket adfærd fra andre borgere, og ikke ud fra overvejelser om, at tilsvarende adfærd fra politiet kræver en særlig hjemmel i retsplejeloven.²⁵⁹ Gammeltoft-Hansen medgiver, at visse indgreb må undtages fra betingelsen som følge af “det ganske specielle forhold, at indgrebet [...] overhovedet ikke kan foretages af private, men kun af det offentlige.”²⁶⁰ Det kan konkluderes, at politiets brug af ansigtsgenkendelse ikke lever op til betingelserne i definitionen af straffeprocessuelle tvangsindgreb, hvorfor der som udgangspunkt ikke er krav om hjemmel, før politiet kan anvende teknologien. Af denne årsag er ansigtsgenkendelse ikke er reguleret som straffeprocessuelt tvangsindgreb i retsplejeloven.

²⁵⁷ U.1979B.1, s. 8

²⁵⁸ Hans Gammeltoft-Hansen: *Straffeprocessuelle tvangsindgreb – retspolitiske studier* (1981) (Juristforbundets forlag), s. 73-74

²⁵⁹ Se hertil Gorm Toftegaard Nielsen: *Hvad er et tvangsindgreb?* (2005), s. 159. Definitionens hensigtsmæssighed kritiseres, idet den omstændighed, at forholdet ikke er kriminaliseret i straffeloven, ikke skyldes, at “indgrebet ikke er meget intensivt, men at der ikke har vist sig noget behov for at kriminalisere, at borgerne bruger denne metode”.

²⁶⁰ U.1979B.1, s. 14-15

5.1.2. International regulering

Man har fra EU-regi gjort en stor indsats for at imødekomme behovet for regulering af den teknologiske udvikling på området for retshåndhævende myndigheders behandling af personoplysninger, herunder brug af kunstig intelligens og ansigtsgenkendelse. Spørgsmålet er, hvorfor EU-reguleringen ikke opfylder behovet for en ensartet og detaljeret regulering. Årsagen skal formentligt findes i forbeholdet vedrørende indre og retlige anliggender, som betyder, at man i praksis ikke omfattes af EU-regulering på området for retshåndhævende myndigheder. EU-retten, som søger at imødekomme behovet for regulering af nye teknologiske muligheder, vil derfor kun påvirke den nationale regulering i de tilfælde, hvor det aktivt tilvælges. Retshåndhævelsesloven er et eksempel herpå. Loven er meget bredt formuleret, samtidigt med at der kan rejses tvivl om, hvorvidt direktivet implementeres korrekt. Det skinner desuden igennem, at implementeringen har baggrund i, at dette skete for at opfylde kravene for deltagelse i det europæiske politisamarbejde – ikke ud fra en betragtning om, at der var behov for klar, detaljeret og gennearbejdet lovgivning på området. Implementeringen formår således ikke at bidrage med en samlet og klar regulering på området. Desuden opstilles der efter EMRK art. 8 visse betingelser for, at anvendelse af ansigtsgenkendelse ikke er konventionsstridig. Såfremt disse betingelser skal få betydning for den konkrete regulering på nationalt niveau, forudsætter dette aktivitet fra lovgivers side,²⁶¹ hvilket der ikke umiddelbart er udsigt til.²⁶² Der er således flere omstændigheder som medfører, at reguleringen på området er fragmenteret og upræcis.

5.2. Vurdering af reguleringen

I dette afsnit diskuteres, om de retlige rammer imødekommer det behov, der er til regulering af politiets brug af ansigtsgenkendelse. I denne vurdering af behovet inddrages forskellige betragtninger, herunder politiets nuværende anvendelse af ansigtsgenkendelse, overvejelser ud fra et menneskeretligt perspektiv og omstændigheder vedrørende ansigtsgenkendelse som teknologi.

²⁶¹ Der henvises til afsnit 2.4.2.3. *EMRK* i metodeafsnittet

²⁶² Der henvises indledningen samt til afsnit 5.2.1. *Nuværende brug af ansigtsgenkendelse i praksis*

5.2.1. Nuværende brug af ansigtsgenkendelse i praksis

Behovet for regulering på området må ses i sammenhæng med, hvordan ansigtsgenkendelse på nuværende tidspunkt anvendes af retshåndhævende myndigheder. Politiet fik første gang mulighed for at anvende ansigtsgenkendelse i et vist omfang i forbindelse med en digital tryghedspakke fra september 2022.²⁶³ Her blev et forsøg med digital offergenkendelse iværksat, hvilket indebar anvendelse af ansigtsgenkendelsesteknologi som hjælpeværktøj til identifikation af ofre i sager om seksuelt misbrug, og erfaringerne med denne brug af ansigtsgenkendelse blev fulgt tæt.²⁶⁴ Redskabet blev senere implementeret som et permanent redskab, da anvendelsen vil “kunne medføre et markant kvalitetsløft i arbejdet med at identificere ofre [...] og øge muligheden for opklaring af sager.”²⁶⁵ Brugen af ansigtsgenkendelse til digital offergenkendelse falder imidlertid uden for afgrænsningen i dette speciale, da det ikke anvendes på en mistænkt. Dog medførte denne brug af ansigtsgenkendelse, at Rigspolitiet overvejede, om teknologien tillige kunne implementeres på andre områder i efterforskningen – særligt på områder, som kræver gennemgang af store mængder billede- og lydmateriale, hvor en indledende screening af materialet vil kunne spare personaleressourcer og tid i efterforskningen. I en skrivelse til Folketinget den 5. september 2024 kunne justitsministeren orientere Folketinget om, at man på forsøgsbasis ville give Københavns Politis mulighed for at anvende “en digital løsning, der ved brug af objekt- og mønstergenkendelsesteknologi, herunder ansigtsgenkendelsesteknologi kan gennemgå og analysere store mængder af indsamlet materiale.”²⁶⁶ Ifølge rigspolitichef Thorkild Fogde ønskede politiet at anvende ansigtsgenkendelse til automatisering af gennemgang af videomateriale frem for at gøre dette manuelt ved brug af “store mængder personaleressourcer”.²⁶⁷ Det drejede sig nærmere bestemt om metoden ‘crunching’, også kaldet retrospektiv ansigtsgenkendelse, hvilket indebærer behandling af en videooptagelse med kunstig intelligens for at “finde ansigter, der kan være interessante for politiet.”²⁶⁸ Der er således ikke mulighed for at anvende ansigtsgenkendelse i realtid. Justitsministeren vil

²⁶³ Justitsministeriet: Digital tryghedspakke - Ni initiativer der skal gøre det tryggere at færdes på nettet (13. september 2022)

²⁶⁴ Folketingets udvalg for Digitalisering og IT's spørgsmål nr. 101 stillet den 6/2 2024, besvaret af justitsministeren den 4/3 2024.

²⁶⁵ Justitsministeriets orientering til Retsudvalget af 21. juni 2024

²⁶⁶ Justitsministeriets orientering til Retsudvalget, 5. september 2024

²⁶⁷ Rigspolitichef vil bruge "crunching" mod svenske lejermordere, Sebastian Juel Ebling (12. august 2024)

²⁶⁸ Ibid.

imidlertid ikke udelukke, at der på et tidspunkt bliver mulighed herfor.²⁶⁹ Ifølge Justitsministeriet udgør databeskyttelsesforordningen, databeskyttelsesloven samt retshåndhævelsesloven de retlige rammer for anvendelse af ansigtsgenkendelse,²⁷⁰ hvilket til dels er overensstemmende med resultatet af den retsdogmatiske analyse i nærværende speciale. Det er imidlertid Justitsministeriets opfattelse, at rammerne er tilstrækkelige, og at Folketinget vil blive inddraget ved behov for ændring af den retlige ramme, hvilket ikke er opstået endnu.²⁷¹ Man har begrænset brugen af ansigtsgenkendelse til efterforskning af sager om alvorlig personfarlig kriminalitet som f.eks. drab, grov vold, voldtægt og lignende overtrædelser, i sager af betydning for statens sikkerhed, dvs. terrorsager og lignende, og i operative situationer med en “manhunt”. Det er positivt, at der opstilles nogle betingelser for brug af ansigtsgenkendelse, men særligt to omstændigheder gør, at de retlige rammer i kombination med de nævnte krav ikke er tilstrækkelige. For det første er der en lav grad af forudsigelighed for borgeren, fordi der ikke lovgives om adgangen til brugen af ansigtsgenkendelse, hvorved reguleringen bliver utilgængelig og uigennemskuelig. For det andet er der ikke mulighed for nogen egentlig kontrol af, om de yderligere opstillede betingelser om personfarlig kriminalitet efterleves i praksis. Den omstændighed, at politiet er blevet pålagt kun at anvende ansigtsgenkendelse retrospektivt i tilfælde, hvor der er tale om grov personfarlig kriminalitet, medfører således ikke, at behovet for regulering på området er imødekommet.

5.2.2. Menneskeretlige overvejelser

Justitsministeriet har tidligere været af en anden opfattelse vedrørende behovet for tilstrækkeligheden af de retlige rammer, såfremt brug af ansigtsgenkendelse skulle tillades. I 2019 udviser daværende justitsminister Nick Hækkerup forståelse for politiets interesse i brug af ansigtsgenkendelse i efterforskningen. Der gives imidlertid samtidigt udtryk for, at tilbageholdenheden med at give grønt lys til politiets brug af ansigtsgenkendelse baserer sig på en række overvejelser om “nogle principielle retlige og praktiske dilemmaer, som vi ikke må se bort fra.”²⁷² Han bemærker, at debatten om ansigtsgenkendelse rejser principielle spørgsmål vedrørende retten til privatliv og fremhæver i denne sammenhæng, at “politiets anvendelse af

²⁶⁹ Justitsministeren »er åben overfor at diskutere« ansigtsgenkendelse i realtid, Philip Sune Dam (6. december 2024)

²⁷⁰ Retsudvalgets spørgsmål nr. 1344 stillet den 13/8 2024, besvaret af justitsministeren den 8/11 2024.

²⁷¹ Pressemeddelelse, Justitsministeriet: “Politiet får grønt lys til ansigtsgenkendelse”, 5. september 2024

²⁷² Københavns Politi: Vi vil gerne bruge ansigtsgenkendelse på borgerne (23. oktober 2019); Jens Beck Nielsen

ansigtsgenkendelsesteknologi [må, red.] overholde nogle strenge retlige krav.”²⁷³ Her henvises bl.a. til internationale forpligtelser. Desuden inddrages forholdet til de databeskyttelsesretlige regler samt risikoen for fejl og misbrug som skal kunne imødegås. Ministeren bemærker senere i et svar til Retsudvalget, at de nævnte principielle spørgsmål må afklares, før teknologien kan tages i brug.²⁷⁴ De internationale forpligtelser, som tidligere Justitsminister Nick Hækkerup henviser til, er bl.a. EMRK. Ud fra analysen af EMRK’s rammer for politiets brug af ansigtsgenkendelse kan det udledes, at politiets brug heraf udgør et intensivt indgreb, hvilket både skyldes det faktum, at ansigtsgenkendelse vil udgøre et indgreb i retten til privatliv, men også at politiets brug heraf kan risikere at have konsekvenser for borgernes udøvelse af andre rettigheder, herunder forsamlings- og ytringsfriheden. Teknologiens iboende sammenhæng med behandling af biometriske data betyder, at det naturligt medfører betydelige risici for grundlæggende rettigheder og frihedsrettigheder.²⁷⁵ I denne forbindelse kan eksempelvis nævnes, at politiets mulighed efter PL § 2 a til at indsamle offentligt tilgængeligt materiale samt at foretage tværgående informationsanalyser betyder, at ansigtsgenkendelsen og en eventuel efterfølgende identificering kan blive meget indgribende. Konsekvenserne ved brug af ansigtsgenkendelse kan være vidtrækkende, og det betyder, at der er krav om klar og præcis lovregulering, som skal være udtryk for en afvejning mellem formålet og nødvendigheden. Brug af ansigtsgenkendelse griber således i høj grad ind i grundlæggende rettigheder, og det bør reguleres tilsvarende grundigt.

5.2.3. Straffeprocessuelle overvejelser

I national ret vurderes behovet for regulering af politiets efterforskningsmidler ud fra, om efterforskningsmidlet kan siges at være et straffeprocessuelt tvangsindgreb, fordi disse anses som særligt indgribende. Såfremt et efterforskningsmiddel er et straffeprocessuelt tvangsindgreb, følger der et krav om klar lovregulering ud fra en betragtning om, at der er behov herfor. I dette afsnit diskuteres, om den omstændighed, at ansigtsgenkendelse ikke er et straffeprocessuelt indgreb, er ensbetydende med, at ansigtsgenkendelse ikke *bør* reguleres som sådan.

²⁷³ Se 1. behandling den 21/01/2020 af beslutningsforslag B 46 (Forslag til folketingsbeslutning om at forbyde offentlige myndigheders anvendelse af ansigtsgenkendelsesteknologi i det offentlige rum) på <https://www.ft.dk/samling/20191/beslutningsforslag/B46/BEH1-50/forhandling.htm>

²⁷⁴ Retsudvalgets spørgsmål 1 til forslag til folketingsbeslutning nr. B 46 stillet den 22/1 2020, besvaret af justitsministeren den 18/2 2020.

²⁷⁵ EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, s. 29

Den teknologiske udvikling

Indsamling af spor, undersøgelser og tekniske analyser anses som et almindeligt efterforskningskridt og derfor ikke et straffeprocessuelt indgreb. Det begrundes med, at det sædvanligvis ikke er strafbart at foretage en sådan indsamling, undersøgelse og analyse for øjeblikket hvor “det måtte svare til en privatfredskrænkelse, men heller ikke før.”²⁷⁶ Definitionen betyder således i praksis, at den generelle regulering af politiets indsamling og behandling af personoplysninger ikke kræver en lovhjemmel og derfor kun er reguleret af almindelige forvaltningsretlige grundsætninger. Gammeltoft-Hansens opfattelse bærer præg af sin tid, da der siden er sket en stor udvikling inden for området for personoplysninger og databeskyttelse. Området har i høj grad bevæget sig i retning af, at indsamling og behandling af personoplysninger kan udgøre et intensivt indgreb i grundlæggende rettigheder, hvilket ikke i samme grad var tilfældet på Gammeltoft-Hansens tid, hvilket bl.a. skyldes den teknologiske udvikling. Gammeltoft-Hansen erkender da også, at tvangsindgrebenes område er “stort, varieret og temmelig uoverskueligt”,²⁷⁷ hvilket bl.a. skyldes, at “Den hastige udvikling inden for såvel den almindelige teknologi som den i snævrere forstand kriminaltekniske formåen har frembragt en broget forå af mulige foranstaltninger, indgreb og andre tiltag.”²⁷⁸ Selvom der i retsplejeloven er opstillet et udtømmende katalog over de straffeprocessuelle tvangsindgreb, medgives at “der med tiden, navnlig i kraft af den teknologiske udvikling, kan forekomme nye efterforskningskridt, som ligeledes vil være omfattet af begrebet.”²⁷⁹ Vurderingen af, hvorvidt brugen af ansigtsgenkendelse er tilstrækkeligt indgribende til at skulle reguleres som straffeprocessuelt tvangsindgreb må derfor inddrage den teknologiske udvikling, og hvad denne i praksis betyder for intensiteten af at anvende efterforskningsmidlet.

Definitionen i praksis

I reguleringen af de straffeprocessuelle tvangsindgreb i retsplejeloven har man som udgangspunkt fulgt definitionen af hvilke efterforskningsmidler, der kræver særlig hjemmel. Der er imidlertid eksempler på, at nogle efterforskningsmidler reguleres i retsplejeloven sammen med de straffeprocessuelle tvangsindgreb, selvom de i mere eller mindre grad ikke lever op til definitionen. Et eksempel herpå er en diskussion i betænkningen vedrørende

²⁷⁶ U.1979B.1, s. 5

²⁷⁷ Ibid., s. 3

²⁷⁸ Ibid., s. 3

²⁷⁹ Bet. 1298/1995 om fotoforevisning mm., s. 18

reguleringen af politiets observation på ikke frit tilgængelige steder.²⁸⁰ Strafferetsplejeudvalget var af den opfattelse, at indgrebet bør være reguleret i retsplejeloven på trods af, at det er tvivlsomt, om det udgør et straffeprocessuelt indgreb.²⁸¹ Et andet eksempel på at definitionen ikke er afgørende for, om et indgreb bør reguleres, findes i Strafferetsplejeudvalgets overvejelser vedrørende en mulig regulering af politiets overvågning på frit tilgængelige steder.²⁸² Her foretages en konkret hensynsafvejning af behov, hensigtsmæssighed og beskyttelse af borgernes grundlæggende frihedsrettigheder. I lovbemærkningerne vedrørende indførelsen af politiets mulighed for at overtage privates TV-overvågning indgår der på samme vis ingen overvejelser, om indgrebet lever op til definitionen af straffeprocessuelle tvangsindgreb. Derimod lægges der vægt på, at reguleringen udspringer af, at politiet havde givet udtryk for et ønske herom, og at man ville sikre muligheden herfor.²⁸³ Den omstændighed, at et givet efterforskningsmiddel ikke lever op til definitionen af et straffeprocessuelt tvangsindgreb, kan derfor ikke medføre den modsætningsslutning, at der derfor ikke er behov for at regulere et efterforskningsmiddel i retsplejeloven. Valget bør i stedet afgøres ud fra en konkret afvejning, hvor indgrebets intensitet og indgriben i grundlæggende rettigheder bør tillægges afgørende vægt.

Spørgsmålet er dog, om de straffeprocessuelle tvangsindgreb, som regulerer politiets indsamling af fotografier og videomateriale, i tilstrækkelig grad imødekommer behovet for regulering på området. Der er imidlertid store variationer i kravene til at foretage disse indgreb, fordi hensynene bag reguleringen ikke tager højde for, hvad det indsamlede materiale efterfølgende kan anvendes til – kun hvorvidt selve indsamlingen udgør et beskyttelsesværdigt indgreb. Det er værd at overveje, om det er hensigtsmæssigt, at der er meget forskellige krav til indsamlingen af materialet alt efter situationen, når det i sidste ende kan bruges til det samme formål. Reguleringen heraf kan siges at være tilstrækkelig for at beskytte individets interesser ved indsamlingen, men ikke ved at materialet senere kan behandles af ansigtsgenkendelse. Den nuværende regulering af straffeprocessuelle tvangsindgreb, som har relevans for brug af

²⁸⁰ Der henvises til Bet. 1298/1995 om fotoforevisning, konfrontation, efterlysning og observation, s. 14 for diskussionen om, hvorvidt observation på ikke frit tilgængelige steder overhovedet realiserer en strafbar gerningsbeskrivelse, fordi straffelovens § 264 a kun kriminaliserer uberettiget adfærd. Retshåndhævende formål er her fremhævet som berettiget.

²⁸¹ Bet. 1298/1995 om fotoforevisning, konfrontation, efterlysning og observation, s. 20

²⁸² Se hertil afsnit 4.1.2.1.2 *Observation på frit tilgængelige steder*

²⁸³ Lovforslag nr. L103, s. 11

ansigtsgenkendelse, er derfor ikke tilstrækkelig eller hensigtsmæssig. Det må derfor overvejes, om der er behov for at regulere brugen af ansigtsgenkendelse som et straffeprocessuelt tvangsindgreb, selvom efterforskningsmidlet ikke lever op til betingelserne i definitionen af straffeprocessuelle tvangsindgreb, og der derfor som udgangspunkt ikke er krav om hjemmel, før politiet kan anvende teknologien.

Samlet set viser den retsdogmatiske analyse af de retlige rammer for politiets anvendelse af ansigtsgenkendelse til brug for efterforskningen, at reguleringen på området er både fragmenteret, uklar og upræcis, hvilket resulterer i en generel usikkerhed i retstilstanden. Derudover er rammerne for brug af ansigtsgenkendelse ikke er tilstrækkelige for at imødekomme det behov, der er for regulering på området, idet brugen af ansigtsgenkendelse kan udgøre et intensivt indgreb i borgerens ret til privatliv. Når der er tegn på, at forsøgsordningen ved Københavns Politi med brug af retrospektiv ansigtsgenkendelse blot er begyndelsen, bør man regulering af brug af ansigtsgenkendelse tilgås proaktivt. Spørgsmålet er, hvordan regulering af området bør gribes an.

5.3. Retspolitiske overvejelser

Formålet med dette afsnit er at komme med retspolitiske overvejelser om, hvordan politiets brug af ansigtsgenkendelse kan reguleres på en mere sammenhængende og hensigtsmæssig måde, hvilket sker med udgangspunkt i de ovenstående betragtninger vedrørende de nuværende retlige rammers utilstrækkelighed og behovet for regulering på området. Forslagene fremsættes i prioriteret rækkefølge.

5.3.1. Regulering af ansigtsgenkendelse som straffeprocessuelt tvangsindgreb

Ud fra retspolitiske overvejelser anbefales, at der sker en regulering af politiets brug af ansigtsgenkendelse i efterforskningen, og at denne regulering bør finde sted i retsplejeloven som et straffeprocessuelt tvangsindgreb på trods af, at ansigtsgenkendelse ikke opfylder definitionen heraf. Fordelen ved at regulere som et straffeprocessuelt tvangsindgreb i retsplejeloven er, 1) at det kræver en lovændring, hvilket forudsætter en demokratisk debat om behovet for regulering, 2) at det vil medføre en klar lovhjemmel med præcise krav til forskellige anvendelser af ansigtsgenkendelse og 3) at domstolskontrol muliggøres. På denne måde sikres overensstemmelse med de krav, der stilles til brugen af ansigtsgenkendelse fra retshåndhævelsesdirektivet og EMRK art. 8. Der kan findes inspiration til den konkrete måde at udforme reguleringen og kravene hertil i AI-forordningen. Forordningen sonderer

eksempelvis mellem brug af ansigtsgenkendelse retrospektivt og i realtid, og der stilles forskellige krav hertil. Vedrørende brug af *retrospektiv ansigtsgenkendelse* foreslås det, at der fastsættes et relativt lavt mistankekrav. Derimod bør kriminalitets- og indikationskravet være højere, fordi ansigtsgenkendelse ud fra en proportionalitetsbetragtning ikke bør anvendes på bagatelagtig kriminalitet, og fordi brugen af ansigtsgenkendelse er overflødig, hvis den er af mindre betydning for efterforskningen. Det findes ikke betænkeligt at henlægge kompetencen til politiet, fordi brug af retrospektiv ansigtsgenkendelse er mindre indgribende. Der bør stilles strengere krav til brug af *ansigtsgenkendelse i realtid*, fordi dette er mere indgribende. Man kunne finde inspiration i kravene til politiets overtagelse af TV-overvågning, jf. RPL § 791 e, idet formålet med indgrebene i et vist omfang kan være sammenfaldende. Indikationskravet vil således være, at der er afgørende grunde til at anvende ansigtsgenkendelsen i realtid, imens kriminalitetskravet er 6 år eller en forsætlig overtrædelse af strfl. kap. 12 eller 13, og som kan medføre eller har medført fare for menneskers liv eller velfærd eller for betydelige samfundsværdier. Der foreslås ikke noget mistankekrav, fordi brugen af ansigtsgenkendelse i realtid, lige som ved overtagelse af TV-overvågning, ikke altid vil være et resultat af en mistanke rettet mod en konkret person. Derudover foreslås, at kompetencen henlægges til retten, og at der her fastsættes et tidsrum og en geografisk afgrænsning. Der bør desuden være krav om en indgrebsadvokat, som kan varetage den generelle offentligheds interesser.

5.3.2. Andre muligheder for regulering på området

Ud over muligheden for at regulere brugen af ansigtsgenkendelse som et straffeprocessuelt tvangsindgreb, ville en mere detaljeret regulering af kravene for behandling af biometriske data ved brug af ansigtsgenkendelse i retshåndhævelsesloven være oplagt. Fordelen ved denne løsning er, at det vil være muligt at opretholde den traditionelle struktur i retsplejeloven, hvor primært de straffeprocessuelle tvangsindgreb reguleres. Desuden er der allerede lagt et fundament for regulering af politiets indsamling og behandling af oplysninger i retshåndhævelsesloven, og dette kan med fordel videreudbygges for at sørge for, at reguleringen bliver sammenhængende og gennemskuelig. Her burde man overveje, om man kunne finde inspiration til yderligere regulering i de bestemmelser, vi har forbehold fra i AI-forordningen. Derudover kunne man udnytte den hjemmel, der i PL § 2 a, stk. 3 er til at udstede bekendtgørelser, som omhandler området for politiets indsamling og behandling af personoplysninger. Hjemlen i stk. 3 til at udstede bekendtgørelser kan desuden anvendes til nærmere regulering af, hvornår politiet må sammenkøre biometriske ansigtsskabeloner med en database med personfotografier med henblik på identifikation af vedkommende, men også til

at regulere de mere tekniske krav til ansigtsgenkendelse som teknologi. Selvom de her nævnte løsninger umiddelbart vil kunne bidrage til en mere sammenhængende regulering for brug af ansigtsgenkendelse – og politiets behandling af personoplysninger generelt – er det en ulempe at vælge disse løsninger frem for regulering i retsplejeloven, fordi sidstnævnte sikrer muligheden for domstolskontrol.

6. Litteraturliste

Retskilder

Lovgivning (love, forordninger, direktiver og konventioner)

- Den Europæiske Unions Charter om Grundlæggende Rettigheder, EU-Tidende 2012, C 326/391 (Chartret)
- Europa-Parlamentets og Rådets forordning (EU) 2024/1689 af 13. juni 2024 om harmoniserede regler for kunstig intelligens og om ændring af forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 og (EU) 2019/2144 samt direktiv 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (forordningen om kunstig intelligens) (AI-forordningen)
- Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (Databeskyttelsesforordningen)
- Europa-Parlamentets og Rådets direktiv 2016/680/EU af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA, EU-Tidende 2016, nr. L 119, side 89 (Retshåndhævelsesdirektivet)
- Lov nr. 285 af 29/04/1992 om den Europæiske Menneskerettighedskonvention
- Lov nr. 410 af 27/04/2017 om retshåndhævende myndigheders behandling af personoplysninger (Retshåndhævelsesloven)
- Lovbekendtgørelse nr. 1270 af 29/11/2019 om politiets virksomhed (politiloven)
- Lovbekendtgørelse nr. 182 24/02/2023 om TV-overvågning (TV-overvågningsloven)
- Lovbekendtgørelse nr. 1160 05/11/2024 af retsplejeloven
- Traktat om den Europæiske Unions Funktionsmåde (TEUF)

Lovforarbejder

- Betænkning 622/1971 om efterforskning i straffesager
- Betænkning 1023/1984 om politiets indgreb i meddelelshemmeligheden og anvendelse af agenter
- Betænkning 1104/1987 om legemsindgreb under efterforskningen
- Betænkning 1298/1995 om fotoforevisning, konfrontation, efterlysning og observation

- Folketingstidende 1998-99, tillæg A, sp. 828 ff. (Forslag til Lov om ændring af retsplejeloven (Beslaglæggelse, edition, fotoforevisning, konfrontation, efterlysning og observation samt prøvesagsordning for advokater m.v.))
- Folketingstidende 1988-89, tillæg A, sp. 2227 ff. (Forslag til Lov om ændring af retsplejeloven (Legemsindgreb))
- Lovforslag nr. L168: Forslag til lov om retshåndhævende myndigheders behandling af personoplysninger (Fremsat den 28. marts 2017) – Lovforslag som fremsat (benævnes Lovforslag nr. L168)
- Lovforslag nr. L171: Lov om ændring af lov om politiets virksomhed og toldloven (Politiets anvendelse af databaserede analyseredskaber og adgang til oplysninger om flypassagerer) (Fremsat den 29. marts 2017) – Lovforslag som fremsat (benævnes Lovforslag nr. L171)
- Lovforslag nr. L20: Lov om ændring af straffeloven, retsplejeloven, erstatningsansvarsloven og medieansvarsloven (Fremsat den 3. oktober 2018) – Lovforslag som fremsat (benævnes Lovforslag nr. L20)
- Lovforslag nr. L103: Lov om ændring af retsplejeloven (Politiets overtagelse af TV-overvågning) (Fremsat den 5. februar 2020) – Lovforslag som fremsat (benævnes Lovforslag nr. L103)

Praksis

EU-Domstolen

- C-205/21

EMD

- S. and Marper mod Storbritannien (2008)
- Gaughran mod Storbritannien (2020)
- Glukhin mod Rusland (2023)

Vejledninger

- EDPB Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement
- EDPB Guidelines 3/2019 on processing of personal data through video devices

Andet

- Retsudvalgets spørgsmål nr. 1344 stillet den 13/8 2024, besvaret af justitsministeren den 8/11 2024.
- B 46 Forslag til folketingsbeslutning om at forbyde offentlige myndigheders anvendelse af ansigtsgenkendelsesteknologi i det offentlige rum af den 27. november 2019
- Retsudvalgets spørgsmål 1 til forslag til folketingsbeslutning nr. B 46 stillet den 22/1 2020, besvaret af justitsministeren den 18/2 2020.
- Folketingets udvalg for Digitalisering og IT's spørgsmål nr. 101 stillet den 6/2 2024, besvaret af justitsministeren den 4/3 2024.
- Justitsministeriets orientering til Retsudvalget, 21. juni 2024 (Orientering om politiets forsøg med digitaliseret offergenkendelse i efterforskning af sager om seksuelt misbrug af børn), 21. juni 2024
- Justitsministeriets orientering til Retsudvalget, 5. september 2024 (Orientering om politiets brug af ansigtsgenkendelsesteknologi i efterforskning)

Litteratur og videnskabelige artikler

- *Akbari, Ali*: Facial Recognition 101 – Technical Insights, 2024
- *Gammeltoft-Hansen, Hans*: Om definitionen af straffeprocessuelle tvangsindgreb i “Jurist uden omsvøb – Festskrift til Gorm Toftegaard Nielsen”, Christian Ejlers’ Forlag, 1. udgave, 2007
- *Gammeltoft-Hansen, Hans*: Straffeprocessuelle tvangsindgreb – retspolitiske studier (1981), Juristforbundets forlag
- *Gammeltoft-Hansen, Hans*: U.1979B.1 (Om afgrænsningen af straffeprocessuelle tvangsindgreb)
- *Kjølbros, Jon Fridrik*: Den Europæiske Menneskerettighedskonvention for praktikere, Jurist- og Økonomforbundets Forlag, 5. udgave, 2020
- *Munk-Hansen, Carsten*: Retsvidenskabsteori, DJØF forlag, 2. udgave, 2018
- *Neergaard, Ulla og Nielsen, Ruth*: EU-ret, Karnov Group, 8. udgave, 2020
- *Rytter, Jens Elo*: Individets grundlæggende rettigheder, Karnov Group, 4. udgave, 2021
- *Selwyn m.fl.*: Facial Recognition Technology – Key Issues and Emerging Concerns, 2024
- *Simmeler, Monika og Canova, Giulia*: Facial recognition technology in law enforcement – Regulating data analysis of another kind, 2025

- *Toftegaard Nielsen, Gorm*: Hvad er et tvangsindgreb? (2005) Juristen, Årgang 87 nr. 5, s. 153–160, DJØF Forlag
- *Vestergaard, Jørn*: Straffeproces – grundtræk af dansk strafferetspleje, Gjellerup Forlag, 1. udgave, 2017

Hjemmesider og avisartikler

- Aftale om Bandepakke IV: Trygge nabolag i hele Danmark (<https://www.justitsministeriet.dk/wp-content/uploads/2023/11/Aftale-om-bandepakke-IV-%E2%80%93-Trygge-nabolag-i-hele-Danmark.pdf>)
- EDPB's hjemmeside (tilgået 6. april 2025) (https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en)
- Eurofound: European Industrial Relations Dictionary: Soft Law (tilgået 13. maj 2025) (<https://www.eurofound.europa.eu/en/european-industrial-relations-dictionary/soft-law>)
- Justitsministeriet: Digital tryghedspakke – Ni initiativer der skal gøre det tryggere at færdes på nettet (13. september 2022) (<https://www.justitsministeriet.dk/wp-content/uploads/2022/09/Digital-tryghedspakke-2022-1.pdf>)
- Justitsministeren »er åben overfor at diskutere« ansigtsgenkendelse i realtid (6. december 2024): Philip Sune Dam (tilgået 9. maj 2025) (<https://www.berlingske.dk/indland/justitsministeren-er-aaben-overfor-at-diskutere-ansigtsgenkendelse>)
- Københavns Politi: Vi vil gerne bruge ansigtsgenkendelse på borgerne (23. oktober 2019): Jens Beck Nielsen (tilgået 1. marts 2025) (<https://www.berlingske.dk/indland/koebenhavns-politi-vi-vil-gerne-bruge-ansigtsgenkendelse-paa-borgerne>)
- Københavns Politi vil have adgang til ansigtsgenkendelse (24. oktober 2019): Mikkel Secher & Ritzau (tilgået 1. marts 2025) (<https://nyheder.tv2.dk/samfund/2019-10-24-koebenhavns-politi-vil-have-adgang-til-ansigtsgenkendelse>)
- Politiet vil skifte mennesker ud med computere i jagten på svenske kriminelle i Danmark (9. august 2024): Mathilde Faurby (tilgået 9. marts 2025) (<https://www.dr.dk/nyheder/politik/politiet-vil-skifte-mennesker-ud-med-computere-i-jagten-paa-svenske-kriminelle-i>)

- Pressemeldelse, Justitsministeriet: "Politiet får grønt lys til ansigtsgenkendelse", 5. september 2024 (<https://www.justitsministeriet.dk/pressemeldelse/politiet-faar-groent-lys-til-ansigtsgenkendelse/>)
- Publikation, Dataetisk Råd: "Hvad er ansigtsgenkendelse?", 2022 (https://dataetiskraad.dk/Media/638037688341688364/Data-Etisk-Raad_Ansigtsgenkedelse_2022.pdf)
- Rigspolitichef vil bruge "crunching" mod svenske lejermordere (12. august 2024): Sebastian Juel Ebling (tilgået 9. marts 2025) (<https://nyheder.tv2.dk/samfund/2024-08-12-rigspolitichef-vil-bruge-crunching-mod-svenske-lejemordere>)
- Så meget videoovervågning er der i Danmark (9. oktober 2019): Emilie Foxil (tilgået 1. marts 2025) (<https://nyheder.tv2.dk/politik/2019-10-09-saa-meget-videoovervaagning-er-der-i-danmark>)