JUSTITIA

DANMARKS UAFHÆNGIGE
JURIDISKE TÆNKETANK

Rapport:

Ansigtsgenkendelsesteknologi

Behov for regulering af politiets anvendelse

Af Birgitte Arent Eiriksson

Ansigtsgenkendelsesteknologi: Behov for regulering af politiets anvendelse

Justitia - Danmarks uafhængige juridiske tænketank
Vesterbrogade 69D, 1. sal. th. 1620 København
www.justitia-int.org
info@justitia-int.org

Justitia er Danmarks eneste juridiske tænketank, der alene har fokus på retssikkerhed og frihedsrettigheder. Justitias formål er gennem analyser af høj faglig kvalitet og fremsættelse af konkrete juridiske løsningsforslag at påvirke den offentlige og politiske dagsorden med henblik på at fremme en politisk kultur, hvor disse værdier nyder den nødvendige respekt.

Rapporten er blevet til med støtte fra Dreyers Fond

Indhold

1 Resume og anbefalinger 2

2 Fokus på politiets anvendelse af ansigtsgenkendelse 5

3 Hvad er ansigtsgenkendelsesteknologi? 7

4 Nationale rammer for anvendelse af ansigtsgenkendelsesteknologi 11

4.1 Retshåndhævelsesloven 11

4.2 Tv-overvågning 12

5 EU-forordning om kunstig intelligens 16

6 Øvrige internationale tilkendegivelser 23

6.1 Europarådet 23

6.2 FN 26

7 Menneskeretlige overvejelser 29

7.1 Retten til privatliv 29

7.2 Øvrige rettigheder og principper 34

8 Dataetiske refleksioner 37

9 Ansigtsgenkendelse i Danmark 41

9.1 Konkret anvendelse 41

9.2 Politiske tilkendegivelser og initiativer 42

10 Ansigtsgenkendelse uden for Danmark 50

10.1 Eksempler på ansigtsgenkendelse i Europa 50

10.2 Ansigtsgenkendelse i USA 59

10.3 Ansigtsgenkendelse i Kina 60

11 Konklusion 64

12 Justitias anbefalinger 68

1 Resume og anbefalinger

Når ansigtsgenkendelsesteknologi anvendes i det offentlige rum, kan det i lande som Kina blive brugt som et uproportionalt magtmiddel med store konsekvenser for borgernes frihedsrettigheder, retssikkerhed og sociale tryghed. Et sådant scenarie er selvfølgelig utænkeligt i Danmark, men også her i landet vil politiets anvendelse af ansigtsgenkendelse til kriminalitetsbekæmpelse være et alvorligt indgreb i borgernes ret til privatliv, fordi unikke biometriske koder for ansigter registreres og spores uden samtykke. Følelsen af konstant at være overvåget vil samtidig kunne true udøvelsen af andre frihedsrettigheder, herunder retten til at forsamle sig og ytre sig, ligesom overvågningsdata i kombination med andre personlige data om borgerne kan anvendes til at danne detaljerede personprofiler, der kan give meget præcise oplysninger om borgernes private forhold. Det gælder ikke mindst med politiets analyseplatform POL-INTEL, der muliggør analyser på tværs af meget store mængder af data fra både interne og eksterne kilder samt offentligt tilgængelige kilder som eksempelvis sociale medier.

Dansk politis anvendelse af ansigtsteknologi har indtil nu været begrænset til verificering af identitet ved paskontrol og digitaliseret offergenkendelse i sager om seksuelt misbrug af børn. Der er dog en aktuel politisk interesse for at udvide politiets muligheder for at anvende ansigtsgenkendelse. Senest har justitsminister Peter Hummelgaard udtrykt, at ansigtsgenkendelsesteknologi bør anvendes af myndighederne, "når fordelene overstiger ulemperne".

En lignende udvikling ses i mange andre europæiske lande. F.eks. har regeringen i Sverige i efteråret 2023 iværksat et initiativ, hvor man vil anvende ansigtsgenkendelsesteknologi i forbindelse med bandekriminalitet. Også i den nye danske bandepakke IV nævnes ansigtsgenkendelsesteknologi som et muligt værktøj.

Der er således meget, der tyder på, at ansigtsgenkendelse hurtigt kan blive et værktøj til kriminalitetsbekæmpelse i Danmark. Det er dog ikke sikkert, at Folketinget vil blive involveret i en sådan beslutning. Justitsministeren har nemlig givet udtryk for, at Folketinget ikke behøver at blive orienteret herom, medmindre der er behov for at justere den retlige ramme.

Politiets anvendelse af ansigtsgenkendelse til kriminalitetsbekæmpelse kan imidlertid være i strid med vores grundlæggende rettigheder, som er beskyttet i Den Europæiske Menneskerettighedskonvention og Den Europæiske Unions Charter om Grundlæggende Rettigheder. Dette skyldes, at politiets anvendelse af teknologien i realtid i langt de fleste tilfælde vil kunne blive anset for uproportional og/eller unødvendig i et demokratisk samfund. Hertil kommer, at det nuværende retsgrundlag for politiets anvendelse af ansigtsgenkendelse er så bredt og uklart, at både anvendelse af teknologien i realtid og retrospektiv anvendelse vil ske på baggrund af regler, som efter Justitias opfattelse ikke kan anses for at leve op til kravet om en klar lovhjemmel ved indgreb i menneskerettigheder.

Der er efter Justitias vurdering behov for en hurtig afklaring af, hvilke udvidelser af politiets anvendelse af ansigtsgenkendelse der kan komme på tale nu og i nærmeste fremtid, ligesom der er behov for at sikre, at der i god tid etableres en meget klar og præcis lovhjemmel.

På grund af det danske retsforbehold vedrørende EU-samarbejdet inden for civil- og strafferet vil AI-forordningens bestemmelser om politiets anvendelse af ansigtsgenkendelse ikke være gældende i Danmark, men vi har mulighed for at tilslutte os denne del af forordningen gennem en tilvalgsretsakt. Det vil dog **efter Justitias opfattelse være mest hensigtsmæssigt at regulere politiets anvendelse af ansigtsgenkendelse nationalt**.

De nationale regler bør efter Justitias opfattelse indeholde et forbud mod politiets anvendelse af ansigtsgenkendelse i realtid. Denne vurdering er på linje med European Data Protection Board, Europarådets ad hoc komite CAHAI og FN's højkommissær for menneskerettigheder.

Hvis det alligevel besluttes, at dansk politi skal have adgang til at anvende ansigtsgenkendelse i realtid, bør det efter Justitias opfattelse kun ske i ganske få tilfælde, hvor der er overhængende fare for tab af liv:

Anbefaling 1: Hvis det besluttes, at politiet må anvende ansigtsgenkendelse i realtid, bør det kun være i situationer, hvor der er tale om overhængende fare for tab af liv.

En reel retrospektiv anvendelse af ansigtsgenkendelse må anses for at være et mindre intenst indgreb end anvendelse i realtid, men udgør stadig et markant indgreb i retten til privatliv. Sammenlignet med f.eks. telefonaflytning og almindelig tv-overvågning må retrospektiv ansigtsgenkendelse anses for mere indgribende, fordi det giver mulighed for at kortlægge en formodet gerningspersons færden præcist og effektivt på en måde, som ikke kendes fra traditionelle overvågningsmetoder. Derfor bør kriminalitetskravet efter Justitias opfattelse også være højere:

Anbefaling 2: Politiets retrospektive anvendelse af ansigtsgenkendelse skal begrænses til lovovertrædelser, der kan straffes med fængsel i 8 år eller derover, og som kan medføre eller har medført fare for menneskers liv eller legeme.

Herudover fremsætter Justitia en række generelle anbefalinger ved regulering af politiets anvendelse af ansigtsgenkendelse i både realtid og retrospektivt:

Anbefaling 3: Generelle anbefalinger til politiets anvendelse af ansigtsgenkendelse:

A. En udvidelse af politiets muligheder for at anvende ansigtsgenkendelse skal ske på baggrund af en bred og åben demokratisk samtale om fordele og ulemper samt en dataetisk konsekvensanalyse.

B. Politiets anvendelse af ansigtsgenkendelse skal reguleres som et straffeprocessuelt indgreb i retsplejeloven, der kræver retskendelse, og reguleres nærmere i politiloven.

C. Der skal ikke ske lagring af biometriske ansigtsdata.

D. Der skal laves en kortlægning og løbende ajourføring af politiets samlede tv-overvågning i det offentlige rum og andre frit tilgængelige steder, herunder også ANPG-kameraer mv. Kortlægningen skal indeholde oplysninger om, i hvilket omfang der er anvendt ansigtsgenkendelse i realtid. Kortlægningen skal være offentlig tilgængelig.

E. Det skal undersøges, om der er behov for regulering af politiets observation i det offentlige rum og andre frit tilgængelige steder.

F. Der skal ske en kortlægning af politiets overtagelse af kameraovervågning fra private og offentlige myndigheder.

G. Det skal undersøges, hvordan der kan sikres en effektiv klageadgang for borgere, som er blevet overvåget af politiet med anvendelse af ansigtsgenkendelse, herunder hvordan borgerne i videst muligt omfang kan blive gjort bekendt med en sådan behandling af deres biometriske ansigtsdata.

H. Politiets anvendelse af ansigtsgenkendelsesteknologi i realtid i det offentlige rum og frit tilgængelige steder og politiets retrospektive anvendelse af teknologien skal evalueres efter 2 år.

Konklusion og anbefalinger uddybes i kapitel 11-12.

2 Fokus på politiets anvendelse af ansigtsgenkendelse

Ansigtsgenkendelse er en form for biometrisk identifikation, der anvender avancerede algoritmer til at analysere og genkende unikke træk og mønstre i et menneskes ansigt for at identificere eller verificere dets identitet. Ansigtsgenkendelse kan f.eks. anvendes til at identificere personer mistænkt for kriminalitet eller overvåge offentlige begivenheder ved at analysere ansigtsbilleder og sammenligne dem med databaser med kendte identiteter.

Politiets anvendelse af ansigtsgenkendelsesteknologi rejser et centralt dilemma. På den ene side repræsenterer teknologien en potentiel styrkelse af sikkerheden og effektiviteten i retshåndhævelsen, idet den muliggør hurtig identifikation og lokalisering af potentielle kriminelle og andre sikkerhedstrusler. På den anden side rejser teknologien alvorlige bekymringer om individets ret til privatliv og beskyttelse af data, idet den indebærer indsamling og behandling af biometriske data, som kan anvendes til intens overvågning og profilering på individniveau.

Hertil kommer, at politiets mulighed for at anvende ansigtsgenkendelsesteknologi i høj grad vil ændre det samlede overvågningsbillede i Danmark. Hidtil er tv-kameraer på frit tilgængelige steder blevet anset som så almindelige, at borgerne forventes at være opmærksomme på dem og naturligt tilpasse deres adfærd herefter. Samtidig har der været en opfattelse af, at den generelle modstand i samfundet mod et "overvågningssamfund" og den politiske kontrol med politiets aktiviteter ville modvirke eventuelle tendenser mod en mere omfattende tv-overvågning af befolkningen.[1] Med ansigtsgenkendelsesteknologi bliver overvågningskameraer og lignende pludselig et markant mere intenst overvågningsværktøj for politiet. Det gælder ikke mindst med politiets analyseplatform POL-INTEL, der muliggør analyser på tværs af meget store mængder af data fra både interne og eksterne kilder samt offentligt tilgængelige kilder som eksempelvis sociale medier.

Rapporten er en invitation til en grundig refleksion over de juridiske, dataetiske og samfundsmæssige konsekvenser af politiets brug af ansigtsgenkendelse. I erkendelse af den hastige udvikling inden for teknologien og dens potentielle indvirkning på samfundet er det Justitias håb, at rapporten kan tjene som et værdifuldt bidrag til den fortsatte debat om, hvorvidt politiet i Danmark bør have mulighed for at anvende teknologien, og i givet fald hvilke betingelser der bør opstilles for at sikre respekten for grundlæggende menneskerettigheder, retsstaten og dataetikken.

Rapporten er opdelt i en række kapitler, hvor kapitel 3 indleder rapporten med en beskrivelse af teknologien og dens anvendelsesmuligheder. I kapitel 4-6 gennemgås de nationale retlige rammer

[1] L 41 om forslag til lov om ændring af retsplejeloven (Beslaglæggelse, edition, fotoforevisning, konfrontation, efterlysning og observation samt prøvesagsordning for advokater m.v.), 8. oktober 1998, Strafferetsudvalgets bemærkninger i afsnit 6.2.2. Se også U.2021.1265

for politiets anvendelse af ansigtsgenkendelse, relevante dele af Europa-Parlamentets og Rådets forslag til forordning om kunstig intelligens (AI-forordningen) samt tilkendegivelser fra Europarådet og FN om ansigtsgenkendelse. I kapitel 7 redegøres der for de menneskeretlige overvejelser ved politiets anvendelse af ansigtsgenkendelse. Kapitel 8 indeholder dataetiske overvejelser. Kapitel 9 beskriver, hvordan teknologien anvendes i Danmark, og hvilke politiske tilkendegivelser og initiativer der har været. I kapitel 10 gives der et kort overblik over status på anvendelsen af ansigtsgenkendelsesteknologi i en række europæiske lande, USA og Kina. Endeligt indeholder kapitel 11-12 rapportens konklusion og anbefalinger.

3 Hvad er ansigtsgenkendelsesteknologi?

Ansigtsgenkendelse er software, som analyserer billeder med henblik på at identificere ansigter. Først anvendes en algoritme til at finde ansigter på et billede (ansigtsopdagelse). Herefter laver algoritmen en biometrisk analyse af ansigtets særlige kendetegn. Ansigtet er unikt på sammen måde som fingeraftryk, og softwaren kan derfor genkende ansigtet på andet billed- eller videomateriale.[2] I en automatiseret proces og i nogle tilfælde ved hjælp af kunstig intelligens, kan man både i realtid og ved retrospektiv analyse finde udvalgte personer på store mængder af videomateriale. Det bliver herved muligt hurtigt og effektivt at kortlægge en persons færden i det offentlige rum, f.eks. i forbindelse efterforskning af kriminalitet. Når sådanne oplysninger sammenholdes med andre indhentede og/eller allerede registrerede oplysninger om en person, vil der desuden kunne foretages profilering af den pågældende[3].

Biometriske data er en samlebetegnelse for denne type personoplysninger baseret på målbare fysiske eller adfærdsmæssige egenskaber, som anvendes til at identificere eller bekræfte en persons identitet. Biometrisk data som f.eks. fingeraftryk og DNA har længe været anvendt til bl.a. at efterforske og retsforfølge kriminalitet, fordi disse oplysninger kan afsløre, om en person matcher bevismateriale, der f.eks. er blevet fundet på et gerningssted.[4]

Ansigtskendelse er ikke én bestemt ting, men en teknologi med en lang række anvendelsesformer.[5] Grundlæggende er teknologien i stand til at identificere, verificere og kategorisere ansigter.

Ansigtsgenkendelse til **verificering** indebærer sammenligning af et ansigt med et digitalt ansigtsbillede (en-til-en sammenligning). Et eksempel på denne form for ansigtsgenkendelse er ved digital paskontrol i lufthavne, hvor den rejsende scanner sit pasbillede, og et kamera samtidig registrerer den rejsendes ansigt, hvorefter automatisk verificering tillader den rejsende at passere kontrolområdet.

Ansigtsgenkendelse til **identificering** indebærer, at et ansigt sammenlignes med en række ansigter i en database med henblik på at afgøre, om det specifikke ansigt matcher et ansigt i referencedatabasen (en-til-mange **sammenligning**). Dette kan ske ved identifikation i **realtid**, hvorved ansigter konstant udskilles fra live-videoer og automatisk sammenlignes med ansigter i en referencedatabase. Der kan også foretages **retrospektiv** identifikation, hvorved ansigtsdataene indledningsvis optages og efterfølgende sammenlignes med data i en database.[6]

---

[2] Dataetisk Råd "Hvad er ansigtsgenkendelse?", 2022.
[3] Police use of Facial Recognition: Factsheet, 2024. Gov.UK. https://shorturl.at/cguxF
[4] Begrebet er bl.a. defineret i EU-forordning 2016/679 om databeskyttelse, art. 4(14).
[5] Hupont, I., Tolan, S., Gunes, H., & Gómez, E. (2022): "The landscape of facial processing applications in the context of the European AI Act and the development of trustworthy systems." Nature Scientific Reports vol 12: 10688. https://doi.org/10.1038/s41598-022-14981-6
[6] Definitionen af identifikation i realtid og retrospektiv identifikation er i overensstemmelse med definitionerne fastlagt i forslag til Europa-Parlamentets og Rådets forordning om harmoniserede regler for kunstig intelligens, jf. betragtning 8, (37) og (38) i forordningsforslaget.

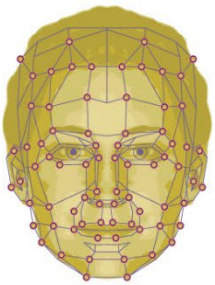
Ansigtsgenkendelse

1

OPTAGELSE AF ANSIGTSBILLEDE

Et kamera optager billede eller video af forbipasserendes ansigt

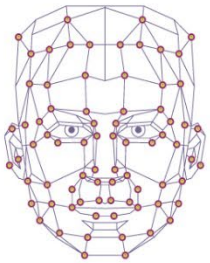
2



ANSIGTSOPDAGELSE

Det bagvedliggende system leder efter generelle karakteristikker ved menneskeansigter og registrerer på den måde, når der er optaget et ansigt

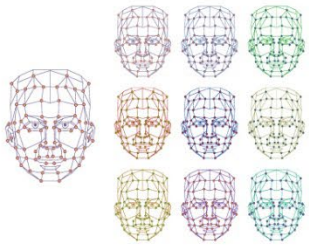
3



BIOMETRISK ANALYSE

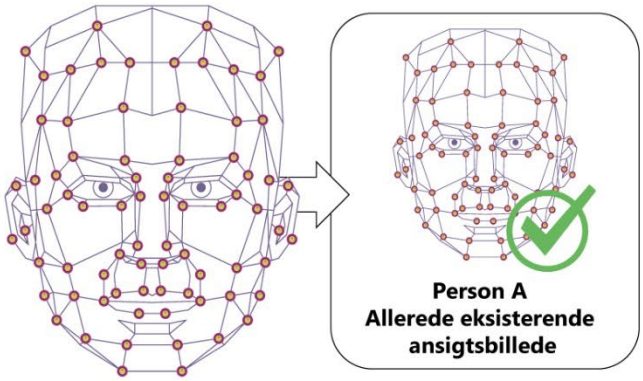
Det bagvedliggende system udarbejder en skabelon over det optagede ansigt ved at justere for bl.a. lys og vinkler, og udleder på den måde de fysiske egenskaber, der er karakteristiske for det pågældende ansigt

4



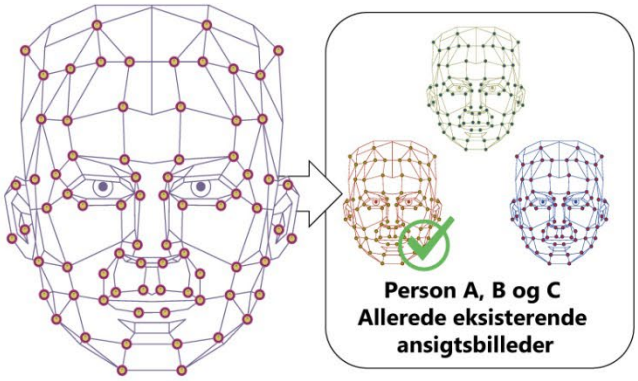
MATCH AF ANSIGTSSKABELON

Den udarbejdede ansigtsskabelon anvendes til at foretage **verificering** (en-til-en-sammenligning), **identificering** (en-til-mange-sammenligning) eller **kategorisering**.



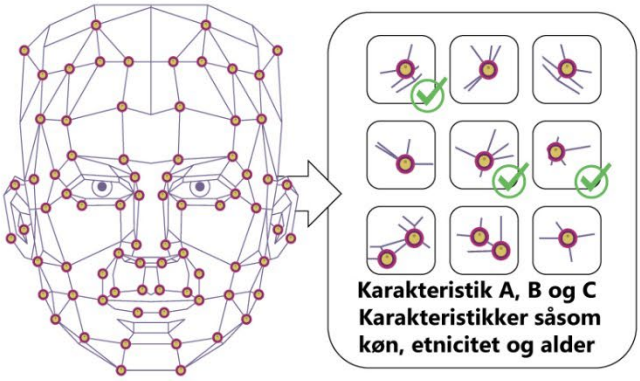
Verificering

Ved **verificering** sammenlignes ansigtsskabelonen med et allerede eksisterende ansigtsbillede. Sammenligningen har til formål at verificere den pågældendes identitet (en-til-en-sammenligning). Denne metode anvendes f.eks. ved digital paskontrol, hvor ansigtsskabelonen sammenlignes med det eksisterende pasfoto.



Identificering

Ved **identificering** sammenlignes ansigtsskabelonen med en række allerede eksisterende ansigtsbilleder fra en database. Sammenligningen har til formål at identificere ansigtet fra ansigtsskabelonen blandt ansigtsbillederne i referencedatabasen (en-til-mange-sammenligning). Denne metode er f.eks. anvendelig inden for efterforskning, hvor optagelser af en ukendt gerningsmand kan lede til identificering af vedkommende.



Kategorisering

Ved **kategorisering** sammenlignes ansigtsskabelonen med en eller flere karakteristika såsom køn, etnicitet og alder med det formål at afgøre, om personen tilhører en bestemt gruppe, såkaldt 'demografisk identifikation'. Teknologien kan også anvendes til 'udtryks- og affektidentifikation, hvor følelser såsom vrede, frygt og glæde udledes fra den biometrisk analyse.

Derudover kan ansigtsgenkendelse anvendes til **kategorisering**, hvor demografisk eller udtryks- og affektidentifikation indsamles og kategoriseres[7]. Her sammenlignes ansigtsskabelonen med en eller flere karakteristika såsom køn, alder og etnicitet med det formål at konstatere, om vedkommende tilhører en bestemt gruppe. Denne form for teknologi er tiltænkt anvendt til bl.a. profilering, hvor formålet er at analysere eller forudsige forhold vedrørende det pågældende individs arbejdsindsats, økonomiske situation, helbredsforhold, personlige præferencer, interesser, pålidelighed, adfærd mv.[8] Ligeledes kan teknologien anvendes til at udlede følelser såsom vrede, frygt og glæde, samt til at vurdere, om folk lyver.[9]

De bagvedliggende algoritmer, som den kunstige intelligens er baseret på, leverer ikke definitive resultater, men derimod sandsynligheder, f.eks. at der er 80 procent sandsynlighed for, at en given person på en video matcher en given person i en database. Anvendelse af ansigtsgenkendelse kræver derfor, at man tager stilling til, hvilken grænseværdi der skal anvendes i vurderingen af, hvem der skal medtages som potentielle match. Denne beslutning har betydning for antallet af henholdsvis falske positive og falske negative resultater.[10]

Teknologien er både udviklet og taget i brug på en lang række forskellige områder mange steder i verden. Det benyttes i alt fra smartphones, overvågningskameraer ved grænsekontroller og sociale pointsystemer.[11] Teknologien anvendes både af offentlige myndigheder og private virksomheder.

En omfattende befolkningsundersøgelse, der bl.a. analyserer befolkningens holdninger til ansigtsgenkendelse, har vist, at mange har et begrænset kendskab til ansigtsgenkendelse, og at flere føler sig mere trygge ved statens anvendelse af teknologien end ved kommercielle aktørers anvendelse.[12]

Politiets anvendelse af ansigtsgenkendelse har været meget omdiskuteret. Teknologien anvendes af politiet flere steder i verden, herunder USA og UK, hvor det både anvendes i kropskameraer og stationære kameraer på offentlige steder.[13] I Danmark er der også en stigende interesse for de muligheder, som teknologien kan have for politiet, se nærmere kapitel 9.2 om politiske tilkendegivelser og initiativer.

[7] Dataetisk Råd "Hvad er ansigtsgenkendelse?", 2022.
[8] Som defineret i bl.a. EU-forordning 2016/679 om databeskyttelse, art. 4(4).
[9] Der har været iværksat et forsøg med denne teknologi ved EU's ydre grænser, se Home | iBorderCtrl.
[10] European Union Agency for Fundamental Rights, Facial recognition technology: Fundamental rights considerations in the context of law enforcement, April 2019, s. 9.
[11] Se nærmere om sociale pointsystemer i afsnit 4 om status på anvendelsen af ansigtsgenkendelse i Kina.
[12] Befolkningsundersøgelsen af udført i regi af Algoritmer, Data og Demokrati-projektet og er tilgængelig her.
[13] Dataetisk Råd "Hvad er ansigtsgenkendelse?", 2022, side 10.

Hvordan politiet kan anvende ansigtsgenkendelsesteknologi

Figuren viser eksempler og er ikke en udtømmende liste.

FINDE PERSONER I REALTID

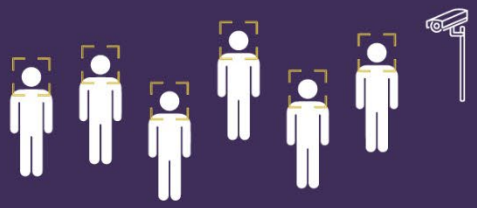
Politiet vil i realtid kunne spore en bestemt persons placering. Dette kan både anvendes til at finde personer, der mistænkes for at have begået eller har til hensigt at begå kriminalitet, eksempelvis en terrorhandling.

KORTLÆGGE FÆRDEN

Politiet kan anvende teknologien retrospektivt under efterforskning til at kortlægge relevante personers færden i det offentlige rum. Herunder mulige gerningspersoner og ofre.

FINDE MISTÆNKTE VED ET GERNINGSTED

Når en forbrydelser er sket, kan politiet retrospektivt identificere personer, der har opholdt sig ved eller tæt på et gerningssted i tidsrummet, hvor en forbrydelse er blevet begået.



IT-KRIMINALITET

Identificere personer, der begår cyberangreb eller deltager i andre lovovertrædelser aktiviteter online.

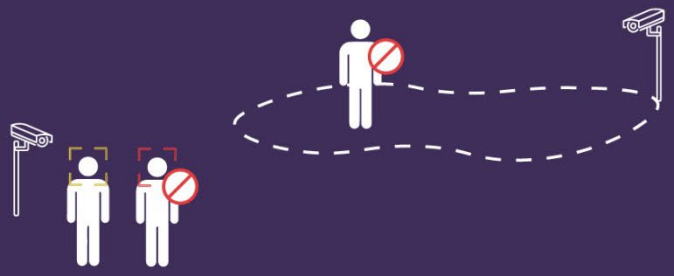
Kan også anvendes til at finde ofre for kriminalitet, som bliver delt online.

SIKKERHED VED ARRANGEMENTER

Ansigtsgenkendelsesteknologi muliggør både adgangskontrol og overvågning af deltageraktiviteter ved arrangementer. Det kan sikre, at kun autoriserede personer deltager og identificere mistænkelig adfærd eller personer, der udgør en sikkerhedsrisiko.

HÅNDHÆVE OPHOLD- OG KONTAKTFORBUD

Hvis personer har fået pålagt et opholds- eller kontatkforbud, kan politiet bruge ansigtsgenkendelsesteknologi til at identificere og spore, hvis de forsøger at bryde forbuddet. Hvis bevæge sig ind i de forbudte områder eller mødes med personer vedkommende ikke må kommunikere med.



AUTOMATISERET RETSHÅNDHÆVELSE

Automatiseret retshåndhævelse indebærer automatisk tildeling af en straf, når en lovovertrædelse begås og samtidig optages af et overvågningskamera med ansigtsgenkendelsesteknologi. For eksempel kan dette forekomme, når en person går over for rødt lys eller anden kriminalitet som for eksempel gadeuorden.

ADFÆRD

Ansigtsgenkendelsesteknologien kan monitorere en menneskemængde og ved hjælp af affektionsanalyse identificere aggressiv og mistænkelig adfærd.

VERIFIKATION

Det kan anvendes til at identificere personers identitet for eksempel ved pas- og grænsekontrol, karantæneregler mv.

4 Nationale rammer for anvendelse af ansigtsgenkendelsesteknologi

Ansigtsgenkendelse kan være et yderst brugbart og effektivt værktøj, men kan samtidig anvendes på måder, som udgør et markant indgreb i såvel retten til privatliv og beskyttelse af personoplysninger som andre grundlæggende frihedsrettigheder og principper. Dette er der redegjort nærmere for i kapitel 7.

I dette kapitel ses der nærmere på de retlige nationale rammer for politiets behandling af biometriske personoplysninger, som følger af retshåndhævelsesloven. Der ses desuden på tv-overvågningsloven, der regulerer privates og offentlige myndigheders muligheder for at foretage tv-overvågning, samt på reglerne for politiets tv-overvågning og politiets adgang til samt overtagelse af andres tv-overvågning.

4.1 Retshåndhævelsesloven

Databeskyttelsesforordningen og databeskyttelsesloven regulerer behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og for anden ikke automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Når politiet behandler personoplysninger, er det imidlertid reglerne i retshåndhævelsesloven,[14] som finder anvendelse.[15] Retshåndhævelseslovens § 3, stk. 1, nr. 12, (og databeskyttelsesforordningen artikel 9) definerer biometriske data således:

> *Biometriske data: 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.*[16]

Biometriske data er underlagt særregler på grund af dataenes særlige karakter. Udgangspunktet i retshåndhævelsesloven er, at behandling af biometriske data med henblik på entydigt at identificere en fysisk person er ulovligt.[17] Behandling af biometriske data kan dog alligevel ske, når det er strengt nødvendigt med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder for at beskytte mod eller forebygge trusler mod

[14] Lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger, der implementerer retshåndhævelsesdirektivet (Europa-Parlamentets og Rådets Direktiv (EU) 2016/680). Retshåndhævelsesloven er senest ændret ved lov nr. 503 og 506 af 23. maj 2018.
[15] Retshåndhævelseslovens § 1.
[16] Retshåndhævelseslovens § 3, stk. 1, nr. 12.
[17] Retshåndhævelseslovens § 10, stk. 1.

den offentlige sikkerhed eller beskytte en fysisk persons vitale interesser, eller hvis behandlingen vedrører oplysninger, som tydeligvis er offentliggjort af den registrerede.[18]

Retshåndhævelsesloven indeholder desuden en række generelle regler om behandlingen af personoplysninger, der altid skal overholdes, bl.a. krav om god dataskik,[19] formålskrav,[20] dataminimering[21] og regler vedrørende videregivelse af oplysninger.[22] Indsamlede oplysninger må ikke opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles.[23]

Datatilsynet fører tilsyn med politiets behandling af personoplysninger.[24] Der er efter loven endvidere mulighed for at lade Datatilsynet udøve den registreredes rettigheder.[25]

4.2 Tv-overvågning

Politiet har flere muligheder for at anvende tv-overvågning som led i arbejdet med at forebygge og efterforske kriminalitet.

Politiet kan **selv iværksætte tv-overvågning**, når det sker **i det offentlige rum og på andre frit tilgængelige steder**. Politiets efterforskningsmæssige beslutninger, herunder opsætning af overvågning, er i sådanne tilfælde alene underlagt en almindelig ulovbestemt proportionalitetsvurdering. Politiets observation i disse situationer kræver således ikke en tilladelse fra retten. [26]

Når politiet derimod iværksætter tv-overvågning af personer, der befinder sig på et **ikke-frit tilgængeligt sted**, skal det ske efter retsplejeloven regler om observation, hvilket bl.a. forudsætter rettens tilladelse.[27]

[18] Retshåndhævelseslovens § 10, stk. 2, jf. § 1, stk. 1. Se også EMD i Rotaru mod Rumænien, 4. maj 2000, præmis 47, hvorefter myndighedernes hemmelige overvågning af borgerne kun er foreneligt, hvis det er "strengt nødvendigt", og en analyse heraf i EU-ret & Menneskeret, Djøf forlag, april 2021.
[19] Retshåndhævelseslovens § 4, stk. 1.
[20] Retshåndhævelseslovens § 4, stk. 2 og § 5.
[21] Retshåndhævelseslovens § 4, stk. 3.
[22] Retshåndhævelseslovens § 4, stk. 5 og § 6.
[23] Retshåndhævelseslovens § 4, stk. 6.
[24] Retshåndhævelseslovens § 37.
[25] Retshåndhævelseslovens § 17, stk. 5, jf. § 40 stk. 1 nr. 6, jf. § 48.
[26] U 2021.1262.
[27] Retsplejelovens § 780.

Retsplejelovens § 791 a

Stk. 1. Politiet kan foretage fotografering eller iagttagelse ved hjælp af kikkert eller andet apparat af personer, der befinder sig på et ikke frit tilgængeligt sted (observation), såfremt

- *1) indgrebet må antages at være af væsentlig betydning for efterforskningen, og*
- *2) efterforskningen vedrører en lovovertrædelse, der efter loven kan medføre fængselsstraf.*

Stk. 2. Observation som nævnt i stk. 1 ved hjælp af fjernbetjent eller automatisk virkende tv-kamera, fotografiapparat eller lignende apparat må dog kun foretages, såfremt efterforskningen vedrører en lovovertrædelse, der efter loven kan medføre fængsel i 1 år og 6 måneder eller derover.

… (stk. 3-8)

Derudover har politiet mulighed for at få **adgang til tv-overvågning, der foretages af private eller af offentlige myndigheder**.

Efter tv-overvågningsloven må **private** som udgangspunkt ikke foretage tv-overvågning af områder med almindelig færdsel.[28] Dette gælder dog ikke for en række virksomheder, der er i større risiko for kriminalitet, f.eks. tankstationer, pengeautomater, pengeinstitutvirksomheder, spillekasinoer, hotel- og restaurationsvirksomheder og butikker mv. De må gerne tv-overvåge egne indgange, bagindgange og facader og arealer der ligger i umiddelbar tilknytning til egne indgange og facader, når tv-overvågningen er klart nødvendig af hensyn til kriminalitetsbekæmpelse.[29]

Privates tv-overvågning uden billedoptagelse af egne indgange og facader og lignende er også tilladt, og der kan også udstedes tilladelse til tv-overvågning, hvis det er nødvendigt af hensyn til kriminalitetsbekæmpelsen.[30]

Boligorganisationer mv. og ejere af idrætsanlæg kan med politiets tilladelse foretage tv-overvågning af visse områder, der benyttes til almindelig færdsel, med henblik på kriminalitetsbekæmpelse.[31]

[28] Tv-overvågningslovens §. 1, stk. 1.
[29] Tv-overvågningslovens § 2. se også Tv-overvågning (datatilsynet.dk)
[30] Tv-overvågningslovens § 2, stk. 1, nr. 4 og 5, jf. § 2, stk. 6.
[31] Tv-overvågningslovens § 2, stk. 2

Offentlige myndigheder, herunder kommuner, må foretage tv-overvågning af egne indgange, bagindgange og facader og må tv-overvåge arealer, som ligger i umiddelbar tilknytning til egne bygningers indgange og facader, når tv-overvågningen er klart nødvendig af hensyn til kriminalitetsbekæmpelse.[32] Politiet kan også give et pålæg til myndigheden om at tv-overvåge.[33]

Kommunerne kan desuden for at fremme trygheden tv-overvåge gade, vej plads eller lignende område, som benyttes til almindelig færdsel, og ligger i umiddelbar tilknytning til en restaurationsvirksomhed.[34] Der er endvidere en bemyndigelse i loven, der har et tryghedsskabende sigte, hvorefter kommunerne kan få tilladelse til at foretage tv-overvågning af gade, vej, plads eller lignende område, som benyttes til almindelig færdsel. [35]

Private virksomheder, offentlige myndigheder, foreninger mv. har pligt til at lade sig registrere i **Politiets Kameraregister over tv-overvågningskameraer (POLCAM)** samt indberette eventuelle væsentlige ændringer.[36] Baggrunden for indførelsen af registrering i POLCAM var Rigspolitiets evaluering af den politimæssige indsats efter terrorangrebene i København den 14.-15. februar 2015, der bl.a. viste, at videooptagelser fra en lang række private tv-overvågningskameraer var afgørende for, at politiet kunne finde og pågribe gerningsmanden. Politiet måtte imidlertid bruge ekstraordinære ressourcer på bl.a. at lokalisere, hvor der var opsat kameraer, da der ikke fandtes et centralt register over private tv-overvågningskameraer.[37]

Der er efter tv-overvågningsloven krav om **skiltning** eller på anden måde synliggørelse af tv-overvågning, hvor der er almindelig adgang.[38]

[32] Tv-overvågningslovens § 2d.
[33] Tv-overvågningslovens § 2d
[34] Tv-overvågningslovens § 2 c, stk. 1. Se også Lov 2020-06-09 nr. 802 om ændring af lov om TV-overvågning. Se også lovforslaget LFF 2020-02-05 nr. 102 om ændring af TV-overvågningsloven (Styrkelse af trygheden og sikkerheden, herunder udvidelse af adgangen til tv-overvågning for private og offentlige myndigheder samt obligatorisk registrering af tv-overvågning) for overvejelserne bag lovændringen.
[35] Tv-overvågningslovens § 2 c, stk. 3.
[36] Jf. Tv-overvågningslovens § 2e, som trådte i kraft den 1. juli 2021, jf. bekendtgørelse 2021-05-28 nr. 1060 om ikrafttræden af § 1, nr. 10, i lov om ændring af lov om tv-overvågning (Styrkelse af trygheden og sikkerheden, herunder udvidelse af adgangen til tv-overvågning for private og offentlige myndigheder samt obligatorisk registrering af tv-overvågning). Se også lov 2020-06-09 nr. 802 om ændring af lov om tv-overvågning og lovforslaget LFF 2020-02-05 nr. 102 om ændring af tv-overvågningsloven (Styrkelse af trygheden og sikkerheden, herunder udvidelse af adgangen til tv-overvågning for private og offentlige myndigheder samt obligatorisk registrering af tv-overvågning) for overvejelserne bag lovændringen punkt 2.1.2.1.
[37] Bemærkningerne i punkt 2.4.2.1. i LFF 2020-02-05 nr. 102 om ændring af tv-overvågningsloven (Styrkelse af trygheden og sikkerheden, herunder udvidelse af adgangen til tv-overvågning for private og offentlige myndigheder samt obligatorisk registrering af tv-overvågning).
[38] Tv-overvågningslovens §§ 3 og 3a. Det er databeskyttelsesforordningen og databeskyttelseslovens regler om oplysningspligt overfor den registrerede. der gælder for hhv. private og offentlige myndigheder.

Billed- og lydoptagelser med personoplysninger, der optages i forbindelse med tv-overvågning, kan **videregives til politiet**, hvis videregivelsen sker i kriminalitetsopklarende øjemed.[39] Det er også muligt at opbevare optagelser i længere tid end de 30 dage, der normalt gælder for sletning, når opbevaringen er nødvendig på grund af en politianmeldelse om strafbare forhold.[40]

Politiet kan også få adgang til tv-overvågning, der foretages af private eller offentlige myndigheder, efter retsplejelovens regler om **beslaglæggelse og edition**.[41]

Desuden kan politiet efter reglerne i retsplejelovens § 791 e i visse tilfælde **overtage tv-overvågning**, der foretages af andre myndigheder eller private i et område, hvis der er afgørende grunde til det med henblik på at forebygge eller efterforske en lovovertrædelse, der efter loven kan straffes med fængsel i 6 år eller derover, eller som udgør en forsætlig overtrædelse af straffelovens kapitel 12 om landsforræderi og andre forbrydelser mod statens selvstændighed og sikkerhed eller kapitel 13 om forbrydelser mod statsforfatningen og de øverste statsmyndigheder, terrorisme m.v., og som kan medføre eller har medført fare for menneskers liv eller velfærd eller for betydelige samfundsværdier.[42] Politiets overtagelse af tv-overvågning er således underlagt strengere betingelser end edition, idet der bl.a. er et skærpet krav til grovheden af den kriminalitet, som politiet skal forebygge eller efterforske via den pågældende tv-overvågning.[43]

§

Retsplejelovens § 791 e

Stk. 1. Politiet kan fra andre myndigheder eller private overtage tv-overvågning i et område, hvis der er afgørende grunde til det med henblik på at forebygge eller efterforske en lovovertrædelse, der efter loven kan straffes med fængsel i 6 år eller derover eller udgør en forsætlig overtrædelse af straffelovens kapitel 12 eller 13, og som kan medføre eller har medført fare for menneskers liv eller velfærd eller for betydelige samfundsværdier. Det gælder dog ikke tv-overvågning i private hjem.

Stk. 2. Indgreb som nævnt i stk. 1 må ikke foretages, hvis det efter indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages at forvolde den eller de personer, som indgrebet rammer, ville være et uforholdsmæssigt indgreb.

Stk. 3. Indgreb efter stk. 1 sker efter rettens kendelse. I kendelsen anføres det område, som indgrebet angår, og de konkrete omstændigheder i sagen, hvorpå det

[39] Tv-overvågningslovens § 4 c, stk. 1, nr. 3.
[40] Tv-overvågningslovens § 4 c, stk. 5
[41] Retsplejelovens kap. 74, §§ 801, 803-807 og 807e.
[42] Retsplejelovens § 791e.
[43] Retsplejelovens § 791e, stk. 1 sammenholdt med § 804, stk. 1.

støttes, at betingelserne for indgrebet er opfyldt. Kendelsen kan til enhver tid omgøres. Endvidere fastsættes det tidsrum, inden for hvilket indgrebet kan foretages. Tidsrummet kan forlænges. Forlængelsen sker ved kendelse.

Stk. 4. Hvis indgrebets øjemed ville forspildes, dersom retskendelse skulle afventes, kan politiet træffe beslutning om at foretage indgrebet. I så fald skal politiet snarest muligt og senest inden 24 timer fra indgrebets iværksættelse forelægge sagen for retten. Retten afgør ved kendelse, om indgrebet kan godkendes, og om det kan opretholdes, og i bekræftende fald for hvilket tidsrum, jf. stk. 3, 2. og 4.-6. pkt. Burde indgrebet efter rettens opfattelse ikke have været foretaget, skal retten give meddelelse herom til Rigsadvokaten. Indgreb, der efter rettens opfattelse ikke burde være foretaget af Politiets Efterretningstjeneste, indberettes til Justitsministeriet.

... (stk. 5-9)

I november 2023 blev den **politiske aftale om bandepakke IV** vedtaget. Det fremgår bl.a. af aftalen under "Fokusområde 5: Flere og bedre værktøjer til myndighederne", at banderne med tidligere bandepakker var blevet presset, men at den organiserede kriminalitet udviklede sig hurtigt, og at der derfor var behov for at give politiet flere og bedre værktøjer. Videre fremgår det, at "aftalepartierne noterer sig i den forbindelse, at politiet er i gang med et forsøg med digitaliseret offergenkendelse i sager om seksuelt misbrug af børn, og aftalepartierne ser frem til at følge erfaringerne i forhold til, om det er et værktøj, der vil kunne bruges f.eks. i indsatsen mod banderne." Det blev desuden aftalt, at der skal ske en "udvidelse af afstandskravet for tv-overvågning fra ca. 30 meter til ca. 100 meter."[44]

5 EU-forordning om kunstig intelligens

I 2018 tilkendegav **Europa-Kommissionen** et ønske om en koordineret tilgang til kunstig intelligens indenfor EU og skitserede et europæisk initiativ hertil.[45] Der blev herefter bl.a. etableret en EU-ekspertgruppe på området (EU's Ekspertgruppe på Højt Niveau om Kunstig Intelligens), Europa-Kommissionen udgav Hvidbog om kunstig intelligens, og Europa-Kommissionen offentliggjorde den 21. april 2021 sin **"AI-pakke"**,[46] der bl.a. indeholdt et forslag til forordning om harmoniserende regler for kunstig intelligens.[47] Her fastsættes bl.a. en definition af højrisikosystemer, som er systemer, der indebærer en betydelig risiko for menneskers sundhed og sikkerhed eller grundlæggende rettigheder. Det gælder eksempelvis systemer til biometrisk fjernidentifikation, en række systemer beregnet

[44] Aftale om bandepakke IV – Trygge nabolag i hele Danmark (justitsministeriet.dk), side 6.
[45] Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget, Kunstig intelligens for Europa, KOM(2018) 237 final, 25. april 2018.
[46] A European approach to Artificial intelligence | Shaping Europe's digital future (europa.eu)
[47] Forslag til Europa-Parlamentets og Rådets forordning om harmoniserende regler for kunstig intelligens (retsakten om kunstig intelligens) og om ændring af visse af unionens lovgivningsmæssige retsakter, COM(2021) 206 final, 21.04.21.

til anvendelse i retshåndhævelsesmæssig sammenhæng, systemer til migrationsstyring, asylforvaltning og grænsekontrol samt visse systemer inden for retspleje.[48]

Det Europæiske Databeskyttelsesråd ("EDPB"), som er et uafhængigt EU-organ, der skal sikre en ensartet anvendelse af databeskyttelsesforordningen og retshåndhævelsesdirektivet i hele EU, og **Den Europæiske Tilsynsførende for Databeskyttelse ("EDPS")**, som EU's uafhængige databeskyttelsesmyndighed, har i forlængelse af offentliggørelsen af Europa-Kommissionens AI-pakke den 21. juni 2021 udtrykt sig uenige i væsentlige dele af forordningsforslaget og bl.a. udtalt følgende:

> *"Biometrisk fjernidentifikation af enkeltpersoner på offentlige steder udgør en høj risiko for krænkelse af enkeltpersoners privatliv med alvorlige følger for befolkningernes forventning om at være anonyme i det offentlige rum. Af disse grunde opfordrer Databeskyttelsesrådet og EDPS til, at der indføres et generelt forbud mod enhver anvendelse af kunstig intelligens til automatisk genkendelse af menneskelige træk på offentlige steder – såsom af ansigter, men også af gangart, fingeraftryk, DNA, stemme, tastetryk og andre biometriske eller adfærdsmæssige signaler – i enhver sammenhæng."* [49]

EDPB og EDPS anbefaler således et totalforbud mod bl.a. anvendelse af automatisk ansigtsgenkendelse i det offentlige rum, og to af medlemmerne har i den forbindelse udtalt, at metoder såsom ansigtsgenkendelse i realtid griber ind i grundlæggende rettigheder i en sådan grad, at selve essensen i disse rettigheder sættes på spil.[50]

Den 12. maj 2022 vedtog EDPB en vejledning om brugen af ansigtsgenkendelse for retshåndhævende myndigheder, som skærper kriterierne for brug af ansigtskendelsesteknologi.[51] EDPB understreger i vejledningen, at ansigtsgenkendelsesværktøjer kun bør anvendes i nøje overensstemmelse med retshåndhævelsesdirektivet. Desuden bør sådanne værktøjer kun anvendes, hvis det er nødvendigt og forholdsmæssigt, som fastsat i Den Europæiske Unions Charter om Grundlæggende Rettigheder (herefter nævnt "Chartret") artikel 52.

EDPB påpeger i vejledningen, at en national lovregel, der implementerer generalklausulen i retshåndhævelsesdirektivets artikel 10, ikke kan anvendes som lovgrundlag for brug af ansigtsgenkendelsesteknologi.[52] Reglen i artikel 10 omhandler retshåndhævende myndigheders behandling af særlige

[48] Det oprindelig forslag til AI-forordningen, betragtning, 38, 39 og 40 og art. 6, stk. 2, jf. bilag III, punkt 1, 6, 7 og 8.
[49] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down 17ecember17d rules on artificial intelligence (Artificial Intelligence Act), s. 2-3. Tilgængelig her.
[50] EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination | European Data Protection Board (europa.eu).
[51] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Tilgængelig her.
[52] Ibid., s. 18.

kategorier af personoplysninger, herunder biometrisk data. Kravet i Chartrets artikel 52 om et klart lovgrundlag nødvendiggør, at der vedtages lovgivning, der specifikt bemyndiger retshåndhævende myndigheder til at anvende ansigtsgenkendelsesteknologi. Denne lovregel skal angive, i hvilke tilfælde, hvordan og i hvilket omfang teknologien kan anvendes.[53]

Endvidere tydeliggør vejledningen, at en person ikke har gjort biometrisk data åbenlyst offentligt ("manifestly public"), hvis vedkommende blot har lagt et billede med sit ansigt på internettet.[54] Det sker kun i tilfælde, hvor vedkommende har offentliggjort selve den biometriske skabelon ("template") til brug for ansigtsgenkendelse, der kan udledes af et billede. Selve det at skabe en biometrisk skabelon er også databehandling.

Ifølge vejledningen bør retshåndhævende myndigheder udføre en konsekvensanalyse vedrørende databeskyttelse forud for anvendelse af ansigtsgenkendelsesteknologi. Fordi ansigtsgenkendelse i de fleste tilfælde i sig selv indebærer en høj risiko for de registreredes rettigheder, bør myndigheden, udover konsekvensanalysen, høre den kompetente tilsynsmyndighed, inden systemet tages i brug.[55] Desuden skal myndigheden være meget opmærksom på sikkerheden grundet følsomheden af dataene. De biometriske datas unikke karakter gør det umuligt for den registrerede at ændre dem, hvis de bliver kompromitteret, f.eks. som følge af et databrud. Den retshåndhævende myndighed bør navnlig sikre, at systemet lever op til de relevante standarder og gennemføre stærke sikkerhedsforanstaltninger til beskyttelse af biometriske templates.

I vejledningen fornyede EDPB således sin opfordring til et forbud mod ansigtsgenkendelse i visse situationer, da biometrisk identifikation i realtid i det offentlige rum indebærer masseovervågning, som udgør et stort indgreb i retten til privatliv og derfor ikke bør finde sted i et demokratisk samfund.[56] AI-understøttet ansigtsgenkendelse, der kategoriserer enkeltpersoner på grundlag af etnicitet, køn samt politisk eller seksuel orientering, er ligeledes ikke foreneligt med Chartret.[57] EDPB anbefalede endvidere, at brugen af ansigtsgenkendelse til at udlede følelser hos fysiske personer forbydes, eventuelt med få begrundede undtagelser. Desuden anførte EDPB, at behandling af personoplysninger i en retshåndhævelsessammenhæng, som er baseret på en database skabt til indsamling af personoplysninger i massevis og på en vilkårlig måde, ikke vil opfylde kravet om streng nødvendighed i henhold til EU-retten.[58]

[53] Ibid.
[54] Ibid., s. 19.
[55] Ibid., s. 24.
[56] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), s. 2-3. Tilgængelig her.
[57] Ibid.
[58] European Data Protecion Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, s. 26.

Den 13. marts 2024 blev forordningsteksten vedtaget af Europa-Parlamentets plenarsamling.[59] Ministerrådet forventes nu formelt at godkende den endelige forordningstekst i april 2024, hvorefter dele af forordningen vil træde i kraft allerede primo 2025.[60]

Med udgangspunkt i den tekst, som Europa-Parlamentet har stemt igennem (herefter nævnt "AI-forordningen"), er der opnået **enighed om at forbyde en række former for kunstig intelligens, der truer borgernes rettigheder**.[61] Det forbydes at anvende ikke-målrettet skrabning af ansigtsbilleder fra internettet eller CCTV-optagelser for at skabe ansigtsgenkendelsesdatabaser.[62] Det forbydes også at anvende følelsesgenkendelse på arbejdspladser og uddannelsesinstitutioner.[63] Desuden forbydes AI-systemer, der manipulerer menneskelig adfærd for at omgå deres frie vilje, og AI-systemer til at udnytte sårbarheder hos mennesker som følge af deres alder, handicap, sociale eller økonomiske situation.[64] Derudover forbydes offentlige myndigheders anvendelse af sociale pointsystemer, der evaluerer eller klassificerer fysiske personers troværdighed på grundlag af deres sociale adfærd i flere sammenhænge eller på grundlag af kendte eller forudsagte personlige egenskaber eller personlighedstræk.[65] Endelig forbydes biometriske kategoriseringssystemer, der bruger følsomme karakteristika som politiske, religiøse, filosofiske overbevisninger, seksuel orientering og race.

Anvendelse af biometrisk fjernidentifikation i realtid

Det anerkendes i AI-forordningens betragtning 32, at anvendelse af AI-systemer til biometrisk fjernidentifikation i realtid af fysiske personer i det offentligt rum med henblik på retshåndhævelse er særligt indgribende. Det skyldes, at politiets mulighed for realtidsovervågning kan påvirke privatlivet for en stor del af befolkningen, der bliver berørt af overvågningen, da det vil være egnet til at fremkalde en følelse af konstant overvågning og indirekte afskrække fra udøvelsen af forsamlingsfriheden og andre grundlæggende rettigheder. Ansigtsgenkendelse i realtid kan således få indflydelse på de berørte personers rettigheder og frihedsrettigheder. Desuden kan tekniske unøjagtigheder i AI-systemer, der er beregnet til biometrisk fjernidentifikation af fysiske personer, føre til forudindtagede resultater og have diskriminerende virkninger. Dette er særligt relevant, når det kommer til alder, etnicitet, race, køn eller handicap.

Det følger også af AI-forordningen, at anvendelsen af AI-systemer til ansigtsgenkendelse i realtid som udgangspunkt skal være forbudt, medmindre det anvendes helt undtagelsesvist og i snævert

[59] Europa-Parlamentets pressemeddelse. Artificial Intelligence Act: MEPs adopt landmark law. 13. marts 2024. Den endelige forordningstekst er tilgængelig her.
[60] Politico. European lawmakers rubber-stamp EU's AI rulebook. 13. marts 2024. Tilgængelig her.
[61] Ibid.
[62] Europa-Parlamentets pressemeddelse. Artificial Intelligence Act: MEPs adopt landmark law. 13. marts 2024. Den endelige forordningstekst er tilgængelig her.
[63] Ibid.
[64] Ibid.
[65] Ibid.

definerede situationer.[66] Politiets brug af ansigtsgenkendelse i realtid må kun finde anvendelse, når det er *strengt nødvendigt* for at opnå en væsentlig offentlig interesse, hvis betydning opvejer de risici, der er forbundet med brugen af teknologien.[67]

AI-forordningen giver ikke klare retningslinjer for, hvordan realtidsteknologien skal anvendes. Det fremgår dog af AIforordningens artikel 5, stk. 1, litra d, at anvendelse af teknologien i realtid til risikovurdering af en persons potentielle kriminelle adfærd baseret på personlige profiler eller personlighedstræk – også kaldet profilering – er forbudt.

Det fremgår desuden af artikel 5, stk. 1, litra h, at brugen af ansigtsgenkendelse i realtid på offentligt tilgængelige områder til håndhævelse af loven er forbudt, medmindre det er strengt nødvendigt for et af de angivne formål:

1) Ved målrettet eftersøgning af specifikke ofre for bortførelse, ved menneskehandel og seksuel udnyttelse af mennesker samt ved eftersøgning af forsvundne personer.
2) Forebyggelse af en specifik, væsentlig og overhængende trussel mod liv eller fysisk sikkerhed af fysiske personer eller ved en reel og umiddelbar eller reel og forudsigelig trussel om et terrorangreb.
3) Ved lokalisering eller identifikation af en person, der er mistænkt, er under efterforskning eller har været dømt for en lovovertrædelse, der er opført i AI-forordningens bilag IIa,[68] og som i medlemsstaten kan straffes med frihedsstraf i mindst 4 år.[69]

Det følger også af AI-forordningen, at der ved ansigtsgenkendelse i realtid skal indføres en række sikkerhedsforanstaltninger ved anvendelse af biometriske identifikationssystemer i det offentlige rum til retshåndhævelsesformål.[70] Dette indebærer forudgående godkendelse af en dommer eller af en uafhængig administrativ myndighed eller hurtigst muligt efter anvendelsen og senest inden for 24 timer.[71] Desuden skal medlemsstaterne i deres nationale ret fastsætte de nødvendige detaljeret

[66] AI-forordningens artikel 5.
[67] AI-forordningens artikel 5, stk. 1, litra h.
[68] AI-forordningens bilag II a opregner følgende alvorlige strafbare handlinger: terrorisme; menneskehandel, seksuel udnyttelse af børn og børnepornografi, ulovlig handel med narkotika og psykotrope stoffer, ulovlig handel med våben, ammunition og sprængstoffer, drab, alvorlig legemsbeskadigelse, ulovlig handel med menneskelige organer og menneskeligt væv, ulovlig handel med nukleare eller radioaktive materialer, kidnapning, ulovlig frihedsberøvelse og gidseltagning, inden for jurisdiktionen af Den Internationale Straffedomstol ulovlig beslaglæggelse af luftfartøjer/skibe, voldtægt, miljøkriminalitet, organiseret eller væbnet røveri, sabotage, deltagelse i en kriminel organisation, der er involveret i en eller flere af de anførte lovovertrædelser.
[69] Se også AI-forordningens betragtning 33.
[70] AI-forordningen artikel 5, stk. 3.
[71] Ibid.

regler for bl.a. tilsynet og indberetning af tilladelser til biometrisk fjernidentifikation i realtid på offentlige steder.[72]

AI-forordningen indeholder også krav om, at den retshåndhævende myndighed skal have gennemført en konsekvensanalyse af grundlæggende rettigheder, når der foretages biometrisk fjernidentifikation i realtid på offentlige steder.[73]

Anvendelse af biometrisk fjernidentifikation retrospektivt

Det følger af AI-forordningen, at myndigheders retrospektive anvendelse af ansigtsgenkendelse kun bør anvendes til formål, der er proportionelle, legitime og strengt nødvendige i forhold til de personer der overvåges, steder og tidsrammer.[74] Desuden må anvendelsen af teknologien aldrig bruges til overvågning af vilkårlige personer. Betingelserne for at bruge ansigtsgenkendelse retrospektivt må desuden ikke bruges til at omgå forbuddet og de strenge undtagelser for anvendelse af ansigtsgenkendelse i realtid.[75]

Det fremgår også af AI-forordningen, at når myndigheder anvender teknologien retrospektivt til at søge efter en person, der er dømt eller mistænkt for at have begået en kriminel handling, skal de indhente en retskendelse forudgående eller hurtigst muligt efter anvendelsen og senest inden for 48 timer.[76] Kravet gælder dog ikke, hvis teknologien anvendes til indledende identifikation af en potentiel mistænkt på grundlag af objektive og verificerbare kendsgerninger, der er direkte knyttet til overtrædelsen.[77]

Danmarks retsforbehold

Med det danske retsforbehold står Danmark i udgangspunktet uden for EU-samarbejdet om civilret, strafferet og politisamarbejde, hvilket giver Danmark frihed til at indføre national lovgivning på disse områder.[78] I en sådan situation kan Danmark dog også med et simpelt flertal i Folketinget vælge at vedtage at tilslutte sig en ny retsakt, kendt som en "tilvalgt retsakt".[79] Et dansk tilvalg vil være bindende og kan ikke trækkes tilbage. Danmark er dog ikke bundet af fremtidige ændringer til en tilvalgt

[72] AI-forordningens artikel 5, stk. 5.
[73] AI-forordningens artikel 5, stk. 2.
[74] AI-forordningens betragtning 95
[75] Ibid.
[76] AI-forordningens artikel 26, stk. 10.
[77] Ibid.
[78] Regeringen, 2015, Samarbejdet om retlige og indre anliggender: en analyse af EU-lovgivning omfattet af retsforbeholdet
[79] Danmark kan tilslutte sig et forslag, når det er fremsat, men ikke endeligt forhandlet. Dette skal ske inden for tre måneder efter, at Europa-Kommissionen har præsenteret forslaget. Danmarks repræsentanter deltager i forhandlingerne, vedtagelsen og afstemningerne i Ministerrådet. Uanset enighed i den endelige lovtekst forpligter Danmark sig til det ende-

retsakt og vil ikke være forpligtet til at acceptere ændringer. Desuden er Danmark ikke forpligtet af andre retsakter med tilknytning til den oprindelige tilvalgte retsakt.[80]

lige resultat. Alternativt kan Danmark vælge at afvente og først tage stilling, når Europa-Kommissionens forslag er endeligt vedtaget af både Europa-Parlamentet og Ministerrådet. Efter dette kan Danmark beslutte at tilslutte sig retsakten. Denne tilgang indebærer, at Danmark ikke deltager i forhandlingerne og beslutningsprocessen i Ministerrådet.
[80] Ibid.

6 Øvrige internationale tilkendegivelser

6.1 Europarådet

Europarådet har også fokus på at udvikle en juridisk ramme for brug af kunstig intelligens, som kan finde anvendelse på brug af ansigtsgenkendelse. Denne ramme kan som på mange andre områder, hvor EU og Europarådet ofte samarbejder om de samme værdier og principper, anses som et supplement til EU's regulering af kunstig intelligens. I 2019 blev der nedsat en ad hoc-komité for kunstig intelligens, **CAHAI**, som har til opgave at undersøge mulighederne og give sit bud på en international retlig ramme for kunstig intelligens, der lever op til Europarådets standarder for menneskerettigheder, demokrati og retssikkerhed.[81] Den juridiske ramme, som Europarådet kan tage i brug i den forbindelse, refereres som "retlig ramme for kunstig intelligens (AI)" og er baseret på Europarådets standarder for menneskerettigheder, demokrati og retsstatsprincippet. Derudover påpeges et behov for eventuelt at benytte eksisterende eller kommende juridisk bindende og/eller ikke-juridisk bindende instrumenter på sektorniveau. Dette sigter mod at levere mere detaljerede retningslinjer, der sikrer, at design, udvikling og implementering af AI sker i overensstemmelse med menneskerettigheder, demokrati og retsstatsprincippet inden for specifikke områder.

Den 17. december 2020 udgav CAHAI sin undersøgelse af den retlige ramme.[82] CAHAI fremhævede bl.a., at brug af kunstig intelligens, der kan forbedre og styrke beskyttelsen af menneskerettigheder, bør tilskyndes. De pegede bl.a. på, at hvis det konstateres, at anvendelsen af kunstig intelligens indebærer betydelige eller ukendte risici for menneskerettighederne, demokratiet eller retsstatsprincippet, og der ikke findes passende afbødningsforanstaltninger inden for de eksisterende retlige rammer, bør staterne overveje at indføre regulering eller andre restriktioner, og hvis nødvendigt, implementere et forbud eller et moratorium. Som eksempler på typer af kunstig intelligens der evt. bør forbydes, nævnes ansigtsgenkendelse i realtid, der kan medføre risiko for masseovervågning.[83]

CAHAI fremhævede, at der allerede eksisterer en vis regulering af området. Denne er imidlertid fragmenteret, og meget af det består af ikke-bindende instrumenter. Derfor skal et bindende juridisk instrument fra Europarådet, tage højde for den regulering, der allerede eksisterer, og forsøge at udfylde de lovgivningsmæssige tomrum.[84]

Som hovedelementer, der bør tages højde for i en juridisk ramme i regi af Europarådet, fremhævede CAHAI, at der bør opstilles krav om inddragelse af menneskeretlige overvejelser ved udvikling af AI-systemer. AI-udviklere og AI-anvendere skal etablere menneskelige tilsynsmekanismer og sikre til-

[81] CAHAI - Ad hoc Committee on Artificial Intelligence. Udvalgets opgavebeskrivelse og medlemmer kan ses her
[82] Feasibility study on a legal framework on AI design, development and application based on CoE standards, adopted by the CAHAI on 17 December 2020. Tilgængelig her.
[83] Ibid., s. 13.
[84] Ibid., s. 25.

strækkelig menneskelig involvering i anvendelsen. Desuden skal der ske behørig og rettidigt kommunikation om klagemuligheder.[85] Medlemsstaterne i Europarådet skal sikre, at AI-systemerne ikke resulterer i ulovlig diskrimination. Desuden skal de inddrage ikke-diskrimination i udbudsprocesser vedrørende AI-systemer.[86]

For at anvendelsen af et AI-system kan være i overensstemmelse med menneskerettighederne, fremhævede CAHAI, at gennemsigtighed er essentielt. Det er vigtigt at forstå, hvordan systemet foretager beslutninger og på hvilket grundlag, hvis der skal være mulighed for at klage over og omgøre en beslutning, der er foretaget af systemet. Derfor skal der på en forståelig måde informeres om, hvordan systemet tager beslutninger. Det er desuden vigtigt, at beslutningsprocesser logges og dokumenteres, så de senere kan gennemgås. Den person, der er genstand for en beslutning taget af et AI system, skal informeres herom. Dette indbefatter de juridiske konsekvenser ved beslutningen og en forklaring på, hvordan beslutningen er taget. Hvis det ikke er muligt at give en forklaring, er det vigtigt, at der føres tilsyn med systemet af en uafhængig myndighed.[87] Udviklere og anvendere af AI-systemer skal være ansvarlige for eventuelle fejl begået af systemet.[88]

Generelt fremhævede CAHAI, at medlemsstater effektivt bør beskytte individer mod AI-drevet masseovervågning, f.eks. i form af ansigtsgenkendelse, da dette ikke er i overensstemmelse med menneskerettighederne, demokratiet og retssikkerheden.[89] Endvidere skal en ny konvention, der regulerer området, ikke være for kategorisk, da der stadig er meget, som man ikke ved. En ny konvention skal derfor være tilstrækkelig fleksibel til at kunne tilpasse sig fremtiden.[90]

I december 2021 afsluttede CAHAI sit arbejde, hvilket mundede ud i en anbefaling til indholdet af en retlig ramme for AI.[91] For effektivt at afbøde risici for menneskerettighederne fandt CAHAI, at en retlig ramme baseret på Europarådets standarder for menneskerettigheder, demokrati og retsstatsprincippet bør have form af et juridisk bindende tværgående instrument.

Reguleringen bør tage udgangspunkt i en risikoklassificering af AI-systemer. Der bør være mulighed for at indføre et forbud mod anvendelse af AI-systemer, som i overensstemmelse med risikoklassificeringen anses for at udgøre en uacceptabel risiko for menneskerettighederne, demokratiets funktion og overholdelsen af retsstatsprincippet.[92] CAHAI fremhævede som eksempel på dette, AI-systemer, der anvender biometri til at identificere, kategorisere eller udlede personers karakteristika eller

[85] Ibid., s. 31.
[86] Ibid., s. 32.
[87] Ibid., s. 33-34.
[88] Ibid., s. 38.
[89] Ibid., s. 37.
[90] Ibid., s. 45.
[91] CAHAI - Possible elements of a legal framework on artificial intelligence, based on the Council of Europe's standards on human rights, democracy and the rule of law. Tilgængelig her.
[92] Ibid., para. 21.

følelser, navnlig hvis de fører til masseovervågning, og AI-systemer der anvendes til social scoring for at bestemme adgangen til væsentlige tjenester.

CAHAI foreslog at medtage en bestemmelse om respekt for ligebehandling og ikke-diskrimination i forbindelse med udvikling, udformning og anvendelse af AI-systemer for at undgå, at der indbygges uberettigede fordomme i AI-systemer.[93] CAHAI anbefalede, at der indføres bestemmelser om robusthed, sikkerhed og cybersikkerhed, gennemsigtighed, forklarbarhed, kontrollerbarhed og ansvarlighed.[94] Når det drejer sig om udvikling, udformning og anvendelse af AI-systemer i den offentlige sektor, bør der som minimum indføres bestemmelser om adgang til effektive retsmidler, obligatorisk ret til menneskelig prøvelse af beslutninger, en forpligtelse for offentlige myndigheder til at gennemføre passende menneskelig gennemgang af processer og til at give meningsfulde oplysninger om AI-systemers rolle i beslutninger.[95]

CAHAI anbefalede endvidere, at der oprettes offentlige registre med lister over AI-systemer, der anvendes i den offentlige sektor. Disse skal indeholde væsentlige oplysninger om systemet, f.eks. dets formål, involverede aktører, grundlæggende oplysninger om modellen og resultatmålinger, samt udfaldet af en menneskerettighedsvurdering af systemet udført af myndigheden.[96]

I juni 2021 udstedte Europarådets rådgivende udvalg under konventionen om beskyttelse af fysiske personer i forbindelse med elektronisk databehandling af personoplysninger (Konvention 108+) en vejledning specifikt om brug af ansigtsgenkendelsesteknologi.[97] Vejledningen adresserer især retten til databeskyttelse.

Vejledning angiver, at lovgivning, der autoriserer brug af ansigtsgenkendelsesteknologi, for hver enkelt anvendelse skal indeholde en detaljeret forklaring på den specifikke anvendelse og det tilsigtede formål, den anvendte algoritmes minimale pålidelighed og nøjagtighed, opbevaringstiden for de anvendte fotos, muligheden for at kontrollere disse kriterier, processens sporbarhed og sikkerhedsforanstaltningerne.[98] Som hovedregel skal samtykke ikke være det, man baserer lovgrundlaget for offentlige myndigheders brug af ansigtsgenkendelse på, i betragtning af magtbalancen mellem de registrerede og myndighederne.[99]

[93] Ibid., para. 27.
[94] Ibid., para. 30.
[95] Ibid., para. 34.
[96] Ibid., para. 61.
[97] Guidelines on facial recognition - Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data. Tilgængelig her.
[98] Ibid., s. 7.
[99] Ibid., s. 9-10.

CAHAI tilendebragte sit arbejde i 2021 og blev efterfulgt af endnu en mellemstatslig ekspertgruppe for kunstig intelligens (CAI).[100] **CAI** har til opgave at formulere et juridisk instrument om udvikling, design og anvendelse af kunstig intelligens systemer baseret på Europarådets standarder for menneskerettigheder, demokrati og retsstatsprincippet, og befordrende for innovation i overensstemmelse med de relevante afgørelser fra Ministerkomitéen.[101] Den 7. juli 2023 offentliggjorde CAI det konsoliderede udkast (Consolidated Working Draft), som er blevet udarbejdet med hjælp fra Europarådets Sekretariat på baggrund af CAIs første udkast (Zero Draft).[102]

Det konsoliderede udkast er endnu ikke endeligt, og der forhandles stadig internt i CAI om den endelige udgave. Udkastene har dog i store træk inkorporeret anbefalingerne fra CAHAI. Eksempelvis lægges der op til, at staterne skal sikre processuelle garantier ved brug af AI,[103] klagemuligheder,[104] ikke-diskrimination[105] og respekt for menneskerettigheder[106] ved både offentlig og privat brug af teknologien.

Mens CAHAIs undersøgelse førte til en anbefaling om at forbyde visse former for kunstig intelligens såsom ansigtsgenkendelse i realtid, lægger CAIs udkast ikke op til et forbud heraf.

6.2 FN

I en rapport om overvågning fra 2019[107] anbefalede FN's Menneskerettighedsråd, at staters køb af teknologi, der kan bruges til overvågning, bør være genstand for offentlig kontrol. Dette kan f.eks. ske ved involvering af relevante statslige organer, der foretager en vurdering af risiciene for menneskerettigheder forbundet med teknologien.[108]

FN's højkommissær for menneskerettigheder udgav i 2020 en rapport om nye teknologiers påvirkning af retten til forsamlingsfrihed.[109] I forbindelse med ansigtsgenkendelse blev det i rapporten anbefalet at indføre et midlertidigt forbud mod brug af ansigtsgenkendelse på forsamlinger.

[100] CAI - Committee on Artificial Intelligence.
[101] Ibid.
[102] Ibid.
[103] CAIs Consolidated Working Draft, Artikel 14.
[104] CAIs Consolidated Working Draft, Artikel 13.
[105] CAIs Consolidated Working Draft, Artikel 9.
[106] CAIs Consolidated Working Draft, Artikel 5.
[107] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression - Surveillance and human rights, Human Rights Council, A/HRC/41/35. Tilgængelig her.
[108] Ibid., para. 52.
[109] Report of the United Nations High Commissioner for Human Rights - Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, Human Rights Council, A/HRC/44/24. Tilgængelig her.

Det blev i rapporten anført, at ansigtsgenkendelse kun bør anvendes, når betingelserne for lovlighed, nødvendighed og proportionalitet er opfyldt. Det er tvivlsomt, om anvendelse af ansigtsgenkendelsesteknologi under fredelige protester nogensinde kan opfylde nødvendigheds- og proportionalitetskravet taget dets indgribende og alvorlige karakter i betragtning. Myndigheder bør helt generelt afholde sig fra at registrere deltagere i forsamlinger. En undtagelse hertil bør som følge af proportionalitetsprincippet kun overvejes, når der er konkret fare for, at der rent faktisk finder alvorlige strafbare handlinger sted, såsom vold eller brug af skydevåben. Eksisterende optagelser bør kun anvendes til identifikation af forsamlingsdeltagere, der er mistænkt for alvorlige forbrydelser.[110] Selvom brug af ansigtsgenkendelse på forsamlinger kraftigt frarådes, bør myndigheder, der alligevel anvender teknologien, kun gøre dette, når der er et klart lovgrundlag for det. Anvendelsen bør tage højde for de menneskeretlige og databeskyttelsesretlige krav.[111]

Desuden skal enhver brug af ansigtsgenkendelsesteknologi være underlagt robuste tilsynsmekanismer. En del af tilsynet kan udføres af uafhængige databeskyttelsesmyndigheder, men staterne bør overveje oprettelse af et uafhængigt organ, helst af retlig karakter, med ansvar for at godkende brugen af ansigtsgenkendelsesteknologi på forsamlinger. Myndighedernes anvendelse af ansigtsgenkendelsesteknologi skal være gennemsigtig og altid underrette offentligheden om, hvornår de bliver eller kan blive registreret, og/eller hvornår deres billeder kan blive behandlet i et ansigtsgenkendelsessystem. Enhver anvendelse af ansigtsgenkendelsesteknologi skal kunne anfægtes af domstolene.[112]

I 2021 udgav FN's højkommissær for menneskerettigheder en rapport om retten til privatliv i den digitale tidsalder.[113] Rapporten nævner, ligesom ovenstående rapport fra 2020 vedrørende forsamlingsfrihed, ansigtsgenkendelsesteknologiers negative indvirkning på retten til privatliv. Højkommissæren lægger i rapporten særligt vægt på, at brug af biometrisk fjernidentifikation i realtid udgør et særligt intensivt indgreb i retten til privatliv, og at brugen heraf giver anledning til alvorlige bekymringer i medfør af menneskeretten.[114] På den baggrund byder FN's højkommissær de seneste begrænsninger og forbud af ansigtsgenkendelse i realtid velkommen, og det anbefales, at stater indfører et moratorium på brugen af biometrisk fjernidentifikation i det offentlige rum, indtil anbefalingerne i rapporten fra 2020 er blevet implementeret.[115] Disse anbefalinger indbefatter, at teknologien

[110] Ibid., para. 35.
[111] Ibid., para. 36.
[112] Ibid., para. 37.
[113] The right to privacy in the digital age, A/HRC/48/31.
[114] Ibid., § 26.
[115] Ibid., § 27.

skal være i overensstemmelse med databeskyttelsesreglerne, trepartstesten, princippet om ikke-diskrimination og at teknologien skal være tilstrækkeligt præcis til at identificere de korrekte individer.[116]

Konklusionerne fra rapporterne i 2020 og 2021 blev gentaget og udvidet i 2022 i endnu en rapport fra FN's højkommissær for menneskerettigheder om retten til privatliv i den digitale tidsalder.[117] Navnlig blev det gentaget, at biometrisk fjernidentifikation kun bør benyttes i det offentlige rum, når den benyttes til at forhindre eller efterforske alvorlige forbrydelser eller alvorlige trusler mod den offentlige sikkerhed, og når alle kravene i den internationale menneskeret er opfyldt.[118]

[116] Ibid., § 59(d).
[117] The right to privacy in the digital age, A/HRC/51/17.
[118] Ibid., § 56, encryption (d).

7 Menneskeretlige overvejelser

Den Europæiske Menneskerettighedskonvention (EMRK) fra 1950 blev inkorporeret i dansk ret i 1992 (inkorporeringsloven), som forpligter Danmark til at overholde konventionen og dets tillægsprotokoller.[119] Hvis en borger mener, at staten har krænket de rettigheder, som vedkommende har i henhold til konventionen, er der adgang til at indgive klage til Den Europæiske Menneskerettighedsdomstol. Klageadgangen er underlagt en række betingelser, herunder at klageren skal have udtømt nationalstatens effektive, nationale retsmidler. [120]

Der findes en lang række konventioner i andre internationale organisationer, som størstedelen af landene i Europa hver især har skrevet under på. I sådanne tilfælde skal EU-lovgivningen på området leve op til konventionens bestemmelser, så medlemsstaterne ikke kommer i konflikt med deres internationale forpligtelser.

Alle lande i Europa, med undtagelse af Rusland og Belarus, har tiltrådt Den Europæiske Menneskerettighedskonvention, som betyder, at borgere kan få deres sag prøvet ved Den Europæiske Menneskerettighedsdomstol i Strasbourg, hvis deres grundlæggende rettigheder bliver krænket af staten eller EU-institutioner.[121]

EU's Charter om grundlæggende rettigheder (herefter nævnt "Chartret") indeholder en omfattende liste over grundlæggende rettigheder og friheder, som er bindende for EU-institutionerne og medlemsstaterne, når de udvikler og anvender EU-lovgivning.[122] Chartret dækker områder såsom menneskerettigheder, borgerlige og politiske rettigheder og sikrer beskyttelse af enkeltpersoners rettigheder inden for EU's retlige rammer.[123] Den blev vedtaget i 2000 og fik retlig status med Lissabontraktaten i 2009.[124] Danmark er desuden forpligtet til at overholde de FN-konventioner, som Danmark har tiltrådt. Danmark har tiltrådt seks konventioner om menneskerettigheder, der giver enkeltpersoner mulighed for at klage over Danmark til FN.[125]

7.1 Retten til privatliv

Ansigtsgenkendelsesteknologi indebærer en række menneskeretlige overvejelser, hvor navnlig retten til privatliv er central. Retten til privatliv bestræber sig bl.a. på at beskytte menneskets værdighed

[119] Lov nr. 285 af 29. april 1992 om Den Europæiske Menneskerettighedskonvention (se lovbekendtgørelse nr. 750 af 19. oktober 1998 for gældende version).
[120] Se mere her om klagemuligheder: Sådan klager du til FN og Den Europæiske Menneskerettighedsdomstol | Justitsministeriet
[121] Konventioner / Folketingets EU-Oplysning
[122] Kristoffersen (2014), EU's charter om grundlæggende rettigheder, DJØF forlag, s. 30
[123] Ibid.
[124] Ibid.
[125] Se her: Sådan klager du til FN og Den Europæiske Menneskerettighedsdomstol | Justitsministeriet

og autonomi, og respekten for denne rettighed er samtidig en forudsætning for udøvelsen af en række øvrige rettigheder, herunder ytringsfriheden, forsamlingsfriheden og retten til at tænke frit.

Privatliv er et bredt begreb, der udover individets generelle privatliv bl.a. omfatter fysisk, psykisk og moralsk integritet samt individets identitet og autonomi.[126] Retten omfatter de aspekter, der relaterer sig til et individs identitet, herunder vedkommendes billede.[127] Menneskets ansigt er et af de mest centrale og åbenbare karaktertræk, der gør det muligt at identificere og skelne mellem individer. Beskyttelse af individets eget billede er derfor en af de mest essentielle komponenter i forbindelse med personlig udvikling.[128] Indsamling, opbevaring og sammenligning af ansigtsbilleder udgør derfor et indgreb i retten til privatliv.

Den omstændighed, at et individ befinder sig i det offentlige rum, indebærer ikke, at beskyttelsen af vedkommendes privatliv ophører.[129] Den Europæiske Menneskerettighedsdomstol har anvendt begrebet en "rimelig forventning" om det at have privatliv i det offentlige rum uden at blive overvåget. Den blotte overvågning af offentlige områder, f.eks. med kameraer, som ikke lagrer de indfangede billeddata udgør ikke i sig selv et indgreb, da de overvågede må være indstillet på at kunne blive observeret under deres færden på offentlige steder. Derimod kan opbevaringen af billedmaterialet udgøre et indgreb pga. den systematiske og vedvarende karakter optagelserne får.[130]

AI-baserede sporingsteknikker kan anvendes på en måde, der i vid udstrækning kan gøre indgreb i et individs privatliv, og som gør det muligt konstant at masseovervåge, følge, identificere og påvirke enkeltpersoner og dermed også påvirke deres moralske og psykologiske integritet.[131]

Ansigtsgenkendelse kan således virke adfærdsændrende, hvilket indebærer risiko for alvorlige konsekvenser for individets integritet, identitet og autonomi, og teknologien rejser i det hele taget spørgsmål om magtbalancen mellem stat og borger. Retten til privatliv indebærer en ret til et privat rum uden AI-baseret overvågning, hvilket er en forudsætning for personlig udvikling og demokrati.[132]

---

[126] Se f.eks. Den Europæiske Menneskerettighedsdomstol, Guide on Article 8 of the European Convention on Human Rights, opdateret den 31. august 2022. Tilgængelig her.
[127] Se f.eks. Den Europæiske Menneskerettighedsdomstol, Lopez Ribalda m.fl. mod Spanien, præmis 87.
[128] Se f.eks. Den Europæiske Menneskerettighedsdomstol, Guide on Article 8 of the European Convention on Human Rights, opdateret den 31. august 2022, pkt. 176, Den Europæiske Menneskerettighedsdomstol, Lopez Ribalda m.fl. mod Spanien, præmis 87-91 og rapport fra FN's højkommissær for menneskerettigheder (OHCHR) "Impact of new technologies on the promotion of human rights in the context of assemblies, including peaceful protests" (UN Doc A /HRC/44/24), 24. juli 2020 præmis 33.
[129] Se f.eks. Den Europæiske Menneskerettighedsdomstol, Lopez Ribalda m.fl. mod Spanien, præmis 88.
[130] EMD: Perry 17/7 2003 pr. 38 og Peck 28/1 2003 pr. 59 samt Den Europæiske Menneskerettighedskonvention med kommentarer af Peer Lorenzen m.fl., 2011, Djøf Forlag, side 652
[131] European Union Agency for Fundamental Rights, Facial recognition technology: Fundamental rights considerations in the context of law enforcement, April 2019, side 23.
[132] CAHAI, Feasibility Study, 17. december 2020, afsnit 3.3.1, pkt. 25.

Efter EMRK artikel 8 skal ethvert indgreb i privatlivet være i overensstemmelse med loven. Dette krav stiller også betingelser til lovens kvalitet, herunder at loven skal være i overensstemmelse med retsstatsprincippet ("rule of law").[133] Den nationale lov skal have klare og detaljerede regler samt være forudsigelig og tilgængelig. Ligeledes stiller Chartrets artikel 7 krav om, at enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation. Chartrets artikel 8 bestemmer, at enhver har ret til beskyttelse af sine personoplysninger. Det er også efter denne bestemmelse, at beskyttelsen af personoplysninger skal være underlagt en uafhængig myndighedskontrol.[134] Efter Chartrets artikel 51, stk. 1, finder Chartrets bestemmelser dog kun anvendelse, når medlemsstaterne handler inden for rammerne af EU-retten. EU-Domstolen har som følge heraf fastslået, at Chartret finder anvendelse, når national lovgivning falder ind under EU-rettens anvendelsesområde, jf. bl.a. sag C-617/10 Hans Åkerberg Fransson.

EU-Domstolen har Justitia bekendt ikke behandlet spørgsmål om anvendelse af ansigtsgenkendelse. Dog har både EU-Domstolen[135] og EMD[136] fastslået, at ansigtsbilleder udgør personoplysninger. I de forenede sager C-293/12 og C-594/12 om logningsdirektivet i forhold til lovforslag om Center for Cybersikkerhed fra april 2014 forholdt EU-Domstolen sig ikke til, om staten har ret til at gøre indgreb i borgeres ret til privatliv, når det handler om at bekæmpe alvorlig kriminalitet – heller ikke gennem logning. Den understregede imidlertid, at dette altid skal være begrænset til det strengt nødvendige. Der skal således være et rimeligt forhold mellem dataindsamlingen og den konkrete anvendelse. EMD har også udtalt, at en persons ansigtsbillede udgør grundlæggende elementer i personers personlighed, da det viser personens unikke karakteristika og adskiller personen fra andre personer. Retten til beskyttelse af ansigtsbillede er derfor en af de væsentlige komponenter i personlig udvikling.[137]

Efter EMRK skal masseovervågning i realtid have klar lovhjemmel, der angiver de betingelser og omstændigheder, der kan give myndighederne mulighed for at iværksætte indgrebet. Indgrebet indebærer imidlertid, at personer, der bliver overvåget, ikke nødvendigvis ved, at det sker og derfor ikke kan forudsige det og tilpasse sin adfærd derefter. Loven skal derfor indeholde minimumsforanstaltninger for at imødegå magtmisbrug. Loven skal angive, hvilke former for lovovertrædelser der kan give anledning til overvågning, og de kategorier af personer der kan undergives overvågning, en

[133] Den Europæiske Menneskerettighedsdomstol, Guide on Article 8 of the European Convention on Human Rights, opdateret den 31. august 2022, s. 10.
[134] EU's Charter om Grundlæggende Rettigheder artikel 8, stk. 3.
[135] C-291/12, M. Schwarz v. Stadt Bochum, 17 October 2013, paras. 22, 48-49.
[136] Szabó and Vissy mod Ungarn, No. 37138/14, 12 January 2016, para. 56
[137] ECtHR, Guide on Article 8 of the European Convention on Human Rights Right to respect for private and family life, home and correspondence, Strasbourg, Council of Europe, 31 August 2019, para. 138

tidsmæssig begrænsning af overvågningen, processer for at vurdere, anvende og opbevare biometrisk data, forholdsregler i forhold til at overføre data til andre parter, og hvornår data skal slettes.[138]

I sagen *Glukhin* mod Den Russiske Føderation fra 2023 blev Konstantin Kotov i 2019 anholdt for at protestere uden forudgående tilladelse, hvilket var i strid med russisk lovgivning. Der blev i forbindelse med identifikationen og anholdelse af den pågældende anvendt tv-overvågning og ansigtsgenkendelsesteknologi i realtid, og spørgsmålet var, om denne brug af ansigtsgenkendelsesteknologi var i strid med EMRK. I forhold til legalitetskravet fandt EMD, at den russiske lovhjemmel næppe opfyldte legalitetskravet, da reglen om brug af ansigtsgenkendelse var for bredt formuleret.[139] Den russiske lovhjemmel tillod behandling af biometriske personoplysninger – herunder ved hjælp af ansigtsgenkendelsesteknologi – i forbindelse med enhver retssag ("in connection with any judicial proceedings"). EMD bemærkede, at der i den russiske lov ikke var angivet nogen grænser for brug af ansigtsgenkendelse, eller hvilke formål der kunne legitimere anvendelsen, kategorier af personer eller behandlingen af følsom persondata.[140] EMD fremhævede, at ansigtsgenkendelse, og særligt brug af ansigtsgenkendelsesteknologi i realtid, stiller skærpede krav til hjemmelsgrundlaget.[141] Navnlig er det ved implementering af ansigtsgenkendelsesteknologi afgørende at have detaljerede regler, der regulerer omfanget og anvendelsen af teknologien samt stærke sikkerhedsforanstaltninger mod risiko for misbrug og vilkårlighed.[142] EMD gik imidlertid ikke mere i dybden med, hvad reglerne for anvendelse af ansigtsgenkendelse burde indeholde.

Et andet krav til masseovervågning i realtid er, at indgrebet er nødvendigt i et demokratisk samfund. Hvis indgrebet blot er "anvendeligt", "rimeligt" eller "ønskværdigt", opfylder det ikke kravet om at være nødvendigt i et demokratisk samfund. Der skal eksistere et "presserende socialt behov" for indgrebet. Desuden skal indgrebet forfølge et legitimt mål og være proportionalt i forhold til det mål, der søges opnået med indgrebet. [143]

I *Gaughran* mod Det Forenede Kongerige skulle EMD tage stilling til, om det udgjorde et indgreb, at klagerens fotografi blev taget ved hans anholdelse og derefter opbevaret på ubestemt tid i politiets lokale database, der anvendte teknikker til ansigtsgenkendelse på det.[144] EMD fandt, at det at tage, opbevare og anvende teknikker til ansigtsgenkendelse på klagerens fotografi udgjorde et indgreb i retten til eget billede efter EMRK artikel 8. EMD fandt videre, at indgrebet ikke var nødvendigt i et

[138] Den Europæiske Menneskerettighedsdomstol, Guide on Article 8 of the European Convention on Human Rights, opdateret den 31. august 2022, s. 143.
[139] Se Den Europæiske Menneskerettighedsdomstol, *Glukhin* mod Den Russiske Føderation, præmis 83.
[140] Ibid, præmis 83.
[141] Ibid, præmis 82.
[142] Ibid., præmis 82.
[143] Ibid., s. 12.
[144] Se Den Europæiske Menneskerettighedsdomstol, *Gaughran* mod Det Forenede Kongerige, præmis 70.

demokratisk samfund.[145] EMD har understreget, at enhver brug af videooptagelser eller andet fotografisk materiale, der anvendes af politiet, skal have klar lovhjemmel, navnlig hvis politiet anvender materialet til andre formål end det formål, som materialet oprindeligt blev indsamlet til.[146]

I den ovenfor nævnte sag *Glukhin* mod Den Russiske Føderation fastslog EMD også, at ikke alle lovovertrædelser kan danne grundlag for brug af ansigtsgenkendelsesteknologi. EMD undlod at udtale sig generelt om, hvorvidt og i hvilke tilfælde ansigtsgenkendelse er i overensstemmelse med eller i strid med EMRK. I den konkrete sag fandt EMD dog enstemmigt, at det russiske politis brug af ansigtsgenkendelse i forbindelse med anholdelsen af Konsantin Kotov var i strid med EMRK artikel 8, da indgrebet ikke kunne anses som nødvendigt i et demokratisk samfund.[147] Dette skyldtes, at Konstantin Kotov udelukkende havde begået en mindre administrativ lovovertrædelse ved ikke at have fået forhåndsgodkendt sin ret til at demonstrere ifølge russisk lov.[148] Det, at Konstantin Kotov blev straffet for et mindre forhold ved ikke at søge om forudgående tilladelse til alene og fredeligt at demonstrere i Moskvas undergrund, var allerede fundet i strid med ytringsfriheden efter EMRK artikel 10, hvilket formentligt også har haft en indflydelse på EMDs vurdering af brugen af ansigtsgenkendelse efter EMRK artikel 8.[149] I forhold til anvendelse af ansigtsgenkendelsesteknologi generelt holdt EMD sig alene til at nævne, at EMD anerkender vigtigheden af teknologien i forbindelse med opklaring af organiseret kriminalitet og terrorisme, men undlod at kommentere på, hvorvidt anvendelse af ansigtsgenkendelsesteknologi generelt er i overensstemmelse med eller i strid med EMRK.[150]

Landene har en vis skønsmargin, når balancen mellem at beskytte den nationale sikkerhed afvejes over for indgreb i privatlivet. Der skal imidlertid være tilstrækkelige foranstaltninger til at beskytte mod misbrug. I vurderingen inddrager EMD de specifikke omstændigheder, herunder arten, omfanget og varigheden af de mulige metoder til at opnå målet, de årsager der kræves for at anvende dem, hvilke myndigheder der har kompetence til at autorisere, udføre og supervisere, samt hvilke retsmidler der er tilgængelige.

Det må på denne baggrund antages, at EMDs vurdering af, om politiets anvendelse af ansigtsgenkendelse i realtid i det offentlige rum er lovlig, vil være en meget konkret vurdering af, om der er en tilstrækkelig klar lovhjemmel, og om brugen samlet set har forfulgt et legitimt formål samt har været nødvendig og proportional. Det følger af proportionalitetsprincippet, at jo mere intensivt indgrebet er, jo mere tungtvejende grunde skal der være for at iværksætte indgrebet. Der vil også blive lagt

[145] Ibid., præmis 97.
[146] Se Den Europæiske Menneskerettighedsdomstol, *Peck* mod Det Forenede Kongerige, præmis 61-61 og Den Europæiske Menneskerettighedsdomstol, *Perry* mod Det Forenede Kongerige, præmis 47-48.
[147] Se Den Europæiske Menneskerettighedsdomstol, *Glukhin* mod Den Russiske Føderation, præmis 89-91.
[148] Ibid., præmis 88.
[149] Ibid., præmis 88.
[150] Ibid., præmis 8.

vægt på, om de berørte borgere efterfølgende får opfyldt de fornødne retssikkerhedsmæssige garantier. EMD har også slået fast, at statens hemmelige overvågning som udgangspunkt skal være strengt nødvendig og bør være underlagt domstolskontrol eller anden effektiv kontrol for at være i overensstemmelse med EMRK artikel 8. Iværksættelse og anvendelse af hemmelig overvågning skal derfor være underlagt kontrol/eftersyn. Dette kan gøres af en dommer, men kan det også være tilstrækkeligt med en anden tilsynsenhed, så længe den er uafhængig af de myndigheder, der udfører overvågningen, og har tilstrækkelig magt og kompetencer. [151]

7.2 Øvrige rettigheder og principper

Ansigtsgenkendelse indebærer behandling af store mængder persondata og forudsætter derfor også omfattende og grundige overvejelser vedrørende **retten til beskyttelse af personoplysninger**.[152]

Et andet område, der har fået en del opmærksomhed i forbindelse med ansigtsgenkendelse, er **retten til ikke at blive diskrimineret**.[153] Diskriminationen kan bl.a. opstå som konsekvens af de valg, der træffes i forbindelse med design, testning og implementering af algoritmerne, på grund af forudindtagethed, der bevidst eller ubevidst kan være inkorporeret i selve algoritmen og via de beslutninger, som mennesker træffer på baggrund af et ansigtsmatch.

Overordnet set er datakvaliteten også afgørende for, om der sker diskrimination. F.eks. er der i flere tilfælde konstateret en betydelig større fejlmargin ved anvendelse af ansigtsgenkendelse på farvede kvinder, fordi hvide mænd ofte har været overrepræsenteret i de anvendte datasæt.[154]

Også **ytringsfriheden**[155] og **forsamlingsfriheden**[156] er centrale rettigheder i forbindelse med ansigtsgenkendelse. Et nødvendigt aspekt af ytringsfriheden er gruppeanonymitet. Ansigtsgenkendelse er egnet til at forhindre denne form for anonymitet, fordi teknologien kan identificere og registrere enkeltindivider selv i store menneskemængder.

Bevidsthed om, at man er under konstant overvågning, er desuden egnet til at virke adfærdsændrende. Dette gælder så meget desto mere, hvis overvågningen indebærer ansigtsgenkendelse. Der opstår i den forbindelse navnlig risiko for, at individer ikke tør ytre sig eller deltage i ellers lovlige demonstrationer i samme grad som ellers. Sådanne konsekvenser udgør alvorlige barrierer for et

[151] Den Europæiske Menneskerettighedsdomstol, Guide on Article 8 of the European Concention on Human Rights, opdateret den 31. August 2022, s. 143
[152] EU-Chartrets art. 8 og EMRK art. 8.
[153] EU-Chartrets art. 21, EMRK art. 14 og art. 12 i protokol nr. 12 til EMRK.
[154] Se også European Union Agency for Fundamental Rights, Facial recognition technology: Fundamental rights considerations in the context of law enforcement, April 2019, pkt. 7.2 og CAHAI, Feasibility Study, 17. december 2020, afsnit 3.3.1, pkt. 28-30.
[155] EU-Chartrets art. 11 og EMRK art. 10.
[156] EU-Chartrets art. 12 og EMRK art. 11.

velfungerende demokrati. Omvendt kan ansigtsgenkendelse også anvendes til at udelukke visse individer fra forsamlinger.[157]

Menneskets **værdighed** er et grundprincip indenfor menneskeretten og retten hertil udgør en selvstændig rettighed i EU-retten. Anvendelse af ansigtsgenkendelse i det offentlige rum indebærer en iboende risiko for at virke adfærdsændrende i en sådan grad, at menneskets mulighed for at leve et værdigt liv bringes i fare.[158]

Ansigtsgenkendelse nødvendiggør desuden en række retlige overvejelser i medfør af **retten til god forvaltning.** Retten omfatter bl.a. ret til aktindsigt og til at modtage en begrundelse for myndighedsafgørelser.[159]

Retten til effektive retsmidler[160] skal også iagttages. Rettigheden indebærer, at individet skal kunne efterprøve enhver foranstaltning, der har indvirkning på vedkommendes øvrige rettigheder, for en domstol. I den forbindelse er også **retten til en retfærdig rettergang** relevant.[161] Overholdelse af retten til effektive retsmidler forudsætter helt grundlæggende, at individet gøres bekendt med, at vedkommendes ansigtsbillede behandles, idet vedkommende ellers ikke vil kunne gøre sin ret gældende.[162]

Desuden kan anvendelse af ansigtsgenkendelse nødvendiggøre overvejelser i forhold til **retten til frihed og sikkerhed**.[163] Retten indebærer, at ingen må berøves sin frihed undtagen i en række særligt definerede tilfælde og i overensstemmelse med loven. Hvis der f.eks. foretages anholdelse eller tilbageholdelse af en person på baggrund af ansigtsgenkendelsesteknologi, er det nødvendigt at foretage grundige overvejelser om samspillet mellem konklusioner draget af kunstig intelligens og efterfølgende menneskelig beslutning og/eller handling. Det er i den forbindelse relevant at fremhæve, at det ikke altid er muligt at forstå beslutningsvejene i et system baseret på kunstig intelligens, hvilket kan gøre det svært eller ligefrem umuligt at efterprøve, om en beslutning truffet af kunstig intelligens er fejlbehæftet. Disse forhold er også relevante i forhold til retten til effektive retsmidler

[157] Se også European Union Agency for Fundamental Rights, Facial recognition technology: Fundamental rights considerations in the context of law enforcement, April 2019, pkt. 7.4 og CAHAI, Feasibility Study, 17. december 2020, afsnit 3.3.1, pkt. 26.
[158] Artikel 1 i EU's Charter om Grundlæggende Rettigheder
[159] Retten til god forvaltning følger af EU-Chartrets art. 41. Selvom bestemmelsen kun gælder EU's institutioner, er der tale om et generelt princip, der binder alle medlemsstaterne, se f.eks. EU-Domstolens dom i sagen C-604/12, H. N. v. Minister for Justice, Equality and Law Reform, Ireland, Attorney General, 8 maj 2014, præmis 49.
[160] EU-Chartrets art. 47 og EMRK art. 13.
[161] EU-Chartrets art. 47 og EMRK art. 6.
[162] Se også også European Union Agency for Fundamental Rights, Facial recognition technology: Fundamental rights considerations in the context of law enforcement, april 2019, pkt. 7.6.
[163] EU-Chartrets art. 6 og EMRK art. 5.

og retten til en retfærdig rettergang, når ansigtsgenkendelse med kunstig intelligens anvendes i forbindelse med retsforfølgelse.[164]

Dertil kommer, at ansigtsgenkendelse generelt kan øve negativ indflydelse på demokratiske grundprincipper og processer, herunder individers sociale og politiske adfærd. Masseovervågning med ansigtsgenkendelse kan være egnet til at virke adfærdsregulerende og -kontrollerende, hvilket bl.a. underminerer individets frie vilje og udøvelse af politiske rettigheder på et generelt plan.[165]

[164] Se også CAHAI, Feasibility Study, 17. december 2020, afsnit 3.3.1, pkt. 22.
[165] Se også CAHAI, Feasibility Study, 17. december 2020, afsnit 3.3.2.

8 Dataetiske refleksioner

Dataetik handler om, hvordan vi bør behandle data, og hvordan vi bør udvikle og anvende nye digitale teknologier. Når databehandling eller teknologi er i konflikt med vores etiske værdier og principper, kan der opstå et dataetisk dilemma. Dataetiske overvejelser skal hjælpe med at tage de ansvarlige beslutninger, hvor man balancerer teknologiens fordele med de potentielle ulemper, den kan have for individer og samfundet. Dataetik går således udover de juridiske rammer og vurderer, hvad der er etisk korrekt.[166]

På baggrund af en stigende offentlig debat og et stort fokus på forskellige dataetiske spørgsmål blev der i 2019 oprettet et særligt råd i Danmark, der beskæftiger sig med dataetik. Formålet med Dataetisk Råd er at skabe et forum, hvor etiske spørgsmål om forholdet mellem på den ene side fordelene ved anvendelse af ny teknologi og på den anden side hensynet til borgernes grundlæggende rettigheder, retssikkerhed og grundlæggende samfundsmæssige værdier, kan drøftes, og hvor en varig indsats for understøttelse af en ansvarlig anvendelse af data kan forankres. Samfundets behov for at anvende data og udnytte de teknologiske muligheder skal tilgodeses og respekteres, og Dataetisk Råd kan bidrage til, at brugen af data sker etisk forsvarligt, og dermed bidrage til en positiv udvikling i brugen af data.[167]

Dataetisk Råd har udpeget 10 centrale dataetiske værdier og principper, som rådet anbefaler, at der tænkes ind i arbejdet med dataetik i praksis.[168] Særligt værdierne/principperne om frihed, privatliv, selvbestemmelse og retssikkerhed må anses for relevante, når det gælder politiets anvendelse af ansigtsteknologi til kriminalitetsbekæmpelse og borgernes tillid til, at dette sker på en forsvarlig og betryggende måde.

[166] Om dataetik | Dataetisk Råd (dataetiskraad.dk)
[167] Om Dataetisk Råd | Dataetisk Råd (dataetiskraad.dk)
[168] Dataetisk Råd, "Dataetik – Sådan gør du" oktober 2021, side 12-15.

B centrale værdier og principper for dataetik

VELFÆRD

Behandling af data skal ske med respekt for og hensyn til sociale forhold, samfund og demokrati.

VÆRDIGHED

Behandling af data må ikke anvendes til at skade det enkelte menneske, og mennesker bør have den primære gavn af databehandlingen.

Det vil sige, at mennesker skal prioriteres før kommercielle og institutionelle interesser.

SELVBESTEMMELSE

Behandling af data skal støtte mennesket i at træffe oplyste og selvstændige valg. Det skal ikke mindske, begrænse eller vildlede menneskets selvbestemmelse.

Det enkelte menneske bør have kontrol over egne data, herunder kontrol med hvilke data, der indsamles, hvad de anvendes til og i hvilke sammenhænge.

PRIVATLIV

Behandling af data skal ske med respekt for privatliv og under beskyttelse af personlige oplysninger. Det bør altid overvejes, hvilke data der er nødvendige, fra hvilke kilder data skal indhentes, og hvor følsomme

disse data anses for at være.

Indhold, omfang og deling af borgernes personlige data bør begrænses mest muligt og ikke opbevares i længere tid end højst nødvendigt.

LIGHED

Behandling af data må ikke diskriminere på baggrund af etnicitet, seksualitet, køn, socioøkonomisk baggrund, politiske meninger, religion, fagforeningsmedlemskab, genetiske data, biometriske data, handicap eller andre sundhedsrelaterede data.

Behandling af data må ikke reproducere fordomme, der marginaliserer og stigmatiserer befolkningsgrupper. Der bør målrettet arbejdes for, at ressourcesvage og udsatte borgere får gavn af den teknologiske udvikling.

Der skal sikres mangfoldighed og diversitet i udvikling og anvendelse af ny teknologi ved for eksempel inddragelse af relevante faggrupper, brugergrupper og organisationer

FRIHED

Behandling af data skal ske med respekt for grundlæggende frihedsrettigheder i et demokratisk samfund. Herunder ytrings-, informations-, religions-, forsamlings- og foreningsfrihed.

RETSSIKKERHED

Behandling af data skal ske med respekt for grundlæggende retssikkerhedsmæssige garantier og retssikkerhedsniveauet i samfundet

GENNEMSIGTIGHED

Behandling af data skal være tilstrækkelig gennemsigtig. Der skal være adgang til indsigt i egne data. Der skal informeres klart og forståeligt om behandlingen af data, databehandlingens formål, funktion, sikkerhed og begrænsninger. Bagvedliggende mønstre skal kunne forklares og retfærdiggøres.

SIKKERHED

Behandling af data skal være tilstrækkelig sikker, robust og pålidelig. Der skal sikres sikkerhed i opbevaring og deling af data, således at data ikke utilsigtet bliver til

gængelige for uvedkommende personer.

Det skal være muligt at overvåge og udøve effektivt tilsyn og kontrol, så fejl og potentielle negative sociale

eller etiske konsekvenser kan identificeres, evalueres, dokumenteres og minimeres.

ANSVARLIGHED

Det skal være muligt at stille mennesker til ansvar. Det skal i alle led være klart hvem, der er ansvarlig for konsekvenserne for udvikling og anvendelse af data. Det gælder blandt andet udviklere, anvendere, myndigheder, virksomheder, samarbejdspartnere og tredjeparter.

Kilde: Dataetisk Råd, "Dataetik – Sådan gør du" oktober 2021

Dataetisk Råd har desuden i udgivelsen "Hvad er ansigtsgenkendelse?" udarbejdet et skema, der kan anvendes til at skabe overblik over, hvad der er relevant at overveje i forbindelse med anvendelse af ansigtsteknologi.[169] Nedenfor har Justitia udfyldt skemaet med de oplysninger, der vurderes centrale for politiets anvendelse af ansigtsteknologi. Skemaet anvendes ved Justitias konkluderende overvejelser og anbefalinger, hvor også Dataetisk Råds anbefalinger til ansigtsgenkendelse i det offentlige rum og alment tilgængelige steder fra oktober 2021 indgår.[170]

Faktor	Ansigtsgenkendelsesteknologi
Formål Hvad er den intenderede effekt af at anvende teknologien?	Eksisterende anvendelse: • Paskontrol. • Eftersøgning af børn, der udsættes for seksuelt misbrug (forsøgsordning). Nye formål kan f.eks. være: • Eftersøgning af andre ofre for kriminalitet. • Eftersøgning af forsvundne personer. • Efterforskning af mulige lovovertrædere. • Håndhævelse af f.eks. opholds- og kontaktforbud. • Sikkerhedsforanstaltning ved arrangementer mv. • Kriminalitetsforebyggelse.
Samtykke Har de personer, som teknologien anvendes på, samtykket til anvendelsen?	• Ingen samtykke.
Adgang til data Hvem har adgang til de data som teknologien anvender og genererer?	• Politiet. • Evt. videregivelse til efterretningstjenester. • Evt. videregivelse til udenlandsk politi. • Tilsynsmyndighed.
Dataproduktion Hvilke data genererer ansigtsgenkendelsen?	• Biometrisk data om ansigt.
Database Hvilke data trækker teknologien på i trænings- og anvendelsesfaserne?	• Billed- og videomateriale fra interne registre i politiet. • Billed- og videomateriale fra eksterne registre og konkrete sager. Mv. fra andre myndigheder i ind- og udland. • Billed- og videomateriale fra overvågning udøvet af offentlige myndigheder og private efter tv-overvågningsloven. • Billed- og videomateriale fra offentligt tilgængelige kilder, herunder sociale medier og lign. • Clearviews software som referencedatabase kan ikke anvendes, da data ikke er indsamlet i overensstemmelse med reglerne om persondatabeskyttelse.[171]

[169] Dataetisk Råds rapport "Hvad er ansigtsgenkendelse?", s. 15. Se link: Data-Etisk-Raad_Ansigtsgenkedelse_2022.pdf (dataetiskraad.dk)
[170] Dataetisk Råds anbefalinger til ansigtsgenkendelse i det offentlige rum og alment tilgængelige steder af 26. oktober 2021. Se link: Dataetisk Råds anbefalinger om ansigtsgenkendelse.pdf (dataetiskraad.dk)
[171] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, s. 5.

Aktør Hvem anvender teknologien?	• Politiet
Målgruppe Hvem anvendes teknologien på?	• Forsvundne personer. • Ofre for kriminalitet. • Eftersøgte. • Mistænkte/sigtede/tiltalte/domfældte personer. • Potentielle kriminelle. • Tilfældige personer udenfor målgruppe (utilsigtet).
Anvendelsesområde Hvor anvendes teknologien?	• Overvågning i det offentlige rum og frit tilgængelige steder. • Overvågning på private steder. • POL-INTEL og dertil hørende interne og eksterne kilder, herunder internettet.
Kvalitet Hvor mange og hvilke fejl begår teknologien?	• Forkert person identificeres. • Teknologien virker dårligere på visse grupper, f.eks. kvinder med mørk hudfarve.[172] • Utilsigtet datafangst. Begrænsede muligheder for at kontrollere og korrigere systemet.
Fejl Hvilken betydning har de fejl som teknologien begår?	• Uberettiget indgreb i retten til privatliv og beskyttelse af personoplysninger. • Påvirkning af andre grundlæggende rettigheder, herunder ytrings- og forsamlingsfrihed. • Risiko for profilering. • Risiko for diskrimination på baggrund af etnicitet, race, køn mv. [173]

[172] https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/ og European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, side 10, punkt 26

[173] Dataetisk Råds anbefalinger til ansigtsgenkendelse i det offentlige rum og alment tilgængelige steder https://nationaltcenterforetik.dk/Media/637895978472559049/Dataetisk%20Ra%C2%B0ds%20anbefalinger%20om%20ansigtsgenkendelse.pdf

9 Ansigtsgenkendelse i Danmark

9.1 Konkret anvendelse

Efter oplysninger fra skiftende justitsministre, jf. kapitel 9.2 nedenfor, anvender politiet i dag ikke overvågning med ansigtsgenkendelsesteknologi i det offentlige rum.[174] Teknologien anvendes (eller har været anvendt) til verificering af identitet i forbindelse med paskontrol i Københavns Lufthavn og anvendes muligvis også i Billund Lufthavn (en-til-en sammenligning). Herudover anvendes teknologien på forsøgsbasis af Rigspolitiets Nationalt Cyber Crime Center til at identificere ofre for seksuelt misbrug børn på tværs af billedmateriale (en-til-mange sammenligning).[175] Københavns Vestegns Politi har desuden af egen drift i 2022 har indkøbt et it-program, der bl.a. indeholder en ansigtsgenkendelsesfunktion, der har været anvendt i to konkrete sager for at finde specifikke børn, der har været udsat for overgreb. [176]

Selvom rapporten alene har fokus på politiets anvendelse af ansigtsgenkendelsesteknologi, bør det kort nævnes, at private aktører allerede anvender ansigtsgenkendelse til en lang række forskellige formål. Det gælder naturligvis globale tech-giganter, hvor mange danskere allerede har vænnet sig til, at telefonen låses op ved hjælp af verificering af ejerens ansigt. Ligeledes anvender Meta og Google bl.a. teknologien til at kategorisere deres brugeres store billedsamlinger og kategorisere de personer, der optræder på billederne.

Teknologien har også vundet indpas hos danske virksomheder. Ansigtsgenkendelse anvendes f.eks. i forbindelse med adgang til fitnesscentre og fodboldstadioner,[177] og ansigter aflæses i butikker med henblik på at aflæse humør, køn, alder mm.[178]

Datatilsynet gav i 2019 tilladelse til, at Brøndby IF kunne behandle følsomme personoplysninger, omfattet af databeskyttelsesforordningens artikel 9 om biometriske data, med det specifikke formål

[174] Se åbent samråd i Retsudvalget om politiets brug af ansigtsgenkendelse, 23/8 2018 (kan ses her), Retsudvalgets. Spørgsmål 926 stillet den 22/6 2018, besvaret af justitsministeren den 21/8 2018, Retsudvalgets spørgsmål 1056 stillet den 23/8 2018, besvaret af justitsministeren den 11/9 2018, Retsudvalgets spørgsmål 1092 stillet den 5/9 2018, besvaret af justitsministeren den 3/10 2018.
[175] Se åbent samråd i Retsudvalget om politiets brug af ansigtsgenkendelse, 23/8 2018 (kan ses her), Retsudvalgets spørgsmål 926 stillet den 22/6 2018, besvaret af justitsministeren den 21/8 2018, Retsudvalgets spørgsmål 1056 stillet den 23/8 2018, besvaret af justitsministeren den 11/9 2018, Retsudvalgets spørgsmål 1092 stillet den 5/9 2018, besvaret af justitsministeren den 3/10 2018. Forsøgene blev ifølge det oplyste igangsat i begyndelsen af 2016, se Retsudvalgets spørgsmål 730 stillet den 22/1 2020, besvaret af justitsministeren den 17/2 2020.
[176] REU Alm del supplerende svar på spørgsmål 1222. Opfølgning på besvarelse af spørgsmål nr. 1222 Alm del fra Folketingets Retsudvalgpdf (ft.dk)
[177] Rapport fra Dataetisk Råd: "Hvad er ansigtsgenkendelse?", oktober 2022.
[178] Nu aflæser butikker dit humør, køn, alder og etnicitet. Manden her udstyrer Danmark med ansigtsscannere, Zetland, 17. maj 2021.

at identificere en fysisk person entydigt.[179] Dette skete i forbindelse med implementeringen af automatisk ansigtsgenkendelse som en del af adgangskontrollen ved indgangene til Brøndby Stadion. I 2023 udvidede Datatilsynet Brøndby IF´s tilladelse til at omfatte holdets udebanekampe, hvilket inkluderede brugen af billeder fra overvågningskameraer på stadioner til registrering af personer, der overtræder klubbens ordensreglement.[180]

Datatilsynet har også taget stilling til et fitnesscenters behandling af oplysninger om biometriske data ved brug af ansigtsgenkendelse som alternativ til nøglekort. Datatilsynet gav i 2022 en advarsel til fitnesscenteret FysioDanmark Hillerød ApS, fordi deres ansigtsgenkendelse blev anvendt på en sådan måde, at kameraer indsamlede biometrisk data om forbipasserende personer, som ikke var kunder i centret, og fordi kunderne ikke blev anmodet om samtykke til brugen af ansigtsgenkendelse til indsamling af statistisk information. Til gengæld vurderede Datatilsynet, at det var lovligt at anvende ansigtsgenkendelse som adgangskontrol for de kunder, som havde givet et informeret samtykke.[181]

9.2 Politiske tilkendegivelser og initiativer

Spørgsmålet om Danmarks anvendelse af ansigtsgenkendelsesteknologi i det offentlige rum har været drøftet politisk ad flere omgange. Første gang emnet fik større opmærksomhed var i 2018. Det skete i forlængelse af, at Ekstra Bladet havde bragt en artikel, hvor det fremgik, at politiet allerede anvendte ansigtsgenkendelsesteknologi uden forudgående politiske drøftelser om emnet.[182] Artiklen medførte en række folketingsspørgsmål fra Retsudvalget til tidligere justitsminister Søren Pape Poulsen[183] samt et åbent samråd om emnet.[184] De primære spørgsmål var, om teknologien var blevet taget i brug, og om der var lovhjemmel til anvendelsen.

Justitsministeren oplyste gentagne gange – modsat hvad artiklen i Ekstra Bladet gav indtryk af – at politiet ikke anvendte overvågning med ansigtsgenkendelsesteknologi i det offentlige rum.[185] Ifølge det oplyste blev teknologien kun anvendt operationelt i én sammenhæng nemlig i forbindelse med

[179] Tilladelse af 24. maj 2019.
[180] Tilladelse af 22. juni 2023.
[181] Afgørelse af 17. marts 2022
[182] Ekstra Bladet: "Dansk politi har taget omstridt teknologi i brug – Ekstra Bladet," af 7. juli 2018.
[183] Retsudvalgets spørgsmål 917, 918, 926, 927, 1056, 1092, 1093, 1094, 1095 og 1096 til justitsministeren fra 2018.
[184] Åbent samråd i Retsudvalget om politiets brug af ansigtsgenkendelse, 23/8 2018. Samrådet kan ses her.
[185] Se åbent samråd i Retsudvalget om politiets brug af ansigtsgenkendelse, 23/8 2018 (kan ses her), Retsudvalgets. Spørgsmål 926 stillet den 22/6 2018, besvaret af justitsministeren den 21/8 2018, Retsudvalgets spørgsmål 1056 stillet den 23/8 2018, besvaret af justitsministeren den 11/9 2018, Retsudvalgets spørgsmål 1092 stillet den 5/9 2018, besvaret af justitsministeren den 3/10 2018.

paskontrol i de såkaldte ABC-gates.[186] Det blev desuden oplyst, at der var tale om ansigtsgenkendelse til verificering (en-til-en sammenligning). Teknologien blev således ikke brugt til identificering (en-til-mange sammenligning). Derudover blev det oplyst, at Nationalt Cyber Crime Center ("NC3") var i gang med at undersøge muligheden for at kunne identificere overgreb mod børn på tværs af billedmateriale, men at teknologien ikke havde været anvendt i konkrete efterforskninger, og at eventuel senere anvendelse af teknologien ville bero på nærmere politiske og juridiske overvejelser.[187]

I et svar til Folketingets Retsudvalg oplyste justitsministeren endvidere, at teknologien "allerede kunne anvendes inden for rammerne af den gældende lovgivning".[188] Han udtalte dog også, at det samtidig var hans klare holdning, at større redskaber såsom anvendelse af ansigtsgenkendelsesteknologi i det offentlige rum ikke ville blive taget i brug, før der har været politiske drøftelser om balancen mellem retshåndhævelse og individets grundlæggende rettigheder.[189]

Da Nick Hækkerup i juni 2019 overtog hvervet som justitsminister blev emnet igen aktuelt. Berlingske bragte den 23. juni 2019 en artikel, der fik Retsudvalget til at stille spørgsmål til emnet. Artiklen i Berlingske antydede, at NC3's eksperimenter med ansigtsgenkendelsesteknologi havde været væsentlig mere omfattende, end hvad tidligere justitsminister Søren Pape Poulsen i 2018 havde givet udtryk for.[190]

Disse oplysninger fik Retsudvalget til at spørge den nye justitsminister om, i hvilken udstrækning Rigspolitiet havde eksperimenteret med ansigtsgenkendelsesteknologi, hvorvidt Rigspolitiet var i besiddelse af den underliggende software til at bruge teknologien, hvilken holdning regeringen havde til brug af ansigtsgenkendelsesteknologi, og hvorvidt ministeren fandt det nødvendigt at inddrage Folketinget, inden teknologien blev taget i brug.[191]

Justitsministeren indhentede til brug for sin besvarelse en udtalelse fra Rigspolitiet, der oplyste, at der hverken aktuelt eller tidligere var blevet anvendt ansigtsgenkendelsesteknologi i videre omfang

[186] Se åbent samråd i Retsudvalget om politiets brug af ansigtsgenkendelse, 23/8 2018 (kan ses her), Retsudvalgets spørgsmål 926 stillet den 22/6 2018, besvaret af justitsministeren den 21/8 2018, Retsudvalgets spørgsmål 1056 stillet den 23/8 2018, besvaret af justitsministeren den 11/9 2018, Retsudvalgets spørgsmål 1092 stillet den 5/9 2018, besvaret af justitsministeren den 3/10 2018. Teknologien blev ifølge det oplyste taget i brug i maj 2016, se Retsudvalgets spørgsmål 730 stillet den 22/1 2020, besvaret af justitsministeren den 17/2 2020.
[187] Se åbent samråd i Retsudvalget om politiets brug af ansigtsgenkendelse, 23/8 2018 (kan ses her), Retsudvalgets spørgsmål 926 stillet den 22/6 2018, besvaret af justitsministeren den 21/8 2018, Retsudvalgets spørgsmål 1056 stillet den 23/8 2018, besvaret af justitsministeren den 11/9 2018, Retsudvalgets spørgsmål 1092 stillet den 5/9 2018, besvaret af justitsministeren den 3/10 2018. Forsøgene blev ifølge det oplyste igangsat i begyndelsen af 2016, se Retsudvalgets spørgsmål 730 stillet den 22/1 2020, besvaret af justitsministeren den 17/2 2020.
[188] Retsudvalgets spørgsmål 1095 stillet den 5/9 2018, besvaret af justitsministeren den 3/10 2018.
[189] Retsudvalgets spørgsmål 1095 stillet den 5/9 2018, besvaret af justitsministeren den 3/10 2018.
[190] Berlingske: "Politiet ville koble tusinder af danskeres billeder til omstridt teknologi »Potentielt er det jo et fantastisk hjælpemiddel«," af 3. august 2019.
[191] Retsudvalgets spørgsmål 144 stillet den 16/8 2019, besvaret af justitsministeren den 10/9 2019.

end det, der blev oplyst i 2018, og at Justitsministeriet ville blive inddraget, før eventuel ibrugtagning af teknologien.[192]

Et forslag til folketingsbeslutning om forbud mod ansigtsgenkendelse blev i begyndelsen af 2020 forkastet af et flertal i Folketinget.[193]

Justitsministeren gav i flere sammenhænge udtryk for, at politiet havde ytret ønske om ibrugtagning af ansigtsgenkendelse, og at ministeren var lydhør over for politiets ønsker samtidig med, at der dog var principielle, praktiske og retlige dilemmaer, der skulle afklares, inden teknologien kunne tages i brug.[194]

Et amerikansk nyhedsmedie bragte en artikel i februar 2020 om, at den amerikanske virksomhed, Clearview AI, havde en kommerciel relation med danske myndigheder, hvilket foranledigede Retsudvalget til at spørge justitsministeren til dette. Det blev i den forbindelse oplyst, at dansk politi ikke modtog varer/tjenesteydelser fra Clearview AI og ikke på noget tidspunkt havde været deres kunde.[195] Eftersom justitsministeren afgrænsede sin besvarelse af spørgsmålet til at angå "danske politimyndigheder", kan det ikke udelukkes, at andre danske myndigheder – f.eks. Forsvarets Efterretningstjeneste – kunne have en kommerciel relation til Clearview AI.

Clearview AI

Clearview AI er en virksomhed, der indsamler og opbevarer billeder af personer fra bl.a. nyhedsmedier og sociale medier som f.eks. Facebook og YouTube, og som gemmes i Clearview AI's database – også efter billederne eventuelt er blevet slettet fra f.eks. Facebook. Clearview AI er ifølge deres egne oplysninger besiddelse af mere end 40+ milliarder billeder.[196] En indsamling af biometriskdata af en hidtil uset skala.[197] Retshåndhævende myndigheder kan tilkøbe sig adgang til databasen med billeder for at kunne anvende den som referencedatabase i forbindelse med ansigtsgenkendelse til identificering.[198] Clearview AI er i den forbindelse blevet markedsført ved at tilbyde 30 dages gratis prøveperioder til ansatte hos politi- og efterretningsmyndigheder.[199]

[192] Retsudvalgets spørgsmål 144 stillet den16/8 2019, besvaret af justitsministeren den 10/9 2019.
[193] Forslag til folketingsbeslutning nr. B 46 om forbud mod ansigtsgenkendelse. Se fordelingen af stemmer her.
[194] Se f.eks. justitsministerens udtalelser i forbindelse med behandlingen af forslag til folketingsbeslutning nr. B 46 om forbud mod ansigtsgenkendelse her samt Retsudvalgets spørgsmål 1 til forslag til folketingsbeslutning nr. B 46 stillet den 22/1 2020, besvaret af justitsministeren den 18/2 2020.
[195] Se Retsudvalgets spørgsmål 998 stillet den 28/2 2020 til justitsministeren, besvaret den 3/4 2020. Justitsministeren oplyste samtidig, at NC3 ifølge Rigspolitiet havde deltaget i en konference, hvor bl.a. Clearview AI præsenterede sit produkt, og at medarbejdere fra NC3 herefter havde afgivet kontaktoplysninger på virksomhedens hjemmeside med henblik på at kunne læse nærmere om produktet.
[196] Clearview AI – Clearview.ai.
[197] The New York Times: "The Secretive Company That Might End Privacy as We Know It", af 19. januar 2020.
[198] Law Enforcement – Clearview AI.
[199] The New York Times: "The Secretive Company That Might End Privacy as We Know It", af 19. januar 2020; og Buzzfeed News: "Police In At Least 24 Countries Have Used Clearview AI", af 25. august 2021.

I marts 2020 blev der stillet yderligere spørgsmål om ansigtsgenkendelse, der vedrørte, om Datatilsynet havde undersøgt, om danske myndigheder havde benyttet Clearview AI eller i øvrigt havde været kunde hos det amerikanske selskab, eller om Datatilsynet var blevet bedt om at vurdere Clearview AI eller andre virksomheders teknologi for ansigtsgenkendelse.[200]

Det fremgik af besvarelsen, at Datatilsynet var bekendt med en medieomtale af en rapport, hvor politi og/eller andre offentlige myndigheder i en række medlemsstater, herunder i Danmark, angiveligt skulle gøre brug af Cleaview AI. Det blev oplyst, at Datatilsynet hverken havde modtaget klager fra registrerede eller anmeldelser om brud på persondatasikkerheden vedrørende danske myndigheders brug af Clearview AI eller tjenester, der på tilsvarende måde anvender ansigtsgenkendelse. Tilsynet havde heller ikke fundet anledning til at indlede undersøgelser på tilsynets eget initiativ.[201]

Spørgsmålet om ibrugtagning af ansigtsgenkendelse blev også kort berørt i forbindelse med behandlingen af en ændring af tv-overvågningsloven i 2020.[202]

I mellemtiden opstod der spørgsmål om, hvorvidt ansigtsgenkendelse allerede var blevet en utilsigtet realitet i Danmark, fordi flere kommuner anvender overvågningskameraer, der er indkøbt fra Kina. Eksperter har i den forbindelse udtalt, at det ikke kan udelukkes, at Kina via bagveje i disse kameraer kan kigge med i de danske overvågede miljøer og samtidig anvende automatisk ansigtsgenkendelse.[203]

I forlængelse heraf blev den daværende justitsminister bedt om at svare på, om installationen af de kinesiske kameraer ifølge ministerens opfattelse kunne udgøre en trussel mod danske statsborgeres personlige frihed. I besvarelsen af spørgsmålet henviste justitsministeren til forsvarsministeren, men tilføjede bl.a. som en generel bemærkning, at når der behandles personoplysninger, har den dataansvarlige pligt til at sikre et passende sikkerhedsniveau, så uvedkommende ikke kan få adgang til de oplysninger, der behandles.[204]

Efterfølgende blev tidligere forsvarsminister Trine Bramsen bedt om at svare på, om ministeren kunne garantere, at de kinesiske kameraer ikke kunne sende krypterede data med, der kan overvåge borgerne. Ministeren indhentede til besvarelse af spørgsmålet oplysninger fra Forsvarets Efterret-

[200] Se Retsudvalgets spørgsmål 1067 stillet den 11/3 2020 til justitsministeren, besvaret den 7/4 2020.
[201] Se Retsudvalgets spørgsmål 1067 stillet den 11/3 2020 til justitsministeren, besvaret den 7/4 2020.
[202] Se debatten i forbindelse med 1. behandlingen af lovforslag nr. L 102 til ændring af lov om tv-overvågning her.
[203] Se f.eks. DR Nyheder om emnet i juni 2021 her og i juli 2021 her.
[204] Spørgsmål nr. S 1680 stillet den 1. juli 2021 af folketingsmedlem Michael Aastrup Jensen (V) til justitsministeren, besvaret den 8. juli 2021.

ningstjeneste, der oplyste, at det generelt ikke er muligt at garantere, at kameraer fra bestemte producenter ikke indeholder bagdøre, og at sådanne skjulte funktioner er meget svære at afsløre. Ministeren tilføjede bl.a., at regeringen er meget opmærksom på risiciene forbundet med ny teknologi.[205]

I november 2021, blev justitsministeren spurgt af Retsudvalget, hvor mange kinesisk procederede overvågningskameraer, der er sat op i Danmark.[206] Ministeren kunne ikke oplyse det præcise antal, da offentlige og private, der opstiller overvågningskameraer, ikke har pligt at oplyse, hvor disse er produceret.[207] Ministeren havde til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Rigspolitiet, der oplyste, at der af politiet er opsat 160 overvågningskameraer fra kinesiske producenter. Rigspolitiet havde besluttet at igangsætte en nærmere kortlægning af politiets overvågningskameraer, herunder i forhold til netværksopkobling og anvendelsesformål. På den baggrund ville Rigspolitiet gennemføre eventuelle nødvendige foranstaltninger, herunder udskiftning af overvågningskameraer, i det omfang en PET-risikovurdering gav anledning hertil.

I oktober 2021 fastholdt justitsministeren, at politiet ikke benytter ansigtskendelse på andre måder end tidligere tilkendegivet, navnlig ved automatiseret paskontrol i Københavns Lufthavn, og at Rigspolitiet er i gang med at undersøge muligheden for at bekæmpe seksuelle overgreb begået mod børn på tværs af billedmateriale, som Rigspolitiet er i besiddelse af som led i behandlingen af straffesager eller har modtaget som led i efterretninger at kunne fremsøge samme forurettede. Det blev oplyst, at redskabet er under udvikling og ikke er blevet anvendt i konkrete efterforskninger.[208]

Forsøget med digital offergenkendelse blev lanceret i den digitale tryghedspakke i september 2022 af tidligere justitsminister Mattias Tesfaye. Tryghedspakken havde bred tilslutning i Folketinget, og det fremgår bl.a., at politiet skal igangsætte forsøg, hvor billed- og videomateriale gennemscannes automatisk med henblik på effektivt at identificere seksuelle overgreb begået mod børn. [209]

[205] Spørgsmål nr. S 1681 stillet den 2. juli 2021 af folketingsmedlem Michael Aastrup Jensen (V) til forsvarsministeren, besvaret den 8. juli 2021.
[206] Spørgsmål nr. S 160 stillet den 2. november 2021 af Retsudvalget til justitsministeren, besvaret den 10. februar 2022
[207] Følger af den seneste ændring af tv-overvågningsloven i 2020 § 2 e, hvorefter private og offentlige myndigheder, der foretager tv-overvågning, inden for rimelig tid skal registrere sig i politiets register over tv-overvågningskameraer (POLCAM).
[208] Retsudvalgets spørgsmål 1567 stillet den 8/9 2021, besvaret af justitsministeren den 5/10 2021.
[209] Aftalepartner omfatter Socialdemokratiet (regeringen), Socialistisk Folkeparti, Radikale Venstre, Enhedslisten, Dansk Folkeparti og Nye Borgerlige. Se aftalen her, særligt afsnit 9, side 8. Se også Bandepakke IV af 8. november, side 6.

Nuværende justitsminister Peter Hummelgaard har i september 2023 bl.a. oplyst, at myndigheder under ministeriet har oplyst, at de ikke anvender ansigtskendelsesteknologi, men at der ikke foreligger et komplet samlet overblik over, hvilke offentlige myndigheder eller private aktører, der anvender ansigtsgenkendelse.[210]

Til besvarelse af spørgsmålet indhentede Justitsministeriet et bidrag fra Rigspolitiet, der i sit svar oplyste, at Københavns Politi ikke på nuværende tidspunkt anvender ansigtsgenkendelsesteknologi til verificering af en rejsendes identitet i forbindelse med grænsekontrollen. Ansigtsgenkendelsesteknologi har dog tidligere været anvendt i perioden fra april 2016 og indtil efteråret 2021 ved den automatiserede ind- og udrejsekontrol, de såkaldte ABC-egate i Københavns Lufthavn. Der er opstillet nye ABC-egates i Københavns Lufthavn og nye ABC-egates i Billund Lufthavn, der på tidspunktet for besvarelsen ikke var taget i brug. Det blev endvidere på ny oplyst, at Rigspolitiet, Nationalt Cyber Crime Center (NC3), i et pilotprojekt anvender ansigtsgenkendelsesteknologi som hjælpeværktøj til gennemsøgning af billed- og videomateriale på et antal afsluttede efterforskninger og på NC3's database med billedmateriale vedrørende seksuelt misbrug af børn.

I et supplerende svar på spørgsmålet blev det oplyst, at Københavns Vestegns Politi af egen drift i 2022 har indkøbt et it-program, der bl.a. indeholder en ansigtsgenkendelsesfunktion, der har været anvendt i to konkrete sager for at finde specifikke børn, der har været udsat for overgreb. Landets øvrige politikredse har oplyst, at kredsene ikke anvender ansigtsgenkendelsesteknologi ud over det ovenfor oplyste.[211]

Et bredt flertal i Folketinget vedtog den 8. november 2023 Bandepakke IV "Trygge nabolag i hele Danmark", hvoraf det fremgår, at politiet, som tidligere oplyst i en række svar til Retsudvalget, er i gang med et forsøg med digitaliseret offergenkendelse i sager om seksuelt misbrug af børn. Det nye i denne sammenhæng er, at det i tilknytning hertil bliver nævnt, at "aftalepartierne ser frem til at følge erfaringerne i forhold til, om det er et værktøj, der vil kunne bruges f.eks. i indsatsen mod banderne."[212] Det kan således udledes af bemærkningen, at det muligvis kan blive relevant at anvende ansigtsgenkendelse til bekæmpelse af bandekriminalitet.

Den 23. november 2023 blev der afholdt et åbent samråd i Udvalget for Digitalisering og IT om anvendelse af ansigtsgenkendelsesteknologi, hvor justitsministeren bl.a. blev spurgt til regeringens

[210] Retsudvalgets spørgsmål 1222 stillet den 28/8 2023, besvaret af justitsministeren den 25/9 2023. Civilstyrelsen, Rigsadvokaten, Styrelsen for Forsyningssikkerhed, Tilsynet med Efterretningstjenesterne og Direktoratet for Kriminalforsorgen har oplyst, at myndighederne ikke anvender ansigtsgenkendelsesteknologi ud over den ansigtsgenkendelsesteknologi, der benyttes til at låse it-udstyr op. Datatilsynet og Domstolsstyrelsen anvender ikke ansigtsgenkendelsesteknologi. Den Uafhængige Politiklagemyndighed har oplyst, at efterforskere i Politiklagemyndigheden har modtaget undervisning i at anvende ansigtsgenkendelsesteknologi, men at teknologien indtil videre ikke har været anvendt i myndigheden.
[211] REU Alm del supplerende svar på spørgsmål 1222. Opfølgning på besvarelse af spørgsmål nr. 1222 Alm del fra Folketingets Retsudvalgpdf (ft.dk)
[212] Bandepakke IV "Trygge nabolag i hele Danmark", 8. november 2023 aftaleteksten side 6.

holdning til dette, og om Folketinget vil blive inddraget, hvis der indføres en udvidet anvendelse af ansigtsgenkendelsesteknologi. Justitsministeren svarede, at han ikke havde en principiel modstand mod anvendelsen, når det sker inden for den databeskyttelsesretlige ramme. Så hvis politiet finder, at anvendelsen er nyttig og respekterer de retlige rammer, er det et værktøj, som politiet skal benytte. Skulle der opstå behov for at justere den retlige ramme, vil det ske med inddragelse af Folketinget. Justitsministeren gav samtidig udtryk for, at anvendelsen af ansigtsgenkendelse spænder vidt, og at han derfor ikke mener, at myndighederne af egen drift skal orientere Folketinget om enhver mindre anvendelse af teknologien. Det blev understreget, at ansigtsgenkendelse af myndighederne indenfor Justitsministeriets område bliver anvendt i et meget begrænset omfang, og at der alene skal ske ibrugtagning af teknologien, hvis der forinden af myndigheden er gjort relevante, juridiske, praktiske og principielle overvejelser. Det blev endvidere oplyst, at regeringen i forbindelse med bandepakken vil følge op på NC3's erfaringer med anvendelse af ansigtsgenkendelsesteknologi i forbindelse med bekæmpelse af digitale seksuelle overgreb mod børn, dog uden at der er truffet beslutning om en yderligere udvidet brug af ansigtsgenkendelse.

Den 10. januar 2024 blev der afholdt et åbent samråd i Udvalget for Digitalisering og IT om forhandlingsmandatet til forhandlingerne om forordningen om kunstig intelligens. Minister for digitalisering og ligestilling Marie Bjerre oplyste om regeringens stillingtagen til ansigtsgenkendelse, at det som udgangspunkt skal være forbudt at bruge ansigtsgenkendelse på offentlige steder i realtid, men at det i et retssamfund også skal være muligt for de retshåndhævende myndigheder at bruge den mest effektive teknologi for at beskytte befolkningen og bekæmpe den mest alvorlige kriminalitet, når der er en overhængende trussel. Ministeren oplyste endvidere, at der er blevet arbejdet på at afgrænse undtagelser til forbuddet, og at det er regeringens foreløbige holdning, at aftalen er landet et balanceret sted. Det blev også bemærket, at Danmark har et retsforbehold på netop denne del af forordningen, og at forordningen på dette område derfor ikke vil være gældende i Danmark. På et spørgsmål om, hvornår det er rimeligt at anvende ansigtsgenkendelse i realtid, svarede ministeren, at det kan anvendes på forbrydelser omfattet af den europæiske arrestordre, ved forbrydelser, der har en strafferamme på over fem år, ved forsvundne børn og terror. Det blev også bemærket, at der skal indbygges forholdsregler ved forudgående tilladelse til brug af ansigtsgenkendelse i realtid og rapportering.[213]

Senest i et svar på et udvalgsspørgsmål af 4. marts 2024 giver justitsministeren udtryk for, at myndighederne bør anvende ansigtsteknologi, når fordelene overstiger ulemperne. Justitsministeren oplyser desuden, at de retshåndhævende myndigheder i øjeblikket kun anvender ansigtsgenkendelsesteknologi i meget begrænset omfang. En mere systematisk eller omfattende anvendelse forudsætter, at myndighederne har gjort sig relevante juridiske, praktiske og principielle overvejelser. Det

[213] Samrådsspørgsmål F, om forhandlingsmandatet i de nuværende forhandlinger om en forordning for kunstig intelligens den 10. januar 2024. Se samrådet her: Tv fra Folketinget / Folketinget (ft.dk)

fremgår desuden af svaret, at regeringen for nuværende ikke har nogen planer om at justere den retlige ramme for politiets anvendelse af ansigtsgenkendelsesteknologi, og at en eventuel justering af den retlige ramme vil ske under sædvanlig inddragelse af Folketinget.[214]

Opsummering

Danske myndigheder anvender kun ansigtsgenkendelsesteknologi i et yderst begrænset omfang. Men der forsøgsordninger i gang og generelt politisk velvilje til at anvende teknologien i et større omfang.

ABC-EGATE

Fra april 2016 og indtil efteråret 2021 blev der anvendt ansigtsgendelseteknologi ved den automatiserede ind- og udrejsekontrol, de såkaldte ABC-egate i Københavns Lufthavn.
(Der er opstillet nye ABC-egates i Københavns og Billund Lufthavn. Dog uvist om det er taget i brug)

DIGITALISERET OFFERGENKENDELSE

Nationalt Cyber Crime Center (NC3) anvender i et pilotprojekt ansigtsgenkendelsesteknologi som hjælpeværktøj til gennemsøgning af billed- og videomateriale på et antal afsluttede efterforskninger og på NC3's database med billedmateriale vedrørende seksuelt misbrug af børn.

[214] DIU Alm.del - endeligt svar på spørgsmål 101, Folketingets samling 2023-24

10 Ansigtsgenkendelse uden for Danmark

Dette afsnit gennemgår anvendelse af ansigtsgenkendelsesteknologi uden for Danmark. Formålet er at præsentere eksempler og identificere tendenser i teknologiens implementering og regulering på tværs af forskellige nationale rammer. Det er ikke en udtømmende gennemgang, men snarere en selektiv analyse af repræsentative cases og observationer. Ved at undersøge disse eksempler kan der opnås en bedre forståelse af teknologiens indvirkning på samfundet, ligesom der kan identificeres potentielle fællestræk og variationer mellem lande. Formålet er at bidrage til en mere informeret debat omkring anvendelsen af ansigtsgenkendelsesteknologi og dens potentielle konsekvenser for borgernes rettigheder og privatliv.

10.1 Eksempler på ansigtsgenkendelse i Europa

På trods af flere års debat om problematikker i tilknytning til ansigtsgenkendelse, herunder de menneskeretlige problemstillinger, er der endnu ikke foretaget en officiel kortlægning af, hvor udbredt ansigtsgenkendelsesteknologi er i EU.[215] Det vides dog med sikkerhed, at flere europæiske lande i de seneste år har foretaget eksperimenter med ansigtsgenkendelsesteknologi i det offentlige rum, og at teknologien anvendes flere steder, herunder særligt med henblik på kriminalitetsforebyggelse, strafforfølgning og retshåndhævelse. I en rapport fra maj 2020 fra organisationen European Digital Rights (EDRi) fremgår det, at mindst 15 europæiske lande, herunder Danmark, har eksperimenteret med biometrisk teknologi som ansigtskendelse i realtid i det offentlige rum, der har ført til masseovervågning.[216]

Europa-Kommissionen har oplyst, at der vil blive sat ind over for den tiltagende brug af ansigtsgenkendelse i Europa.[217] Den 21. april 2021 fremlagde Europa-kommissionen et nyt udspil til en fælles

[215] F.eks. fremgår det af en rapport fra den Europæiske Unions Agentur for Grundlæggende Rettigheder, November 2019, at "*[o]nly limited information is currently available on the possible use or tests of live facial recognition technologies in other EU Member States.*", se Facial recognition technology: fundamental rights considerations in the context of law enforcement, European Union Agency for Fundamental Rights, s. 13.
[216] EDRi, Ban Biometric Surveillance, 13. Maj 2020. Se bl.a. side 7.
[217] Formanden for Europa-Kommissionen, tyske Ursula von der Leyen, lovede i 2019, at hun inden for de første 100 dage efter den nye kommissions tiltræden ville sikre »en koordineret europæisk tilgang til de menneskelige og etiske konsekvenser af kunstig intelligens« (https://ec.europa.eu/commission/presscorner/detail/en/ip_20_403). I 2020 kom POLITICO i besiddelse af et udkast til et whitepaper, der bl.a. beskrev, hvordan en "future regulatory framework could go further and include a time-limited ban on the use of facial recognition technology in public spaces", hvilket potentielt kunne medføre, at "the use of facial recognition technology by private or public actors in public spaces would be prohibited for a definite period (e.g. 3-5 years) during which a sound methodology for assessing the impacts of this technology and possible risk management measures could be identified and developed," (POLITICOS artikel af januar 2020 og dokumentet 'Structure for the White Paper on artificial intelligence – a European approach'). Dette blev yderligere underbygget, da Financial Times i august 2019 kunne afsløre, at EU-Kommissionen planlagde at sikre EU-borgernes udtrykkelige rettigheder over brugen af deres ansigtsgenkendelsesdata som led i reguleringen af kunstig intelligens (Financial Times artikel). I en tale fra Februar 2021 var genklangen af Von der Leyens tidligere løfte om øget regulering til at spore (Keynote Speech by President von Der Leyen at the 'Masters of Digital 2021' event).

europæisk regulering af kunstig intelligens, som også omfatter brug af ansigtsgenkendelsesteknologi.[218] Den 8. december 2023 nåede Europa-Parlamentets og Ministerrådets forhandlere til enighed om en aftale til fælles EU-regler for anvendelse af kunstig intelligens, som også indeholder regler om ansigtsgenkendelse.[219] Den endelige tekst forventes først offentliggjort i 2024. En lækker dokument er beskrevet i kapitel 5.

En udtømmende gennemgang af, hvordan det ser ud med ansigtsgenkendelse i de øvrige europæiske lande, er ikke mulig indenfor rammerne af denne rapport, men præsentationen af anvendelsen i de følgende syv europæiske land kan give et overordnet indtryk af brugen af ansigtsgenkendelse.

Frankrig

Det franske politi har anvendt ansigtsgenkendelsesteknologi til at sammenligne billeder af tidligere anholdte, mistænkte og dømte personer med overvågningsbilleder i forbindelse med efterforskning og strafforfølgelse siden 2012.[220] Det fremgår af officielle rapporter fra 2018 og 2019, at politiet har otte millioner billeder af personer i databasen, og at databasen blev brugt 375.747 gange i 2019.[221]

I februar 2019 blev det første eksperiment med ansigtsgenkendelse i de franske gader foretaget i forbindelse med karnevalet i Nice.[222] Det franske datatilsyn Commission National de L'informatique et des Libertés (CNIL) har forholdt sig kritisk til brugen af ansigtsgenkendelse, ligesom den administrative domstol i Marseille i februar 2020 nedlagde forbud mod myndighedernes planer om at foretage et eksperiment med ansigtsgenkendelse på to skoler.[223]

I november 2020 stod det klart, at fremtidens franske sikkerhedsstrategi vil indebære en udvidet brug af ansigtsgenkendelse, da Indenrigsministeriet i en hvidbog om intern sikkerhed betonede teknologiens hensigtsmæssighed i beskyttelsen af den franske befolkning og i samme forbindelse beskrev den eksperimentelle brug af teknologien i det offentlige rum som "highly desireable".[224] Der er allerede blevet foretaget afgørende lovgivningsskridt for at realisere denne vision, idet den franske præsident i december 2019 fik fjernet en bestemmelse i den dagældende politilovgivning, der forbød sammenligning af biometrisk data indsamlet ved store forsamlinger med en referencedatabase,[225]

[218] Forslag til Europa-Parlamentets og Rådets Forordning om harmoniserede regler for kunstig intelligens (Retsakten om Kunstig Intelligens) og om ændring af visse af Unionens lovgivningsmæssige retsakter.
[219] https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai
[220] How facial recognition is taking over a French city, artikel fra 4. august 2021.
[221] Report by the National Assembly (kun på fransk); og Civil liberty groups question facial recognition France tech rollout, artikel fra 10. maj 2021.
[222] How facial recognition is taking over a French city, artikel fra 4. august 2021; se også Nice vil teste ansigtsgenkendelse på den offentlige motorvej, artikel fra d. 18. februar 2019 (oversat).
[223] CNIL Report 2019; og Facial recognition challenged by French administrative court, artikel fra 29. maj 2020.
[224] Livre blanc de la sécurité intérieure | Ministère de lIntérieur (interieur.gouv.fr) (kun på fransk); og French white paper on internal security makes several proposals for the use of facial recognition in France, artikel fra 27. november 2020.
[225] Macrons Global Security bill passed into law in France, artikel fra 19. April 2021.

samt senest i april 2021, hvor regeringen fik vedtaget en lovbestemmelse, der muliggør politiets brug af droner og kropskameraer til overvågning i forbindelse med protester mm.[226]

I juni 2023 vedtog det franske senat udkast til en lov, der har til formål at regulere brug af ansigtsgenkendelsesteknologi.[227] Lovforslaget fastsætter en grænse for, hvornår ansigtsgenkendelsesteknologi kan anvendes. Det består af et forbud mod bl.a. biometrisk identifikation i offentligheden eller steder, som er tilgængelige for offentligheden, uagtet om foretages i realtid eller retrospektivt.[228] Herudover etablerer lovforslaget regulatoriske rammer og mulighed for forsøg af tre års varighed af ansigtsgenkendelsesteknologi i offentligheden. Forsøgene kan tillades, når en stor offentlig interesse taler herfor efter forhåndsgodkendelse og under løbende permanent kontrol.[229]

Italien

I Italien er der også blevet eksperimenteret med anvendelse af ansigtsgenkendelsesteknologi. Bl.a. erhvervede den italienske stat i 2017 et ansigtsgenkendelsessystem i realtid, som den italienske databeskyttelsesenhed dog forbød i april 2021, fordi der manglede lovhjemmel til implementeringen.[230] I sin afgørelse lagde databeskyttelsesenheden vægt på, at implementering af teknologien ville signalere et radikalt skift i måden, hvorpå overvågning foretages; fra målrettet overvågning af få individer til overvågning af alle med det formål at identificere enkelte individer.[231] Systemet var også tiltænkt at skulle anvendes til at overvåge migranter og asylansøgeres ankomst ved de italienske kyster.[232]

I 2022 indledte den italienske databeskyttelsesenhed en undersøgelse mod to italienske kommuner for deres brug af ansigtsgenkendelse.[233] I forbindelse hermed forbød databeskyttelsesenheden brug af ansigtsgenkendelsesteknologi indtil december 2023, dog med mulighed for forlængelse, indtil der kommer tilstrækkelig lovregulering af området. Forbuddet gælder imidlertid ikke efterforskninger foretaget af retsvæsnet eller anden kriminalitetsbekæmpelse.

---

[226] Proposition de loi n° 504, adoptée par lAssemblée nationale relative à la sécurité globale (assemblee-nationale.fr) (kun på fransk); og Macrons Global Security bill passed into law in France, artikel fra 19. April 2021.
[227] Proposition de loi n°1342, adoptée par le Sénat, relative à la reconnaissance biométrique dans l'espace public (kun på fransk).
[228] Proposition de loi relative à la reconnaissance biométrique dans l'espace public (kun på fransk).
[229] Proposition de loi relative à la reconnaissance biométrique dans l'espace public (kun på fransk).
[230] Initial wins in Italy just two months after the launch of Reclaim Your Face, European Digital Rights (EDRi); og Databeskyttelsesenhedens afgørelse (oversat).
[231] Ibid.
[232] Face recognition at Italian borders shows why we need a ban, artikel af the European Data Protection Supervisor og the European Data Protection Board; se også Den Viminale-Guarantor sammenstød af privatlivets fred på ansigtsgenkendelse i realtid, artikel fra januar 2021 (oversat).
[233] Pressemeddelse af italiensk databeskyttelsesenhed: "Videosorveglianza: stop del Garante privacy a riconoscimento facciale e occhiali smart. L'Autorità apre istruttorie nei confronti di due Comuni" af 14. November 2022 (kun på italiensk).

Nederlandene

Det nederlandske politi har siden 2016 anvendt ansigtsgenkendelsesteknologi til at identificere mistænkte og efterlyste personer gennem en database, der indeholder biometriske data fra samtlige mistænkte og tidligere dømte i alvorlige straffesager siden 2010.[234] Databasen indeholder således informationer fra op mod 1,4 millioner mennesker.[235] De biometriske data kan opbevares i mange år, og det nederlandske politi og justitsministerium har erkendt, at der er en reel risiko for, at følsomme oplysninger om personer, der senere er fundet uskyldige, opbevares uberettiget i databasen.[236]

Lignende den allerede eksisterende database for mistænkte og tidligere dømte kunne flere medier i 2023 berette, at det nederlandske politi havde etableret en database med millioner af billeder af mennesker, som var migreret til Nederlandene fra ikke-EU-lande.[237] Der er tale om en database etableret sideløbende med databasen for mistænkte og tidligere dømte, og der benyttes ligeledes ansigtsgenkendelsesteknologi til denne database.[238] Billederne er blevet optaget til databasen i forbindelse med indgivelse af pasbillede til ansøgning om opholdstilladelse – uagtet om migranterne har været mistænkte eller dømt for lovbrud.

På trods af den i forvejen betænkelige implementering af teknologien, udtalte den nederlandske justitsminister i et åbent brev i november 2019, at staten var åben over for idéen om, at politiet skulle kunne udføre eksperimenter med ansigtsgenkendelse.[239] En professor ved Twente Universitet har sidenhen afdækket, at der bliver foretaget eksperimenter med ansigtsgenkendelsesteknologi på politiets kropskameraer.[240] I en rapport fra juli 2021 konkluderede the Edinburgh International

[234] The rise and rise of biometric mass surveillance in the EU, the Edinburgh International Justice Initiative (EIJI), 7. juli 2021, s. 61: og https://www.bitsoffreedom.nl/wp-content/uploads/2019/11/het-ware-gezicht-van-gezichtsherkenning-stechnologie.pdf (kun på hollandsk). Se også udgivelsen fra Dataetisk Råd om "Hvad er ansigtsgenkendelse?", udgivet 11. november 2022, side 10, om den hollandske model, hvor politiet har oprettet en særlig biometri-enhed med ansvar for ansigtsgenkendelse, der på forespørgsel arbejder med at identificere personer, uden at kende til den konkrete sag.
[235] The rise and rise of biometric mass surveillance in the EU, the Edinburgh International Justice Initiative (EIJI), 7. juli 2021, s. 61., og Dutch police facial recognition database includes 1.3 million people, artikel fra 22. juli 2019.
[236] The rise and rise of biometric mass surveillance in the EU, the Edinburgh International Justice Initiative (EIJI), 7. juli 2021, s. 61; Ansigtsgenkendelse i det offentlige rum: Skal vi være tilfredse med det?, artikel fra januar 2020. (oversat); og Titusinder af mennesker kan være uberettiget i politiets ansigt database, artikel fra 16. marts 2021 (oversat).
[237] NL Times, "Millions of passport photos of innocent foreigners in police face database", af 4. februar 2023.
[238] Utrecht University, "Expats, asylum seekers and foreign students in biometric police database," af 16. februar 2023. https://nltimes.nl/2023/02/04/millions-passport-photos-innocent-foreigners-police-face-database
[239] Letter from the Minister of Justice and Security, 20th of November 2019.
[240] The rise and rise of biometric mass surveillance in the EU, the Edinburgh International Justice Initiative (EIJI), 7. juli 2021, s. 63.

Justice Initiative, at det præcise indhold af eksperimenterne med ansigtsgenkendelsesteknologi i Nederlandene er uklart, og at det er svært at finde frem til forsøgets præcise detaljer, formål, og retssikkerhedsgarantier.[241]

Storbritannien

I 2019 afsagde High Court of England and Wales dom over politiets brug af ansigtsgenkendelsesteknologi, herunder om anvendelsen er forenelig med menneskeretten og relevant databeskyttelseslovgivning.[242]

Dommen vedrørte lovligheden af Sydwales politis anvendelse af ansigtsgenkendelsesprogrammet "AFR Locate"[243] såvel generelt som i forbindelse med to specifikke begivenheder, hvor sagens klager var til stede. Sydwales Politi var den første britiske politikreds til at anvende ansigtsgenkendelsesteknologi i realtid i forbindelse med omkring 50 begivenheder mellem 2017 og 2019.[244] Anvendelsen foregik ved, at en algoritme sammenlignede billeder af personer fra konkrete overvågningslister med billeder fra begivenhederne i realtid.[245] Overvågningslisterne bestod af mellem 400 og 800 personer, der alle figurerede på listerne, fordi de enten var (a) eftersøgt, (b) ulovligt på fri fod, (c) mistænkt, (d), personer med behov for beskyttelse (f.eks. efterlyste personer), om end individer, hvis tilstedeværelse til specifikke begivenheder forårsagede særlig bekymring, (f) personer af interesse for politiet og (g) sårbare personer.[246]

Af hensyn til retssikkerheden var anvendelsen underlagt en række begrænsninger, herunder *at* politiet informerede befolkningen om anvendelsen af teknologien på forhånd, *at* indgreb forudsatte, at et match først var blevet efterset og bekræftet af en kontrollant, og *at* de indsamlede biometriske oplysninger på personer, der ikke var en del af overvågningslisterne, blev slettet automatisk og med det samme.[247]

Første instans ved High Courts erklærede i 2019 anvendelsen af teknologien for at være forenelig med artikel 8 i EMRK. I vurderingen af, om indgrebet var proportionelt, lagde domstolen særligt vægt

[241] The rise and rise of biometric mass surveillance in the EU, the Edinburgh International Justice Initiative (EIJI), 7. juli 2021, s. 63.
[242] R v The Chief Constable of South Wales, High Court of Justice, 4. september 2019.
[243] 'AFR' står for 'Automated Facial Recognition'. Ansigtsgenkendelsesteknologien blev i Storbritannien anvendt i to forskellige programmer: 1) 'AFR Identify' og 2) 'AFR Locate'. AFR Identify er en bagudrettet form for ansigtsgenkendelse til at opklare allerede begået kriminalitet, hvor f.eks. overvågningsbilleder af ukendte gerningsmænd kan sammenlignes med en database af billeder af tidligere dømte i forbindelse med en efterforskning. AFR Locate er ansigtsgenkendelse, der analyserer billeder i realtid, f.eks. i forbindelse med større begivenheder, hvor live-billeder fra begivenhederne sammenlignes med en database af billeder fra en konkret overvågningsliste, som myndighederne har udarbejdet. Dommen vedrørte alene anvendelsen af AFR Locate. Se R v The Chief Constable of South Wales, High Court of Justice, 4. september 2019, præmis 27 og 28.
[244] Ibid., præmis 28.
[245] Ibid., præmis 36.
[246] Ibid., præmis 30 og 31.
[247] Ibid., præmis 32, 37 og 39.

på, *at* teknologien var blevet anvendt på en åben og transparent måde, *at* indgrebet var afgrænset med hensyn til tid og sted, *at* den blev anvendt med det specifikke og afgrænsede formål at identificere bestemte personer, *at* anvendelsen havde ført til to anholdelser, *at* ingen var blevet fejlagtigt anholdt, og *at* indgrebet var begrænset til den næsten øjeblikkelige algoritmiske behandling og efterfølgende sletning af de biometriske data.[248]

Dommen blev efterfølgende anket til appelinstansen – the Court of Appeal of England and Wales – der i august 2020 omstødte dommen.[249] The Court of Appeal of England and Wales fandt, at anvendelsen af ansigtsgenkendelsesteknologien ikke havde klar lovhjemmel (ikke var in acordance with the law) og at grænserne for, hvem der kunne komme på overvågningslisterne, havde været for vide.[250] Der var endvidere ikke taget tilstrækkelig højde for, at overvågningen kunne medføre indirekte diskrimination.[251]

En tilsvarende ansigtsgenkendelsesteknologi har også været anvendt af andre politikredse i Storbritannien. London Metropolitan Politi gennemførte f.eks. i perioden mellem 2016 og 2019 ti test af ansigtsgenkendelse.[252] Anvendelsen og udarbejdelsen af overvågningslister blev i en rapport fra London Policing Ethics Panel og sidenhen også i en akademisk rapport udarbejdet af Essex Universitet kritiseret for at mangle proportionalitetsvurdering og gennemsigtighed, ligesom der sattes spørgsmålstegn ved forskningsmetodologien og eksperimenternes etiske fundament.[253] I en rapport fra 2019 konkluderede House of Commons Science and Technology Committee tillige, at staten burde vente med anvendelsen af ansigtsgenkendelsesteknologi, indtil en tilstrækkelig præcis og retssikkerhedsmæssig betryggende lovgivningsramme var på plads.[254] Med henvisning til ovennævnte dom afsagt af High Courts erklærede staten dog, at den nuværende lovgivning allerede indeholdt en tilstrækkelig beskyttelse mod uproportionelle indgreb, ligesom den britiske justitsminister udtalte, at ansigtsgenkendelsesteknologien blev anvendt inden for disse rammer.[255]

[248] Ibid, præmis 101.
[249] R v The Chief Constable of South Wales, Court of Appeal, 11. august 2020.
[250] Ibid., se bl.a. præmis 90,91, 94 og 120.
[251] Ibid, præmis 199-202
[252] Facial recognition technology: fundamental rights considerations in the context of law enforcement, European Union Agency for Fundamental Rights, s. 12.
[253] Interim Report on Live Facial Recognition, London Policing Ethics Panel (2018); og Independent Report on the London Metropolitan Police Services Trial of Live Facial Recognition Technology, University of Essex, juli 2019.
[254] The House of Commons Science and Technology Committees report, juli 2019, side. 14-19; se også Facial recognition technology: police powers and the protection of privacy, artikel fra 31. marts 2021.
[255] Debate about facial recognition technology on Monday 16 March 2020; se også Facial recognition technology: police powers and the protection of privacy, artikel fra 31. marts 2021.

Sidenhen valgte London Metropolitan Police at kommissionere sin egen rapport fra National Physical Laboratory i samarbejde med University of Kent.[256] Rapporten udkom i marts 2023, og dens konklusioner har fået politiet til at genoptage brugen af ansigtsgenkendelsesteknologi i forbindelse med tv-overvågning i realtid.[257]

Store dele af den europæiske debat om ansigtsgenkendelsesteknologi udspringer af eksemplerne fra Storbritannien, men teknologien er længe blevet testet og anvendt i flere andre europæiske lande.[258]

Sverige

I Sverige har politiets brug af ansigtsgenkendelsesteknologi i forbindelse med efterforskning og strafforfølgning været godkendt af Den Svenske Databeskyttelsesenhed siden oktober 2019.[259] I februar 2021 fandt den Svenske Databeskyttelsesenhed imidlertid, at det svenske politi ulovligt havde behandlet personlige data i strid med svensk datalovgivning ved at have anvendt Clearview AI til at identificere individer ved flere lejligheder.[260] Den svenske stats implementering af teknologien har dog ikke været begrænset til formål om strafforfølgning og forebyggelse af kriminalitet, idet teknologien bl.a. også er blevet anvendt i et piloteksperiment på en svensk skole i november 2018 for at kontrollere elevernes fremmøde.[261] Den Svenske Databeskyttelsesenhed udstedte i den forbindelse en bøde til skolen for at have handlet i strid med EU's databeskyttelseslovgivning.[262]

I lyset af den seneste bølge af vold i Sverige har den svenske regering præsenteret en ny kameraoffensiv, der blandt andet skal give politiet bedre betingelser for at bruge ansigtsgenkendelse, automatisk aflæsning af nummerplader og direkte adgang til trafikkameraer.

Den svenske regering nedsatte i starten af 2023 en kameraovervågningsundersøgelse, der består af to dele. I den første del undersøges behovet for forenklede regler for kameraovervågning for kommuner og regioner. Udgangspunktet er, at tilladelseskravet til kommuner og regioner fjernes, når de

[256] Facial Recognition Technology In Law Enforcement Equitability Study, Final Report, March 2023, National Physical Laboratory.
[257] Forbes: "UK Police Forces To Resume Use Of Live Facial Recognition," af 6. April 2023.
[258] Official LFT Deployments in 2020; og Statistik fra Sywales´ Politi.
[259] Politimyndighedens samråd med Datainspektionen, 23. oktober 2019 (kun på svensk). Se også Facial Recognition Technologies from a Swedish Data Protection Perspective, artikel fra 27. oktober 2020, og Police Use of Facial Recognition Tech Approved in Sweden, artikel fra 25. oktober 2019.
[260] Swedish DPA: Police unlawfully used facial recognition app, European Data Protection Board, 12. februar 2021, og afgørelsen fra Integritetsskyddsmyndigheten af 10. februar 2021 (kun på svensk).
[261] Facial recognition in school renders Swedens first GDPR fine, pressemeddelelse af The European Data Protection Board, 22. August 2019; How to interpret Swedens first GDPR fine on facial recognition in school, artikel af The International Association of Privacy Professionals; og In the EU, facial recognition in schools gets an F in data protection, artikel af Accessnow, 10. december 2019.
[262] Den Svenske Databeskyttelsesenheds afgørelse af 20. August 2019. Se også artiklen 'Facial Recognition Technologies from af Swedish Data Protection Perspective' af 26. oktober 2020.

vil kameraovervåge offentlige steder. I den anden del undersøges de øgede muligheder for kameraovervågning for politiet. Det undersøges også, om det er muligt for politiet i højere grad at foretage kameraovervågning med droner, og om der kan indføres flere undtagelser fra kravene om visning af kameraovervågning. Det skal føre til, at politiet kan få bedre betingelser for at bruge kameraovervågning med automatisk aflæsning af nummerplader, få adgang til kameraovervågningsmateriale fra andres overvågning, fx trafikkameraer, og i højere grad kunne bruge ansigtsgenkendelse til at kunne identificere eksempelvis bandemedlemmer. På den baggrund undersøges mulighederne for, at politiet kan få øget adgang til overvågningskameraer, så antallet af faste og mobile overvågningskameraer øges fra det nuværende mål på 1.600 overvågningskameraer til 2.500 overvågningskameraer i 2024.[263]

Der er endvidere besluttet som led i den svenske regerings kameraoffensiv mod bandekriminalitet, at det svenske politi, Trafikverket og den svenske transportstyrelse undersøger, hvordan politiet inden for rammerne af eksisterende regler kan få øget adgang til kamerasystemer, der er tilknyttet den statslige transportinfrastruktur med det formål, at politiet i realtid skal kunne overvåge begivenheder og bestemte geografiske områder for effektivt at bekæmpe og modvirke kriminalitet. En redegørelse for mulighederne herfor skal være den svenske regering i hænde marts 2024.[264]

Tyskland

I Tyskland varierer anvendelsen af ansigtsgenkendelsesteknologi som følge af de enkelte delstaters selvstyre.[265] Tyskland har imidlertid længe eksperimenteret med ansigtsgenkendelsesteknologi, idet de første piloteksperimenter blev udført så tidligt som i 2003 i Bielefeld og Coesfeld, 2004 i Mönchengladbach og 2009 i Düsseldorf.[266] Implementeringen af teknologien har dog været særligt tiltagende i de seneste år. I en rapport fra juli 2021 konkluderede the Edinburgh International Justice Initiative således, at der generelt er en stigende tendens til at implementere biometrisk overvågning i Tyskland, og i 2021 udtalte den tyske indenrigsminister ligeledes, at anvendelsen af ansigtsgenkendelse i Tyskland er fordoblet hvert år siden 2018, og at teknologien er blevet anvendt på 4.403 personer i 2020.[267] I april 2020 udtalte den tyske overvågningsproducent Dallmeier endvidere, at dets overvågningssystem, med indbygget mulighed for biometrisk analyse, blev anvendt af det tyske politi i mindst 19 byer.[268] Af de 19 byer er Köln særligt iøjnefaldende, idet der i november 2020 var

[263] Pressemeddelelse af 5. oktober 2023: Ny kameraoffensiv mot de kriminella nätverken – nya och bättre verktyg till Polismyndigheten - Regeringen.se
[264] Pressemeddelelse af 13. oktober 2023: Polismyndigheten ska få ökad tillgång till befintliga kamerasystem - Regeringen.se
[265] The rise and rise of biometric mass surveillance in the EU, the Edinburgh International Justice Initiative (EIJI), 7. juli 2021, s. 19.
[266] Ibid.
[267] Ibid; og Question about number of people identified with facial recognition technology (kun på tysk).
[268] Dallmeier presents success record for video security in the German "Safe City" segment, 29. april 2020; og The rise and rise of biometric mass surveillance in the EU, the Edinburgh International Justice Initiative (EIJI), 7. juli 2021, s. 23.

omkring 79 overvågningskameraer i brug til ansigtsgenkendelse.[269] I januar 2021 fandt Den Administrative Domstol i Köln, at overvågningen indebar en så væsentlig risiko for borgernes retssikkerhed, at den i en afgørelse udstedte et påbud til Köln Politi om øjeblikkeligt at stoppe overvågningen, indtil en domstol har truffet endelig afgørelse i sagen.

Et andet bemærkelsesværdigt eksempel på Tysklands implementering af ansigtsgenkendelsesteknologi er Hamborgs Politis anvendelse af teknologien i forbindelse med G20-topmødet i juli 2017. Under topmødet blev der indsamlet biometriske data fra store menneskemængder, som efterfølgende blev henlagt i den nu slettede database, hvor den blev sammenlignet med billeder af tidligere mistænkte og dømte. I en efterfølgende rapport konkluderede Hamborgs Kommissær for Databeskyttelse og Informationsfrihed, at anvendelsen var i strid med databeskyttelseslovgivningen, som senere blev fulgt op med et påbud til politiet om at slette databasen.[270] Den Administrative Domstol i Hamborg omstødte imidlertid denne afgørelse, idet den fandt, at kommissæren ikke havde haft hjemmel til at træffe afgørelsen.[271] Domstolens afgørelse er siden anket.[272] Politiet endte dog med at slette databasen den 28. marts 2020.[273] Hamborgs Kommissær for Databeskyttelse og Informationsfrihed har sidenhen også truffet afgørelse i en sag vedrørende den kontroversielle amerikanske virksomhed Clearview AI, hvor virksomhedens database erklæres ulovlig efter GDPR-regler.[274]

Østrig

Det østrigske politi har siden december 2019 brugt ansigtsgenkendelsesteknologi i en forsøgsfase.[275] Den østrigske indenrigsminister har i den forbindelse udtalt, at ansigtsgenkendelsesteknologi udelukkende er tiltænkt anvendt til bekæmpelse af alvorlig kriminalitet, såsom bankrøverier og drab.[276] I 2020 blev teknologien anvendt i forbindelse med 931 straffeovertrædelser.[277] Ifølge Amnesty er der omkring 600.000 mistænkte og tidligere dømte personer registreret i databasen til brug for ansigtsgenkendelse. Amnesty har kritiseret brugen af teknologien med henvisning til, at indgrebet ikke lever

[269] The rise and rise of biometric mass surveillance in the EU, the Edinburgh International Justice Initiative (EIJI), 7. juli 2021, s. 20.
[270] Facial recognition technology: fundamental rights considerations in the context of law enforcement, European Union Agency for Fundamental Rights, s. 12; Rapporten fra Hamborgs Kommisær for Databeskyttelse og Informationsfrihed (kun på tysk); og DPAs order to delete database (kun på tysk).
[271] The rise and rise of biometric mass surveillance in the EU, the Edinburgh International Justice Initiative (EIJI), 7. juli 2021, s. 28; og Decision of The Hamburg Administrative Court, 23. oktober 2019 (kun på tysk).
[272] Ibid.; og DPAs appeal, 13. marts 2020 (kun på tysk).
[273] Hamburg Police deletes the biometric database for facial recognition created in the course of the G20 investigations, 28. maj 2020.
[274] Ruling of the Hamburg Data Protection Authority on 27th of January 2020 (se også Hamburg: HmbBfDI issues decision initiating administrative proceedings against Clearview AI Inc.).
[275] Evidence shows why we need a law against biometric mass surveillance, kampagne af the European Data Protection Supervisor og the European Data Protection Board; se også "Digital ansigtsgenkendelse i 931 forbrydelser", artikel fra 23. november 2020 (kun på tysk).
[276] Ibid.; og Answer to parliamentary question (kun på tysk).
[277] Ibid.; se også Politi: Grasserende brug for ansigtsgenkendelse, artikel fra November 2020 (oversat).

op til kravet om at være "foreskrevet ved lov" i medfør af EMRK.[278] På trods af indenrigsministerens tidligere udtalelse om en tydelig afgrænset benyttelse af teknologien kunne flere nyhedsmedier i september 2020 rapportere om, at politiet havde anvendt teknologien til at identificere demonstranter under en større demonstration i Wien, hvilket umiddelbart blev bekræftet i indenrigsministerens senere svar på et parlamentarisk spørgsmål.[279]

10.2 Ansigtsgenkendelse i USA

En udtømmende gennemgang af omfanget af ansigtsgenkendelse i USA er ikke mulig indenfor rammerne af denne rapport. Det følgende er derfor blot for at give en fornemmelse af, hvordan ansigtsgenkendelsesteknologi finder anvendelse i USA.

Organisationen Fight for the Future[280] har udarbejdet et interaktivt kort, der – i det omfang organisationen er bekendt med det – angiver, hvor i USA, der anvendes ansigtsgenkendelsesteknologi, og hvor der på lokalt og statsligt niveau er iværksat tiltag til at begrænse anvendelsen.[281]

I juni 2021 offentliggjorde the US Government Accountability Office desuden en rapport, der viser, at 20 ud af 42 adspurgte føderale myndigheder med virke indenfor retshåndhævelse ejede eller anvendte et system med ansigtsgenkendelsesteknologi.[282] De enkelte myndigheders konkrete anvendelse af teknologien varierer og omfatter bl.a. efterforskning i straffesager, overvågning og verifikation af rejsendes identitet.[283]

Der er Justitia bekendt ikke vedtaget nogen specifik føderal lovgivning i USA vedrørende anvendelse af ansigtsgenkendelsesteknologi, hvilket har givet anledning til kritik.[284] Bl.a. indstillede tre store udbydere af ansigtsgenkendelsesteknologi – IBM, Amazon og Microsoft – deres udbud af ydelserne til retshåndhævende myndigheder i USA i 2020 i et opråb om, at området skulle reguleres på betryggende vis.[285]

---

[278] Austria: Call for ban on facial recognition for criminal prosecution, artikel fra 18. maj 2021; se også Amnestys rapport (kun på tysk).
[279] Police in Austria use facial recognition for demonstrations, artikel fra 16. september 2020; og Answer to parliamentary question (kun på tysk).
[280] Fight for the Future er en organisation der arbejder for at forsvare grundlæggende rettigheder i den digitale tidsalder. Information om organisationen kan tilgås her
[281] Kortet kan tilgås her.
[282] GAO, Facial Recognition Technology – Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks, juni 2021.
[283] GAO, Facial Recognition Technology – Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks, juni 2021, s. 17 ff.
[284] The International Association of Privacy Professionals (IAPP): "Will there be federal facial recognition regulation in the US? (iapp.org)", af 11. februar 2021 og CNBC: "Rules around facial recognition and policing remain blurry (cnbc.com)", af 12. juni 2021.
[285] Se What is the Azure Face service? - Azure Cognitive Services | Microsoft Docs, We are implementing a one-year moratorium on police use of Rekognition (aboutamazon.com) og IBM CEO's Letter to Congress on Racial Justice Reform

Samtidig er der på tværs af USA vedtaget en række lokale forbud mod myndighedernes anvendelse af ansigtsgenkendelse, hvor San Fransisco med vedtagelsen af et forbud i maj 2019 var den første amerikanske by ti at indføre et sådan forbud. Forbuddenes nærmere indhold og omfang varierer.[286] Desuden er der vedtaget/påtænkes vedtaget en række lokale/statslige love, der regulerer anvendelsen af ansigtsgenkendelse bl.a. via gennemsigtighedskrav[287] eller forbud mod visse former for ansigtsgenkendelsesteknologi, f.eks. politiets anvendelse af kropskameraer med ansigtsgenkendelsesteknologi.[288]

Ansigtsgenkendelse og regulering af teknologien skabte debat under Black Lives Matter demonstrationerne i sommeren 2020, hvor det kom frem, at politiet ved flere lejligheder havde anvendt ansigtsgenkendelsesteknologi.[289] Også i forbindelse med "the Capitol Riot" den 6. januar 2021 blev der sat opmærksomhed på teknologien.[290] Ikke desto mindre er der ikke indført regulering af teknologien på føderalt niveau i USA, og adskillige byer og stater, herunder Virginia og Californien, har for nylig ophævet eller begrænset deres forbud mod brug af ansigtsgenkendelsesteknologi.[291]

10.3 Ansigtsgenkendelse i Kina

Det er uvist, hvor udbredt den kinesiske regerings anvendelse af det sociale pointsystem og ansigtsgenkendelse er. En fyldestgørende kortlægning af dette emne ville i sig selv kræve et særdeles omfattende stykke arbejde, der falder uden for denne rapports grænser. Dette afsnit om Kina er derfor blot for at give en fornemmelse af omfanget af anvendelsen af ansigtsgenkendelse i Kina, hvad teknologien kan blive brugt til, og hvilke muligheder – og ikke mindst ulemper – der er forbundet med at leve i et overvågningssamfund.

Idéen bag det sociale pointsystem i Kina er, at kinesiske borgere, virksomheder og myndigheder bliver overvåget, og på den baggrund bliver den pågældendes person eller virksomheds troværdighed vurderet, hvilket danner grundlag for at tildele henholdsvis straf og belønning. Der sker med

[286] Se Ban Facial Recognition
[287] Se The Mercury News: "BART adopts new transparency rules for surveillance tech (mercurynews.com)", af 13. September 2018.
[288] Se Electric Frontier Foundation: "Victory! California Governor Signs A.B. 1215 | Electronic Frontier Foundation (eff.org)", af 9. oktober 2019.
[289] Lawfare: "On Facial Recognition, the U.S. Isn't China—Yet - Lawfare (lawfareblog.com)", af 14. august 2020, Gothamist: "NYPD Used Facial Recognition Technology In Siege Of Black Lives Matter Activist's Apartment - Gothamist", af 14. august 2020, US News: "States Push Back Against Use of Facial Recognition by Police | California News | US News", af 5. maj 2021 og Buzzfeed News: "Minneapolis Police Can Use Facial Recognition And License Plates Readers To Identify Protesters (buzzfeednews.com)", af 30. maj 2020.
[290] The International Association of Privacy Professionals (IAPP): "Will there be federal facial recognition regulation in the US? (iapp.org)", af 11. februar 2021
[291] Reuters: "Focus: U.S. cities are backing off banning facial recognition as crime rises", af 12. maj 2022.

andre ord en rating af den enkelte person eller virksomhed på baggrund af indsamlet og analyseret data fra en række forskellige kilder.[292]

Mange nyhedsmedier har skrevet sporadisk om både det sociale pointsystem og ansigtsgenkendelse i Kina og har kunnet berette om, at ansigtsgenkendelse bl.a. anvendes til at stoppe tyveri af toiletpapir fra offentlige toiletter og til at forhindre fodgængere i at gå over for rødt lys.[293] Sidstnævnte sker bl.a. ved at udskamme folk offentligt via billedopslag på digitale skilte, der viser offentligheden ansigterne på dem, der ikke har respekteret det røde lys.[294] Som eksempler på pointreducerende adfærd i det sociale pointsystem er bl.a. nævnt dårlig bilkørsel, rygning i ikke-ryger zoner, køb af for mange videospil, at poste fake news online, ikke at besøge sine forældre på jævnlig basis eller at snyde i online-spil.[295] Restriktioner i den enkeltes muligheder for at optage banklån, benytte sig af fly- og togrejser samt begrænsninger i uddannelses- og jobmuligheder er nævnt som eksempler på mulig straf.[296]

Mediernes afbildning af Kinas sociale pointsystem er imidlertid blevet kritiseret for at være misvisende og unuanceret og for at blande systemet sammen med øvrige foretagender i Kina.[297]

Efter sigende anvendes der kunstig intelligens sammen med Kinas mange millioner overvågningskameraer i forbindelse med det sociale pointsystem, men det egentlige omfang heraf fremstår uklart.[298] Videoovervågning med ansigtsgenkendelse er desuden blot én (måske mindre) del af det nuværende sociale pointsystem i Kina, der fortsat i høj grad opereres manuelt.[299]

En vigtig detalje i den forbindelse er dog, at der sideløbende med det sociale pointsystem foregår massiv videoovervågning med ansigtsgenkendelse i Kina. Som eksempel kan systemet "Skynet" nævnes. Skynet, der er udviklet af virksomheden Megvii, udgør et omfattende netværk af statsovervågede overvågningskameraer i Kina. Systemet omfatter flere 100 millioner kameraer.[300] Der anvendes ansigtsgenkendelsesteknologi i forbindelse med overvågningen, men det er pt. ikke dokumenteret, at Skynet er integreret med det sociale pointsystem.[301] Kameraerne registrerer alt i realtid, og en

[292] Kai Strittmatter, We Have Been Harmonised – Life in China's Surveillance State, 2019, s. 201–203.
[293] CNN: "Chinese park goes hi-tech to stop toilet paper thieves - CNN", af 21. marts 2017 og How China Tracks Everyone – YouTube.
[294] CNET: "How China uses facial recognition to control human behavior - CNET", af 11. August 2020.
[295] Business Insider: "China Social Credit System, Punishment and Rewards Explained", af maj 2021, tilgængelig her.
[296] South China Morning Post: "What is China's Social Credit System and Why is it Controversial", af august 2020, tilgængelig her, Business Insider: "China Social Credit System, Punishment and Rewards Explained," af maj 2021, tilgængelig her.
[297] Se f.eks. ChenChen Zhang – Governing (through) trustworthiness: Technologies of power and subjectification in China's Social Credit System, September 2020 og Robert Schuman Centre for Advanced Studies 2020/28, Liav Orgad & Wessel Reijers, How to make the perfect citizen? Lessons from China's Model of Social Credit System.
[298] PhD Drew Donelly, An Introduction to the China Social Credit System, 15. September 2021, tilgængelig her
[299] ibid.
[300] ibid.
[301] ibid.

medarbejder hos Skynet har oplyst, at over 3.000 eftersøgte borgere blev fundet via Skynets ansigtsgenkendelse på ét år.[302] Som et andet eksempel kan nævnes en video fra 2017, hvor BBC ved et iscenesat forsøg viste, at det tog Kinas regering syv minutter at lokalisere en journalist i Kina ved at anvende landets videoovervågning med ansigtsgenkendelse.[303]

Selvom det sociale pointsystem endnu ikke er færdigimplementeret, og selvom ansigtsgenkendelse tilsyneladende kun er en mindre del af et langt mere komplekst evalueringssystem, er der utvivlsomt tale om en styringsform, der ideologisk set eksemplificerer, hvad ansigtsgenkendelse i (måske) yderste konsekvens kan medføre.[304]

Der er en række love og regler på nationalt niveau, der dækker forskellige aspekter af ansigtsgenkendelsesteknologi.

Kina's National Information Security Standardization Technical Committee (TC260) indførte den 1. maj 2023 krav om datasikkerhed for brugen af ansigtsgenkendelsesteknologier, som omfatter regler om private virksomheders indsamling, behandling og opbevaring af data.[305] Det antages imidlertid af forskere og eksperter, at mens offentlige myndigheder opfordres til at kigge på de nye regler ved udarbejdelse og brug af ansigtsgenkendelsesteknologier, så er de ikke bundet heraf.[306]

Den 1. november 2021 trådte Lov om Beskyttelse af Personlige Oplysninger i kraft i Kina.[307] Loven er i høj grad baseret på EU's databeskyttelsesforordning.[308] Artikel 26 i loven regulerer specifikt håndtering af biometrisk data opsamlet til brug for ansigtsgenkendelse. Loven kræver, at "billedindsamlings- og personligt identifikationsudstyr" på offentlige steder kun må installeres, når det er nødvendigt for at opretholde den offentlige sikkerhed.[309] Desuden må den indsamlede biometriske data kun bruges til at opretholde den offentlige sikkerhed, medmindre de enkelte personers særskilte samtykke er indhentet. Det er dog også i forhold til denne regulering uvist, i hvilken udstrækning offentlige myndigheder er bundet af den, omend det antages, at staten er forpligtet af artikel 26.[310]

[302] How China Tracks Everyone - YouTube
[303] BBC: "In Your Face: China's all-seeing state - BBC News", af 10. december 2017.
[304] Yan Luo, & Rui Guo, Facial Recognition in China: Current Status, Comparative Approach and the Road Ahead, 25 U. Pa. J.L. & Soc. Change 153 (2022).
[305] ibid.
[306] Ibid., side 164.
[307] Personal Information Protection Law of the People's Republic of China
[308] The Personal Information Protection Law: China's Version of the GDPR?, Columbia Journal of Transnational Law, 14. februar 2022.
[309] Personal Information Protection Law of the People's Republic of China
[310] Brookings, "Seven major changes in China's finalized Personal Information Protection Law," af 23. august 2021; Yan Luo, & Rui Guo, Facial Recognition in China: Current Status, Comparative Approach and the Road Ahead, 25 U. Pa. J.L. & Soc. Change 153 (2022).

Det er således uvist, hvorvidt den kinesiske regulering af ansigtsgenkendelse også gælder for den kinesiske stat, eller om reguleringen alene gælder for private aktører. Det fremgår dog, at Kina er begyndt at regulere området – muligvis med inspiration fra Europa.

11 Konklusion

Når teknologi med ansigtsgenkendelse anvendes i det offentlige rum, kan det i lande som Kina blive brugt som et uproportionalt magtmiddel med store konsekvenser for borgernes frihedsrettigheder, retssikkerhed og sociale tryghed. Et sådant scenarie er selvfølgelig utænkeligt i Danmark, men også her vil politiets anvendelse af ansigtsgenkendelse til kriminalitetsbekæmpelse være et alvorligt indgreb i vores ret til privatliv, fordi unikke biometriske koder for ansigter registreres og spores uden samtykke. Følelsen af konstant at være overvåget vil samtidig kunne true udøvelsen af andre frihedsrettigheder, herunder retten til at forsamle sig og ytre sig, ligesom overvågningsdata i kombination med andre personlige data om borgerne kan anvendes til at danne detaljerede personprofiler, der kan give meget præcise oplysninger om borgernes private forhold. Det gælder ikke mindst med politiets analyseplatform POL-INTEL, der muliggør analyser på tværs af meget store mængder af data fra både interne og eksterne kilder samt offentligt tilgængelige kilder som eksempelvis sociale medier.

Dansk Politis anvendelse ansigtsteknologi har indtil nu været begrænset til verificering af identitet ved paskontrol og digitaliseret offergenkendelse i sager om seksuelt misbrug af børn. Der er dog en aktuel politisk interesse for at udvide politiets muligheder for at anvende ansigtsgenkendelse. Dette fremgår bl.a. af Bandepakke IV "Trygge nabolag i hele Danmark", hvor et bredt flertal i Folketinget i november 2023 var enige om at følge politiets erfaringer med forsøget med digitaliseret offergenkendelse i sager om seksuelt misbrug af børn for at se, om ansigtsgenkendelse også kan bruges som et værktøj i indsatsen mod f.eks. banderne.

Justitsminister Peter Hummelgaard i et samråd den 23. november 2023 oplyst, at han er af den opfattelse, at politiet skal anvende værktøjet, hvis det er nyttigt i arbejdet, så længe det sker inden for de nuværende databeskyttelsesretlige rammer. Justitsministeren gav samtidig udtryk for, at der ikke var behov for at orientere Folketinget om enhver anvendelse af teknologien. Efterfølgende har digitaliserings- og ligestillingsminister Marie Bjerre i et samråd i januar 2024 oplyst, at regeringen mener, at ansigtsgenkendelse i realtid på offentligt område skal kunne anvendes på forbrydelser omfattet af den europæiske arrestordre, ved forbrydelser der har en strafferamme på over fem år, ved forsvundne børn og i forbindelse med terror.[311] Senest har justitsministeren i et svar på et udvalgsspørgsmål den 4. marts 2024 givet udtryk for, at myndighederne bør anvende ansigtsteknologi, når fordelene overstiger ulemperne. Justitsministeren har desuden oplyst, at regeringen for nuværende

[311] Den europæiske arrestordre er en juridisk mekanisme, der gør det muligt for medlemslandene i EU, at anmode om og kræve udlevering af en person, der er mistænkt for eller dømt for alvorlige forbrydelser.

ikke har nogen planer om at justere den retlige ramme for politiets anvendelse af ansigtsgenkendelsesteknologi, og at en eventuel justering af den retlige ramme vil ske under sædvanlig inddragelse af Folketinget.[312]

Ansigtsgenkendelsesteknologien har allerede vundet terræn i flere andre europæiske lande, herunder Østrig, Finland, Frankrig, Tyskland, England, Grækenland, Ungarn, Italien, Letland, Litauen, Nederlandene og Slovenien. I Sverige har regeringen i efteråret 2023 iværksat et initiativ, hvor man vil anvende ansigtsgenkendelsesteknologi i forbindelse med bandekriminalitet. Flere af de nævnte lande er omtalt i kapitel 10.1. Ansigtsgenkendelse er således allerede en del af politiets værktøjskasse i flere europæiske lande, og med de seneste politiske udmeldinger i Danmark er det sandsynligt, at lignende skridt snart vil blive taget for at styrke kriminalitetsbekæmpelsen herhjemme.

En udvidelse af politiets anvendelse af ansigtsgenkendelse skal dog ske med respekt for vores menneskeretlige forpligtelser. Borgernes grundlæggende ret til privatliv mv. er ikke nogen absolut rettighed. Staten kan foretage indgreb i retten, hvis 1) indgrebet forfølger et legitimt formål, 2) indgrebet har en klar lovhjemmel, og 3) indgrebet kan anses for at være proportionalt og nødvendigt i et demokratisk samfund.

Legitimt formål
Justitia anerkender, at politiets anvendelse af ansigtsgenkendelsesteknologi til kriminalitetsbekæmpelse tjener et legitimt formål og samtidig kan være egnet til at bekæmpe visse former for kriminalitet.

Klart lovgrundlag
Politiets anvendelse af ansigtsgenkendelse har derimod ikke et klart lovgrundlag i dag. Efter retshåndhævelsesloven § 10, stk. 2, jf. stk. 1, kan politiet anvende biometriske data, hvis det er strengt nødvendigt for at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder for at beskytte mod eller forebygge trusler mod den offentlige sikkerhed eller beskytte en fysisk persons vitale interesser, eller hvis behandlingen vedrører oplysninger, som tydeligvis er offentliggjort af den registrerede.

Denne bestemmelse regulerer imidlertid alene politiets generelle behandling af biometriske data og har ikke særlig fokus på ansigtsgenkendelsesteknologi, der sammen med kameraovervågning mv. kan udgøre et meget intenst indgreb i retten til privatliv og andre afledede rettigheder. Samtidig kan der – i modsætning til fingeraftryk og DNA-profiler – meget nemt indhentes offentligt tilgængelige fotos af personer på sociale medier mv., som kan anvendes til at skabe biometriske data, hvilket næppe har været i personernes bevidsthed ved offentliggørelsen.

[312] DIU Alm.del - endeligt svar på spørgsmål 101, Folketingets samling 2023-24

Bestemmelsen i retshåndhævelsesloven indeholder desuden vide skøn, som politiet selv skal foretage, ligesom der bl.a. savnes regler om, i hvilke tilfælde, hvordan og i hvilket omfang teknologien kan anvendes. Hertil kommer, at retsplejelovens bestemmelse om observation alene regulerer politiets tv-overvågning mv. på ikke frit tilgængeligt sted, og at kravene er meget lave.

Den Europæiske Menneskerettighedsdomstol (EMD) har allerede i sagen Glukhin mod Den Russiske Føderation, der er omtalt i kapitel 7.1, vurderet, at det ikke er alle former for kriminalitet, der kan retfærdiggøre tv-overvågning og ansigtsgenkendelsesteknologi i **realtid**, og at denne form for overvågning stiller skærpede krav til hjemmelsgrundlaget. Der skal derfor være detaljerede regler, som regulerer omfanget og anvendelsen af teknologien samt stærke sikkerhedsforanstaltninger mod risikoen for misbrug og vilkårlighed.

Det er derimod uafklaret i EMD´s praksis, hvilke krav der kan stilles til retsgrundlaget for politiets **retrospektive** anvendelse af ansigtsgenkendelse. Henset til, hvor intenst indgreb i privatlivet også en retrospektiv anvendelse vil udgøre, og hvor uklart det gældende retsgrundlag er, kan også denne form for overvågning efter Justitias opfattelse blive anset for et uberettiget indgreb i borgernes ret til privatliv og beskyttelse af personoplysninger. Efter Justitias opfattelse bør der således også her stilles krav om et klart retsgrundlag, som både politi og borgere kan forholde sig til.

Proportionel og nødvendig i et demokratisk samfund

Da det endnu ikke er afklaret, hvilke ønsker regeringen har til politiets anvendelse af ansigtsgenkendelse, og der endnu ikke er gjort forsøg på specifikt at regulere politiets anvendelse af teknologien, er det vanskeligt at vurdere, om anvendelsen vil kunne anses for proportionel og nødvendig i et demokratisk samfund. Dette vil nemlig bl.a. afhænge af, hvornår og hvordan politiet skal kunne bruge teknologien, herunder formålet med anvendelsen, hvilke lovovertrædelser der kan komme i betragtning, hvilke kategorier af personer teknologien kan anvendes på, om teknologien skal anvendes i realtid og/eller retrospektivt, hvor teknologien skal anvendes, hvilke retsgarantier der fastsættes for at beskytte borgerne, og om det sikres, at teknologien ikke benyttes til at gruppere individer efter hudfarve, etnicitet, seksualitet eller andre diskriminerende formål.

Politiets anvendelse af ansigtsgenkendelse i realtid vil dog efter Justitias opfattelse i langt de fleste tilfælde kunne blive anset for uproportional og unødvendig i et demokratisk samfund, fordi teknologien kan anvendes til intens overvågning og profilering på individniveau og derfor vil udgøre et meget intens indgreb i borgernes ret til privatliv mv. En reel retrospektiv anvendelse af ansigtsgenkendelse må anses for at være et mindre intenst indgreb, men udgør stadig et markant indgreb i retten til privatliv.

Justitia finder på denne baggrund, at der er behov for en grundig afklaring af, hvilke udvidelser af politiets anvendelse af ansigtsgenkendelse der kan komme på tale nu og i nærmeste

fremtid, samt at det sikres, at der i god tid etableres en meget klar og præcis lovhjemmel, som samtidig sikrer, at anvendelsen kan anses for proportional og nødvendig i et demokratisk samfund.

Nedenfor i kapitel 12 fremsættes en række anbefalinger om politiets anvendelse af ansigtsgenkendelse, hvor der sondres mellem anvendelse i realtid og retrospektiv anvendelse. Hensigten med anbefalingerne er i videst muligt omfang at beskytte borgerne mod indgreb i deres grundlæggende rettigheder, beskytte mod misbrug og vilkårlighed samt sikre retssikkerheden.

12 Justitias anbefalinger

Danmark har et retsforbehold vedrørende EU-samarbejdet inden for civil- og strafferet. Det betyder, at bestemmelserne i AI-forordningen vedrørende politiets anvendelse af ansigtsgenkendelse ikke er gældende i Danmark. Danmark har dog mulighed for at tilslutte sig denne del af AI-forordningen gennem en tilvalgsretsakt.

Efter Justitias opfattelse vil det imidlertid være mest **hensigtsmæssigt at håndtere reguleringen af politiets anvendelse af ansigtsgenkendelse nationalt**. Det vil give Danmark mulighed for at forme og tilpasse lovgivningen i overensstemmelse med egne normer og prioriteter og samtidig sikre, at beslutninger om brug af teknologien sker efter omhyggelig overvejelse af de potentielle konsekvenser for borgernes rettigheder og retssikkerhed, og at lovgivningen løbende kan tilpasses den teknologiske udvikling. Beskyttelsesniveauet i den nationale lovgivning bør naturligvis som minimum være på linje med AI-forordningen, men giver samtidig mulighed for at fastsætte en endnu mere betryggende ramme.

Ansigtsgenkendelse i realtid skaber alvorlige konsekvenser for borgernes rettigheder og andre risicis. Det kan føre til omfattende og intens overvågning, der underminerer vores grundlæggende ret til privatliv og afledede rettigheder som f.eks. vores ret til at forsamle os og ytre os, hvilket er afgørende i et demokratisk retssamfund. Derudover kan der opstå problemer med forudindtagethed og diskrimination på grund af fejl og svagheder i den underliggende teknologi, ligesom der kan opstå problemer med potentiel misbrug og/eller risiko for, at teknologien målrettes bestemte befolkningsgrupper, politiske aktivister eller andre, der kan blive genstand for politisk overvågning.

Det er på denne baggrund **Justitias vurdering, at der bør fastsættes et forbud mod politiets anvendelse af ansigtsgenkendelse i realtid.** Denne vurdering er på linje med European Data Protection Board, Europarådets ad hoc komite CAHAI og FN's højkommissær for menneskerettigheder.

Hvis det alligevel besluttes, at dansk politi skal have adgang til at anvende ansigtsgenkendelse i realtid, bør det efter Justitias opfattelse indsnævres, som beskrevet i første anbefaling nedenfor.

1. Politiets må kun anvende ansigtsgenkendelse i realtid ved overhængende fare for tab af liv.

Ifølge AI-forordningen bliver der bl.a. mulighed for, at politiet kan anvende ansigtsgenkendelsesteknologi i realtid, når det er strengt nødvendigt til bekæmpelse af kriminalitet, som kan straffes med fængsel 4 år eller derover. Justitsminister Peter Hummelgaard og digitaliseringsminister Marie Bjerre har som det fremgår af kapitel 9.2 heller ikke afvist muligheden for, at dansk politi kan anvende ansigtsgenkendelse i realtid i det offentlige rum for at bekæmpe alvorlig kriminalitet og terror mv.

Det er efter Justitias opfattelse afgørende, at politiets anvendelse af ansigtsgenkendelse i realtid begrænses i videst muligt omfang for at beskytte borgernes grundlæggende rettigheder og retssikkerhed. Der er således behov for en nøje afvejning af på den ene side teknologiske fremskridt og muligheder og på den anden side respekten for grundlæggende menneskerettigheder, retsstatsprincipper og dataetiske værdier.

Hvis det besluttes, at dansk politi skal have adgang til at anvende ansigtsgenkendelse i realtid, anbefaler Justitia, at anvendelsen begrænses til situationer, hvor der er overhængende fare for tab liv. Det vil gøre det muligt for politiet at anvende teknologien i f.eks. terrorsager eller sager om bortførelse med henblik på voldtægt af børn og/eller drab

2. Politiets retrospektive anvendelse af ansigtsgenkendelse skal begrænses til lovovertrædelser, der kan straffes med fængsel i 8 år eller derover, og som kan medføre eller har medført fare for menneskers liv eller legeme.

Retrospektiv anvendelse af ansigtsgenkendelse må anses for at være et mindre intenst indgreb end anvendelse i realtid, men udgør stadig et markant indgreb i retten til privatliv. Sammenlignet med f.eks. telefonaflytning og almindelig tv-overvågning må retrospektiv ansigtsgenkendelse anses for mere intenst, fordi det giver mulighed for at kortlægge en formodet gerningspersons færden præcist og effektivt på en måde, som ikke kendes fra traditionelle overvågningsmetoder. Derfor bør kriminalitetskravet efter Justitias opfattelse også være højere.

Det følger allerede af retshåndhævelseslovens § 10, stk. 2, jf. stk. 1, at politiet kun må anvende biometrisk data, når det er strengt nødvendigt for at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, 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

Som nævnt i rapportens konklusion i det foregående kapitel anser Justitia det nuværende retsgrundlag for at være for bredt og upræcist, og at der er behov for en nærmere regulering. For så vidt angår spørgsmålet om, i hvilke sagstyper politiet bør kunne anvende retrospektiv ansigtsgenkendelse, anbefaler Justitia, at der fastsættes krav om, at der skal være tale om kriminalitet, som kan medføre eller har medført fare for menneskers liv eller legeme, og som kan straffes med fængsel i 8 år eller derover. Justitia er klar over, at det er et kriminalitetskrav, som kun tillader anvendelse af ansigtsgenkendelse ved meget begrænsede kriminalitetstyper, men det er efter Justitias vurdering nødvendigt, når der er tale om et så intenst indgreb i privatlivets fred.

Anbefalingen læner sig til dels op ad kriminalitetskravet for bl.a. aflytning og tv-overvågning jf. retsplejelovens §§ 781, stk. 1, nr. 3, og stk. 5, og 791 e, stk. 1, med den undtagelse, at disse to indgreb forudsætter, at lovovertrædelsen kan straffes med fængsel i 6 år eller derover og også giver mulighed for indgreb, når der er tale om fare for "betydelige samfundsværdier." Justitia mener ikke, at "betydelige samfundsværdier" bør inkluderes i en bestemmelse om anvendelse af ansigtsgenkendelsesteknologi, da denne formulering tidligere har givet hjemmel til brug af aflytning ved grove tyverier i private virksomheder.[313]

Hvis det alligevel findes nødvendigt at inkludere flere alvorlige kriminalitetstyper, bør strafferammen for disse efter Justitias opfattelse selvsagt være fængsel i 6 år eller derover. Det betyder, at strafferammen efter Justitias opfattelse under alle omstændigheder bør være højere end den strafferamme på minimum 4 år der fremgår af den AI-forordningstekst, som Europa-Parlamentet den 13. marts 2024 har godkendt, artikel 5, stk. 1, litra h, iii.

3. Generelle anbefalinger til politiets anvendelse af ansigtsgenkendelse i både realtid og retrospektivt

A. En udvidelse af politiets muligheder for at anvende ansigtsgenkendelse bør ske på baggrund af en bred og åben demokratisk samtale om fordele og ulemper samt en dataetisk konsekvensanalyse.

Anbefalingen blev opstillet af Dataetisk Råd i oktober 2021 sammen med en række andre anbefalinger til generel ansigtsgenkendelse i det offentlige rum og alment tilgængelige steder.

Justitia kan tilslutte sig anbefalingen, der må anses for særlig vigtig, når det gælder politiets anvendelse af ansigtsgenkendelse. Da en sådan anvendelse har stor og direkte betydning for borgernes grundlæggende rettigheder og retssikkerhed, er det vigtigt at sikre et solidt beslutningsgrundlag, der er forankret i Folketinget, og drøftet bredt. Justitia anser det derfor for ubetryggende, at justitsministeren for nylig gav udtryk for, at der ikke er behov for at orientere Folketinget om enhver anvendelse af teknologien. Dette skal også ses i lyset af, at det gældende retsgrundlag for politiets anvendelse af ansigtsgenkendelse efter Justitias opfattelse er meget bredt og uklart, hvilket kan give anledning til en for vidtgående fortolkning af mulighederne indenfor den nuværende retlige ramme.

Ifølge den forordningstekst, som Europa-Parlamentet den 13. marts 2024 har godkendt, artikel 5, stk. 2, skal der gennemføres en konsekvensanalyse vedrørende grundlæggende rettigheder, inden der

[313] U2020.2197H

gives tilladelse til biometrisk fjernidentifikation i realtid på offentlige steder. Justitia foreslår en bredere dataetisk konsekvensanalyse, som både skal udarbejdes ved anvendelse af ansigtsgenkendelse i realtid og retrospektivt.

B. Politiets anvendelse af ansigtsgenkendelse skal reguleres som et straffeprocessuelt indgreb i retsplejeloven, der kræver retskendelse, og reguleres nærmere i politiloven.

Den stigende udbredelse af tv-overvågning, som kombineret med ansigtsgenkendelsesteknologi giver politiet mulighed for meget intens overvågning af borgerne, skaber behov for en øget beskyttelse af borgernes grundlæggende rettigheder og retssikkerhed.

Justitia anser det i den forbindelse for afgørende, at der i retsplejelovens fastsættes klare og præcise regler om forudgående indhentelse af en retskendelse, herunder at en sådan overvågning kun må rettes mod en eller flere af politiet kendte personer. Det gælder uanset, om der er tale om ansigtsgenkendelse i realtid eller retrospektiv anvendelse. Dette er på linje med artikel 5, stk. 3, og artikel 26, stk. 10, i den AI-forordningstekst, som Europa-Parlamentet den 13. marts 2024 har godkendt, hvor der også indgår krav om retskendelse. Efter Justitias opfattelse bør der desuden fastsættes nærmere regler om politiets anvendelse af ansigtsteknologi i politiloven.

En tilsvarende anbefaling følger af en analyse fra Institut for Menneskerettigheder om politiets brug af ansigtsgenkendelse i det offentlige rum fra 2024, som bl.a. anbefaler en klar og præcis lovhjemmel i politiloven og retsplejeloven samt krav om retskendelse.[314] Desuden har Dataetisk Råd allerede i oktober 2021 anbefalet en klar, specifik og formålsafgrænset lovhjemmel ved anvendelse af ansigtsgenkendelse.

C. Der skal ikke ske lagring af biometrisk data.

Politiets anvendelse af ansigtsgenkendelse må som udgangspunkt ikke føre til lagring af biometriske data, der repræsenterer en borgers ansigt som en form for unik kode. Sådanne data må efter Justitias opfattelse udelukkende lagres, hvis og så længe det er strengt nødvendigt for en straffesag.

Hvis det alligevel besluttes, at der skal lagres biometriske ansigtsdata, skal der efter Justitias opfattelse fastsættes nærmere regler herom som det kendes fra politiets lagring af fingeraftryk og DNA-profiler. Disse regler bør i så fald også indeholde bestemmelse om, at biometriske ansigtsdata om tilfældige forbipasserende personer ("no hits"), som ikke indgår i en målrettet søgning, skal slettes inden for den teknisk muligt korteste tidsramme.

[314] Institut for Menneskerettigheder, "Politiets brug af ansigtsgenkendelse i det offentlige rum", februar 2024, side 1.

Dataetisk Råd har ligeledes i oktober 2021 anbefalet, at anvendelse af ansigtsgenkendelse ikke bør føre til lagring af biometriske data.

D. Der skal laves en kortlægning og løbende ajourføring af politiets samlede tv-overvågning i det offentlige rum og andre frit tilgængelige steder, herunder også ANPG-kameraer mv. Kortlægningen skal indeholde oplysninger om, i hvilket omfang der er anvendt ansigtsgenkendelse i realtid. Kortlægningen skal være offentlig tilgængelig.

Politiets mulige fremtidige brug af ansigtsgenkendelse vil udgøre et betydeligt indgreb i de berørte borgeres privatliv, hvilket forudsætter gennemsigtighed og ansvarlighed omkring omfang mv. I dag findes der ingen samlede oversigt eller anden form for dokumentation af politiets anvendelse af tv-overvågning og ansigtsgenkendelsesteknologi.

Efter Justitias opfattelse er der behov for en kortlægning og løbende ajourføring af politiets samlede overvågning i det offentlige rum og andre frit tilgængelige steder, der dokumenterer både omfang og formål med politiets brug af tv-overvågning, APNG, bodycams, droner, ansigtsgenkendelse og andre relaterede teknologier. Dette vil ikke kun give offentligheden indsigt i overvågningens anvendelse, men også bidrage til at sikre, at politiet agerer i overensstemmelse med lovgivningen, at overvågningen er afbalanceret og i overensstemmelse med demokratiske principper, samt at borgernes grundlæggende rettigheder i videst muligt omfang respekteres. En sådan gennemsigtighed må samtidig anses for afgørende for at opretholde tilliden mellem samfundet og de retshåndhævende myndigheder. Der bør desuden etableres klare mekanismer og retningslinjer for rapportering og gennemsigtighed i forbindelse med politiets brug af ansigtsgenkendelse.

Dataetisk Råd har ligeledes i oktober 2021 anbefalet, at anvendelse af ansigtsgenkendelse bør være oplistet i en offentlig tilgængelig fortegnelse, og at anvendelsen bør være baseret på åbenhed om formål, anvendelse, metode og teknologi.

E. Det skal undersøges, om der er behov for regulering af politiets observation i det offentlige rum og andre frit tilgængelige steder.

Indtil nu er politiets tv-overvågning og andre metoder til at foretage observationer af borgere på frit tilgængelige steder ikke blevet reguleret i retsplejeloven. Det betyder, at politiet har omfattende beføjelser til at overvåge borgere uden behov for retskendelse eller andre sikkerhedsmekanismer. Gennem tiden har dette bl.a. været begrundet med, at politiets tv-overvågning på frit tilgængelige steder er underlagt den almindelige ulovbestemte proportionalitetsgrundsætning, som indebærer, at politiet ikke uden omhyggelig vurdering af indgrebet kan iværksætte tv-overvågning af borgernes

færden.[315] Derudover er tv-kameraer på frit tilgængelige steder også blev anset som så almindelige, at borgerne forventes at være opmærksomme på dem og naturligt tilpasse deres adfærd herefter.[316] Endvidere har der været en opfattelse af, at den generelle modstand i samfundet mod et "overvågningssamfund" og den politiske kontrol med politiets aktiviteter ville modvirke eventuelle tendenser mod en mere omfattende tv-overvågning af befolkningen.[317] Desuden har der været ressourcemæssige hensyn og prioritering af politiets indsats også sat begrænsninger for omfanget af tv-overvågning på frit tilgængelige steder.[318]

Vi er dog et andet sted i dag med voksende opmærksomhed på de rettighedsmæssige konsekvenser ved et overvågningssamfund samt nye politiker og udvidelser af politiets beføjelser, som har resulteret i større og større indgreb i privatlivets fred. Samtidig har samfundet i høj grad ændret sig teknologisk, hvor kunstig intelligens og deraf ansigtsgenkendelsesteknologi har muliggjort nye effektive og intense muligheder for overvågning. Det gælder ikke mindst med politiets analyseplatform POL-INTEL, der muliggør analyser på tværs af meget store mængder af data fra både interne og eksterne kilder samt offentligt tilgængelige kilder som eksempelvis sociale medier. Hertil kommer politiets muligheder for at modtage kameraovervågningsmateriale fra private og offentlige myndigheder samt muligheden for selv at overtage en sådan overvågning i realtid, når særlige betingelser er opfyldt.

Denne udvikling rejser efter Justitias opfattelse spørgsmål om, hvorvidt der nu er behov for en regulering af politiets overvågning i det offentlige rum for at sikre en afbalanceret beskyttelse af borgernes grundlæggende rettigheder og retssikkerhed. Justitia anbefaler derfor, at justitsministeren iværksætter en undersøgelse af, om der er behov for en regulering af politiets anvendelse af observation i det offentlige rum og andre frit tilgængelige steder.

F. Der skal ske en kortlægning af politiets overtagelse af kameraovervågning fra private og offentlige myndigheder.

I lyset af den ovennævnte udvikling inden for politiets overvågningskapacitet og det politiske ønske om øgede muligheder for politiet til at anvende ansigtsgenkendelsesteknologi, er det efter Justitias opfattelse nødvendigt at undersøge, hvordan politiets administrerer reglerne om overtagelse af kameraovervågning fra private og offentlige myndigheder, herunder om reglerne overholdes og praktiseres efter hensigten.

[315] L 41 om forslag til lov om ændring af retsplejeloven (Beslaglæggelse, edition, fotoforevisning, konfrontation, efterlysning og observation samt prøvesagsordning for advokater m.v.), 8. oktober 1998, Strafferetsudvalgets bemærkninger i afsnit 6.2.2. Se også U.2021.1265
[316] Ibid.
[317] Ibid.
[318] Ibid.

Justitia anbefaler derfor, at justitsministeren iværksætter en kortlægning af politiets overtagelse af kameraovervågning fra private og offentlige myndigheder efter retsplejelovens § 791 e.

G. Det skal undersøges, hvordan der kan sikres en effektiv klageadgang for borgere, som er blevet overvåget af politiet med anvendelse af ansigtsgenkendelse, herunder hvordan borgerne i videst muligt omfang kan blive gjort bekendt med en sådan behandling af deres biometriske ansigtsdata.

Hvis politiets får mulighed for at anvende ansigtsgenkendelse til kriminalitetsbekæmpelse, er det vigtigt, at der sikres en effektiv klageadgang for borgerne og en effektiv kontrol med politiets behandling og anvendelse af biometriske oplysninger.

Klagesystemet for politiets behandling af personoplysninger, adfærd og handlinger samt efterforskningsskridt er præget af en vis kompleksitet for borgerne. Der er flere veje for at indgive forskellige klager i forbindelse med politiets aktiviteter og efterforskning. Politiets dispositioner, såvel inden som uden for strafferetsplejen, behandles og afgøres som udgangspunkt af politidirektøren. Adfærdsklager over politiet behandles, efterforskes og afgøres af Den Uafhængige Politiklagemyndighed (DUP). Borgere, der ønsker at klage over politiets behandling af personoplysninger, skal henvende sig til den myndighed, der er dataansvarlig. Ifølge retshåndhævelsesloven har den registrerede ret til at modtage oplysninger fra den dataansvarlige myndighed, medmindre denne ret skal begrænses af hensyn til private eller offentlige interesser. Myndigheden har beføjelse til at udskyde eller begrænse retten til indsigt, og i visse tilfælde kan det være umuligt for myndigheden at oplyse, om der behandles oplysninger om den registrerede. Hvis myndigheden træffer afgørelse om at nægte, begrænse, udsætte eller undlade den registrerede hans rettigheder, har den registrerede mulighed for at klage til Datatilsynet. [319]

Justitia anbefaler, at justitsministeren iværksætter en undersøgelse af, hvordan der kan sikres en effektiv klageadgang for borgere, som er blevet overvåget af politiet med anvendelse af ansigtsgenkendelse, herunder hvordan borgerne i videst muligt omfang kan blive gjort bekendt med, at politiet har behandlet biometriske oplysninger om deres ansigt. Det anbefales endvidere, at justitsministeren iværksætter en undersøgelse af, hvordan der kan sikres et uafhængigt løbende tilsyn med politiets behandling af biometriske ansigtsdata.

Institut for Menneskerettigheder har i deres analyse fra 2024 også anbefalet et effektivt tilsyn og klageadgang for berørte borgere.[320]

[319] Politi og retsvæsen (emne) (datatilsynet.dk)
[320] Politiets brug af ansigtsgenkendelse i det offentlige rum

H. Politiets anvendelse af ansigtsgenkendelsesteknologi i realtid i det offentlige rum og frit tilgængelige steder og politiets retrospektive anvendelse af teknologien skal evalueres efter 2 år.

For at sikre, at ansigtsgenkendelsesteknologi bliver benyttet af politiet på en hensigtsmæssig og betryggende måde, som befolkningen kan have tillid til, anbefaler Justitia, at de nationale regler om politiets anvendelse af teknologien skal evalueres efter 2 år gennem en revisionsbestemmelse. Det giver mulighed for at tilpasse lovbestemmelsen, hvis det skulle vise sig, at teknologien bliver anvendt på uhensigtsmæssige måder, der ikke var forudset eller overvejet inden reguleringen, eller hvis teknologiens udvikling giver anledning til ændret og/eller yderligere regulering.

JUSTITIA

DANMARKS UAFHÆNGIGE
JURIDISKE TÆNKETANK