

Politiets brug af ansigtsgenkendelse¹

Denne artikel er tildelt
en CC-By 4.0 licens

Tanja Kammersgaard Christensen, lektor, ph.d. og Lene Wachter Lentz, lektor, ph.d.,
begge Juridisk Institut, Aalborg Universitet

Facial recognition technology has the potential to enhance police investigations, but risks significant intrusions into fundamental rights, such as the right to privacy. Drawing on the European Convention on Human Rights (ECHR), the AI Act, and the EU Law Enforcement Directive, this article examines the two uses of facial recognition granted to Danish police in 2024: victim recognition in cases of child sexual abuse and facial recognition of suspects in serious violent crimes. At present, the use of facial recognition by Danish police is guided solely by political decisions, resulting in highly ambiguous frameworks regarding the types of cases in which the technology may be used and the databases that may be cross-referenced. The article argues for clear legal authorization in compliance with the Law Enforcement Directive.

Keywords

Facial recognition, Police, AI-Act, Law Enforcement Directive
Ansigtsgenkendelse, Politi, AI-forordningen, Retshåndhævelsesdirektivet

1. Indledning

Dansk politi har på enkelte områder anvendt ansigtsgenkendelsesteknologi, herunder som verifikation i Københavns Lufthavn² og som en forsøgsordning for at optimere identifikation af børn, der har været udsat for seksuelt misbrug (dette var led i en ny digital tryghedspakke, der skulle bekæmpe it-kriminelle, Digital tryghedspakke 2022 og JM juni 2024/1).

Den 21. juni 2024 udsendte justitsministeriet en pressemeddelelse om, at forsøgsordningen i sager om seksuelt misbrug af børn ville blive gjort permanent, og at politiet fremover vil kunne bruge ansigtsgenkendelse som "et hjælpeværktøj til at scanne materiale, og der vil blive foretaget en endelig identifikation og sammenkædning af sager af en efterforsker." (JM juni 2024/2). Justitsministeren havde allerede tidligere på året udtalt, at ansigtsgenkendelsesteknologi har "... et stort og værdifuldt potentiale, og (at) den vil kunne hjælpe og understøtte politiets arbejde og også efterforskning på

1. Police use of facial recognition technology
2. Spm. 926 (alm del) fra Folketingets Retsudvalg, besvaret 21/8-2018, og opfølgning på besvarelse af spm. 1222 (alm del) fra Folketingets Retsudvalg, den 21/11-2023.

*forskellig vis.*³ Endnu en pressemeddelelse fra Justitsministeriet fulgte den 5. september 2024, hvor politiet fik grønt lys til at bruge ansigtsgenkendelse i efterforskningen af sager om blandt andet alvorlig personfarlig kriminalitet som drab, grov vold og voldtægt (JM september 2024/2).

De to pressemeddelelser blev udsendt samme år, som EU vedtog AI-forordningen,⁴ der bl.a. indeholder en meget restriktiv regulering af politiets brug af ansigtsgenkendelse. Som følge af Danmarks retsforbehold gælder AI-forordningen ikke for dansk politi. Derimod er Danmark forpligtet af EU' retshåndhævelsesdirektiv,⁵ der er implementeret i dansk ret ved Lov om retshåndhævende myndigheders behandling af personoplysninger (herefter retshåndhævelsesloven),⁶ og som regulerer politiets behandling af personoplysninger. At politiet indsamler, lagrer og fremsøger personbilleder, der betragtes som biometriske personoplysninger, er udtryk for en indgribende teknologi, hvilket afspejles i direktivets krav til lovhjemmel, formålsbestemthed, nødvendighed mv. (IMR 2024 og Justitia 2024).

Denne artikel analyserer, om de retlige rammer for dansk politis brug af ansigtsgenkendelsesteknologi er i overensstemmelse med den nationale ret, der implementerer EU-retten, og Den Europæiske Menneskerettighedskonvention (EMRK). Særligt med fokus på de to situationer, hvor dansk politi for nylig har fået mulighed for at bruge ansigtsgenkendelse: offergenkendelse i sager om seksuelle overgreb mod børn, og ansigtsgenkendelse af mistænkte for alvorlig personfarlig kriminalitet.

Politiets ønske om brug af ansigtsgenkendelse er også aktuelt i andre nordiske lande. Således har politiet i Norge efter godkendelse i 2023 brugt ansigtsgenkendelse i en større sag om overgreb mod børn, hvorved 190 børn blev identificeret (Kristoffersen 2024). Også svensk politi har fået tilladelse af den svenske Datainspektion til at anvende et program til ansigtsgenkendelse mod det svenske register over signalementer (Datainspektionen 2019). Denne artikels analyser og konklusioner er derfor også relevante for Norge og Sverige.

I afsnit 2 redegøres kort for teknologien, hvorefter afsnit 3 indeholder en analyse af den internationale retlige ramme for ansigtsteknologi, dels som et indgreb i privatlivet, jf. EMRK art. 8, dels som behandling af biometriske personoplysninger, jf. EU' retshåndhævelsesdirektiv og EU Charter om

3. Svar på § 20-spørgsmål S 788 Om ansigtsgenkendelse, Lisbet Bech-Nielsen, 5/4-2024, <https://www.ft.dk/samling/20231/spoergsmaal/s788/index.htm>

4. Europa-Parlamentets og Rådets forordning (EU) 2024/1689 af 13/6-2024 om harmoniserede regler for kunstig intelligens.

5. Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27/4-2016.

6. Lov nr. 410 af 27/4-2017. Kan læses her: <https://www.retsinformation.dk/eli/lta/2017/410>. Retshåndhævelsesdirektivet er implementeret i Sverige ved Brotttsdatalag (2014:1177), https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/brottsdatalag-20181177_sfs-2018-1177. I Norge findes tilsvarende regulering i Lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven) <https://lovdata.no/dokument/NL/lov/2010-05-28-16>. Se øvrige nationale gennemførelser her: <https://eur-lex.europa.eu/legal-content/DA/NIM/?uri=CELEX:32016L0680&qid=1745235693814>

grundlæggende rettigheder. Herefter følger i afsnit 4 en nærmere analyse af den danske retshåndhævelseslov, hvorefter fokus i afsnit 5 rettes mod de to danske situationer, hvor ansigtsgenkendelse for nylig er blevet muligt, for at afklare om brugen sker i overensstemmelse med retshåndhævelsesdirektivet. Herefter afrundes med en konklusion i afsnit 6.

Denne artikel er tildelt
en CC-BY 4.0 licens

2. Definition af ansigtsgenkendelse

I det følgende tages udgangspunkt i AI-forordningens definition af ansigtsgenkendelse.⁷ Det helt centrale element er, at der med teknologien sker behandling af biometriske data (EDPB 2023, s. 10), der i GDPR, retshåndhævelsesdirektivet og AI-forordningen defineres som *“personoplysninger, som følge af specifik teknisk behandling vedrørende en fysisk persons fysiske, fysiologiske eller adfærdsmæssige karakteristika som f.eks. ansigtsbilleder eller fingeraftryksoplysninger.”*⁸ Ansigtsgenkendelse opdeles typisk i to kategorier: en-til-en-verifikation og identifikation.

Efter AI-forordningen sker ansigtsgenkendelse til *verifikation*, når der sker en *“automatiseret, en-til-en-verifikation, herunder autentificering, af fysiske personers identitet ved at sammenligne deres biometriske data med tidligere afgivne biometriske data”*⁹ Her vil politiet sammenligne et enkelt billede af en person, med et bestemt billede i deres systemer for at få en verifikation af, om det er samme person. Ifølge forordningens præambelbetragtning 17 sker biometrisk verifikation alene for at bekræfte en bestemt fysisk persons identitet, og da sådanne systemer ofte kræver personens tilstedeværelse, anses systemer, der alene anvender verifikation, ikke for at være lige så indgribende på fysiske personers grundlæggende rettigheder, som systemer, der anvendes til identifikation.

AI-forordningen definerer i art. 3, nr. 35 ansigtsgenkendelse til *identifikation* som *“automatiseret genkendelse af fysiske, fysiologiske, adfærdsmæssige eller psykologiske menneskelige træk med henblik på at fastslå en fysisk persons identitet ved at sammenligne den pågældende persons biometriske data med biometriske data om enkeltpersoner lagret i en database.”* Her vil politiet anvende ansigtsgenkendelse til at finde en bestemt person blandt en gruppe af personer f.eks. indenfor et specifikt område, på et billede eller i en database. Politiets system vil behandle alle indsamlede ansigter fra en video eller et billede og herved danne en skabelon af personerne på billedet. Herefter kan systemet kontrollere, om de dannede skabeloner matcher med en person, som systemet kender i forvejen. For at kunne anvende denne form for ansigtsgenkendelse, skal politiet kunne sammenligne de nye skabeloner

7. Europa-Parlamentets og Rådets forordning (EU) 2024/1689 af 13/6-2024.

8. AI-forordningen art. 3, nr. 34, retshåndhævelsesdirektivets art. 3, nr. 13, og GDPR art. 4, nr. 14.

9. AI-forordningen art. 3, nr. 36.

med en database, der består af en masse skabeloner eller prøver. Det vil sige, at systemet er afhængig af, at politiet har en række billeder, de har lavet skabeloner af i forvejen (EDPB 2023, s. 10).

Ansigtsgenkendelsen er mere indgribende, hvis det sker til *identifikation i realtid*. Her vil optagelsen af de biometriske data ske samtidig med sammenligningen og identifikationen, f.eks. ved et kamera på offentligt sted, der ved hjælp af ansigtsgenkendelsesteknologi identificerer personer med det samme. I AI-forordningen angives det, at sammenligning og identifikation kan ske øjeblikkeligt, næsten øjeblikkeligt eller uden væsentlig forsinkelse og stadig være i realtid. Man kan ikke omgå begrebet realtid og de hertil hørende restriktioner ved, at AI-systemet foranlediger mindre forsinkelser (præambelbetragtning 17). Ansigtsgenkendelse i realtid regnes i AI-forordningen for at "*være særligt indgribende i de berørte personers rettigheder og friheder, for så vidt som det kan påvirke privatlivets fred for en stor del af befolkningen, skabe en følelse af konstant overvågning og indirekte afskrække fra udøvelsen af forsamlingsfriheden og andre grundlæggende rettigheder.*" (præambelbetragtning 32). Dette er også baggrunden for, at ansigtsgenkendelse i realtid ifølge AI-forordningen som udgangspunkt er forbudt, jf. nedenfor afsnit 3.2.

3. International ramme

Først redegøres for den retlige ramme for politiets brug af ansigtsgenkendelse, der følger af Den Europæiske Menneskerettighedskonvention, som Danmark har ratificeret og inkorporeret og derfor er forpligtet af. Dernæst redegøres for de retlige rammer i EU-samarbejdet.

3.1. EMRK – Indgreb i retten til privatliv

Ved politiets brug af ansigtsgenkendelse er det navnlig artikel 8 om beskyttelse af privatliv, der er relevant. Det fremgår af praksis fra Den Europæiske Menneskerettighedsdomstol (EMD), at begrebet privatliv ikke udtømmende kan defineres (Niemitz mod Tyskland, 1992, pkt. 29, og Peck mod Storbritannien, 2003, pkt. 57). Det er også fastslået, at privatlivet i visse tilfælde kan omfatte en person, der interagerer med andre, også i det offentlige rum (Glukhin mod Rusland, 2023, pkt. 64, og Ivashchenko mod Rusland, 2018, pkt. 63).

Myndighedernes indgreb i retten til privatliv må kun ske, når det følger af lov (legalitet), og når det er nødvendigt (proportionalitet) for at varetage et legitimt formål, jf. art. 8, stk. 2. EMD har vurderet, at hvis politiet monitorerer borgere med kamera (uden at optage) på offentligt område, vil dette ikke i sig selv udgøre et indgreb, men anderledes, hvis der sker en systematisk

eller permanent optagelse af personer, navnlig hvor det omfatter billedet af en identificeret person (Glukhin mod Rusland, pkt. 66).¹⁰

EMD har forholdt sig til ansigtsgenkendelse i Glukhin mod Rusland (2023), hvor hr. Glukhin havde foretaget en solo-demonstration med et banner i metroen i Moskva. Politiet havde opdaget forbrydelsen ved hjælp af rutineovervågning af metrosystemet, hvorefter Glukhin blev identificeret ved hjælp af ansigtsgenkendelse, og ligeledes blev overvågning og ansigtsgenkendelse i metroen anvendt til at lokalisere og anholde Glukhin (pkt. 68-72).¹¹ Denne behandling af Glukhins personlige data, inklusiv brugen af ansigtsgenkendelse, var et indgreb i hans ret til respekt for privatlivet, jf. art 8.

EMD tilkendegav: *"... it is essential in the context of implementing facial recognition technology to have detailed rules governing the scope and application of measures, as well as strong safeguards against the risk of abuse and arbitrariness. The need for safeguards will be all the greater where the use of live facial recognition is concerned."* (pkt. 82) Ved vurderingen af om russisk lov levede op til disse krav, tilkendegav EMD: *"The domestic law does not contain any limitations on the nature of situations which may give rise to the use of facial recognition technology, the intended purposes, the categories of people who may be targeted, or the processing of sensitive data. Furthermore, the Government did not refer to any procedural safeguards accompanying the use of facial recognition technology in Russia, such as the authorisation procedures, the procedures to be followed for examining, using and storing the data obtained, any supervisory control mechanisms or the available remedies."* (pkt. 83).

Her er EMD ganske præcis i sine krav til kvaliteten og indholdet af den nationale lov, der tillader brug af ansigtsgenkendelsesteknologi, også at der skal etableres en række processuelle garantier for brugen, såsom autorisations- og kontrolmekanismer (pkt. 83, jf. pkt. 77, med reference til S. og Marper mod Storbritannien, 2008, pkt. 99, og P. N. mod Tyskland, 2020, pkt. 62.6 og 87).

I proportionalitetsvurderingen fandt EMD, at politiets metoder over for Glukhin var særligt indgribende, især når det involverede ansigtsgenkendelse i realtid, og henset til at Glukhin kun blev straffet med bøde for sin solo-demonstration (pkt. 86 og 87). Indgrebet, der ikke var berettiget ud fra "a pressing social need", var derfor heller ikke "necessary in a democratic society." (pkt. 89-90). Samlet set var der tale om en krænkelse af art 8.

Denne artikel er tildelt
en CC-BY 4.0 licens

10. EDPB mener derimod, at realtidsovervågning kan være mere indgribende, end at videoovervågningsmateriale opbevares og efter en begrænset tidsramme slettes (EDPB 2020, s. 11).

11. Se hertil Gaughran mod UK, 2020, pkt. 69-70, hvor EMD fandt, at opbevaring af personfotografier med muligheden for at anvende ansigtsgenkendelsesteknologi var et indgreb i retten til privatliv, jf. art. 8.



Denne artikel er tildelt
en CC-By 4.0 licens

3.2. EU-retten

EU Charter om grundlæggende rettigheder gælder for medlemsstaterne, når de gennemfører EU-lovgivning.¹² Charteret indeholder i art. 7 en beskyttelse af retten til respekt for privatliv, familieliv, hjem og kommunikation, og i art. 8 en udtrykkelig formuleret ret til beskyttelse af personoplysninger. Personoplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag, jf. art. 8, stk. 2. Det følger af art. 52, stk. 1, at enhver begrænsning i udøvelsen af Chartrets rettigheder og friheder, skal være fastlagt i lovgivningen og respektere disse rettigheders og friheders væsentligste indhold.¹³

Danmark er som følge af retsforbeholdet ikke forpligtet af AI-forordningen om politiets brug af AI, dog er det alligevel værd at hæfte sig ved den restriktive tilgang til ansigtsgenkendelse, som EU og de øvrige medlemslande udviser. Bekymringen angår risiko for følelsen af masseovervågning og krænkelse af de grundlæggende rettigheder, herunder retten til privatlivets fred (præambelbetragtning 43). AI-forordningen indeholder grundlæggende et forbud mod at etablere og bruge databaser for ansigtsgenkendelse ved en ikkemåltrettet indsamling ("scraping") af ansigtsbilleder fra internettet eller kameraovervågning, jf. art. 5, stk. 1, litra e. Det er også som udgangspunkt forbudt for politi og retshåndhævende myndigheder at anvende systemer til biometrisk fjernidentifikation i realtid på offentlige steder, medmindre og kun i det omfang det er strengt nødvendigt til et af de nærmere angivne formål, såsom måltrettet søgning af forsvundne personer mv., konkret og omfattende trussel på livet eller at identificere mistænkte til grove forbrydelser, såsom mord, voldtægt, væbnet røveri mv., jf. art. 5, stk. 1, litra h. Før anvendelse af et sådant system, gælder en række krav, såsom at politiet skal indhente tilladelse fra en retslig myndighed eller en uafhængig administrativ myndighed, jf. art. 5, stk. 2 og 3.

Danmark er derimod forpligtet af retshåndhævelsesdirektivet,¹⁴ som er implementeret ved retshåndhævelsesloven.¹⁵ Når Danmark på denne måde gennemfører EU-ret, gælder Chartret på dette område. I forbindelse med implementeringen af retshåndhævelsesdirektivet lagde lovgiver vægt på en korrekt implementering af direktivet, bl.a. ved at affattelsen af de danske regler skulle lægge sig tæt op ad direktivets ordlyd, for at der ikke kunne rejses tvivl om implementeringen.¹⁶ Dette taler for, at der ved fortolkningen af direktivet, som Danmark grundet implementeringen er folkeretligt forpligtet til at følge (Sørensen 2018, s. 323), alligevel kan lægges vægt på nogle af de principper, vi kender fra EU-retten, herunder pligten til EU-konform fortolk-

12. EU's Charter om Grundlæggende rettigheder (2010/C 83/02), art. 51(1).

13. Om samspillet mellem Chartret og EMRK, se Chartrets art. 52, stk. 3.

14. Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27/4-2016.

15. Lov nr. 410 af 27/4-2017.

16. Lovforslag nr. 168, af 28/3-2017, pkt. 1.1.

ning, ligesom praksis fra Den Europæiske Unions Domstol (EUD) kan anvendes som fortolkningsbidrag ved fortolkningen af retshåndhævelsesloven.¹⁷

Denne artikel er tildelt
en CC-BY 4.0 licens

4. Retshåndhævelsesloven

I det følgende rettes fokus på den danske regulering med en gennemgang af de centrale krav i retshåndhævelsesloven (og direktivet) til formålsbestemthed, streng nødvendighed og krav om lovhjemmel, inden der kort redegøres for de processuelle krav i loven om konsekvensanalyse og høring af Datatilsynet.

4.1. Formålsbestemthed

Behandling af personoplysninger skal *"indsamles til udtrykkeligt angivne og legitime formål og ikke behandles på en måde, der er uforenelig med disse formål"*.¹⁸ I den engelske udgave af direktivet er betingelserne for formålets gyldighed i art. 4, stk. 1, litra b angivet som *"specified, explicit and legitimate purposes"*, altså specifikke, eksplicitte og legitime formål og ikke som i den kortere danske oversættelse *"udtrykkeligt angivne og legitime"* formål. Efter den engelske ordlyd fremgår det klart, at der opstilles krav til beskrivelsen af formålet med indsamlingen af personoplysninger, hvilket tillige fremgår af præambelbetragtning nr. 26. Kravet om formålsbestemthed er en forudsætning for, at der kan foretages den vurdering af nødvendigheden, som følger af retshåndhævelseslovens § 4, stk. 3¹⁹ og den danske implementering må derfor skulle fortolkes i overensstemmelse med ordlyden af direktivet og retspraksis knyttet hertil, jf. C-14/83 von Colson.

Spørgsmålet er, hvor konkret formålet med indsamlingen skal være beskrevet i lovgivningen. Ifølge retspraksis fra EUD om fortolkningen af direktivet, *"... må formålene med behandlingen af biometriske og genetiske data ikke beskrives i for generelle vendinger, men kræver, at de er tilstrækkeligt præcise og konkrete til at gøre det muligt at vurdere, om den nævnte behandling er "strengt nødvendig"*.²⁰ Det er dermed ikke tilstrækkeligt bare at henvise til, at indsamlingen af personoplysninger sker til f.eks. formålene beskrevet i retshåndhævelseslovens § 1, stk. 1, som er at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger (Vogiatzoglou et al., 2022, s. 34, med yderligere referencer, Koning 2020, s. 67-68, samt EDPB 2020, s. 9, hvor det er angivet, at: *"Sikkerhed" eller "personers sikkerhed" som eneste begrundelse for videoovervågning er ikke tilstrækkelig specifikt"*).

17. Hertil kommer, at Danmark rent folkeretligt vil anvende fortolkningsreglen ved folkeretten (Rytter 2024, s. 63). Resultatet vil derfor formentlig være, at Danmark skal fortolke direktivkonformt, både fra et EU-retligt og et folkeretligt perspektiv.

18. Direktivets art. 4, stk. 1, litra b, implementeret i retshåndhævelseslovens § 4, stk. 2, dog med en lidt anderledes ordlyd.

19. Jf. generaladvokat Pikamäe's forslag til afgørelse i C-118/22 NG, præmis 53, og Hahn 2021, s. 31-44.

20. C-205/21, straffesagen mod V.S., pr. 124.

Formålet skal være beskrevet, så alle involverede parter, herunder den registrerede, tilsynet og øvrige parter kan forstå, hvad personoplysningerne konkret anvendes til (Se Hert et al. 2021, s. 12 om denne forståelse). Formålet skal derfor være tydeligt beskrevet, forklaret og gennemsigtigt (Koning 2020, s. 68). Samtidig gælder det, at jo mere indgribende behandlingen er, jo mere specifik skal formålet være beskrevet (Koning 2020, s. 66).

Hvis politiet vælger at bruge ansigtsgenkendelse på billeder eller video-materiale – der oprindeligt har været indsamlet til ét formål – til et andet formål, kræver dette tillige, at det nye formål fastlægges. Efter retshåndhævelseslovens § 5, stk. 1 kræves, at den nye behandling også sker på baggrund af lov, er nødvendig og forholdsmæssig i forhold til dette andet formål (se tillige Hert et al. 2021, s. 12 om denne forståelse).

4.2. *Strengt nødvendig*

Det følger af retshåndhævelseslovens § 4, stk. 3, at de oplysninger politiet behandler, skal være relevante og tilstrækkelige, og at de ikke må omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles. De oplysninger, der behandles, skal altså være proportionelle og nødvendige til formålet. Når ansigtsgenkendelse omfatter biometriske og dermed særligt beskyttede personoplysninger, skal behandlingen af oplysningerne ikke blot være nødvendig, men *strengt nødvendig*, jf. retshåndhævelseslovens § 10.²¹ Det betyder, at formålet med behandlingen ikke med rimelighed må kunne nås lige så godt på en anden måde, der er mindre indgribende i de registreredes grundlæggende rettigheder.²² Hertil kommer, at kravet om strengt nødvendig medfører, at der ikke kan anvendes ansigtsgenkendelsesteknologi på alle borgere udifferentieret. EUD har bl.a. taget stilling til indsamling af biometriske data på alle, der var rejst sigtelse mod i forbindelse med, at de havde begået *"en forsætlig strafbar handling, der retsforfølges ex officio"*.²³ Her fandt EUD, at selvom lovgivningen var begrænset til dem, der var rejst sigtelse mod, så var det ikke i sig selv et element, der talte for, at indsamlingen var begrænset til det strengt nødvendige. EUD påpegede endvidere, at hvis der allerede foreligger tilstrækkelige beviser i sagen, taler dette for, at indsamling af biometriske data ikke er nødvendig.²⁴ Vurdering af nødvendigheden må omfatte alle de relevante forhold, *"bl.a. arten og grovheden af den formodede lovovertrædelse, som den pågældende er blevet sigtet for at have begået, de særlige omstændigheder i forbindelse med denne overtrædelse, den eventuelle forbindelse mellem den nævnte overtrædelse og andre verserende sager, tidligere kriminel adfærd eller den pågældendes individuelle profil."*²⁵

21. For en nærmere analyse af forskellen mellem nødvendig og strengt nødvendig, Naarttijärvi 2023.

22. C-205/21 straffesagen mod V.S., pr. 126.

23. C-205/21 straffesagen mod V.S., pr. 129.

24. C-205/21 straffesagen mod V.S., pr. 131.

25. C-205/21 straffesagen mod V.S., pr. 132.

EU's Datatilsynsråd (EDPB) har uddybende om kravet om streng nødvendighed tilkendegivet, at den skønsmargen, der er tillagt de retshåndhævende myndigheder ved brug af biometriske data, er begrænset til et absolut minimum (EDPB 2023, s. 22).

4.3. *Krav om lovhjemmel og indholdet heraf*

Efter retshåndhævelsesdirektivets art. 8 gælder et krav om lovhjemmel: *"Medlemsstaterne fastsætter bestemmelser om, at behandling kun er lovlig, hvis og i det omfang denne behandling er nødvendig, for at en kompetent myndighed kan udføre en opgave med henblik på artikel 1, stk. 1, og at den sker på grundlag af EU-retten eller medlemsstaternes nationale ret."* Dette krav ses dog umiddelbart ikke implementeret i retshåndhævelsesloven. I forarbejderne til retshåndhævelsesloven og implementeringen af art. 8, fremgår det, at det er en betingelse, at behandlingen sker på grundlag af EU-retten eller medlemsstaternes ret. Der tages dog ikke stilling til denne betingelse i forarbejderne, hverken i de indledende bemærkninger til bestemmelsen, eller i bemærkningerne til § 9. Hvorfor denne betingelse er udeladt, fremgår dermed ikke klart af forarbejderne.²⁶ Uanset det manglende krav i national implementering, vil kravet om lovhjemmel efter EU-rettens forrang betyde, at der skal være hjemmel til politiets behandling af personoplysninger.

Kravet om lovhjemmel i retshåndhævelsesdirektivet præciseres i art. 10 for behandling af særlige kategorier af personoplysninger, såsom biometriske data med det formål entydigt at identificere en fysisk person, således at behandlingen kun er lovlig, hvis det er strengt nødvendigt og behandlingen er hjemlet i EU-retten eller national ret.

Efter direktivets art. 8 og præambelbetragtning 26, må behandling af personoplysninger kun finde sted til specifikke formål fastlagt ved lov. Det følger dog af præambelbetragtning 33, at: *"Når dette direktiv henviser til medlemsstaternes nationale ret, et retsgrundlag eller en lovgivningsmæssig foranstaltning, kræver det ikke nødvendigvis en lov, der er vedtaget af et parlament, med forbehold for krav i henhold til den forfatningsmæssige orden i den pågældende medlemsstat."* Selvom kravet om lovhjemmel dermed ikke kræver en lov, vedtaget af det nationale parlament, følger det alligevel af præambelbetragtning 33, at *"En sådan national ret i medlemsstaterne, et sådant retsgrundlag eller en sådan lovgivningsmæssig foranstaltning bør imidlertid være klar(t) og præcis(t), og anvendelse heraf bør være forudsigelig for de personer, der er omfattet af dets/dens anvendelsesområde, jf. retspraksis fra Domstolen og Den Europæiske Menneskerettighedsdomstol."* Det må dermed kunne udledes, at selvom det ikke er et krav, at loven er vedtaget af et parlament, så skal der være tale om enten en national lov, et retsgrundlag eller en anden lovgivningsmæssig foranstaltning, hvilket derfor ikke kan omfatte f.eks. en kortfattet, meddelt politisk beslutning. Præambelbetragtning 33 angiver en række minimumskrav til den nationale ret, der hjemler behandling

26. Lovforslag nr. 168 fremsat den 28/3-2017, pkt. 2.3.3.5 og s. 67.

af personoplysninger, det fremgår heraf, at: "... formålene, de personoplysninger, der skal behandles, formålene med behandlingen og procedurerne for sikring af personoplysningernes integritet og fortrolighed samt procedurerne for deres tilintetgørelse og derved i tilstrækkelig grad sikre oplysningerne mod risikoen for misbrug og vilkårlighed." Sammenholdt med praksis fra EMD, kan der ikke være tvivl om, at brugen af ansigtsgenkendelse kræver lovhjemmel.

Kravet om lovhjemmel er uddybende gennemgået af EDPB, som har tilkendegivet: "Den nationale lovgivning skal være tilstrækkelig klart affattet til at give de registrerede tilstrækkelig viden om, under hvilke omstændigheder og forhold dataansvarlige er bemyndiget til at gribe til sådanne begrænsninger. Dette omfatter eventuelle forudsætninger for behandling såsom specifikke typer af bevismateriale samt nødvendigheden af retslige eller interne tilladelser." (EDPB 2023, s. 22). En henvisning til den generelle bestemmelse i retshåndhævelsesloven, der implementerer retshåndhævelsesdirektivets art. 10, vil ifølge EDPB ikke opfylde kravet om lovhjemmel. Der skal være tale om en specifik lovhjemmel, der opfylder minimumskravene som anført i direktivet, samt i EMRK og Chartret (EDPB 2023, s. 22).

4.4. Konsekvensanalyse og høring af Datatilsynet

Udover disse tre materielle krav om formålsbestemthed, strengt nødvendig og lovhjemmel, gælder to mere processuelle krav, som kort redegøres for her. Efter direktivets art. 27, implementeret i retshåndhævelseslovens § 25, skal politiet, inden de tager nye teknologier i brug, der vil medføre en høj risiko for fysiske personer, analysere teknologiens konsekvenser for beskyttelsen af personoplysninger (en konsekvensanalyse). I relation til ansigtsgenkendelsesteknologi har EDPB fastslået, at en konsekvensanalyse er et obligatorisk krav, idet anvendelsen af teknologien netop sandsynligvis vil indebære en høj risiko for fysiske personer (EDPB 2023, s. 28).

Det er centralt, at konsekvensanalysen foretages forud for behandlingen, idet formålet med analysen bl.a. er at den dataansvarlige bliver opmærksom på konsekvenserne ved behandlingen, og derved kan bestemme tilstrækkelig sikkerhed for behandlingen (Hansen 2024, s. 428).

Efter retshåndhævelseslovens § 25, stk. 2, skal konsekvensanalysen indeholde følgende elementer: "... En generel beskrivelse af de planlagte behandlingsaktiviteter, en vurdering af risiciene for de registreredes rettigheder, de foranstaltninger, der påtænkes for at imødegå disse risici, garantier, sikkerhedsforanstaltninger og mekanismer, som kan sikre beskyttelse af personoplysninger og påvise overholdelse af denne lov, under hensyntagen til de registreredes og andre berørte personers rettigheder og legitime interesser."

Selv om der alene skal ske en "generel" beskrivelse af de planlagte behandlingsaktiviteter, kan beskrivelsen dog ikke være for overordnet, når konsekvensanalysen bl.a. skal bruges til politiets vurdering af risici for de registreredes rettigheder og tilsynsmyndighedens efterprøvelse (Hansen 2024, s. 433).

Videre følger det af retshåndhævelseslovens § 26, at den dataansvarlige i visse situationer skal høre Datatilsynet, inden nye teknologier tages i brug. En forudgående høring skal bl.a. ske, hvis den type behandling der tages i brug, navnlig ved brug af nye teknologier, mekanismer eller procedurer, vil indebære en høj risiko for de registreredes rettigheder.

EDPB har tilkendegivet, at de fleste tilfælde af indførelse og anvendelse af ansigtsgenkendelsesteknologi vil indebære en høj risiko for de registreredes rettigheder. Derfor bør den myndighed, der indfører ansigtsgenkendelsesteknologi, høre den kompetente tilsynsmyndighed forud for indførelsen af systemet (EDPB 2023, s. 29). Datatilsynet har udarbejdet en liste over behandlingsaktiviteter, der er underlagt kravet om forudgående høring af tilsynet efter retshåndhævelseslovens § 26. Her er særligt nævnt brug af ansigtsgenkendelsesteknologi som led i overvågning af et offentligt tilgængeligt område, ved innovative måder til behandling af biometriske eller genetiske personoplysninger og ved behandling af særlige kategorier af personoplysninger i stort omfang som led i profilering, evaluering eller scoring (Datatilsynet 2024). Datatilsynet vil på baggrund af konsekvensanalysen og øvrigt indleveret materiale tage stilling til, om den planlagte behandling vil overtræde bestemmelserne i retshåndhævelsesloven, og vurdere om politiet i tilstrækkelig grad har identificeret og forhindret de potentielle risici, der er ved behandlingen.

5. Ansigtsgenkendelse i en dansk efterforskningssammenhæng

Politiets efterforskning er reguleret i retsplejeloven, som dog ikke på nuværende tidspunkt indeholder en regulering af ansigtsgenkendelse. Relevant i denne sammenhæng er, at der i retsplejelovens kapitel 72 er hjemmel til at optage foto af sigtede og i et vist omfang også af ikke-sigtede, ligesom der forefindes forskellige politidatabaser med foto- og videomateriale. Omdrejningspunktet for den hidtidige regulering i retsplejeloven har været indgrebet over for borgeren ved ransagning, telefonaflytning mv., ikke hvordan politiet efterfølgende (eller måske samtidig?) bearbejder, optimerer og ”beriger” det materiale, de har sikret.

Politolovens § 2 a indeholder en generel hjemmel til, at politiet foretager tværgående informationsanalyser på grundlag af de oplysninger, politiet behandler, når det er nødvendigt af hensyn til udførelsen af politiets opgaver, jf. § 2.²⁷ Det følger videre af stk. 2, at politiet kan indsamle og behandle oplysninger fra offentligt tilgængelige kilder, når det er nødvendigt af hensyn til udførelsen af politiets opgaver. Her ses altså en bred hjemmel til sammenkøring af politiets registre, data og materiale.

27. § 2 a blev indsat ved lov 671 af 8/6-2017, se nugældende politilov, lovbekendtgørelse nr. 1270 af 29/11/2019.

Nedenfor følger en analyse af de to situationer, hvor dansk politi på nuværende tidspunkt har fået tilladelse til at anvende ansigtsgenkendelse til identifikation.

5.1 Offergenkendelse i billedmateriale af seksuelle overgreb

Efter et forsøg med offergenkendelse i 2023 konkluderede dansk politis Nationale enhed for Særlig Kriminalitet (NSK), at teknologien medførte et markant kvalitetsløft på området, og på baggrund af en anbefaling fra Rigspolitiet besluttede Justitsministeren i juni 2024 at gøre ordningen permanent (JM juni 2024/1). Ansigtsgenkendelse til offergenkendelse blev dermed politisk besluttet, og der findes ikke et lovgrundlag eller andet, der regulerer anvendelsen af teknologien. Det er derfor primært Justitsministeriets pressemeddelelse, der informerer om anvendelsen af teknologien.²⁸

I forhold til retshåndhævelseslovens krav om formålsbestemthed kan det konstateres, at NSK i konsekvensanalysen for offergenkendelsesapplikationen (NSK 2025) beskriver formålet således: "At understøtte efterforskernes identifikation af mindreårige ofre for seksuelt misbrug i digitalt billedmateriale". I NSK's evalueringsrapport af forsøgsordningen blev præsenteret to anvendelsesmuligheder for teknologien (NSK 2024, s. 4), som anses for at kunne uddybe formålet med behandlingen:

"Anvendelse 1

Her sammenholdes et billede af et offer med NC3's billeddatabase. Hensigten er at undersøge, hvorvidt offeret på billedet allerede er kendt af politiet, og om offeret figurerer i andet kendt materiale. Denne viden kan understøtte efterforskerens identifikation af offeret og eventuel sammenkædning af sager.

Anvendelse 2

Her sammenholdes et billede af et offer med billeder fra kosterne i en sag. Dette for at finde flere billeder af offeret i den konkrete efterforskning, som kan understøtte efterforskerens identifikation af offeret og målrette efterforskningen."

Lovgrundlaget for anvendelsen af teknologien er ifølge NSK's konsekvensanalyse henholdsvis politilovens § 2, stk. 1, nr. 3, om at bringe strafbar virksomhed til ophør, samt efterforske og forfølge strafbare forhold, jf. straffelovens § 235 om udbredelse og besiddelse af billedmateriale om seksuelle overgreb mod børn samt retshåndhævelseslovens §§ 9 og 10, som hjemler behandling af personoplysninger for henholdsvis almindelige og biometriske data, under yderligere betingelser.

28. Ved aktindsigt i politiets konsekvensanalyse har vi modtaget NSK's risikovurdering og evalueringsrapport i forbindelse med forsøgsordningen, samt NSK's konsekvensanalyse af 3/2-2025 og hertil hørende risikovurdering.

Om anvendelsen af teknologien har Justitsministeren i sin orientering til Folketinget oplyst, at NSK har udviklet en app med ansigtsgenkendelsesteknologi, *"... som er anvendt til at sammenholde billeder af et offer med politiets billeddatabase eller med billedmateriale fra en konkret sag. Teknologien er alene blevet brugt som hjælpeværktøj til scanning af billedmateriale, mens den endelige identifikation og sammenkædning af sager/billedmateriale er foretaget af en efterforsker."* (JM juni 2024/1). De personoplysninger, der indgår i systemet, kommer ifølge NSK fra ofre for seksuelt misbrug og fremstilling, distribution og besiddelse af materiale om seksuelt misbrug af børn. Der kan dog i enkelte tilfælde også indgå billeder af gerningspersoner. NSK har ikke et overblik over, hvor mange ofre (registrerede), der indgår i systemet, men angiver, at det er flere tusinde, og at der indgår op til 400.000 billeder alene til forsøget med digitaliseret offergenkendelse. Der indsamles ikke nye data i forbindelse med forsøget, idet oplysningerne allerede er gemt på NC3's billeddatabase og på konkrete sager. Systemet bruges til, ved hjælp af ansigtsgenkendelsesteknologi, at beregne ansigtsvektorer for ansigter i databasen. Vektorerne bliver sammenlignet, og i den hertil udviklede app, vises de 100 ansigter, som vektorerne er tættest på i en prioriteret rækkefølge. Der er dermed tale om ansigtsgenkendelse ved identifikation ved brug af billeder, som politiet allerede har.

I NSK' evalueringsrapport anbefales det på baggrund af forsøgsordningen, at den udviklede offergenkendelsesapplikation bl.a. anvendes til følgende tre scenarier, hvor systemet har vist sig velegnet: *"1. Afklaring af om et offer optræder i NC3's billeddatabase. 2. Hjælp til identifikation af ofre for grooming. 3. Hjælp til identifikation af ofre for tredjepartsgerningsmand."* (NSK 2024, s. 20). Det fremgår i øvrigt ikke klart af rapporten, om systemet også vil kunne blive brugt i andre tilfælde.

I det følgende analyseres om de helt centrale krav og principper i retshåndhævelsesloven er opfyldt for at anvende ansigtsgenkendelse til brug for offergenkendelse.

Efter princippet om dataminimering må der alene behandles personoplysninger, der er tilstrækkelige, relevante og ikke omfatter mere, end hvad der kræves for at opfylde formålene med behandlingen. Da der er tale om biometriske data, er det et yderligere krav, at disse oplysninger alene behandles, når det er strengt nødvendigt.

Ifølge evalueringsrapporten anvender politiet systemet til digitaliseret offergenkendelse på to måder: Enten ved at sammenholde et billede af et offer med NC3's billeddatabase for at undersøge, om offeret i forvejen er kendt af politiet, og om offeret figurer i kendt materiale, eller ved at sammenholde et billede af et offer med bevismateriale fra en konkret sag (NSK 2024, s. 4). Det fremhæves dog, at den applikation politiet har udarbejdet til brug for digitaliseret offergenkendelse ikke selv kan identificere ofrene, da der i systemet ikke er knyttet identitet til billederne. Efterforskeren skal derfor selv, via referencer til tidligere sager, eller på baggrund af spor i billederne, identificere

ofrene (NSK 2024, s. 6 og NSK Internt notat 2025), s. 1). Selvom systemet ikke selv identificerer offeret, bruges ansigtsgenkendelsen, og dermed de biometriske data, med det formål entydigt at identificere en fysisk person, hvorfor behandlingen skal være strengt nødvendig, jf. retshåndhævelseslovens § 10.

Det kan være svært at vurdere, om brug af ansigtsgenkendelsen i disse situationer er strengt nødvendigt, når dette ikke er egentligt beskrevet og vurderet i rapporten. Der kan dog alligevel rejses spørgsmål i relation til nødvendigheden, bl.a. idet NSK i evalueringsrapporten angiver, at teknologien har sværere ved at foretage ansigtssammenligning, jo yngre børnene er, hvilket er en generel udfordring ved brug af ansigtsgenkendelsesteknologi (NSK 2024, s. 12 og 32). Spørgsmålet er derfor, om det er den rigtige teknologi at anvende, eller om formålene kunne opnås med mindre indgribende metoder, som f.eks. ved at se på billedernes unikke hashværdi. Vurderingen af om systemet er strengt nødvendigt, vil dog skulle foretages i første omgang af Datatilsynet.

Som lovhjemmel for anvendelsen af applikationen henvises også til straffelovens § 235, som giver hjemmel til at kunne strafforfølge gerningspersoner der: "... udbreder utugtige fotografier, film, andre utugtige visuelle gengivelser eller lignende af personer under 18 år". Med henvisningen til denne bestemmelse, er det tvivlsomt, om det er nødvendigt at kende identiteten på ofrene. Straffelovens § 235 straffer den som udbreder eller besidder billedmateriale om seksuelle overgreb mod børn. Her er strafferammen højere i særligt skærpende tilfælde, hvilket bl.a. er: "*hvor barnets liv udsættes for fare, hvor der anvendes grov vold, hvor der forvoldes barnet alvorlig skade, eller hvor der er tale om udbredelse af mere systematisk eller organiseret karakter.*" Omfanget af gerningspersonens forbrydelse er dermed relevant, mens identiteten på offeret i billedmaterialet måske i de fleste tilfælde er mindre relevant, hvorfor der kan stilles spørgsmål til relevansen af en hjemmel heri til at identificere ofre.

I risikovurderingen ses NSK at have vurderet, at stort set alle elementer, der er medtaget i vurderingen, er grønne og scorer mellem 1-5 point, hvilket betyder at der er "ingen eller meget lav risiko" for den registrerede, og at ingen handling er påkrævet. Dette gælder sikkerhed, jura, bias, tekniske fejl mv. Samlet set vurderes offergenkendelsesapplikationen derfor af NSK til kun at medføre en lav risiko for de registreredes rettigheder.²⁹

Det kan konkluderes, at brugen af ansigtsgenkendelse til digitaliseret offergenkendelse, lider af nogle alvorlige mangler for at kunne leve op til kravene i retshåndhævelsesloven og direktivet. Den manglende lovhjemmel strider mod retshåndhævelsesdirektivet. Den grundighed, der er forbundet med det lovforberedende arbejde, der udmøntes i en klar lovhjemmel, gør, at der ville have været klarere rammer og større gennemsigtighed omkring anvendelsen af teknologien. Det er derfor svært at vurdere, om ansigtsgenkendelsen egentlig er nødvendig i de af politiet angivne scenarier.

29. Aktindsigt i NSKs konsekvensanalyse og tilhørende risikovurdering.

5.2. *Ansigtsgenkendelse af mistænkte for alvorlig personfarlig kriminalitet*
Politiet har siden september 2024 fået adgang til at bruge ansigtsgenkendelse i efterforskningen af sager om blandt andet alvorlig personfarlig kriminalitet som drab, grov vold og voldtægt. Dette skete ved en politisk beslutning mellem regeringen og fire andre partier (JM september 2024/2). Om baggrunden har Justitsministeren henvist til brugen af ansigtsgenkendelse til offergenkendelse, og at politiet har overvejet, om der er andre steder, hvor teknologien også kan styrke politiets efterforskning. Rigspolitiet har derfor, særligt i lyset af de sager, der har været, hvor unge svenskere er blevet hyret til at begå drab i Danmark, ønsket at Københavns Politi får mulighed for at installere systemer, der giver mulighed for at bruge objekt- og mønstergenkendelsesteknologi, samt ansigtsgenkendelsesteknologi, der kan gennemgå og analysere store mængder af indsamlet videomateriale (JM september 2024/1).³⁰ Politiet har på baggrund af den politiske beslutning startet et pilotprojekt om brug af objekt- og ansigtsgenkendelse hos Københavns Politi.³¹

Ansigtsgenkendelse til dette formål adskiller sig fra ansigtsgenkendelse til offergenkendelse, bl.a. ved at omfanget af brugen af teknologien vil være større, idet det kan anvendes på en større mængde billed- og videomateriale end den, der alene er indsamlet i databasen vedrørende seksualforbrydelser, idet politiet råder over store fotodatabaser og lister over privat og offentlig videoovervågning i hele landet. Danmark er et af de lande i verden med flest kameraer pr. indbygger. Ifølge tal fra organisationen Sikkerhedsbranchen fra 2019 er der i Danmark opsat ca. 1.500.000 overvågningskameraer. 300.000 af de kameraer er politiets egne, mens de resterende tilhører private borgere eller erhvervsvirksomheder. Selvom det ikke er alle kameraerne, som tilhører politiet, kan politiet få adgang til optagelser fra de resterende ca. 1.200.000 kameraer (Foxil 2019).

Derudover vil indgrebet formentlig også være større for den enkelte borger, idet man må formode, at der er flere borgere uden tilknytning til kriminaliteten, der optræder på politiets videomateriale indhentet fra sådanne kameraer, end der er på billedmateriale relateret til seksualforbrydelser. Det betyder også, at der må kunne stilles større krav til proportionalitet og til anvendelsen af teknologien, idet flere vil kunne blive påvirket.

I pressemeddelelsen fra Justitsministeren angives meget overordnet, at politiet i første omgang vil bruge ansigtsgenkendelsesteknologi i efterforskningen af alvorlig personfarlig kriminalitet som for eksempel drab og voldtægt samt i sager af betydning for statens sikkerhed og i særlige

30. Datatilsynet valgte få dage efter at stille en række spørgsmål til Rigspolitiet om politiets brug af ansigtsgenkendelse til retshåndhævende formål. Datatilsynet spurgte bl.a. ind til konsekvensanalyser og forudgående høring af Datatilsynet. Rigspolitiet har hertil svaret, at da projektet omkring ansigtsgenkendelse stadig er i de indledende faser, og politiet på nuværende tidspunkt er i gang med at anskaffe et brugbart system,.

31. I forbindelse med udarbejdelsen af denne artikel, har vi bl.a. fået aktindsigt i Rigspolitiets konsekvensanalyse, DPO påtegning til pilotprojektet, og notat om de strafbare forhold, der kan danne grundlag for anvendelsen af ansigtsgenkendelse i pilotprojektet.

operative situationer. For at kunne vurdere proportionalitet mv., vil der kræves et formål, der i overensstemmelse med retshåndhævelsesloven er udtrykkeligt angivet og sagligt. Dette vil f.eks. kunne opnås, hvis det konkretiseres, hvilke strafbestemmelser og eventuelle strafferammer, ansigtsgenkendelse kan anvendes til. I Rigspolitiets "Notat om de strafbare forhold, der kan danne grundlag for anvendelse af ansigtsgenkendelse i pilotprojekt" af 13/12-2024, redegøres for de strafbare forhold, der kan danne grundlag for brug af ansigtsgenkendelse. Her angives konkrete strafbestemmelser, herunder bl.a. drab, jf. strfl. § 237, forsøg på drab, grov vold, jf. strfl. § 245, voldtægt, jf. strfl. § 216, terrorsager efter strfl. §§ 114-114j og operative sager med "manhunt". Idet Justitsministeren i sin orientering til Folketingets Retsudvalg har angivet, at ansigtsgenkendelse også må anvendes ved lignende overtrædelser, angives i notatet yderligere eksempler på, hvornår systemet kan anvendes. Herunder i sager om vold (strfl. § 119), vidnetrusler (strfl. § 123), seksualforbrydelser (§§ 216-225) mv. Det understreges dog, at det beror på en konkret vurdering, om teknologien kan bruges i disse situationer, og at listen i notatet ikke er udtømmende. (Politi straf forhold 2024, s. 1-3)

Også ved denne anvendelse af ansigtsgenkendelsesteknologi gælder et krav om lovhjemmel, jf. retshåndhævelsesdirektivet. Dette uddybes i EDPB's retningslinjer for anvendelse af ansigtsgenkendelsesteknologi på retshåndhævelsesområdet, hvor EDPB har beskrevet et scenarie, som i stor stil minder om det, vi på nuværende tidspunkt ved om politiets tiltag. Scenariet omhandler en situation, hvor man netop vil bruge ansigtsgenkendelse til opklaring af optøjer (EDPB 2023, s. 46, scenarie 3). Her præciserer EDPB, at det at en national lov indeholder en generisk bestemmelse – hvor behandling af biometriske data med det formål entydigt at identificere en fysisk person er tilladt, hvis det er strengt nødvendigt og underlagt passende garantier for den berørte persons rettigheder og frihedsrettigheder – ikke er tilstrækkelig klar i sin ordlyd til at opfylde kravet om lovhjemmel i retshåndhævelsesdirektivet. Loven skal være klar nok i sin ordlyd til at give enkeltpersoner en passende indikation af de betingelser og omstændigheder, hvorefter ansigtsgenkendelse kan anvendes. En kortfattet politisk beslutning omkring anvendelsen vil derfor ikke være nok. Dette bekræftes af Rigspolitiets Data Protection Officer (DPO), der i påtegningen af pilotprojektet påpeger, at omfanget af oplysninger samt karakteren heraf, tilsiger at en egentlig hjemmel skal tilvejebringes, men først hvis politiet ønsker, at gøre brug af ansigtsgenkendelse som fast redskab. (Politi DPO påtegning 2025, s. 1-2). Hvad der ligger til grund for denne vurdering om, at lovhjemlen først skal sikres, hvis systemet tages i brug som fast redskab, er dog ikke klart, og spørgsmålet er, om en sådan opfattelse er korrekt. Politiet foretager en behandling af biometriske data, der efter retshåndhævelsesdirektivets art. 10 kræver en lovhjemmel, og dette må gælde uanset, om der er tale om et pilotprojekt eller en mere permanent ordning.

Derudover præciserer EDPB, at dataminimering bl.a. vil kunne ske ved, at der sættes begrænsninger for, hvilket billedmateriale der må indgå i

efterforskningen. Dette kunne f.eks. afgrænses til billeder, der viser grov kriminel adfærd, eller til billeder, der har en direkte tidsmæssig og geografisk forbindelse til forbrydelsen. På den måde vil man også minimere antallet af personer uden mistanke, der fremgår af billederne. Såfremt mængden af billeder allerede her kan begrænses, vil det også kunne gøre brugen af ansigtsgenkendelse mindre nødvendig, og en mindre indgribende metode vil f.eks. være at materialet gennemgås af politiansatte. Et andet element, der påpeges af EDPB er, at de registrerede ofte ikke kender til omfanget af overvågningen, og at deres video- og billedmateriale indgår i ansigtsgenkendelse hos politiet, hvilket ifølge EDPB forstærker indgrebets intensitet. Det har den konsekvens, at der netop i disse tilfælde stilles større krav til formål og proportionalitet.

Sammenfattende hvis politiet ønsker at begynde at anvende ansigtsgenkendelse i de af justitsministerens godkendte situationer, kræver det en konkret lovhjemmel, hvor der tages stilling til behandlingen af personoplysninger og overensstemmelsen med retshåndhævelsesloven og direktivet.

5.3. *Ansigtsgenkendelse i realtid*

Dansk politi ses ikke på nuværende tidspunkt at have en regulering, der giver mulighed for ansigtsgenkendelse til identifikation i realtid. Det er formuleret i den politiske aftale fra september 2024, "at politiet får mulighed for at søge efter objekter og ansigter på tværs af videomateriale, som politiet indhenter i forbindelse med efterforskning af en konkret sag, men ikke for at anvende ansigtsgenkendelse i realtid." (JM september 2024/2). Det er således tilkendegivet, at politiet "i første omgang [vil] bruge ansigtsgenkendelsesteknologi i efterforskningen af alvorlig personfarlig kriminalitet som for eksempel drab og voldtægt samt i sager af betydning for statens sikkerhed og i særlige operative situationer. Det gælder blandt andet såkaldte "manhunt"-situationer, hvor politiet eftersøger en farlig gerningsperson ... "

De uklare rammer for ansigtsgenkendelsen af mistænkte for alvorlig personfarlig kriminalitet kan dog give anledning til bekymring ved, at der i politiets operative arbejde kan ske en udvidende fortolkning af, hvad politiet har lov til og hvordan. I efterforskningen af alvorlige, hastende sager vil det være nærliggende for politiet at indhente eller måske endda overtage videoovervågning fra f.eks. private eller andre offentlige myndigheder for at kunne bruge ansigtsteknologi til at udfinde mistænkte. Selv om der i "manhunt"-situationerne indføres en vis forsinkelse, er det ikke oplagt, at det bringes udenfor begrebet "identifikation i realtid", hvor risikoen for krænkelse af privatlivet er størst, som anerkendt af EU i AI-forordningen.

6. Konklusion

EU har med AI-forordningen og retshåndhævelsesdirektivet valgt en restriktiv tilgang til den nye ansigtsgenkendelsesteknologi som et værktøj for politiet, i erkendelse af at kun udførlige, retlige rammer kan sikre hensynet til privatlivet og modvirke følelsen af generel overvågning i samfundet.

Danmark har valgt en helt anden tilgang: Alene ved politisk beslutning er ansigtsgenkendelse nu muligt for politiet ved offergenkendelse i sager om seksuelle overgreb mod børn, og ved ansigtsgenkendelse af mistænkte for alvorlig personfarlig kriminalitet. I begge tilfælde er den politiske beslutning kortfattet og uden egentlige rammer for, hvad der kan sammenkøres og i hvilke sager. Dette indebærer en risiko for udvidelse af brugen af værktøjet til efterforskning af anden kriminalitet, mindre alvorlige sager eller hvor der allerede er efterforskningsmæssigt grundlag for tiltale spørgsmål, og ansigtsgenkendelsesteknologien derfor ikke er strengt nødvendig. Politiets operative beslutninger om brug af ansigtsgenkendelse vil ofte skulle træffes hurtigt, og i fravær af retlige rammer vil dette ske uformelt og med kun begrænset mulighed for efterfølgende kontrol. Faste retlige rammer for brugen af ansigtsteknologi er det bedste værn mod vilkårlighed, udvidet brug af den meget indgribende teknologi og manglende kontrol med indgrebet.

En medvirkende årsag til den danske tilgang kan muligvis være, at retshåndhævelsesloven ved implementeringen i 2017 ikke tydeligt nok har implementeret direktivets krav om lovhjemmel, om end EDBP's tydelige tilkendegivelse af krav om lovhjemmel til politiets brug af ansigtsgenkendelse må være justitsministeriet bekendt.

Mens justitsministeren flere gange har italesat den efterforskningsmæssige gevinst ved ansigtsgenkendelse, herunder effektivitet i opklaringen, forekommer det, at de alvorlige risici for privatlivskrænkelser, herunder følelsen af overvågning, ikke egentlig anerkendes af lovgiver. Det er op til lovgiver at definere spillerummet for politiets virksomhed, og det nærliggende vil være at sikre en demokratisk proces for at skabe retlige rammer om en så indgribende metode som politiets brug af ansigtsgenkendelse.

Kontaktoplysninger

Tanja Kammersgaard Christensen: tkc@law.aau.dk

Lene Wachter Lentz: lwle@law.aau.dk

Litteratur

De Hert, Paul og Sajfert, Juraj, 2021: *"The fundamental right to personal data protection in criminal investigations and proceedings: Framing big data policing through the purpose limitation and data minimization principles of the directive (EU) 2016/680"*

Hert et al. 2021

DOI: <http://dx.doi.org/10.2139/ssrn.4016491>



Foxil, Emilie: "Så meget videoovervågning er der i Danmark", TV2, 9/10-2019 (Foxil 2019)
Link: <https://nyheder.tv2.dk/politik/2019-10-09-saa-meget-videoovervaagning-er-der-i-danmark>

Hahn, Isabel, 2021: Purpose limitation in the time of data power: is there way forward? *European Data Protection Law Review (EDPL)*, 7(1), 31-44 (Hahn 2021) DOI: <https://doi.org/10.21552/edpl/2021/1/7>

Hansen, Marit: "Data protection impact assessment" i "The EU law enforcement directive (LED) A commentary", Eleni Kosta, and Franziska Boehm (red.), 2024. (Hansen 2024)
DOI: <https://doi.org/10.1093/law/9780192855220.001.0001>

Koning, Merel Elize: "The purpose and limitations of purpose limitation", ph.d.-afhandling, 2020. (Koning 2020)

Link: https://merelkoning.nl/wp-content/uploads/2020/10/M.Koning_The-purpose-and-limitations-of-purpose-limitation_thesis.pdf

Kristoffersen, Kai Jæger: "Barneansikter i overgrepsvideo sjekket mot passregister – identifiserte nesten 200 ofre", nrk 1/6-2024, (Kristoffersen 2024)

Link: https://www.nrk.no/nordland/omegle-saken_-kripos-brukte-eget-verktoy-for-a-identifisere-190-barn-i-overgrepssak-1.16901885

Naarttijärvi, Markus, 2023: *AI and Sensitive Personal Data Under the Law Enforcement Directive: Between Operational Efficiency and Legal Necessity*. In: Gill-Pedro, E., Moberg, A. (eds) YSEC Yearbook of Socio-Economic Constitutions 2023. YSEC Yearbook of Socio-Economic Constitutions, vol 2023. Springer, Cham. (Naarttijärvi 2023)

DOI: https://doi.org/10.1007/16495_2023_57

Rytter, Jens Elo: "Individets grundlæggende rettigheder", 5. udg., 2024 (Rytter 2024)

Sørensen, Karsten Engsig: "Pligten til EU-konform fortolkning", s. 323 i "EU-retten i Danmark", 2018, af Birgitte Egelund Olsen og Karsten Engsig Sørensen (red.) (Sørensen 2018)

Vogiatzoglou, Plixavra og Marquenie, Thomas: "Assessment of the implementation of the Law Enforcement Directive", 2022, (Vogiatzoglou et al, 2022) Link: [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL_STU\(2022\)740209_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740209/IPOL_STU(2022)740209_EN.pdf)

Øvrige kilder:

Datainspektionen 23/10-2019: "Förhandssamråd om Polismyndighetens planerade användning aprogramvara för ansiktsgenkänning mot signalementsregistret" (Datainspektionen 2019) <https://www.imy.se/globalassets/dokument/ovrigt/2019-10-23-polisen-forhandssamrad.pdf>

Datatilsynets liste over behandlingsaktiviteter, der er underlagt kravet om forudgående høring af tilsynet efter retshåndhævelseslovens § 26, af 31/1-2024 (Datatilsynet 2024), <https://www.datatilsynet.dk/Media/638423966496872688/Liste%20efter%20retshandh%C3%A6velseslovens%20%26,%20stk.%203.pdf>

Digital tryghedspakke, der skulle bekæmpe it-kriminelle, jf. regeringens nyhed af 13/9-2022 (Digital tryghedspakke 2022) <https://www.regeringen.dk/nyheder/2022/ny-digital-tryghedspakke-skal-bekaempe-it-kriminelle/>,

EU's Datatilsynsråd, EDPB: "Retningslinjer 3/2019 om brug af videoudstyr til behandling af personoplysninger, version 2.0, vedtaget den 29/1-2020 (EDPB 2020) https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_da.pdf

EU's Datatilsynsråd, EDPB: "Retningslinjer 5/2022 for anvendelse af ansigtsgenkendelsesteknologi på retshåndhævelsesområdet" Version 2.0, vedtaget den 26/4-2023 (EDPB 2023) https://www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frt-lawenforcement_v2_da.pdf

Institut for Menneskerettigheder, februar 2024: "Politiets brug af ansigtsgenkendelse i det offentlige rum" (IMR 2024) <https://menneskeret.dk/files/media/document/Politiets%20brug%20af%20ansigtsgenkendelse.%20Analyse%2C%20Institut%20for%20Menneskerettigheder%2C%20februar%202024.pdf>

Denne artikel er tildelt
en CC-BY 4.0 licens

Denne artikel er tildelt
en CC-BY 4.0 licens

Justitia, rapport af Birgitte Arent Eiriksson, 2024: "Ansigtsgenkendelsesteknologi Behov for regulering af politiets anvendelse" (Justitia 2024), https://justitia-int.org/wp-content/uploads/2024/03/Rapport_Ansigtsgenkendelsesteknologi-behov-for-regulering-af-politiets-anvendelse_FINAL.pdf

Justitsministeriets "Orientering om politiets forsøg med digitaliseret offergenkendelse i efterforskning af sager om seksuelt misbrug af børn" af 21/6-2024 (JM juni 2024/1) <https://www.ft.dk/samling/20231/almdel/DIU/bilag/145/2885095/index.htm>

Justitsministeriets pressemeddelelse: "Ny teknologi skal hjælpe politiet i indsatsen mod seksuelt misbrug af børn", 21/6-2024 (JM juni 2024/2) <https://www.justitsministeriet.dk/pressemeddelelse/ny-teknologi-skal-hjaelpe-politiet-i-indsatsen-mod-seksuelt-misbrug-af-boern/>

Justitsministeriet: "Orientering om politiets brug af ansigtsgenkendelsesteknologi i efterforskningen" af 5/9-2024 (JM september 2024/1) <https://www.justitsministeriet.dk/wp-content/uploads/2024/09/Orientering-af-Folketingets-Retsudvalg-om-politiets-brug-af-ansigtsgenkendelsesteknologi-i-efterforskning.pdf>

Justitsministeriets pressemeddelelse 5/9-2024: "Politiet får grønt lys til ansigtsgenkendelse" (JM september 2024/2) <https://www.justitsministeriet.dk/pressemeddelelse/politiet-faar-groent-lys-til-ansigtsgenkendelse/>

NSK Evalueringsrapport "Forsøg med digitaliseret offergenkendelse", 1/2-2024 (NSK 2024) (aktindsigt)

NSK "Konsekvensanalyse for offergenkendelsesapplikationen", 3/2-2025 (NSK 2025) (aktindsigt)

NSK internt notat: "Rammer for anvendelse af offergenkendelsesapplikationen", 4/2-2025 (NSK internt notat 2025) (aktindsigt)

Rigspolitiet "Notat om de strafbare forhold, der kan danne grundlag for anvendelsen af ansigtsgenkendelse i pilotprojekt", 13/1-2024 (Politi straf forhold 2024) (aktindsigt)

Rigspolitiet: "DPO påtegning – pilotprojekt om brug af objekt- og ansigtsgenkendelse", 12/2-2025 (Politi DPO påtegning 2025) (aktindsigt)

EMD-Domme:

Gaughran mod UK, 13/2-2020 (45245/15)

Glukhin mod Rusland, 4/7-2023 (11519/20)

Ivashchenko mod Rusland, 13/2-2018 (61064/10)

Niemietz mod Tyskland, 16/12-1992 (13710/88)

Peck mod Storbritannien, 28/1-2003 (44647/98)

P. N. mod Tyskland, 11/6-2020 (74440/17)

S. og Marper mod Storbritannien, 4/12-2008 (30562/04 og 30566/04)

EUD-Domme:

C-14/83 von Colson.

C-205/21 straffesagen mod V.S

C-118/22 NG samt generaladvokat Pikamäe's forslag til afgørelse