

DATAETISKE PERSPEKTIVER

Politiets brug af ansigtsgenkendelse



Dataetisk Råd

København 2025.

Dataetisk Råd er en offentlig myndighed, som rådgiver om etiske udfordringer ved nye digitale teknologier.

Læs mere på **dataetiskraad.dk**

Projektet bag denne rapport har i rådet været forankret i en referencegruppe bestående af:

- Mathias Broman Bukhave,
- Mikael Jensen, og
- Birgitte Kofoed Olsen.

Referencegruppen er bistået med teknisk rådgivning af rådsmedlem Peter Damm.

Projektet er udarbejdet med sekretariatsbistand fra projektleder Frej Klem Thomsen.

Layout og illustrationer ved Grobowski.

Indholdsfortegnelse

Sammenfatning	4
Forord	8
1. Hvad er ansigtsgenkendelse?	10
1.1. Hvordan fungerer den kunstige intelligens?	17
2. Hvordan kan politiet anvende ansigtsgenkendelse?	20
2.1. Automatiseret paskontrol	23
2.2. Offergenkendelse i materiale med seksuelt misbrug af børn	25
2.3. Retrospektiv eftersøgning i materiale fra det offentlige rum	26
2.4. Retrospektiv billedsøgning i materiale fra relevante personer	28
2.5. Realtidseftersøgning i det offentlige rum	29
2.6. Identifikation af ukendte personer i fysiske interaktioner	31
3. Hvad er de juridiske rammer for politiets brug af ansigtsgenkendelse?	33
4. Hvad er der på spil?	37
4.1. Seks argumenter for ansigtsgenkendelse	38
4.2. Seks argumenter mod ansigtsgenkendelse	49
5. Dataetisk Råds position og anbefalinger	67
Konklusion	70

Sammenfatning

Denne rapport fra Dataetisk Råd analyserer de dataetiske spørgsmål, som dansk politis anvendelse af ansigtsgenkendelsesteknologi rejser. Dataetisk Råd arbejder med at rådgive beslutningstagere og stimulere den demokratiske debat. Formålet med rapporten er således at skabe et solidt grundlag for en informeret politisk og offentlig debat om, hvornår politiet bør bruge teknologien, og hvordan den kan anvendes på en dataetisk forsvarlig måde.

Hvad er ansigtsgenkendelse?

Ansigtsgenkendelse er en form for kunstig intelligens, der kan finde personer i et billede, analysere deres ansigtstræk, og sammenligne med ansigtstræk i andre billeder for at finde den samme person. Teknologien har været under hastig udvikling det seneste årti, og har i dag så høj kvalitet, at den anvendes i mange sammenhænge.

Hvordan kan politiet bruge ansigtsgenkendelse?

Dansk politi bruger i 2025 ansigtsgenkendelse til:

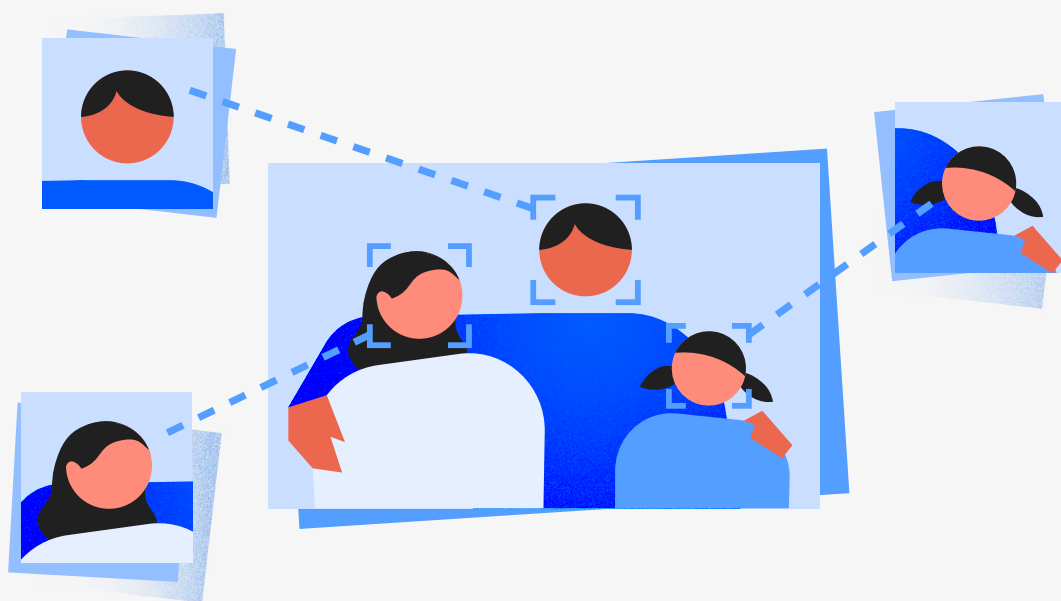
- **Automatiseret paskontrol**, hvor ansigtsgenkendelse tjekker, at rejsende kan vise gyldigt pas.
- **Offergenkendelse i sager om seksuelt misbrug af børn**, hvor ansigtsgenkendelse hjælper med at finde ud af, om ofre er kendt fra tidligere sager.
- **Retrospektiv eftersøgning i materiale fra det offentlige rum** i sager om særligt alvorlig, personfarlig kriminalitet, hvor ansigtsgenkendelse hjælper med at finde personer, der er knyttet til alvorlig kriminalitet i billedmateriale fra kameraer placeret i det offentlige rum.

Derudover kunne dansk politi bruge ansigtsgenkendelse til:

- **Billedsøgning i materiale fra relevante personer**, der er knyttet til efterforskning af særligt alvorlig, personfarlig kriminalitet, hvor ansigtsgenkendelse kunne hjælpe med at finde relevante billeder, for eksempel på et offers mobiltelefon.

I andre lande, herunder Storbritannien og USA, anvender politiet også ansigtsgenkendelse til blandt andet:

- **Eftersøgning i realtid i det offentlige rum**, hvor ansigtsgenkendelse hjælper med at identificere eftersøgte, således at politiet kan rykke ud og pågribe dem.
- **Identifikation af ukendte personer i fysiske interaktioner**, hvor ansigtsgenkendelse hjælper med at fastslå identiteten på en person, som politiet interagerer med, for eksempel i forbindelse med en kropsvisitation.



Hvad er de juridiske rammer?

EU's AI-forordning forbyder ansigtsgenkendelse i realtid i offentlige rum, med få undtagelser, og stiller strenge krav om dokumentation, kontrol og menneskelig efterprøvning i andre brugsscenarier. Danmark er dog på grund af retsforbeholdet ikke bundet af disse regler, hvilket giver bredere handlemuligheder end i andre EU-lande. Anvendelsen er derfor i Danmark først og fremmest underlagt de europæiske menneskerettighedskonventioner, især beskyttelsen af privatliv, samt de danske regler for politiets indhentning og anvendelse af billedmateriale i blandt andet retshåndhævelsesloven.

For og imod ansigtsgenkendelse

Politiets brug af ansigtsgenkendelse har været kontroversiel. Både fortalere og kritikere har fremført en række argumenter for og imod politiets brug af teknologien. Rapporten identificerer og diskuterer 12 centrale argumenter, seks for og seks imod teknologien.

Fortalere har hævdet, at ansigtsgenkendelse:

- kan aflaste politiet og frigive ressourcer,
- kan afskrække kriminalitet, ved at øge risikoen for at blive identificeret,
- kan forbedre mulighederne for efterforskning, og derved føre til opklaring af flere forbrydelser,
- kan effektivisere efterforskning, og derved gøre opklaring hurtigere,
- kan hjælpe med at finde eftersøgte personer, og
- ikke vil være et problem, hvis man ikke har noget at skjule.

Kritikere har omvendt hævdet, at ansigtsgenkendelse:

- kan begå fejl, hvilket kan få alvorlige konsekvenser for uskyldige borgere,
- kan have bias, hvor teknologien virker dårligere på visse befolkningsgrupper,
- kan have en "afkølede" effekt, hvor borgere ændrer adfærd af frygt for overvågning,
- kan begrænse borgernes privatliv, når teknologien indsamler informationer,
- kan misbruges af enkeltpersoner, hackere eller myndigheder, og
- kan føre til en uetisk glidning mod stadig mere indgribende anvendelser.

Rapportens analyse viser styrker og svagheder ved disse argumenter, og hvordan det ofte er nødvendigt at vurdere dem i relation til det konkrete brugsscenarie.

Dataetisk Råds position og anbefalinger

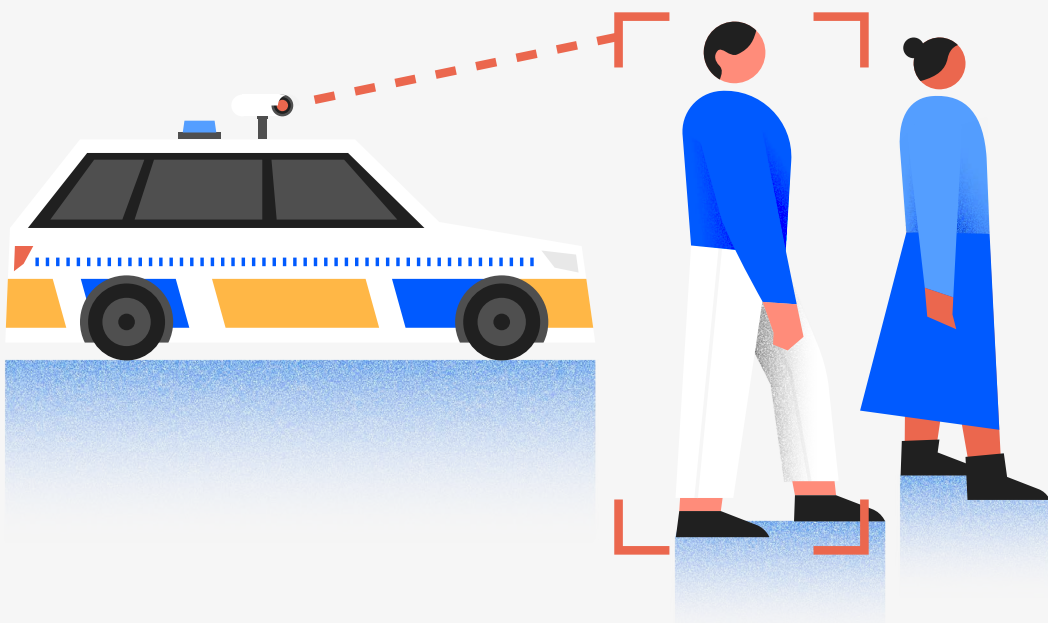
Dataetisk Råd vurderer, at dansk politis brug af ansigtsgenkendelse kan være dataetisk forsvarlig i visse brugsscenarier, såfremt bestemte betingelser er opfyldt. Dette er tilfældet for de fire første brugsscenarier, hvor af tre aktuelt findes i Danmark: Automatiseret paskontrol, offergenkendelse i sager om seksuelt misbrug af børn, retrospektiv eftersøgning i materiale fra det offentlige rum i sager om særligt alvorlig, personfarlig kriminalitet, og billedsøgning i materiale fra relevante personer, der er knyttet til efterforskning af særligt alvorlig kriminalitet.

Omvendt vurderer rådet, at dansk politi *ikke* bør have mulighed for at anvende ansigtsgenkendelse til eftersøgning i realtid i det offentlige rum eller til identifikation af ukendte personer i fysiske interaktioner.

Dataetisk Råd anbefaler, at Folketinget og regeringen udarbejder særskilt lovgivning for politiets anvendelse af ansigtsgenkendelse, der:

- Tydeligt tillader de fire første og forbyder mere vidtgående brugsscenarier, herunder det femte og sjette brugsscenarie, Dataetisk Råd har vurderet.
- Præciserer de betingelser, som skal stilles til politiets anvendelser, herunder overvejer hvornår der skal stilles krav om dommerkendelse, hvilket efter rådets opfattelse især vil være relevant ved retrospektiv eftersøgning i materiale fra det offentlige rum.
- Pålægger politiet at offentliggøre oplysninger om blandt andet anvendelsesomfang, fejlprocenter og tekniske specifikationer.
- Indfører tekniske og organisatoriske standarder, der skal minimere risikoen for fejl, bias og misbrug, herunder krav om logning og dokumentation af kvalitet.

Endelig anbefaler Dataetisk Råd, at Folketinget og Regeringen evaluerer og om nødvendigt opdaterer eksisterende regler for politiets adgang til billedmateriale, idet disse regler er indført på et tidspunkt, hvor videoovervågning i det offentlige rum havde et langt mindre omfang.



Forord

"Teknologien kommer ikke bare til at løfte kvaliteten af efterforskningen. Den sparer også tid og hænder."

Peter Hummelgaard, Justitsminister

"Politiets brug af ansigtsgenkendelse på offentlige steder kan udgøre en risiko for ret til privatliv og databeskyttelse."

Institut for Menneskerettigheder

I Dataetisk Råd arbejder vi for, at nye digitale teknologier udvikles og anvendes på et etisk grundlag, hvor vi som samfund tager behørigt hensyn til både de positive og negative konsekvenser, som teknologien kan have. Det er efter min mening et vigtigt arbejde, fordi udviklingen går rivende stærkt, og fordi teknologierne kan have store konsekvenser for os.

Ansigtsgenkendelse er et centralt eksempel på en teknologi, hvor dataetikken er vigtig. Teknologien har det seneste årti udviklet sig fra mest at være eksperimenter, til et redskab, som er blevet vidt udbredt både i private og offentlige sammenhænge. Det kan være hjælpsomt, men også bekymrende og kontroversielt.

Det har både i Danmark og internationalt været særligt kontroversielt, når politiet anvender ansigtsgenkendelse. Den debat er blevet fornyet i Danmark de seneste år, fordi dansk politi er begyndt at bruge ansigtsgenkendelse på nye måder. Politiet har siden 2016 brugt ansigtsgenkendelse til at udføre automatisk paskontrol i Københavns lufthavn. Siden er politiet blandt andet begyndt at anvende ansigtsgenkendelse til at hjælpe med at identificere kendte ofre i sager om seksuelt misbrug af børn, og i efteråret 2024 besluttede Justitsministeren at igangsætte et pilotprojekt, hvor Københavns politi skulle anvende ansigtsgenkendelse til eftersøgning i sager om alvorlig kriminalitet. Denne udvikling mod stadig flere anvendelser kunne godt tænkes at fortsætte. I udlandet har politi i Storbritannien og USA for eksempel også brugt ansigtsgenkendelse til eftersøgning i realtid, og til at identificere ukendte personer.

Når politiet bruger ansigtsgenkendelse, er der flere forskellige etiske hensyn på spil. På den ene side kan teknologien bidrage til at opklare alvorlig kriminalitet, og frigøre ressourcer, som kan gøre gavn på andre måder. På den anden side kan teknologien reducere personers privatliv, begå fejl, og have bias mod bestemte befolkningsgrupper. Når vi skal overveje om og hvordan politiet skal have mulighed for at bruge ansigtsgenkendelse, er det afgørende at vurdere både argumenter for og imod i lyset af vores etiske værdier og principper.

Med denne rapport ønsker Dataetisk Råd at bidrage til en informeret og nuanceret debat om politiets brug af ansigtsgenkendelse i Danmark. Rapporten gennemgår ansigtsgenkendelse som teknologi, de juridiske rammer, eksisterende og mulige anvendelser ved politiet, samt en række af de centrale etiske argumenter for og imod. På den baggrund præsenterer Dataetisk Råd sin vurdering af, hvilke rammer vi i Danmark bør sætte for teknologien. Hvornår er det etisk forsvarligt at lade politiet bruge den? Hvornår må vi sige, at en måde at anvende ansigtsgenkendelse er uetisk? Og hvilke krav skal vi stille i de situationer, hvor vi giver politiet mulighed for at bruge teknologien?

Dataetisk Råd har under arbejdet med denne rapport haft stor gavn af dialog med en række medarbejdere ved politiet, som arbejder med ansigtsgenkendelse. Vi skylder tak for den åbenhed og hjælpsomhed som vi har mødt hos Københavns Politi, Københavns Vestegns Politi, National enhed for Særlig Kriminalitet, og Rigspolitiet.

Ansigtsgenkendelse er en kompleks teknologi, som kan vække stærke følelser. Ofte går det hurtigt, når vi skal forholde os til komplekse etiske problemstillinger. Det er mit håb, at rapporten kan danne afsæt for den grundige refleksion, som emnet fortjener. Kun ved at tænke os godt om, kan vi sammen finde den rette balance mellem de forskellige hensyn som er på spil, både i dag og i fremtiden, i takt med at teknologien udvikler sig.



Johan Busse

Formand for Dataetisk Råd

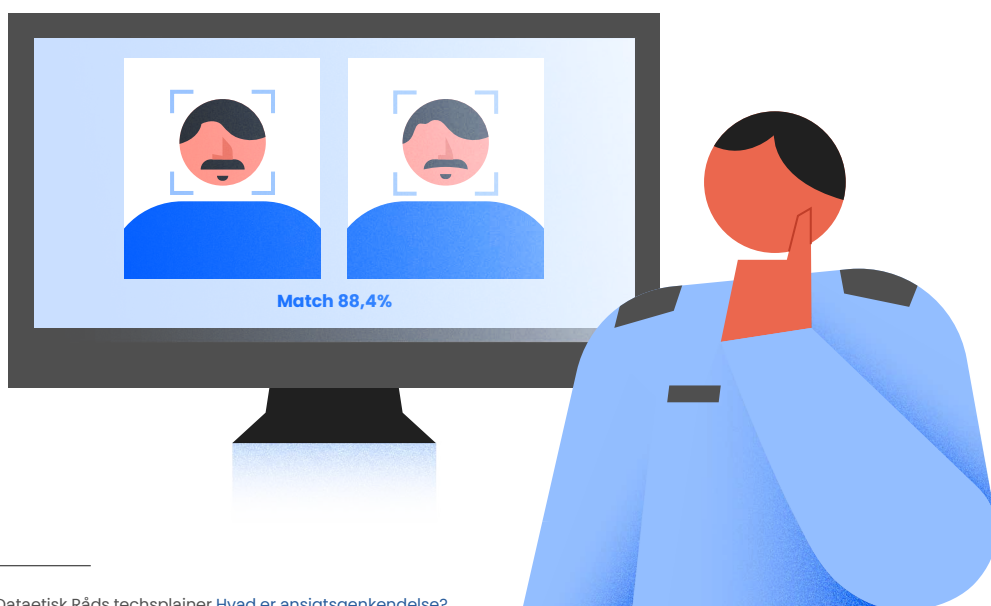
1. Hvad er ansigtsgenkendelse?

Ansigtsgenkendelse er en særlig type kunstig intelligens. Det specielle ved ansigtsgenkendelse er, at teknologien kan identificere mennesker, som optræder på et billede. Det gør den ved at opdage, analysere og sammenligne menneskers ansigter.¹

Ansigtsgenkendelse anvendes i dag af myndigheder, virksomheder og private borgere til mange forskellige opgaver. Tre almindelige eksempler er kamerafokusering, adgangskontrol og eftersøgning.

Ansigtsgenkendelse kan bruges til kamerafokusering ved at hjælpe med at stille skarpt på de ansigter, som optræder på et billede. De fleste digitale kameraer har en indbygget funktion, som lader kameraet opdage menneskelige ansigter, og automatisk indstille fokus på disse ansigter. Det hjælper brugeren med at tage gode billeder.

Ansigtsgenkendelse kan også bruges til adgangskontrol ved at hjælpe med at bekræfte en persons identitet. For eksempel kan de fleste mobiltelefoner låse telefonen op ved at genkende ejerens ansigt. Telefonen bruger kameraet til at sammenligne ansigtet på den person, som prøver at åbne telefonen, med et billede af ejerens ansigt, og giver adgang, hvis det er den samme person på de to billeder.



¹ Se også Dataetisk Råds techsplainer [Hvad er ansigtsgenkendelse?](#)

Endelig kan ansigtsgenkendelse bruges til eftersøgning, ved at hjælpe med at finde en bestemt person i et datasæt med mange forskellige billeder. Teknologien sammenligner hvert af de ansigter som optræder på hvert billede med den eftersøgte, og markerer hvert af de billeder, hvor den har fundet personen. Det kan for eksempel bruges til at finde alle de ferie billeder, hvor et bestemt familiemedlem optræder, men det kan også bruges af politiet til at finde en mistænkt på video fra overvågningskameraer.

Hvordan virker ansigtsgenkendelse?

Ansigtsgenkendelse er en kunstig intelligens, som kan analysere et billede af et ansigt. En computer kan ikke af sig selv kigge på og forstå et billede, sådan som mennesker kan. Kunstig intelligens er i stedet nødt til at læse et billede matematisk.

Pixel

Et grafisk punkt i et billede. Et digitalt billede består ofte af flere millioner pixels.

Billedanalyse

Kunstig intelligens som kan analysere et digitalt billede, og finde ud af hvad billedet forestiller.

Et digitalt billede består af tusindvis af små grafiske punkter, som tilsammen danner billedet. Et sådant punkt kaldes en **pixel**. Hver pixel har en værdi, som fortæller hvilken farve den skal have.

Et digitalt billede består derfor matematisk set af en lang serie tal, som angiver farveværdien for hver pixel i billedet. For at forstå et billede, må den kunstige intelligens analysere denne serie tal, og forsøge at regne ud, hvad billedet forestiller. Det kaldes at kunstig intelligens laver **billedanalyse**.²

Billedanalyse var helt frem til begyndelsen af det 21. århundrede en svær opgave for kunstig intelligens, men bruges i dag til mange ting. Det kan for eksempel hjælpe med at beskrive og kategorisere billeder, så en computer kan skelne mellem billeder af en kattekillung og billeder af en banan. Det kan også bruges til at filtrere indhold på digitale platforme, for eksempel for automatisk at fjerne billeder, som overtræder platformens retningslinjer.

² I den engelsksprogede faglitteratur tales om "object recognition" og "object classification".

Ansigtsgenkendelse er den særlige form for billedanalyse, som lader en computer analysere billeder af ansigter. På et overordnet niveau løser ansigtsgenkendelse tre opgaver:

- Ansigtsopdagelse, som opdager hvor der findes ansigter i et billede
- Biometrisk analyse, som laver matematiske aftryk af ansigterne
- Personidentifikation, som sammenligner ansigtsaftryk³

Ansigtsopdagelse

Den mest grundlæggende opgave for ansigtsgenkendelse er at opdage, hvor i billeddata, der findes ansigter. Først når den har fundet ud af, hvor der findes et ansigt, kan den kunstige intelligens løse eventuelle andre opgaver.

Når den skal opdage ansigter, forsøger den kunstige intelligens at finde strukturer i billeddata, som minder om de strukturer menneskelige ansigter plejer at have: øjne, næse, mund, hage, ører, osv.

Analysens resultat er en matematisk afgrænsning af et eller flere ansigter i billeddata.

Ansigtfokus på digitale kameraer

Den måske mest almindelige erfaring med ansigtsopdagelse er, når det anvendes i digitale kameraer. De fleste digitale kameraer kan bruge ansigtsopdagelse til automatisk at indstille kameraet, så det fokuserer på ansigter i midten af billedet. Det hjælper typisk brugeren med at tage bedre billeder.

(Rahman & Kehtarnavaz 2008)



³ Se Hupont, et al. 2022. I faglitteraturen afgrænses begrebet "ansigtsgenkendelse" nogle gange til den opgave, som vi her kalder "personidentifikation". Vi anvender det her lidt bredere, så det også inkluderer de forudgående skridt med at opdage og analysere ansigter.

Biometrisk analyse

Den anden opgave for ansigtsgenkendelse er at lave en biometrisk analyse af de ansigter, som den kunstige intelligens har opdaget i billeddata.

Den kunstige intelligens analyserer billedet for at finde en række målepunkter på ansigtet – for eksempel let genkendelige steder på panden, ørerne, kindbenene, læberne og mundvigene, øjenkrogene, hagen, næseryggen og næseborene. I alt måles typisk cirka 80 målepunkter.⁴

Resultatet af analysen er et **ansigtsaftryk** – et matematisk kort over ansigtet.

Mennesker har forskellige ansigter, og enhver person har sit eget unikke ansigtsaftryk, på samme måde som vi kender fra fingeraftryk.

Ansigtsaftryk

Et matematisk kort over et ansigt baseret på et sæt af målepunkter, som findes på alle ansigter.

Personidentifikation

Den tredje opgave for ansigtsgenkendelse er at identificere personer, som optræder på et billede. Det er nok især denne opgave, som mange umiddelbart forbinder med teknologien.

For at identificere personer skal den kunstige intelligens først løse de andre to opgaver. Den skal opdage hvor på et billede der findes ansigter, og analysere ansigtsaftrykkene på disse ansigter.

Reference

Ansigtsaftryk i en database, som kan sammenlignes med det ansigtsaftryk, brugeren gerne vil identificere.

For at identificere en person sammenligner den kunstige intelligens de ansigtsaftryk den har fundet på billedet med et eller flere ansigtsaftryk fra en database. Aftrykkene i databasen er **referencer**, normalt fra personer, hvis identitet brugeren allerede kender. An-

sigtsgenkendelse kan kun identificere en person, hvis personens ansigtsaftryk er en reference i databasen. Hver gang den sammenligner et ansigtsaftryk med en reference,

⁴ Se UNICRI & INTERPOL 2025.

regner den kunstige intelligens ud, hvor meget de to aftryk matematisk set minder om hinanden. Hvis to ansigtsaftryk minder meget om hinanden, er der sandsynligvis tale om aftryk fra den samme person.⁵

1-til-1-genkendelse

Ansigtsgenkendelse, som sammenligner et ansigtsaftryk fra en person på et billede med et bestemt ansigtsaftryk i en database, for at vurdere om de to ansigtsaftryk er fra den samme person.

Personidentifikation kan bruges på mange måder, både til at verificere en persons identitet, og til at identificere en ukendt person. Når en kunstig intelligens skal verificere en persons identitet, så sammenligner den ansigtsaftrykket på et billede med et ansigtsaftryk fra en bestemt person. Det kaldes også for **1-til-1-genkendelse**. Hvis de to ansigtsaftryk minder meget om hinanden, så bekræfter systemet, at der er tale om den samme person. Verifikation bruges ofte til adgangskontrol.

Kameralås på mobilen

Mange har prøvet ansigtsgenkendelse til verifikation for at låse op for en mobiltelefon. Ejeren kan dele et billede af sit ansigt med telefonen, som bruger ansigtsgenkendelse til at aflæse ejerens ansigtsaftryk. Når en bruger vil låse telefonen op, så kan telefonen bruge kameraet til at sammenligne denne persons ansigtsaftryk med ejerens ansigtsaftryk. Hvis de to ansigter minder meget om hinanden, så verificerer telefonen ejerens identitet, og låser automatisk op.

1-til-mange-genkendelse

Ansigtsgenkendelse, som sammenligner et ansigtsaftryk fra en person på et billede med alle ansigtsaftryk i en database, for at vurdere, om ansigtsaftrykket minder om en af referencerne.

Når kunstig intelligens skal identificere en ukendt person, så sammenligner den personens ansigtsaftryk med alle de referencer, som findes i en database. Det kaldes for **1-til-mange-genkendelse**. Hver gang den kunstige intelligens sammenligner to aftryk, regner den ud hvor meget de matematisk set minder om hinanden. Til

⁵ Se Kortli, et al. 2020; Li, et al. 2020.

sidst kan den kunstige intelligens for eksempel vise brugeren de ansigter i databasen, som minder mest om den ukendte persons ansigt, eller de referencer, som minder så meget om ansigtsaftrykket, at det med en vis sandsynlighed er den samme person.

Automatisk billedsortering og -tagging

Mange har prøvet at bruge ansigtsgenkendelse til at identificere personer, når en computer automatisk sorterer eller markerer billeder. Mange digitale kameraer kan automatisk sortere billeder, så alle billeder af en bestemt person samles i en særlig folder. Og mange digitale platforme kan genkende brugere, og foreslå at man "tagger" dem, når man deler et billede på platformen.

Demografisk identifikation

Ansigtsgenkendelse handler om at identificere personer, men kunstig intelligens kan også bruges til andre slags analyser af ansigter. Kunstig intelligens kan for eksempel bruges til at analysere billeder af ansigter, for at finde ud af personers karaktertræk, såsom deres køn eller alder. Det kaldes for demografisk identifikation.

Når den skal vurdere personers karaktertræk bruger den kunstige intelligens en statistisk model, som viser hvordan forskelle i personers ansigter typisk hænger sammen med forskellige karaktertræk. Den statistiske model gør det muligt for den kunstige intelligens, at gætte på for eksempel hvilket køn eller alder en person har.⁶

Man kan kombinere demografisk identifikation med personidentifikation, men de to typer ansigtsgenkendelse kan også bruges uafhængigt af hinanden. Hvis demografisk identifikation bruges alene, så identificerer den ikke hvem personer er, men kun hvilke karaktertræk de har.

Demografisk identifikation er en sværere opgave for ansigtsgenkendelse end personidentifikation. Det skyldes at ansigtstræk ikke altid hænger tæt sammen med karaktertræk. Det kender de fleste, når man som menneske skal forsøge at vurdere andre. Det kan for eksempel være svært at vurdere en persons alder, fordi nogle personer ikke ser ud på den måde, der er typisk for deres aldersgruppe.

6 Se Zheng, et al. 2020.

Kundeanalyse i butikker

Mange butikker kan være interesserede i at vide, hvilken slags kunder der besøger butikken. Nogle butikker bruger demografisk identifikation til at registrere for eksempel hvor mange kunder butikken har haft fra forskellige kundegrupper, eller hvornår en bestemt kundegruppe typisk handler. (Kulager 2021).

Afsløring af seksuel orientering

I et berømt studie har forskere vist, at en specielt trænet kunstig intelligens var i stand til at vurdere personers seksuelle orientering, ved at analysere profilbilleder fra et datingsite. Ved at kigge på fem billeder af en person kunne den skelne mellem hetero- og homoseksuelle mænd i 91% af tilfældene, og mellem hetero- og homoseksuelle kvinder i 83% af tilfældene. I begge tilfælde var dette langt mere præcist, end når mennesker forsøgte at løse samme opgave. (Wang & Kosinski 2018).

Affektidentifikation

Kunstig intelligens kan også lave ansigtsanalyse for at vurdere, hvad personer på et billede føler. Er personen på billedet for eksempel vred eller afslappet? Glad eller ked af det? Bange eller tryk? Når mennesker kigger på hinanden, forsøger vi instinktivt at aflæse følelser, blandt andet ved at se på, hvad ansigtet udtrykker. En kunstig intelligens kan forsøge at gøre mennesker kunsten efter ved også at analysere disse udtryk. Det kaldes at den kunstige intelligens identificerer personers affekt.

Når en kunstig intelligens skal vurdere en persons følelser, er metoden lidt den samme, som når den skal vurdere karaktertræk. Den kunstige intelligens bruger en statistisk model til at genkende bestemte ansigtsudtryk, som typisk hænger sammen med en bestemt følelse. Den kan for eksempel genkende en mund, der er formet som et smil, og have information om, at et smil statistisk er forbundet med glæde.⁷

Ligesom demografisk identifikation er formålet med affektidentifikation ikke at identificere hvem en person er. Analysen viser i stedet hvilke følelser et ansigt giver udtryk for.

⁷ Se Ko 2018; Li & Deng 2020.

Og ligesom demografisk identifikation har opgaven vist sig at være teknisk vanskelig, fordi mennesker kan give udtryk for følelser på forskellige måder, og undertrykke eller skjule følelser.⁸

Kundetilfredshed og lyssky adfærd i butikker

Mange butikker kan have interesse i at vide, om kunder har været tilfredse med at handle i butikken. Nogle butikker bruger kameraer og affektidentifikation til at vurdere, om kunden virker glad og tilfreds, eller skuffet og frustreret, når de forlader butikken. Butikker kan også have en interesse i at holde øje med mistænkelig adfærd, for eksempel for at forhindre butikstyveri. Nogle butikker bruger affektidentifikation til at forsøge at opdage mistænkelig adfærd og advare personalet. (Kulager 2021).

1.1. Hvordan fungerer den kunstige intelligens?

Kunstig intelligens til ansigtsgenkendelse har eksisteret i flere årtier. I mange år virkede teknologien imidlertid bedst på meget standardiserede billeder. Kunstig intelligens havde ofte svært ved at genkende ansigter, hvis ikke billedet var taget fra en bestemt vinkel, med et bestemt lys, og alle ansigter var i samme størrelsesforhold. Det ændrede sig da man fra 2010'erne og frem begyndte at udvikle ansigtsgenkendelse baseret på dybe neurale netværk.⁹

Et **neuralt netværk** er en bestemt måde at designe en computeralgoritme, som ofte bruges til at lave kunstig intelligens. Et neuralt netværk består af knudepunkter – ”digitale neuroner” – som er forbundet med hinanden. Hvert af knudepunkterne i et neuralt netværk modtager data, udfører en matematisk operation på det, og sender nye data videre i netværket. Det

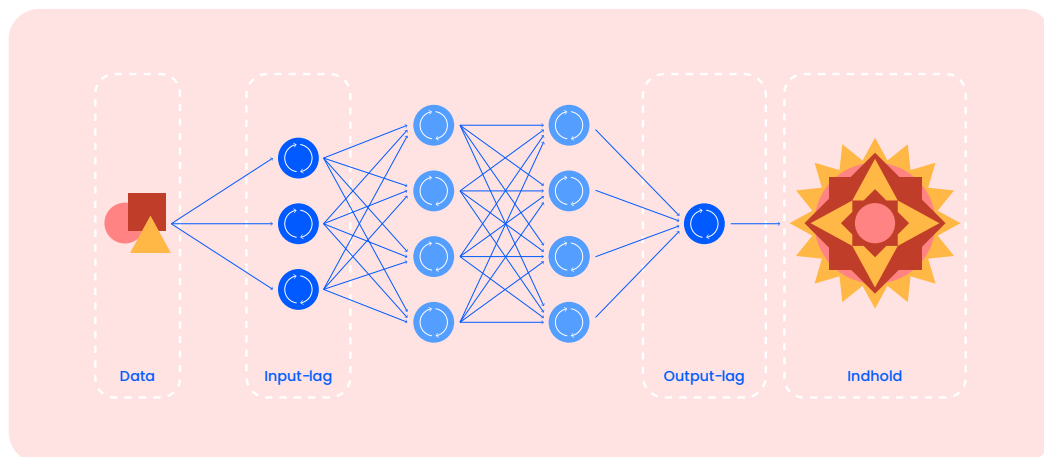
Neuralt netværk

En kunstig intelligens, der består af et system af digitale knudepunkter, som hver for sig udfører matematiske operationer og udveksler data.

⁸ Se Khare, et al. 2024; Kaur & Kumar 2024; Pereira, et al. 2024; Rehman, et al. 2025.

⁹ Se Li, et al. 2020; Taskiran, et al. 2020; Wang & Deng 2021.

sidste lag af digitale neuroner beregner det endelige resultat, for eksempel hvor der findes ansigter, hvilket ansigtsaftryk et ansigt har, eller hvor meget to ansigtsaftryk minder om hinanden. Modellen kaldes et neuralt netværk, fordi det kan minde om den måde biologiske neuroner er organiseret i en menneskelig hjerne.



Neurale netværk kan være mere eller mindre komplekse afhængigt af hvor mange knudepunkter og lag der er i netværket. En simpel opgave kan ofte løses af relativt enkle neurale netværk, mens mere vanskelige opgaver som billedanalyse ofte kræver såkaldt "dybe" neurale netværk med mange knudepunkter og lag.

I dag er mange slags ansigtsgenkendelse i stand til at løse opgaver på niveau med eller bedre end mennesker. Det gælder eksempelvis verifikation. Omvendt er der opgaver, hvor det stadig er vanskeligt at træne ansigtsgenkendelse med høj kvalitet. Det gælder for eksempel demografisk identifikation.¹⁰

Hvordan udvikler man ansigtsgenkendelse?

Moderne ansigtsgenkendelse er en avanceret kunstig intelligens – typisk et dybt neuralt netværk. Den form for avanceret kunstig intelligens er for kompleks til, at mennesker kan programmere den i detaljer. Ansigtsgenkendelse udvikles derfor typisk med **maskinlæring**.

Maskinlæring betyder, at udvikleren bruger én form for kunstig intelligens – en læringsalgoritme – til at bygge en anden kunstig intelligens, ved at "træne" på data. For

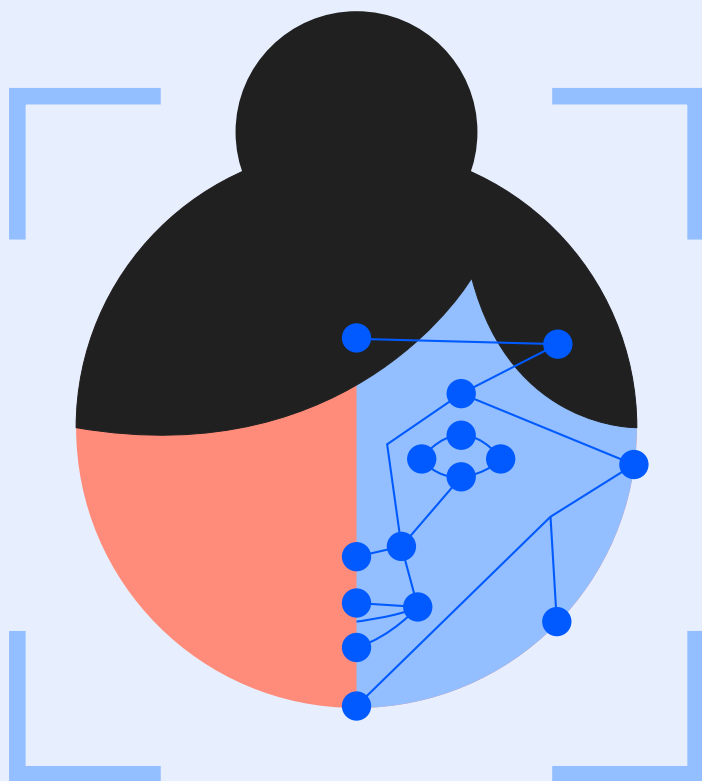
¹⁰ Se Hupont, et al. 2022; Zheng, et al. 2020.

at udvikle ansigtsgenkendelse bruger man træningsdata med tusindvis af billeder af ansigter. Læringsalgoritmen tester hvor god den kunstige intelligens er til at genkende ansigterne i træningsdata. Efter hver test justerer læringsalgoritmen gradvist den kunstige intelligens, for at gøre den bedre og bedre, indtil den er blevet så god som muligt.

Maskinlæring er helt afhængig af kvaliteten af træningsdata. Det var, især da man først begyndte at bruge maskinlæring, til at udvikle kunstig intelligens til ansigtsgenkendelse, en væsentlig udfordring at skaffe store træningsdatasæt af høj kvalitet.

Maskinlæring

En metode til at udvikle kompleks kunstig intelligens, ved at "træne" den på store mængder data.



2. Hvordan kan politiet anvende ansigtsgenkendelse?

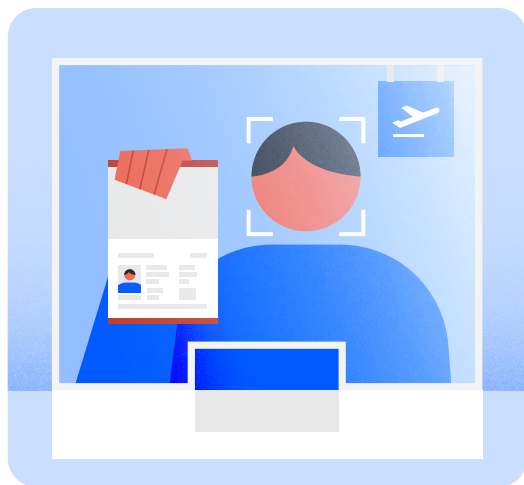
Ansigtsgenkendelse kan bruges på mange forskellige måder. I dette kapitel præsenterer vi seks brugsscenarier for politiets anvendelse af ansigtsgenkendelse.

De første tre brugsscenarier findes alle i Danmark i 2025. Politiet har i dag mulighed for at anvende ansigtsgenkendelse til automatiseret paskontrol, offergenkendelse og retrospektiv eftersøgning i det offentlige rum.

Politiet har siden 2016 anvendt ansigtsgenkendelse i Københavns lufthavn ved såkaldte "ABC-egates". Ved en sådan port udføres paskontrollen maskinelt og automatisk.¹¹ En computer scanner den rejsendes pas, og et kamera tager et billede af personen. Ansigtsgenkendelse sammenligner ansigtsaftryk fra passet med aftrykket fra billedet af personen i paskontrollen. Hvis de to aftryk minder tilstrækkeligt meget om hinanden, så verificeres den rejsendes identitet.

I 2023 igangsatte politiets Nationale enhed for Særlig Kriminalitet (NSK) et pilotprojekt med anvendelse af ansigtsgenkendelse til identifikation af kendte ofre i billedma-

teriale med seksuelt misbrug af børn.¹² Politiet modtager ofte i sådanne sager større samlinger materiale. Ansigtsgenkendelse anvendes til at sammenligne ansigter på ofre i det nye materiale med ansigter på ofre som kendes fra tidligere sager. Derved kan visse ofre identificeres, ligesom det bliver muligt at samle materiale med samme offer, og etablere sammenhænge mellem kendte og nye sager. Ved at anvende ansigtsgenkendelse kan dette gøres hurtigere, end når samme analyse foretages rent manuelt.



¹¹ Devantier 2015; Justitsministeriet 2018

¹² Projektet var en del af udmøntningen af Regeringens digitale tryghedspakke fra 2022. Justitsministeriet 2024b.

I efteråret 2024 indgik Regeringen en aftale med Socialistisk Folkeparti, Danmarksdemokraterne og Konservative om at give politiet mulighed for at anvende ansigtsgenkendelse til eftersøgning af personer i forbindelse med særligt farlig kriminalitet.¹³ Ansigtsgenkendelse foretages i dette tilfælde retrospektivt, således at politiet indhenter billedmateriale for eksempel fra kameraer på offentlige steder, som derpå analyseres. Rigspolitiet har i marts 2025 oplyst, at Københavns Politi som de første har igangsat et pilotprojekt med teknologien.¹⁴

Denne rapport fokuserer på ansigtsgenkendelse, men det er værd at bemærke, at politiet ofte kombinerer ansigtsgenkendelse med **objektgenkendelse** til de samme formål. Objektgenkendelse minder teknisk om ansigtsgenkendelse, men snarere end et bestemt ansigt forsøger den kunstige intelligens at finde bestemte objekter, for eksempel en bestemt cykel, et bestemt møbel, eller en bestemt påklædning. I mange henseender rejser objektgenkendelse de samme dataetiske spørgsmål og udfordringer som ansigtsgenkendelse. Det synes eksempelvis ikke at gøre en væsentlig forskel for en persons privatliv, om man registrerer vedkommendes færden i det offentlige rum ved at benytte ansigtsgenkendelse til at finde billeder af personens ansigt, eller objektgenkendelse til at finde billeder af personens cykel og påklædning. Selvom rapporten ikke særskilt behandler objektgenkendelse, forekommer det således rimeligt at antage, at analysen i vidt omfang kan overføres til politiets brug af objektgenkendelse.

Objektgenkendelse

Billedanalyse, hvor den kunstige intelligens finder billeder med et bestemt objekt eller en bestemt type objekt.

I tillæg til de tre brugsscenarier, som aktuelt findes i Danmark, kan det være relevant at overveje brugsscenarier som kunne blive aktuelle i dansk sammenhæng. Det er vanskeligt at forestille sig, at man i Danmark skulle anvende ansigtsgenkendelse til den form for omfattende overvågning som kendes fra visse autoritære stater, hvor et netværk af kameraer i det offentlige rum, som foretager ansigtsgenkendelse i realtid, kombineres med en meget omfattende referencedatabase, hvilket gør det muligt at foretage kontinuerlig og meget detaljeret registrering af almindelige borgeres færden og adfærd. Men der findes brugsscenarier, der på den ene side ikke går så langt, men på den anden side går længere end vi indtil nu har gjort i Danmark.

¹³ Justitsministeriet 2024

¹⁴ Rigspolitiet 2025.

Et fjerde brugsscenarie er ansigtsgenkendelse til billedsøgning i materiale knyttet til en person fra en sag med alvorlig kriminalitet. Ansigtsgenkendelse kan eksempelvis anvendes på de billeder som findes på en telefon eller computer som tilhører et offer eller en mistænkt. I modsætning til pilotprojektet ved Københavns politi vedrører dette brugsscenarie således ikke materiale indhentet fra kameraer i det offentlige rum. Dansk politi anvender ikke i 2025 ansigtsgenkendelse på denne måde, men det er Dataetisk Råds forståelse, at brugsscenariet har været afprøvet.¹⁵ Formålet med at anvende ansigtsgenkendelse i dette brugsscenarie kan eksempelvis være, at undersøge om en bestemt person findes i billedmaterialet, eller at isolere alle billeder af et offer, for at efterforskere kan se hvilke personer ofret optræder i selskab med. Ligesom når ansigtsgenkendelse anvendes til at identificere kendte ofre i sager om seksuelt misbrug af børn (brugsscenarie 2), er fordelene ved at anvende ansigtsgenkendelse derfor fortrinsvis, at politiet derved sparer menneskelige ressourcer, da alternativet er, at efterforskere manuelt gennemgår billederne.

I Storbritannien har politiet i en årrække haft mulighed for at anvende ansigtsgenkendelse til eftersøgning i realtid. Det betyder, at man udarbejder en liste med eftersøgte personer, som man har billedreferencer af. Normalt er der tale om personer, som er eftersøgt i forbindelse med alvorlig kriminalitet. Kameraer i det offentlige rum analyserer forbipasserende og sammenligner med personerne på listen. Hvis systemet genkender en person fra listen sender det en alarm til politiet. Derved kan politiet rykke ud, og pågribe den pågældende.¹⁶

I USA har betjente i nogle stater mulighed for at identificere ukendte personer, som de interagerer fysisk med, ved at anvende ansigtsgenkendelse. Det betyder at en betjent, som stopper en person på gaden, og ønsker at identificere vedkommende, kan tage et billede af personen, og anvende ansigtsgenkendelse til at forsøge øjeblikkeligt at identificere den pågældende. Ofte benytter betjente et såkaldt kropsbåret kamera til at tage billedet, som derpå kan sende billeddata til en server, der kan udføre ansigtsgenkendelse. Disse servere har typisk adgang til store referencedatabaser, for eksempel ved at trække på identificerede personers billeder i offentlige registre.¹⁷

For hvert af de seks brugsscenarier kan det være relevant at afklare en række faktuelle forhold:

¹⁵ Bech-Nielsen 2024.

¹⁶ Se Oxley, et al. 2024; Metropolitan Police 2025.

¹⁷ Se: Ringrose 2019; Seacrest & Snider 2025; Laperruque 2025.

- **Formål:** Hvad er den intendede effekt af at anvende teknologien?
- **Målgruppe:** Hvem anvendes teknologien på?
- **Anvendelsesområde:** Hvor anvendes teknologien?
- **Samtykke:** Har de personer, som teknologien anvendes på, samtykket til anvendelsen?
- **Dataproduktion:** Hvilke data genererer ansigtsgenkendelsen?
- **Database:** Hvilke data trækker teknologien på i trænings- og anvendelsesfaserne?
- **Adgang:** Hvem har adgang til de data, som teknologien anvender og genererer?
- **Information:** Hvordan oplyses målgruppen?
- **Kvalitet:** Hvor mange og hvilke fejl begår teknologien?
- **Konsekvenser:** Hvilken betydning har eventuelle fejl som teknologien begår?
- **Bias:** Virker teknologien lige godt for alle grupper?

De næste afsnit gennemgår de seks brugsscenarier, og beskriver hvert brugsscenarie i lyset af disse forhold. For visse forhold findes meget begrænsede informationer. I disse tilfælde markerer rapporten hvad Dataetisk Råd har vurderet, at man kan formode om det pågældende forhold.

2.1. Automatiseret paskontrol

Dansk politi har anvendt ansigtsgenkendelse til automatiseret paskontrol i Københavns lufthavn siden 2016.¹⁸ Automatiseret paskontrol foregår ved, at en computer i en såkaldt ABC-egate scanner den rejsendes pas, og derfra henter ansigtsaftrykket på den person, som passet tilhører.¹⁹ Samtidig tager et kamera placeret i porten et billede af den rejsende. Den kunstige intelligens udleder ansigtsaftrykket fra billedet af den rejsende, og sammenligner de to ansigtsaftryk. Hvis aftrykkene minder tilstrækkeligt meget om hinanden, så verificeres den rejsendes identitet.

¹⁸ Se: Devantier 2015; Justitsministeriet 2018. Rigspolitiet betegner dette "automatiseret grænsekontrol", jf. formålet med kontrollen. Vi anvender her betegnelsen "paskontrol" som udtryk for den konkrete funktion som ansigtsgenkendelse udfører. Rigspolitiet oplyser, at portene i juni 2024 er udskiftet med en nyere version. Rigspolitiet oplyser videre, at der i deres terminologi er tale om "biometrisk sammenstilling", ikke ansigtsgenkendelse, idet ansigter ikke sammenlignes med et mønster eller optagelser lagret i en database. Dataetisk Råd bruger i denne rapport begrebet ansigtsgenkendelse i en lidt bredere forstand, jf. kapitel 1, hvorefter også denne form for en-til-en-verifikation falder under begrebet.

¹⁹ Disse biometriske data findes på nyere pas, som er udstyret med en biometrisk chip. Automatiseret paskontrol er således kun tilgængelig for rejsende, som er i besiddelse af et pas med en sådan chip.

Formålet med automatiseret paskontrol er grænsekontrol, ligesom ved manuel paskontrol, således at alene personer med gyldigt pas gives adgang til fly eller dansk territorium. Ansigtsgenkendelse anvendes som erstatning for manuel kontrol for at begrænse politiets brug af menneskelige ressourcer til denne opgave. Anvendelsens **målgruppe** er rejsende til og fra lande som kræver gyldigt pas, dvs. lande udenfor Schengen-samarbejdet, og **anvendelsesområdet** er alene de dertil indrettede og tydeligt markerede porte i Københavns Lufthavn og Billund Lufthavn.

Automatiseret paskontrol er frivillig, idet rejsende har mulighed for at vælge menneskelig paskontrol i stedet, og således kan **samtykke** til anvendelsen. Ansigtsgenkendelsen producerer et billede af den rejsende og et derfra udledt ansigtsaftryk. Disse data kan i princippet gemmes, men bliver det efter Dataetisk Råds forståelse ikke, ligesom det er svært at se hvilket formål det skulle tjene, at gemme dem. Der er derfor ikke, så vidt Dataetisk Råd forstår, **adgang** til disse data. Paskontrollen kan også producere, lagre og dele andre data, for eksempel data om at den pågældende person har passeret paskontrollen, eller tjek af status i Interpols databaser, men adskiller sig i denne forbindelse ikke fra menneskelig paskontrol.

Automatiseret paskontrol trækker i anvendelsen på data lagret på den rejsendes pas samt et billede taget ved porten, og er derfor ikke afhængig af adgang til en **database** med yderligere referencer. Det er Dataetisk Råds forståelse, at den anvendte model er trænet på de store kommercielle datasæt, som i dag anvendes af de fleste udviklere.

Den automatiske paskontrol er tydeligt markeret i form af særskilte porte med et synligt kamera, og en skærm som giver brugere **information** om hvordan de skal gennemføre paskontrollen. Der er imidlertid meget sparsom information, både i selve lufthavnen og på politi og lufthavns hjemmesider, om at der anvendes ansigtsgenkendelse, og hvordan systemet fungerer.

Konsekvenserne ved fejl er enten at en rejsende fejlagtigt afvises (falsk negativ), og i den forbindelse henvises til manuel paskontrol, eller at en rejsende fejlagtigt godkendes med et ugyldigt pas (falsk positiv). Data om systemets fejlrate er ikke tilgængelige, men man må i udgangspunktet forvente, at fordi automatiseret paskontrol udfører 1-til-1-verifikation på ansigtsaftryk af høj kvalitet, vil **kvaliteten** være meget høj, og eventuelle **bias** vil have begrænset effekt.²⁰

²⁰ Effekten af bias afhænger til dels af fejlrate, fordi denne påvirker hvor ofte bias i praksis har effekt. Selv et system, som eksempelvis laver dobbelt så mange fejl for en bestemt gruppe, vil have begrænset negativ effekt, hvis det så godt som aldrig laver fejl.

2.2. Offergenkendelse i materiale med seksuelt misbrug af børn

National enhed for Særlig Kriminalitet (NSK) igangsatte i 2023 et pilotprojekt med anvendelse af ansigtsgenkendelse til identifikation af kendte ofre i billedmateriale med seksuelt misbrug af børn.²¹ I denne type sager indhenter politiet ofte store mængder billedmateriale. Der kan eksempelvis være tale om en harddisk med en samling på tusindvis eller titusindvis af billeder, som en gerningsmand har erhvervet gennem flere år i internetfora og chatgrupper. Ansigtsgenkendelse anvendes af efterforskere til at sammenligne de ofre, som optræder i det nye materiale, med ofre som kendes fra materiale indhentet i tidligere sager. Anvendelsens **målgruppe** er således ofre i sager vedrørende seksuelt misbrug af børn, og **anvendelsesområdet** billedmateriale beslaglagt i sager som efterforskes af politiet. Resultatet er for hver søgning en serie af referencebilleder, der statistisk minder mest om ofret i det pågældende billede. Anvendelsen foretages fysisk af efterforskere på et værksted ved politiets Nationale enhed for Særlig Kriminalitet. Den endelige vurdering af, om der er tale om et kendt offer, er i alle tilfælde en menneskelig efterforskers ansvar.

Formålet med at anvende ansigtsgenkendelse i dette brugsscenarie er at effektivisere efterforskningen. Ved at identificere kendte ofre kan politiet skelne mellem materiale, som allerede kendes fra tidligere sager, materiale som er nyt, men vedrører kendte ofre, og materiale som er nyt, og vedrører ikke tidligere kendte ofre. Anvendelsen gør ifølge politiet arbejdet betragteligt lettere og hurtigere for efterforskere end manuel gennemgang, og kan derved både frigøre ressourcer, og i nogle tilfælde hjælpe med hurtigere opklaring. Det er ikke muligt at indhente **samtykke** til anvendelsen, idet ofrene ikke er identificerede før anvendelsen.

Ved at anvende ansigtsgenkendelse **produceres** biometriske ansigtsaftryk af de ofre, som optræder i materialet, og ofrene kan i nogle tilfælde identificeres, når et nyt billede kan kobles til en sag med et identificeret offer. I andre tilfælde kan det alene fastslås, at flere billeder forestiller det samme ukendte offer. Relevante informationer om for eksempel tidspunkt, sted og karakteren af overgreb kan gemmes på selve sagen, men adskiller sig ikke i denne forbindelse fra de informationer som kan gemmes ved rent menneskelig analyse.

²¹ Se: Justitsministeriet 2024b.

Offergenkendelse trækker i anvendelsen på den **database** dansk politi har med tidligere beslaglagt billedmateriale. Billederne i denne database udgør referencerne for den kunstige intelligens, hvorimod der ikke søges med reference til andre billeddata, herunder offentligt tilgængelige billeder. NSK anvender en open source model, hvis funktion til ansigtsopdagelse er lokalt fintunet. Da der er tale om ekstremt følsomme data, er **adgang** til værktøjet og databaserne begrænset til de relevante medarbejdere, konkret efterforskere ved NSK som arbejder på de pågældende sager. Aktivitet i systemerne logges og monitoreres for at undgå usaglig anvendelse. Der er meget begrænset offentligt tilgængelig **information** om anvendelsen.²²

Konsekvenserne ved fejl er, at et ukendt offer overses, fordi det fejlidentificeres som et kendt offer (falsk positiv fejl), eller at materiale om et kendt offer ikke knyttes til den relevante sag, fordi ofret fejlidentificeres som ukendt (falsk negativ fejl). Fordi ansigtsgenkendelse anvendes på materiale af meget svingende billedkvalitet, og benytter en meget stor referencedatabase, er opgaven teknisk vanskelig. Af samme grund præsenteres resultatet altid for menneskelige efterforskere, som manuelt foretager den endelige vurdering. Ikke desto mindre viser NSKs test, at det er muligt at opnå høj **kvalitet**, forstået således at relevante billeder præsenteres for efterforskeren. Politiets interne test af **bias** viser, at den største udfordring knytter sig til at identificere ofre på billeder hvor der er væsentlig aldersforskel, samt at det i almindelighed er vanskeligere at identificere ofre, jo yngre de er. Derimod har det ikke været muligt at finde statistisk signifikant bias på tværs af køn eller etnicitet.²³

2.3. Retrospektiv eftersøgning i materiale fra det offentlige rum

Københavns politi har siden marts 2025 kørt et pilotprojekt, hvor kredsene som de første i Danmark har fået mulighed for at anvende ansigtsgenkendelse til retrospektiv eftersøgning i videomateriale fra det offentlige rum.²⁴ Politiet kan anvende teknologien i forbindelse med efterforskning af særligt alvorlig, personfarlig kriminalitet, såsom drab, terror og kidnapninger. Projektet er et resultat af en politisk aftale indgået i ef-

22 Når vi i dette afsnit henviser til "offentlig tilgængelig information" henviser vi til information som er kommunikeret mod offentligheden af de relevante myndigheder. Udover denne findes der visse mængder begrænset information i mediernes dækning af politiets anvendelse, samt i for eksempel ministerielle svar på udvalgs spørgsmål i Folketinget.

23 NSK har delt dokumentation for disse test med Dataetisk Råd, men materialet er ikke offentligt tilgængeligt.

24 Projektet betegnes af politiet som "mønstergenkendelse", da det dækker over både ansigtsgenkendelse og objektgenkendelse. Vi fokuserer her på brugen af ansigtsgenkendelse, jf. bemærkninger om objektgenkendelse i begyndelsen af dette kapitel.

teråret 2024.²⁵ Ansigtsgenkendelse foretages i dette tilfælde retrospektivt, således at politiet først indhenter billedmateriale fra kameraer på offentlige steder, som derpå analyseres. Der er derfor en vis forsinkelse mellem de aktiviteter som filmes og politiets analyse af samme.

Formålet med at anvende ansigtsgenkendelse i dette brugsscenario er at give politiet bedre muligheder for at identificere eftersøgte personer i det offentlige rum, for eksempel for at kortlægge personens færden og adfærd, herunder hvilke andre personer vedkommende interagerer med. Dette er typisk ikke muligt ved manuel analyse, ganske enkelt fordi der kan være tale om hundreder eller tusinder af timers video.

Anvendelsesområdet er relevante dele af det offentlige rum, hvorfra politiet har både mulighed for at indhente videomateriale, og en formodning om, at den eftersøgte kunne optræde. **Målgruppen** for anvendelsen er de personer som har passeret et kamera i det offentlige rum, og derfor optræder i det indhentede materiale. Den konkrete eftersøgte vil normalt være en mistænkt i en sag der efterforskes som særligt alvorlig, personfarlig kriminalitet. Det er almindeligvis ikke muligt at indhente **samtykke** fra de pågældende personer, idet de i de fleste tilfælde er ukendte inden søgningen og ikke identificeres.

Databasen med referencebilleder trækkes fra sagens øvrige materiale, eller indhentes specifikt til eftersøgningen eksempelvis fra offentlige registre eller sociale medier. Det er Dataetisk Råds formodning, at politiet også til dette brugsscenario anvender en kommerciel model, som er trænet på de store, kommercielle databaser, der anvendes af de fleste udviklere.

Anvendelsen **producerer** biometriske ansigtsaftryk af de personer som optræder i materialet, og registrerer hvor i materialet personer, som ligner den eftersøgte, optræder. Rigspolitiet oplyser, at hverken de genererede ansigtsaftryk eller data om identifikation af den eftersøgte lagres, men anvendelsen gør det muligt både at notere de steder, hvor den eftersøgte faktisk optræder, og deraf at udlede informationer om den pågældende, eksempelvis vedkommendes færden, påklædning, og interaktioner med andre. Disse informationer kan gemmes på sagen, ligesom ved manuel gennemgang. **Adgang** til de pågældende data er i udgangspunktet begrænset til efterforskere knyttet til den konkrete sag, men må i øvrigt formodes at følge de generelle bestemmelser for adgang til sagsmateriale ved politiet. Dataetisk Råd har ikke kunnet identificere offentligt tilgængelig **information** om anvendelsen.

25 Justitsministeriet 2024c; Rigspolitiet 2025.

Der findes ikke offentligt tilgængelig information om **kvaliteten** eller **bias** for dette brugsscenarie. Billedmateriale fra det offentlige rum vil ofte være af relativt lav kvalitet, og materialets omfang vil alt andet lige gøre det mere vanskeligt korrekt at identificere en eftersøgt, ganske enkelt fordi mange (irrelevante) personer typisk vil optræde i materialet. Man kan derfor rimeligvis formode, at kvaliteten vil være lavere og bias højere end i visse andre brugsscenarier. **Konsekvenserne** ved fejl er i ét tilfælde, at et irrelevant billede fejlagtigt identificeres som et billede af den pågældende person (falsk positiv), og i det andet tilfælde, at et relevant billede overses fordi den eftersøgte ikke identificeres (falsk negativ). I det første tilfælde vil det ofte være muligt for menneskelige efterforskere at korrigere fejlen, fordi det manuelt kan slås fast, at der er tale om en fejl.

2.4. Retrospektiv billedsøgning i materiale fra relevante personer

Et fjerde brugsscenarie er retrospektiv billedsøgning i materiale som er indhentet fra personer knyttet til en sag om alvorlig kriminalitet. Ansigtsgenkendelse kan eksempelvis anvendes på de billeder, som findes på et offers telefon eller computer. Rigspolitiet oplyser, at dette brugsscenarie ikke findes ved dansk politi i 2025. Det er imidlertid Dataetisk Råds forståelse, at brugsscenariet tidligere har været afprøvet, samt at det er teknisk lettilgængeligt, hvorfor det kan være relevant at tage dataetisk stilling til det.

Formålet med at anvende ansigtsgenkendelse i dette brugsscenarie er at identificere og isolere relevante billeder. En moderne mobiltelefon eller computer kan indeholde meget store mængder billedmateriale. Ofte vil størstedelen af sådant materiale være irrelevant for en given sag, og det kan kræve betragtelige menneskelige ressourcer at foretage en manuel gennemgang af materialet. En efterforsker kan eksempelvis være interesseret i at finde eventuelle billeder af en mistænkt på ofrets telefon, eller billeder som viser ofret i selskab med andre personer, for at få et indtryk af ofrets omgangskreds. Ved at anvende ansigtsgenkendelse kan de relevante billeder hurtigt identificeres og isoleres, uden at efterforskeren behøver gennemse det irrelevante materiale.

Anvendelsesområdet er således materiale, som er indhentet fra ofre, mistænkte eller andre personer med tilknytning til en sag om alvorlig kriminalitet, og anvendelsens **målgruppe** er de personer, som optræder på dette billedmateriale. Det vil typisk ikke være muligt at indhente **samtykke** fra personer på billederne, idet deres identitet ikke kendes før anvendelsen.

Anvendelsen **producerer** biometriske ansigtsaftryk af de personer som optræder i materialet. Disse data behøves ikke lagret når anvendelsen er afsluttet, ligesom de ikke behøver knyttes til en identitet. En søgning i materialet kan eksempelvis vise de billeder i materialet, hvor en person minder mest om den søgte, men behøver ikke at fastslå hvem de pågældende er. Ved at lokalisere relevant materiale kan efterforskere også udlede informationer, for eksempel om ofre eller mistænktes adfærd. Sådanne informationer kan gemmes på sagen, men svarer normalt til de informationer, der ville udledes og gemmes ved manuel gennemgang. **Adgang** til de pågældende data må forventes at være begrænset til efterforskere knyttet til den konkrete sag, men vil i øvrigt falde under de almindelige bestemmelser for adgang til sagsmateriale ved politiet.

Databasen med referencer kan enten udgøres af dele af det indhentede billedmateriale, eller af billeder indhentet på anden vis, for eksempel et billede af en mistænkt som er fundet offentligt tilgængeligt. Hvis dansk politi skulle tage denne anvendelse i brug, ville man med overvejende sandsynlighed benytte en kommerciel model, som var trænet på de store, kommercielle databaser, der anvendes af de fleste udviklere. Fordi anvendelsen ikke er aktuel i Danmark, findes der ikke offentligt tilgængelig **information** om brugsscenarioet.

Konsekvenserne ved fejl vil i nogle situationer være, at et irrelevant billede fejlagtigt kategoriseres som et billede af den søgte (falsk positiv), og i andre at et relevant billede overses, fordi en søgt ikke identificeres som sådan (falsk negativ). Sådanne konsekvenser vil kunne mitigeres, fordi ansigtsgenkendelse her alene anvendes som støtte for menneskelige efterforskere, der arbejder på den pågældende sag. Givet at brugsscenarioet ikke findes i Danmark findes der ikke offentligt tilgængelig information om systemets **kvalitet** eller **bias**, men man kan med rimelighed formode at kvaliteten ville være høj, og bias beskedent.

2.5. Realtidseftersøgning i det offentlige rum

Ved retrospektiv eftersøgning anvendes ansigtsgenkendelse med en vis forsinkelse relativt til de begivenheder som optræder i billedmaterialet. Men det er også muligt at anvende ansigtsgenkendelse i realtid. Dette brugsscenarie findes ikke i Danmark i 2025, men er i europæisk sammenhæng kendt fra blandt andet Storbritannien. Eftersøgning i realtid gør det muligt at forsøge at identificere eftersøgte for derved at kunne pågribe dem. I praksis udarbejder politiet en liste med de mest eftersøgte personer, for eksempel mistænkte i sager om alvorlig kriminalitet. Ansigtsgenkendelse i det

offentlige rum analyserer løbende forbigående og vurderer, om de er identiske med en person på listen. Hvis systemet genkender en person fra listen, sender det en alarm til politiet, som kan rykke ud og pågribe den pågældende.²⁶

Formålet med eftersøgning i realtid i det offentlige rum er at kunne identificere og opsøge den eftersøgte person, for at kunne hjælpe, afhøre eller anholde den pågældende. **Målgruppen** er således personer som passerer et kamera i det offentlige rum. **Anvendelsesområdet** er de steder i det offentlige rum, hvor politiet har installeret kameraer med den fornødne tekniske kapacitet.²⁷ Det er typisk ikke muligt, at indhente **samtykke** fra de personer, som opholder sig i eller passerer de pågældende dele af det offentlige rum, om end det er muligt at informere om anvendelsen, for eksempel ved skiltning.

Ved anvendelsen **produceres** biometriske ansigtsaftryk af de personer som filmes, og i de tilfælde hvor en person genkendes logges data om dette. De førstnævnte data gemmes efter Dataetisk Råds forståelse ikke, og det er da heller ikke klart hvilken funktion dette skulle tjene. Data om positive identifikationer kan logges for eksempel med henblik på at vurdere systemets kvalitet, eventuelt i pseudonymiseret form. Data om eftersøgte som er blevet identificeret, for eksempel at vedkommende blev identificeret et bestemt sted på et bestemt tidspunkt, kan gemmes i tilknytning til sagen, for eksempel som baggrund for en pågribelse. Myndigheder vil kunne anvende forskellige politikker for **adgang** til data, men i udgangspunktet vil adgang normalt alene bestå af den alarm, som sendes til relevante medarbejdere ved en positiv identifikation. Disse medarbejdere kan enten foretage en manuel vurdering via kameraer, eller sende betjente til stedet for at foretage en vurdering i interaktion med den pågældende person.

Data til **databasen** med referencer af eftersøgte personer vil antageligt normalt trækkes fra de relevante sager, og kan i sidste ende komme både fra offentlige registre og offentligt tilgængelige data såsom sociale medier. De anvendte modeller vil ofte være trænet på de store kommercielle databaser, som i dag anvendes af de fleste udviklere. Der findes i eksempelvis britisk sammenhæng relativt detaljeret **information** om brugsscenariet, inklusiv offentligt tilgængelige resultater af tests og data om anvendelse og fejlreter.

²⁶ Se Oxley, et al. 2024; Metropolitan Police 2025.

²⁷ Ansigtsgenkendelse i realtid forudsætter rent teknisk, at sådanne kameraer enten har mulighed for i realtid at sende de pågældende data til en central server ved politiet, hvor de kan behandles, eller at der lokalt installeres en computer som kan udføre ansigtsgenkendelse i tilknytning til hvert kamera eller gruppe af kameraer.

Ansigtsgenkendelse i realtid på materiale fra det offentlige rum er i udgangspunktet en krævende opgave for den kunstige intelligens, fordi billedmaterialet ofte har relativt lav kvalitet, og fordi antallet af personer som skal vurderes kan være meget højt. Ikke desto mindre synes de offentligt tilgængelige data fra Storbritannien at indikere, at det er muligt at opnå høj **kvalitet** og begrænset **bias**. Denne kvalitet er vigtig, fordi **konsekvenserne** ved fejl kan være alvorlige. I det ene tilfælde overses en eftersøgt person fordi ansigtsgenkendelse ikke identificerer vedkommende (falsk negativ); i det andet tilfælde fejlidentificeres en irrelevant person som eftersøgt, og udsættes potentielt for en uberettiget politiaktion, for eksempel en anholdelse (falsk positiv).

2.6. Identifikation af ukendte personer i fysiske interaktioner

Det sidste brugsscenarie, som vi denne rapport præsenterer, er muligheden for at bruge ansigtsgenkendelse til at identificere ukendte personer i fysisk interaktion med politiet. En fysisk interaktion skal her forstås sådan, at politiet står ansigt til ansigt med den pågældende, for eksempel fordi de har stoppet vedkommende i en bil eller til fods. Politiet har i Danmark ret til at kræve at borgere identificerer sig i sådanne situationer, ikke desto mindre kunne det i nogle situationer være relevant at forsøge at identificere en person med ansigtsgenkendelse, eksempelvis hvis vedkommende nægter at oplyse sin identitet, er ude af stand til at svare, eller hvis der er mistanke om, at personen oplyser en falsk identitet. Anvendelsen foregår i praksis typisk ved, at en betjent tager et billede af den pågældende, og overfører dette til en central server, hvor den kunstige intelligens sammenligner billedet med referencer i en database. Betjenten modtager et svar i form af billeder af og oplysninger om de personer, som systemet vurderer minder mest om den pågældende. Brugsscenariet findes ikke i Danmark i 2025, men kendes eksempelvis fra USA.²⁸

Formålet med anvendelsen er altså, at identificere en ukendt person, som indgår i en fysisk interaktion med politiet. **Målgruppen** er ukendte personer, som indgår i sådanne interaktioner, og **anvendelsesområdet** er de steder og situationer hvor betjente interagerer med og kan have interesse i at identificere ukendte borgere. Det er i princippet muligt at indhente **samtykke**, men fordi anvendelsen er mest relevant når en borger nægter at oplyse sin identitet, er ude af stand til at svare, eller mistænkes for at have

28 Se: Ringrose 2019; Seacrest & Snider 2025; Laperruque 2025.

oplyst falsk identitet, vil det i praksis være af begrænset relevans at anvende ansigtsgenkendelse i dette brugsscenarie, hvis der stilles krav om samtykke til anvendelsen.

Ved anvendelsen **produceres** et digitalt billede samt et biometrisk ansigtsaftryk af den ukendte person. Disse data kan lagres efter anvendelsen, men dette er hverken nødvendigt eller formålstjenstligt. For så vidt en person identificeres, kan informationer om vedkommendes identitet gemmes, eksempelvis som en del af en rapport om interaktionen. I denne henseende adskiller anvendelsen sig imidlertid ikke fra andre måder at identificere personer i sådanne situationer.

Anvendelsen forudsætter etableringen af en **database** med referencer som kan sammenlignes med de personer, politiet ønsker at identificere. Identifikation bliver alt andet lige mere præcis, jo større denne database er, ganske enkelt fordi systemet kun kan identificere personer som optræder i databasen. Træning af selve modellen vil typisk trække på de store kommercielle databaser med billedmateriale, som de fleste udviklere i dag anvender. **Adgang** til data kan begrænses til de medarbejdere som er ansvarlige for at understøtte og udvikle systemet, med undtagelse af selve resultatet af ansigtsgenkendelsen, som deles med den betjent, der ønsker at identificere en person. Der findes i amerikansk sammenhæng offentligt tilgængelig information om politiets brug af ansigtsgenkendelse, om end meget af denne **information** er knyttet til anvendelsen ved de mange individuelle myndigheder i forskellige byer og stater.

Identifikation af en ukendt person er en teknisk krævende opgave sammenlignet med visse andre brugsscenarier, idet billedet af den ukendte person kan være af svingende kvalitet, og der ofte vil være en meget omfattende database af referencer at sammenligne med. Det har imidlertid ikke været muligt for Dataetisk Råd i dette projekt at finde information om **kvalitet og bias** i de systemer som anvendes i amerikansk sammenhæng, udover de standardiserede tests som udføres af NIST (se afsnit om indvendingen at ansigtsgenkendelse vil lave fejl nedenfor). **Konsekvenserne** af fejl kan være potentielt alvorlige, hvad enten en person som faktisk er relevant for politiet, for eksempel fordi vedkommende er eftersøgt, fejlidentificeres som en irrelevant person (falsk negativ), eller en person som ikke er relevant fejlidentificeres som en person der er relevant, for eksempel en eftersøgt (falsk positiv). Af samme grund overlades den endelige vurdering normalt til den betjent som har igangsat anvendelsen, om end man i den forbindelse kan være bekymret for risikoen for automatiseringsbias.²⁹

²⁹ Automatiseringsbias er en tendens til at fæste overdreven lid til automatiske systemer som kunstig intelligens, for eksempel således at agenten holder op med selvstændigt at vurdere situationen. Se: Goddard, et al. 2011; Lyell & Coiera 2017.



3. Hvad er de juridiske rammer for politiets brug af ansigtsgenkendelse?

Når man skal overveje hvordan dansk politi bør have mulighed for at anvende ansigtsgenkendelse, er det relevant at forholde sig til hvad de juridiske rammer for anvendelsen er, især eventuelle rammer som ikke kan ændres af Regeringen og Folketinget. Dansk politis muligheder for at bruge ansigtsgenkendelse er reguleret af både europæisk og dansk lovgivning, som tilsammen sætter rammerne for lovlig anvendelse.

I EU er politiets anvendelse af ansigtsgenkendelse først og fremmest reguleret af AI-forordningen. Forordningen forbyder politiets anvendelse af ansigtsgenkendelse i realtid i det offentlige rum, undtagen til eftersøgning af ofre eller mistænkte i særligt farlige situationer.³⁰ Selv i disse situationer stiller forordningen krav om, at politiet på forhånd skal have evalueret og registreret systemet, og at politiet får tilladelse til at bruge det i den konkrete situation, for eksempel ved en dommerkendelse. Politiets øvrige muligheder for

30 Se især forordningens artikel 5, stk 1(h): <https://artificialintelligenceact.eu/article/5/>

at anvende ansigtsgenkendelse, for eksempel til efterforskning efter at en forbrydelse er begået, falder næsten alle under forordningens bestemmelser om højrisiko-systemer. En markant undtagelse er politiets brug af ansigtsgenkendelse til verifikation af identitet, for eksempel ved automatisk paskontrol i lufthavnen. Når det gælder højrisiko-systemer, stiller forordningen krav om blandt andet risiko-håndtering, kontrol af datasæt, teknisk dokumentation, logning, kvalitetsstyring og menneskelig efterprøvning.

De øvrige EU-lande kan alene give politiet tilladelse til at anvende ansigtsgenkendelse igennem national lovgivning indenfor de overordnede rammer, som AI-forordningen sætter. Danmark er imidlertid i kraft af retsforbeholdet ikke bundet af forordningens bestemmelser om politiets brug af ansigtsgenkendelse. Det giver dansk politi bredere rammer for at anvende ansigtsgenkendelse end politiet i de øvrige EU-lande.

Selvom dansk politis brug af ansigtsgenkendelse ikke er bundet af disse bestemmelser i AI-forordningen, så er den reguleret af en række andre bestemmelser. Det gælder den Europæiske Menneskerettighedskonvention, EU's charter om grundlæggende rettigheder, samt retshåndhævelsesloven, som fastsætter specifikke bestemmelser for politiet.

Både EMRK og EU's charter fastsætter en individuel ret til privatliv, som sætter grænser for, hvordan dansk politi lovligt kan anvende ansigtsgenkendelse. EMRK's artikel 8, stk. 1 og EU's charter artikel 7, stk. 1 fastslår i enslydende formuleringer, at "enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance." Bestemmelserne fortolkes således, at de også gælder når individer færdes i det offentlige rum, på den måde at folk har ret til den form for privatliv, som man rimeligvis kan forvente. Eksempelvis kan man ikke rimeligvis forvente, at andre i det offentlige rum ikke i forbifarten ser eller hører en, men man kan godt rimeligvis forvente, at myndighederne ikke systematisk overvåger hvad den enkelte borger siger og gør. Både konventionen og chartret giver mulighed for indgreb i retten til privatliv når visse betingelser er opfyldt. Det gælder eksempelvis når et sådant indgreb er lovbestemt og nødvendigt for et legitimt formål. Et eksplicit eksempel på et sådant formål er at forhindre kriminalitet.

Justitia vurderer i analysen af EMRKs betydning for dansk politis mulighed for at anvende ansigtsgenkendelse, at spørgsmålet om hvorvidt "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.”³¹ Om politiets anvendelse af ansigtsgenkendelse i realtid i det offentlige rum er lovlige eller ulovlige ifølge EMRK og EU’s charter, vil ifølge denne analyse afhænge af både præcis hvordan politiet anvender ansigtsgenkendelse, og af hvor klar og præcis lovhjemmel Folketinget har etableret for denne brug.

Den danske regering har ved flere lejligheder indtaget det synspunkt, at dansk politi kan anvende ansigtsgenkendelse indenfor rammerne af Danmarks forpligtelser under EMRK og EU’s charter uden yderligere lovhjemmel.³² Regeringen besluttede også i efteråret 2024, at lade dansk politi anvende ansigtsgenkendelse i et pilotprojekt til efterforskning af sager om bl.a. grov personfarlig kriminalitet eller statens sikkerhed uden at tilvejebringe en særskilt hjemmel eller præcisere lovhjemmelen yderligere. En endegyldig vurdering af, om dansk politis brug af ansigtsgenkendelse lever op til bestemmelserne i EMRK og EU’s charter vil ultimativt skulle foretages af henholdsvis den Europæiske Menneskerettighedsdomstol (EMD) og EU-domstolen.

Dansk politis mulighed for at anvende ansigtsgenkendelse er centralt reguleret af retshåndhævelsesloven.³³ Loven implementerer EU direktivet om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger.³⁴ Selvom Danmark også på dette område er undtaget i kraft af retsforbeholdet, tilsluttede Danmark sig i 2017 direktivet, da dette var en forudsætning for deltagelse i det europæiske Europol-samarbejde. Retshåndhævelsesloven forbyder politiet at behandle ”biometriske data med det formål entydigt at identificere en fysisk person”, undtagen ”når det er strengt nødvendigt og [foretages med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder for at beskytte mod eller forebygge trusler mod den offentlige sikkerhed].”³⁵

Formålsskravet begrænser groft sagt politiets muligheder for at anvende ansigtsgenkendelse til at identificere fysiske personer, således at det alene må bruges til at forhindre eller opklare forbrydelser. Nødvendighedskravet begrænser politiets

31 Arent Eiriksson 2024, p.33.

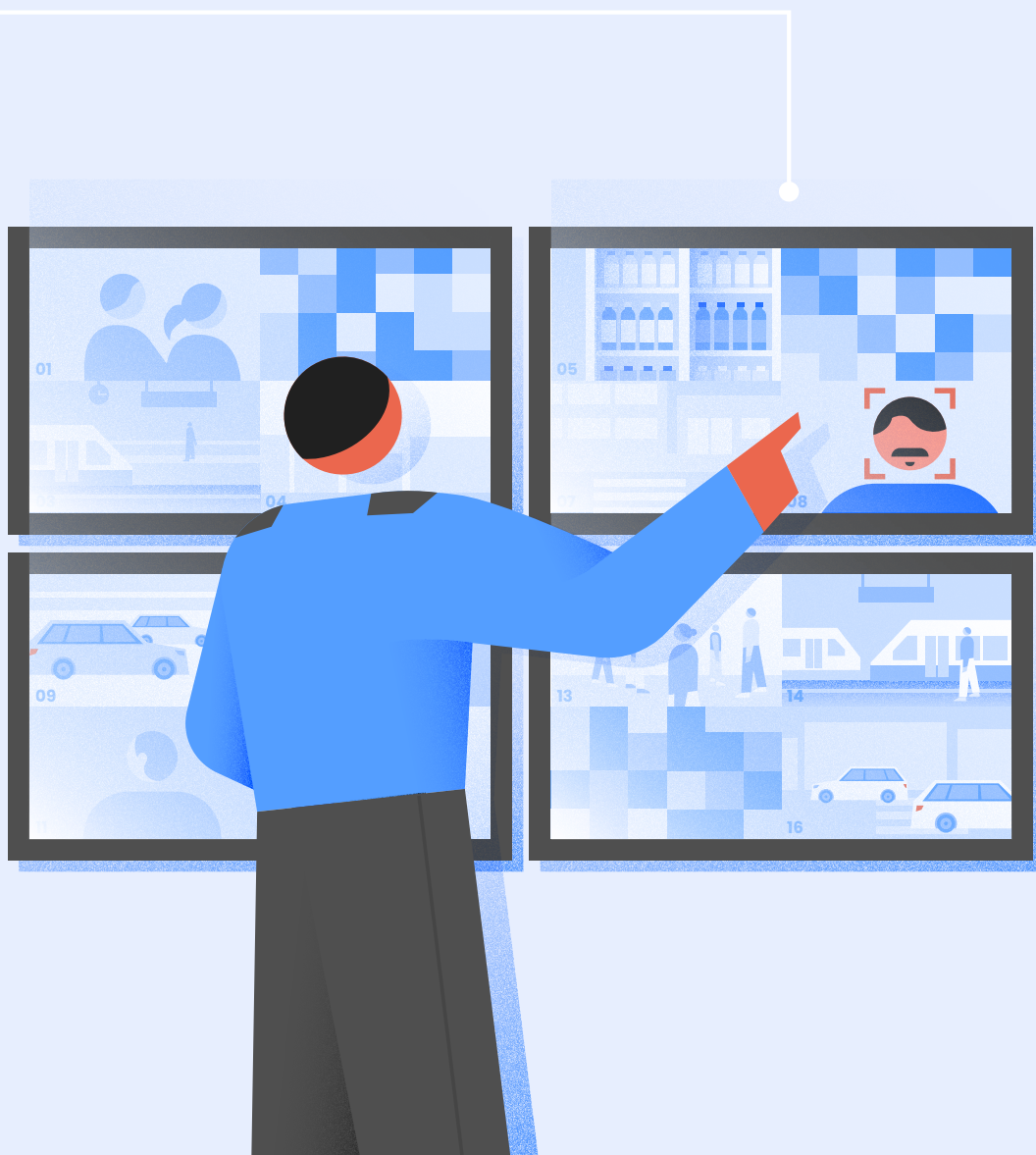
32 Se eksempelvis Justitsminister Peter Hummelgaards besvarelse af Retsudvalgets spørgsmål om regler for brug af biometri i efterforskning. Justitsministeriet 2024a.

33 <https://www.retsinformation.dk/eli/ita/2017/410>

34 EU-direktiv 2016/680 af 27. april 2016.

35 Udover krav til formål og streng nødvendighed stiller loven også krav til hvordan politiet skal behandle de pågældende data, herunder krav om god dataskik, dataminimering og betingelser for videregivelse af oplysninger. Rigspolitiet har overfor Dataetisk Råd fremhævet, at kravet alene gælder ansigtsgenkendelse til entydig identifikation af en fysisk person, mens andre anvendelser af ansigtsgenkendelse ikke er omfattet af bestemmelsen.

anvendelse til situationer, hvor anvendelse er "strengt nødvendig" for at forfølge disse formål. Meget afhænger derfor af, hvordan kravet om streng nødvendighed fortolkes. Man kunne anlægge den restriktive tolkning, at det ikke er strengt nødvendigt at anvende ansigtsgenkendelse til at identificere personer for at forebygge og efterforske forbrydelser, hvis der findes andre metoder til at forebygge og efterforske de samme forbrydelser, selv hvis de alternative metoder er mindre succesfulde eller mere ressourcekrævende. Man kunne også anlægge en mere lempelig tolkning, hvor anvendelse af ansigtsgenkendelse er strengt nødvendig, når blot anvendelse vil føre til selv minimalt bedre forebyggelse og efterforskning eller være mindre ressourcekrævende end alternativer.



4. Hvad er der på spil?

Ansigtsgenkendelse er en teknologi, som mange har stærke holdninger til. Særligt politiets brug af ansigtsgenkendelse har været omdiskuteret, både i Danmark og i mange af de lande, vi sammenligner os med.

Fortalere har blandt andet fremført, at ansigtsgenkendelse kan hjælpe politiet med at fange forbrydere og finde eftersøgte. Derved kan teknologien forhindre forbrydelser og beskytte potentielle ofre.

Kritikere har blandt andet hævdet, at ansigtsgenkendelse indskrænker menneskers privatliv, og kan afskrække uskyldig adfærd.³⁶ De har også peget på, at teknologien kan begå fejl og have bias, så den virker bedre for nogle grupper og værre for andre grupper.³⁷ Desuden har de udtrykt bekymring for, at teknologien kan misbruges, og for at anvendelse kan føre til en glidebane mod stadig mere uetiske måder at bruge teknologien.³⁸

Men hvad er der egentlig på spil? Hvordan skal man forstå de forskellige argumenter for og imod? Er alle argumenter lige gode? Og hvis ikke, hvordan ved man så om et argument er godt eller dårligt?

Dette kapitel præsenterer og diskuterer tolv almindelige dataetiske argumenter – seks for og seks imod politiets brug af ansigtsgenkendelsesteknologi. Når man skal tage stilling til politiets brug af ansigtsgenkendelse, er det vigtigt at gøre sig klart, hvor gode eller dårlige de forskellige argumenter er. Derfor analyserer kapitlet også argumenterne, og viser hvordan de kan vurderes.³⁹ Ved at skabe overblik over argumenterne, og analysere deres styrker og svagheder, kan man opnå et informeret grundlag for at tage samlet stilling til, hvornår dansk politi bør have mulighed for at anvende ansigtsgenkendelse.⁴⁰

36 Se Access Now, et al. 2021; Skovgaard 2021; Heikkilä 2022.

37 Se Bacchini & Lorusso 2019; Grother, et al. 2019; Robinson, et al. 2020; Molnar 2019.

38 Se Waelen & Brey 2022; Smith & Miller 2022.

39 For overordnet diskussion af argumenter for og imod brug af AGT, se Brey 2004; Smith & Miller 2022; Waelen & Brey 2022; Selinger & Leong 2024.

40 Se Dataetisk Råds [Dataetik – sådan går du](#).

Det er imidlertid værd at holde sig for øje, at politiet kan bruge ansigtsgenkendelse på mange forskellige måder. Argumenterne præsenteres og diskuteres i dette kapitel på et generelt niveau. For at tage stilling til om og hvordan politiet bør have mulighed for at anvende ansigtsgenkendelse, er man nødt til at vurdere argumenter i tilknytning til den konkrete anvendelse. En begrundelse kan være et stærkt argument for eller imod brugen af ansigtsgenkendelse i ét brugsscenarie, men et svagt argument i en anden situation. Dataetisk Råds samlede vurdering, position og anbefalinger præsenteres i næste kapitel.

4.1. Seks argumenter for ansigtsgenkendelse

"Ingen lovlydig borger har efter min opfattelse taget skade af at blive filmet med kriminalitets-bekæmpende kameraer."

Preben Bang Henriksen, Retsordfører (V)

"Det effektiviserer politiets arbejde."

Karina Lorentzen,
Retsordfører (SF)

"Teknologien strømliner arbejdet og gør det muligt for efterforskerne at handle hurtigere, end hvis de ikke havde haft teknologien."

Thaddeus Johnson, Kriminolog

Fortalere for at lade politiet bruge ansigtsgenkendelse kan fremføre en række forskellige argumenter. I dette afsnit kigger vi på seks af de mest almindelige begrundelser:

- **Politiets brug** af ansigtsgenkendelse vil aflaste politiet
- **Politiets brug** af ansigtsgenkendelse vil afskrække kriminelle
- **Politiets brug** af ansigtsgenkendelse vil føre til opklaring af flere forbrydelser
- **Politiets brug** af ansigtsgenkendelse vil føre til hurtigere opklaring af forbrydelser
- **Politiets brug** af ansigtsgenkendelse vil hjælpe med at finde eftersøgte
- **Politiets brug** af ansigtsgenkendelse vil ikke være et problem, hvis man ikke har noget at skjule

Politiets brug af ansigtsgenkendelse vil aflaste politiet

Dansk politi foretager jævnligt manuel analyse af billeder. Ved manuel analyse bruger man ikke ansigtsgenkendelse, men sætter ganske enkelt en politibetjent til at gennemse billedmaterialet. En første mulig begrundelse for brug af ansigtsgenkendelse er, at det vil aflaste politiet, hvis man kan anvende ansigtsgenkendelse til at analysere billedmateriale, enten som støtte til eller som egentlig erstatning for menneskelig analyse.

Aflastning

Politiets brug af AGT vil aflaste politiet og frigive ressourcer.

De frigivne ressourcer kan bruges på vigtige opgaver, som vil hjælpe borgere.

Derfor bør politiet have mulighed for at bruge AGT.

Menneskelig billedanalyse kan være meget ressourcekrævende, især hvis politiet arbejder med store mængder billedmateriale. Ansigtsgenkendelse vil ofte hurtigt og effektivt kunne gennemse det pågældende materiale, og for eksempel finde de steder i materialet, hvor en eftersøgt person optræder. Ved at bruge ansigtsgenkendelse kan man altså frigive de ressourcer, som rent manuel gennemgang ville have krævet, og benytte dem til andre formål.

Det er også troværdigt, at det vil være værdifuldt at frigive politiets ressourcer. Dansk politi udfører mange vigtige opgaver som på forskellig vis hjælper borgerne. Givetvis er det ofte nødvendigt for politiet at prioritere ressourcer, ganske enkelt fordi det ikke er muligt at løse alle opgaver. Hvis brug af ansigtsgenkendelse kan frigive ressourcer, så kan disse ressourcer altså flyttes til andre opgaver, hvor de kan gøre gavn. Helt enkelt formuleret, så kan man bruge de arbejdstimer man sparer på manuel gennemgang af billedmateriale til i stedet at patruljere, efterforske, og på anden vis servicere borgerne.

Umiddelbart er begrundelsen således overbevisende. Det er imidlertid værd at overveje hvor *stærk* begrundelsen er. Det afhænger oplagt af hvor stor en effektiviseringsgevinst man kan opnå, men også af hvordan de frigjorte ressourcer bruges, og hvor meget gavn dette gør.

Effektiviseringsgevinsten vil alt andet lige være større, jo mere billedmateriale politiet arbejder med. Hvis politiet meget sjældent laver manuel gennemgang af billedmateriale, så vil brug af ansigtsgenkendelse spare relativt få arbejdstimer. Hvis politiet omvendt laver meget omfattende manuel gennemgang af billedmateriale, så vil gevinsten potentielt være stor.

En bekymring i denne forbindelse kan være, at begrundelsen risikerer at skabe incitament til at indhente større mængder billedmateriale, ganske enkelt fordi man derved kan opnå større effektiviseringsgevinster og således bedre kan retfærdiggøre brug af ansigtsgenkendelse. Dansk politi har i dag relativt vide muligheder for både at udføre og indhente billedovervågning, særligt i det offentlige rum.⁴¹ Politiet kan dels selvstændigt opsætte kameraer som filmer, men politiet har også mulighed for at indhente billedmateriale fra overvågning udført af andre, for eksempel fra kameraer opsat af virksomheder og private personer. Det er således i vidt omfang op til politiet, hvor meget billedmateriale man vil indhente og arbejde med.

Imidlertid bliver den politimæssige gevinst ved at analysere billedmateriale antageligt gradvist mindre, jo mere materiale man analyserer. Man kan, med et teknisk udtryk, formode at den marginale nytteværdi ved manuel billedanalyse er faldende. Den faldende marginale nytteværdi betyder, at jo flere ressourcer politiet bruger på manuel billedanalyse, jo større bliver sandsynligheden for, at disse ressourcer ville kunne bruges bedre på andre opgaver. Når man skal vurdere gevinsten ved at anvende ansigtsgenkendelse kan det derfor være værd at tage udgangspunkt i, hvad gevinsten ville være under den *optimale* fordeling af ressourcer, snarere end under den *aktuelle* fordeling af ressourcer. Derved undgår man både at brug af ansigtsgenkendelse kan komme til at se meget fordelagtigt ud, hvis man anvender uforholdsmæssigt mange ressourcer på manuel billedanalyse, og omvendt, at brug af ansigtsgenkendelse kan komme til at se mindre fordelagtigt ud, alene fordi man bruger for få ressourcer på billedanalyse.

Politiets brug af ansigtsgenkendelse vil afskrække kriminelle

En anden almindelig begrundelse for politiets brug af ansigtsgenkendelse er, at brug af ansigtsgenkendelse kan afskrække potentielle kriminelle fra at begå forbrydelser. Det er en udbredt antagelse at overvågning kan have en afskrækkende effekt. Hvis brug af ansigtsgenkendelse styrker politiets overvågning kunne man formode, at den afskrækkende effekt også ville blive stærkere.

Afskrækkelse

Politiets brug af AGT vil afskrække potentielle kriminelle og derved forhindre forbrydelser.

Det er vigtigt at afskrække forbrydelser af hensyn til de mulige ofre.

Derfor bør politiet have mulighed for at bruge AGT.

⁴¹ For et overblik, se: Arent Eiriksson 2024, p.12-16.

Og hvis brug af ansigtsgenkendelse faktisk har en sådan effekt, så synes det at tale for, at lade politiet bruge ansigtsgenkendelse.

Det er nok de færreste som ikke er enige i, at det er vigtigt at forhindre forbrydelser. Men argumentets styrke kan afhænge af hvilke forbrydelser, fordi nogle forbrydelser gør mere skade end andre. Uanset at det kan være ubehageligt at være udsat for eksempelvis lommetyveri eller hærværk, så er det oftest endnu værre at blive udsat for grove forbrydelser som vold eller voldtægt. Argumentets styrke afhænger derfor til dels af, *hvilke typer* forbrydelser brug af ansigtsgenkendelse vil afskrække.

Argumentets styrke afhænger også af *hvor mange* forbrydelser politiets brug af ansigtsgenkendelse vil afskrække. Det er imidlertid meget vanskeligt at vurdere dette spørgsmål, fordi der endnu findes meget få studier af den kriminalpræventive effekt af politiets brug af ansigtsgenkendelse. Et enkelt fremtrædende studie når dog frem til, at der findes en sådan effekt. Studiet sammenligner kriminalitetsrater i 268 amerikanske byer over en periode på ca. 20 år, og konkluderer at de byer, hvor politiet regelmæssigt benyttede ansigtsgenkendelse, oplevede et fald i voldelige forbrydelser på 3% med et særligt stort fald for drab.⁴² Det er imidlertid ikke muligt ud fra dette studie at afgøre, om dette fald skyldes en afskrækkende effekt ved ansigtsgenkendelse som sådan, eller for eksempel en afskrækkende effekt ved at politiet i de pågældende byer blev bedre i stand til at opklare forbrydelser (se nedenfor, om argumentet at brug af ansigtsgenkendelse vil føre til opklaring af flere forbrydelser).



42 Johnson, et al. 2024.

Givet at der er meget begrænsede studier af den afskrækkende effekt ved brug af ansigtsgenkendelse kan det være relevant at kigge på den afskrækkende effekt ved overvågning mere generelt. Brug af ansigtsgenkendelse, kunne man argumentere, udgør i en relevant forstand en intensivering af overvågning, og for så vidt at overvågning har en afskrækkende effekt kan man derfor formode, at denne vil blive forstærket. Spørgsmålet bliver så, hvor stærk den afskrækkende effekt af overvågning i almindelighed er.

Kameraovervågning er blevet brugt til at forhindre kriminalitet i mange årtier, og kriminologer har foretaget omfattende studier, der sammenligner antallet af forbrydelser i områder med og uden overvågning, eller i det samme område før og efter man indfører overvågning. Den overraskende konsensus i disse studier er, at kameraovervågning har meget begrænset effekt.⁴³ Et omfattende metastudie viser en samlet effekt på 13% reduktion i områder med kameraovervågning relativt til områder uden. Denne effekt varierer imidlertid meget på tværs af områder og type af forbrydelse. For mange typer forbrydelser, inklusive voldelig kriminalitet, er der slet ingen målbar effekt, mens den stærkeste effekt ses på salg af narkotika og tyveri, især biltyverier fra parkeringspladser og -kældre. I den danske debat henvises ind imellem til et svensk studie fra 2021, som faktisk viste en begrænset afskrækkende effekt på voldelig kriminalitet ved introduktion af kameraovervågning i udsatte boligområder i Göteborg.⁴⁴ Det bør dog bemærkes at studiet er baseret på meget små effektstørrelser, idet det samlede antal overfald over tre år i de ti studerede boligområder var 232, i gennemsnit ca. et halvt overfald per boligområde per måned. I sammenligning med de meget omfattende data i internationale metastudier må resultaterne betragtes som forholdsvis usikre.

Der kan være flere grunde til, at overvågning har en begrænset eller ingen effekt. Det kan eksempelvis skyldes at kriminelle ikke er opmærksomme på overvågningen, at de er bevidste om overvågningen men tager forholdsregler, for eksempel ved at maskere ansigtet, at de ikke reagerer rationelt på risici, eller at forbrydelser blot forskydes til områder med mindre overvågning.

Det kan virke rimeligt at antage, at politiets brug af ansigtsgenkendelse vil have en afskrækkende effekt eller forstærke den afskrækkende effekt overvågning allerede har. Der findes imidlertid endnu meget begrænset evidens for at brug af ansigtsgenkendelse har en afskrækkende effekt, og hvor stor den i givet fald er. På et generelt

43 Welsh & Farrington 2009; Piza, et al. 2019; Thomas, et al. 2022.

44 Gerell 2021.

niveau er den afskrækkende effekt af kameraovervågning begrænset, og primært knyttet til bestemte typer kriminalitet. Samlet set kan der være grundlag for en vis skepsis overfor antagelsen om, at politiets brug af ansigtsgenkendelse i sig selv vil have en afskrækkende effekt. Hvis man mener, at en sådan effekt er usikker, bør man tillægge argumentet relativt begrænset vægt.

Politiets brug af ansigtsgenkendelse vil føre til opklaring af flere forbrydelser

En tredje almindelig begrundelse er, at politiets brug af ansigtsgenkendelse vil hjælpe politiet med at opklare flere forbrydelser. Dansk politi modtager årligt (i runde tal) 400-500.000 anmeldelser.⁴⁵ Af disse fører godt en tredjedel til en sigtelse, og omkring 45.000 straffelovsovertrædelser dømmes årligt.⁴⁶ Det forekommer umiddelbart sandsynligt, at brug af ansigtsgenkendelse i nogle tilfælde vil kunne hjælpe med at opklare og retsforfølge forbrydelser, som ellers ville forblive uopklarede eller ikke føre til dom.

Mere opklaring

Politiets brug af AGT vil hjælpe politiet med at opklare forbrydelser, som ellers ikke ville blive opklaret.

Det er vigtigt af opklare forbrydelser af hensyn til ofrene, og for at forhindre fremtidige forbrydelser.

Derfor bør politiet have mulighed for at bruge AGT.

Det er også plausibelt, at det er vigtigt at opklare flere forbrydelser. Det skyldes blandt andet at opklaring kan give ofre fred i sindet. For mange ofre kan det være tilfredsstillende, og en hjælp til at lægge forbrydelsen bag sig, at opleve at retfærdigheden sker fyldest. Opklaring kan også være med til at forhindre fremtidige forbrydelser. Den kriminologiske forskning viser, at det kan have præventiv effekt at opklare forbrydelser og straffe kriminelle, både fordi truslen om straf kan afskrække potentielle kriminelle og fordi visse straffe inkapaciterer gerningsmanden.⁴⁷

Selvom begrundelsen umiddelbart virker plausibel er det værd at overveje, hvor stærk den er. Begrundelsens styrke afhænger dels af *hvor mange* flere forbrydelser brug af ansigtsgenkendelse vil hjælpe med at opklare, og dels af *hvor meget* gavn det gør,

⁴⁵ Se <https://www.dst.dk/da/Statistik/emner/sociale-forhold/kriminalitet/anmeldte-forbrydelser>

⁴⁶ Tal fra Danmarks Statistiks statistikbank "STRAF40".

⁴⁷ Von Hirsch, et al. 1999; Kennedy 2009; Braga & Weisburd 2012; Nagin 2013. En vigtig pointe i forskningen er, at det fortrinsvis er ændringer i risikoen for at blive straffet, som kan virke afskrækkende. Ved at øge denne risiko kan brug af ansigtsgenkendelse derfor tænkes at have en indirekte afskrækkende effekt.

at opklare disse forbrydelser. Hvis brug af ansigtsgenkendelse fører til opklaring af mange forbrydelser, og dette har en stor gavnlig effekt, enten for ofrene eller ved at forhindre fremtidige forbrydelser, så peger argumentet på en stærk grund til at bruge ansigtsgenkendelse. Hvis omvendt brug af ansigtsgenkendelse fører til opklaring af få forbrydelser, eller hvis opklaring af disse forbrydelser ikke gør meget gavn, så er argumentet ikke en stærk begrundelse for at lade politiet bruge ansigtsgenkendelse.⁴⁸

Det kan imidlertid være vanskeligt at vurdere, hvor mange forbrydelser brug af ansigtsgenkendelse kan hjælpe med at opklare, og hvor stor gavn dette vil gøre. Ligesom for begrundelsen om afskrækkelse ovenfor, findes der fortsat relativt få studier, som belyser hvor stor en forskel det gør, når politiet bruger ansigtsgenkendelse til at hjælpe med at opklare forbrydelser. De foreløbige bedste data kommer fra USA, hvor en række amerikanske stater de seneste år har indført forbud mod at lade politiet anvende ansigtsgenkendelse. Disse forbud kan fungere som et naturligt eksperiment, idet interventionen gør det muligt at sammenligne opklaring i stater før og efter forbuddet med opklaring i stater som ikke har indført et forbud. Et konferencepapir fra 2025 anslår at det i staten Virginia har ført til at 2,4% færre forbrydelser opklares.⁴⁹ Omvendt viser analysen af 34 amerikanske byer fra 13 stater i et speciale fra universitetet Georgetown ingen statistisk signifikant effekt på opklaringen af voldelig kriminalitet.⁵⁰ Ingen af disse studier er fagfællebedømt forskning, og de må derfor betragtes som relativt usikre kilder.

Det virker rimeligt at antage, at effekten vil variere afhængigt af hvordan ansigtsgenkendelse bruges og hvilke forbrydelser der er tale om. Men det er også værd at holde sig for øje, at effekten vil afhænge af hvad alternativet er. Hvis alternativet eksempelvis er, at billedmateriale analyseres grundigt af mennesker, så kan man forestille sig, at det vil gøre en relativt lille forskel at bruge ansigtsgenkendelse. Effekten af at bruge ansigtsgenkendelse kan i en sådan situation fortrinsvis være aflastning af politiet (jf. den første begrundelse ovenfor).

48 Et ydertilfælde er den situation, hvor opklaring af en forbrydelse gør mere skade end gavn, for eksempel hvis et autoritært styre håndhæver uretfærdige love som kriminaliserer fredelig demokratisk modstand. I en sådan situation vil det tale imod at lade politiet anvende ansigtsgenkendelse, hvis dette vil føre til opklaring af flere sådanne forbrydelser.

49 Kim & Joo 2025.

50 Latkowski 2024.

Politiets brug af ansigtsgenkendelse vil føre til hurtigere opklaring af forbrydelser

En fjerde begrundelse er, at politiets brug af ansigtsgenkendelse vil føre til hurtigere opklaring af forbrydelser. På den måde kan brug af ansigtsgenkendelse hjælpe politiet, også i sager som ville være blevet opklaret under alle omstændigheder.

Hurtigere opklaring

Politiets brug af AGT vil hjælpe politiet med hurtigere at opklare forbrydelser.

Det er vigtigt af opklare forbrydelser hurtigt af hensyn til ofrene.

Derfor bør politiet have mulighed for at bruge AGT.

Det forekommer rimeligt, at det er vigtigt at opklare en forbrydelse så hurtigt som muligt, først og fremmest af hensyn til ofrene, som kan have brug for en hurtig opklaring for at komme videre ovenpå forbrydelsen.

Begrundelsens styrke afhænger, ligesom for de forrige begrundelser, dels af hvor stor en forskel det faktisk gør for politiets arbejde at bruge ansigts-

genkendelse, og dels af hvor stor en forskel det gør for ofrene, at forbrydelser opklares hurtigt. Antageligt vil nogle måder at bruge ansigtsgenkendelse gøre en større forskel end andre, men det har ikke været muligt at finde studier af, hvilken forskel brug af ansigtsgenkendelse gør for hvor hurtigt politi kan opklare forbrydelser. Samtidig er det værd at holde sig for øje, at begrundelsen alt andet lige nok hviler på et svagere hensyn end visse af de andre begrundelser. Uanset at det kan være vigtigt, at hjælpe ofre med hurtigere at få opklaret forbrydelser, så vil det antageligt være mere væsentligt for eksempel at forhindre forbrydelser.

Politiets brug af ansigtsgenkendelse vil hjælpe med at finde eftersøgte

En femte begrundelse kan være, at politiets brug af ansigtsgenkendelse vil kunne hjælpe med at finde eftersøgte. Eftersøgte kan være mistænkte i en sag, men de kan også være eksempelvis ofre og vidner. I disse tilfælde tjener eftersøgningen til at opklare eller forhindre en forbrydelse. En eftersøgt kan også være en forsvunden person, som har brug for hjælp, selvom de ikke

Eftersøgning

Politiets brug af AGT vil hjælpe politiet med at finde eftersøgte.

Det er vigtigt af finde eftersøgte, enten for at opklare og forhindre forbrydelser, eller for at hjælpe den eftersøgte.

Derfor bør politiet have mulighed for at bruge AGT.

nødvendigt har været offer for en forbrydelse, eksempelvis mindre børn eller demente ældre. I disse tilfælde tjener eftersøgning til at hjælpe den forsvundne.

I begge typer sager virker det plausibelt at ansigtsgenkendelse kan hjælpe politiet. I nogle tilfælde vil ansigtsgenkendelse gøre det muligt at finde eftersøgte, som man ellers ikke ville have fundet. I andre tilfælde vil ansigtsgenkendelse hjælpe med hurtigt at finde eftersøgte, som man ellers ville have fundet for sent, for eksempel efter at en eftersøgt mistænkt har begået en forbrydelse, eller efter at en forsvunden er kommet til skade.

Det virker også oplagt, at det er vigtigt at politiet kan finde eftersøgte, uanset om det tjener til at opklare og forhindre forbrydelser, eller til at hjælpe en forsvunden. Spørgsmålet er derfor hvor stærk begrundelsen er? Dette afhænger først og fremmest af hvor stor en forskel brug af ansigtsgenkendelse vil gøre. Hvor mange flere forbrydelser kan opklares og forhindres? Hvor mange flere forsvundne, som ellers ikke ville være blevet fundet i tide, kan hjælpes? I begge tilfælde er det vigtigt at vurdere hvilken forskel brug af ansigtsgenkendelse gør sammenlignet med alternativet. Ligesom for begrundelsen, at brug af ansigtsgenkendelse vil føre til opklaring af flere forbrydelser, kan forskellen i nogle tilfælde være beskeden, eksempelvis hvis alternativet er, at mennesker ser det samme billedmateriale grundigt igennem. I så fald kan brug af ansigtsgenkendelse først og fremmest have den fordel, at det sparer menneskelige ressourcer. Men i visse tilfælde vil det være afgørende at foretage en eftersøgning hurtigt på en måde som ofte er vanskelig for mennesker men let for en kunstig intelligens. I sådanne tilfælde vil brug af ansigtsgenkendelse lettere kunne gøre en forskel for ikke blot brugen af menneskelige ressourcer, men også for om eftersøgningen lykkes eller ej.

Politiets brug af ansigtsgenkendelse vil ikke være et problem, hvis man ikke har noget at skjule

Den sjette og sidste begrundelse for at lade politiet bruge ansigtsgenkendelse er, at politiets brug af ansigtsgenkendelse ikke vil være et problem, hvis man ikke har noget at skjule. Variationer af denne begrundelse dukker ofte op i debatter om overvågning og privatliv. Ideen er at personer, som bliver mål for ansigtsgenkendelse, groft sagt kan deles i to grupper: lovlige borgere og "personer som har noget at skjule". Ansigtsgenkendelse er ikke et problem for gruppen af lovlige

Ikke noget at skjule

Politiets brug af AGT er ikke et problem, hvis man ikke har noget at skjule.

Hvis man får et problem, fordi man har noget at skjule for politiet, så er man selv ude om det.

Derfor bør politiet have mulighed for at bruge AGT.

borgere, fordi de netop ikke har noget at skjule. Selv hvis personer fra denne gruppe mister privatliv ved at politiet bruger ansigtsgenkendelse, så udgør dette ifølge argumentet ikke et dataetisk problem, fordi dette tab af privatliv ikke får negative konsekvenser for borgeren.

Det samme kan naturligvis ikke siges om den anden gruppe. Politiets brug af ansigtsgenkendelse vil i en vis forstand udgøre et problem for de personer som "har noget at skjule". I deres tilfælde kan tab af privatliv have alvorlige negative konsekvenser i form af retsforfølgelse og straf. Men, hævder argumentet, vi bør ikke tage hensyn til disse personers behov for at undgå sådanne negative konsekvenser. Tværtimod. Personer som handler på en måde, som kan få politiet til at reagere, er ansvarlige for at have bragt sig i denne situation, og vi har gode grunde til at bruge ansigtsgenkendelse, hvis det kan hjælpe med at afsløre dem (jf. begrundelsen om at ansigtsgenkendelse vil føre til opklaring af flere forbrydelser).

Der kan være flere grunde til at være skeptisk over for argumentet.⁵¹ For det første fordi udtrykket, at man "ikke har noget at skjule" er tvetydigt. I en snæver forstand er det kun personer, som har begået en forbrydelse, som har noget at skjule for politiet. I denne forstand er gruppen af personer, som "har noget at skjule" meget lille. Men det "at have noget at skjule" kan også forstås bredere. Det kan ganske enkelt betyde, at der er personlige informationer, som man har grunde til ikke at dele med andre, herunder politiet. Der kan være mange grunde til, at en person har det sådan. Det kan for eksempel være, at det vil føles pinligt at dele disse informationer med andre, eller at det ganske enkelt er ubehageligt at føle sig overvåget.⁵²

For det andet synes argumentet at forudsætte, at der ikke findes begrundelser for at beskytte personers privatliv, som også gælder for personer som har noget at skjule. Men det er ikke givet, at vi kan tilsidesætte dataetiske hensyn til privatliv, alene fordi en person har noget at skjule. De legitime grunde vi har til at beskytte privatliv kunne også gøre sig gældende for personer som i en eller anden henseende har noget at skjule, helt oplagt når det vil være ydmygende eller ubehageligt at dele personlige informationer, som ikke er relevante for det kriminelle forhold politiet har god grund til at efterforske. I sådanne tilfælde virker det mere rimeligt at mene, at man må afveje hensynet til at efterforske en forbrydelse mod de negative konsekvenser tab af privatliv kan have for den pågældende.

⁵¹ For en generel kritik, se: Solove 2007.

⁵² Se også Dataetisk Råds etiksplainer [Dataetik og privatliv](#).

Samlet set er det tvivlsomt om det er rigtigt, at brug af ansigtsgenkendelse ikke er et problem, hvis man ikke har noget at skjule. Selv hvis det er korrekt, at man ikke bliver retsforfulgt hvis man ikke har handlet ulovligt, så kan det have negative konsekvenser at miste privatliv, også når man er lovlydig. Og det er tvivlsomt, at det ikke kan være et problem at bruge ansigtsgenkendelse på personer, som har handlet ulovligt, fordi der kan være dataetiske grunde til at beskytte også deres privatliv.

Argumenter for politiets brug af ansigtsgenkendelse

Der findes en række begrundelser for, at lade politiet bruge ansigtsgenkendelse. Mange begrundelser er plausible, fordi ansigtsgenkendelse kan tjene vigtige formål, som at beskytte og hjælpe borgere. Men begrundelserne kan være stærkere eller svagere.

Begrundelsernes styrke må vurderes i hvert enkelt brugsscenarie, ved at kigge på hvilken forskel det konkret vil gøre for politiets arbejde, at bruge ansigtsgenkendelse.

Der findes fortsat meget lidt viden om hvilken effekt brug af ansigtsgenkendelse kan forventes at have i forskellige brugsscenarier. De gavnlige effekter af at bruge ansigtsgenkendelse er derfor behæftet med stor usikkerhed.

I nogle tilfælde vil den direkte effekt være beskeden, hvis alternativet er at mennesker udfører den samme opgave. I sådanne tilfælde er den primære begrundelse for at bruge ansigtsgenkendelse, at man derved frigiver menneskelige ressourcer, som kan bruges til at løse andre opgaver.

Argumentet, at ansigtsgenkendelse kan frigive ressourcer, må tilsvarende vurderes for hvert brugsscenarie. Det spiller i den forbindelse en rolle både hvor mange ressourcer som frigives, og hvor meget gavn det i praksis gør, at frigive disse ressourcer.

4.2. Seks argumenter mod ansigtsgenkendelse

"Det er problematisk, at man vil give politiet lov at bruge en indgribende efterforskningsmetode, uden at en uafhængig myndighed skal indover for at tage stilling."

Birgitte Eiriksson, Direktør i Justitia

"Folk kan begynde at ændre deres adfærd for at undgå at tiltrække sig opmærksomhed, selv hvis de ikke er i gang med en kriminel handling."

Thaddeus Johnson

"Ansigtsgenkendelse er et indgreb af så vidtgående karakter, at det er på linje med andre indgreb, der normalt forudsætter domstolenes indblanding."

Mikael Sjöberg, Formand for Dommerforeningen

Kritikere kan fremføre en række forskellige argumenter imod at lade politiet bruge ansigtsgenkendelse. I dette afsnit kigger vi på seks af de mest almindelige indvendinger:

- **Politiets brug** af ansigtsgenkendelse vil være fejlbehæftet
- **Politiets brug** af ansigtsgenkendelse vil have bias
- **Politiets brug** af ansigtsgenkendelse vil afskrække uskyldig adfærd
- **Politiets brug** af ansigtsgenkendelse vil reducere borgeres privatliv
- **Politiets brug** af ansigtsgenkendelse vil kunne misbruges
- **Politiets brug** af ansigtsgenkendelse vil føre til en uetisk glidebane

Politiets brug af ansigtsgenkendelse vil være fejlbehæftet

En første indvending mod politiets brug af ansigtsgenkendelse er, at teknologien vil lave fejl. Selvom der er gjort store tekniske fremskridt med ansigtsgenkendelse det seneste årti, så vil teknologien ind imellem ikke genkende eller fejlidentificere en person. Det er vigtigt at undgå sådanne fejl, hævder argumentet videre, fordi de kan have alvorlige konsekvenser.

Fejl

Politiets brug af AGT vil være fejlbehæftet.

Det er vigtigt, at politiet ikke begår disse fejl, fordi de kan have alvorlige konsekvenser.

Derfor bør politiet ikke bruge AGT.

Ingen teknologier er fejlfri, og det er derfor korrekt, at ansigtsgenkendelse uundgåeligt vil begå fejl, når politiet bruger teknologien.

Falsk negativ fejl

Et billede og en reference forestiller den samme person, men identificeres som to forskellige personer.

Falsk positiv fejl

Et billede og en reference forestiller forskellige personer, men identificeres som den samme person.

Det er også troværdigt, at det er vigtigt at undgå fejl, fordi de kan have alvorlige negative konsekvenser, om end alvoren vil afhænge af brugsscenarioet. Ansigtsgenkendelse kan lave **falsk negative fejl**, hvor den overser, at to billeder forestiller den samme person. Det kan for eksempel betyde, at automatisk paskontrol nægter adgang til en rejsende med gyldigt pas, men det kan også betyde, at politiet ikke finder en eftersøgt, som man kunne have fundet. Ansigtsgenkendelse kan også lave

falsk positive fejl, hvor den kunstige intelligens vurderer, at billeder af to forskellige personer forestiller den samme person. Det kan for eksempel betyde, at automatisk paskontrol giver adgang til en rejsende med ugyldigt pas, men det kan også føre til, at politiet igangsætter en aktion, eksempelvis en anholdelse, mod en uskyldig person. I de fleste tilfælde vil det være ubehageligt, at være genstand for en sådan aktion. I nogle situationer kan det udgøre en alvorlig risiko, for eksempel fordi den egentligt eftersøgte er farlig, og politiet anvender magt ved anholdelsen.

Spørgsmålet er, hvor stærk indvendingen er. Det afhænger dels af hvor alvorlige konsekvenserne af fejl er i det konkrete brugsscenarie. Men det afhænger også hvor mange fejl ansigtsgenkendelse laver, og hvor mange fejl alternativer vil føre til. Det er derfor helt afgørende, at vurdere hvor godt teknologien virker.

For at vurdere kvaliteten af ansigtsgenkendelse kan man udføre systematiske tests. En sådan test foregår i grove træk ved, at man laver to store datasæt med billeder af personer: et testsæt, med billeder af personer som systemet skal forsøge at identificere, og et referencesæt, som indeholder billeder af nogle af de personer, som optræder i testsættet, og billeder af personer, som ikke optræder i testsættet. Derpå får man systemet til at forsøge at identificere alle personer i testsættet, og måler hvor mange falsk positive og falsk negative fejl systemet begår.

I slutningen af 2022 udførte det britiske National Physical Laboratory (NPL) en omfattende test af den ansigtsgenkendelse, som britisk politi anvender.⁵³ Testen forsøgte at identificere 405 testpersoner i forskellige scenarier ved at sammenligne med referencedatabaser bestående af 1000, 10.000 og 178.000 billeder. I visse scenarier genkendte ansigtsgenkendelse alle testpersoner, og begik således ikke en eneste fejl. I det mest udfordrende scenarie, hvor ansigtsgenkendelse skulle genkende personer i (simuleret) real-tidsvideo, havde ansigtsgenkendelse en sand positiv rate på 89%, og en falsk positiv rate på 0.002–0.017%. Det vil sige, at ansigtsgenkendelse overså personer, som den burde genkende, i 11% af tests, og fejlidentificerede en person i mellem en ud af 5000 og en ud af 60.000 tests.

Det er værd at bemærke, at NPLs scenarier testede ansigtsgenkendelses "positiv rate", og blandt andet derfor indeholdt datasættene ikke billeder af testpersoner, som *ikke* optrådte i referencedatabasen.⁵⁴ Kritikere har fremført, at testen ikke giver et retvisende indtryk af, hvor mange falsk positive fejl systemet begår i praksis, og pegede i 2023 på, at cirka 85% af de positive identifikationer som Engelsk politi havde fået ved at bruge ansigtsgenkendelse var falsk positive (150 ud af 175 "matches").⁵⁵ Til dette kunne man indvende, at det er falsk positivraten som faktisk er udtryk for den risiko den enkelte borger løber for at blive fejlidentificeret når teknologien anvendes, mens andelen af falsk positive i gruppen som identificeres positivt primært er udtryk for hvor mange ressourcer politiet skal bruge på at verificere resultatet. Endelig er det værd at nævne, at det engelske Metropolitan Police i sin seneste årsrapport for brugen af ansigtsgenkendelse til eftersøgning i realtid oplyser, at systemet fra september 2024 til september 2025 blev anvendt 207 gange, scannede ca. 3.1 millioner ansigter, og slog alarm 2077 gange, hvoraf 10 tilfælde viste sig at

⁵³ Mansfield 2023.

⁵⁴ Sand positive rate defineres som antallet af falsk positive resultater delt med det samlede antal negative resultater.

⁵⁵ Se: Big Brother Watch 2023. Organisationen karakteriserer misvisende denne målestok som falsk positivraten, men der er egentlig tale om såkaldt "false discovery rate", idet falsk positiv rate er defineret som $FP / (FP + TN)$ og false discovery rate som $FP / (FP + TP)$, hvor FP er falsk positive, TN sande negative og TP sande positive.

være en falsk positiv fejl. Det giver en falsk positiv rate på ca. 0,0003%, og en "false discovery rate" på ca. 0,5%.⁵⁶

Et andet sæt tests udføres løbende af det US amerikanske National Institute for Standards and Technology (NIST).⁵⁷ I testen indstilles ansigtsgenkendelse groft sagt så den laver falsk positive fejl i 0.3% af anvendelser, og NIST måler antallet af falsk negative fejl.⁵⁸ I 2025 laver de bedste systemer i NISTs tests falsk negative fejl i 0.07–0.17% af tests, når det anvendes på billeder af høj kvalitet, og i 4–6% af test når billederne har lavere kvalitet.⁵⁹

Sådanne test viser først og fremmest hvor mange fejl ansigtsgenkendelse laver i de særlige scenarier, som testes. Man kan derfor ikke slutte direkte fra testresultaterne til hvad fejlraten vil være, hvis dansk politi bruger ansigtsgenkendelse. Ikke desto mindre giver tests en indikation af, hvor godt man realistisk kan forvente at ansigtsgenkendelse vil virke.

For at vurdere, hvor stærk indvendingen er, er det ikke tilstrækkeligt at anslå hvor mange fejl ansigtsgenkendelse vil lave. Det centrale dataetiske spørgsmål er, hvor høj kvaliteten skal være, for at det er dataetisk forsvarligt at anvende systemet. Svaret afhænger som tidligere nævnt af, hvilke konsekvenser forskellige fejl vil have. Disse konsekvenser kan variere på tværs af brugsscenarier. Den dataetisk acceptable fejlrate må derfor vurderes for det enkelte brugsscenarie.

Uanset hvor mange fejl ansigtsgenkendelse begår, er det også relevant at sammenligne dette med, hvor mange fejl der begås, hvis politiet ikke anvender ansigtsgenkendelse. Selv hvis ansigtsgenkendelse laver mange fejl, så er indvendingen ikke overbevisende, hvis alternativet er, at man laver endnu flere fejl når man *ikke* bruger ansigtsgenkendelse. I en sådan situation får man flere af de negative konsekvenser, som indvendingen drejer sig om, hvis man ikke bruger ansigtsgenkendelse. Indvendingens styrke afhænger i sidste ende af, hvor mange *flere* fejl det fører til, når politiet bruger ansigtsgenkendelse.

⁵⁶ Se Metropolitan Police 2025.

⁵⁷ Se: <https://pages.nist.gov/frvt/html/frvtIN.html>

⁵⁸ AI-systemer til klassificering anvender beslutningstærskler, Beslutningstærsklen afgør hvordan balancen er mellem de to typer fejl. Sættes tærsklen højt vil systemet lave flere af den ene type fejl og færre af den anden; sættes tærsklen lavt vil systemet omvendt lave færre af den første type fejl og flere af den anden. For at standardisere testen kalibrerer NIST AGT således, at alle de testede systemer har samme falsk positiv fejlrater. Falsk positiv raten indstilles konkret ved at teste systemet på billeder, som ikke har en reference, og justere systemets beslutningstærskel indtil det i 0.3% af tilfældene fejlagtigt identificerer en sådan person som et medlem af referencesættet.

⁵⁹ I det første tilfælde består begge sæt af "mugshots", dvs. billeder som tages af politiet når de anholder en mistænkt. I det andet tilfælde består referencesættet af billeder fra visum-ansøgninger og testsættet af billeder fra kioskameraer.

Politiets brug af ansigtsgenkendelse vil have bias

En anden almindelig indvending er, at politiets brug af ansigtsgenkendelse vil have bias. Det er vigtigt, at politiets værktøjer ikke har sådanne bias, hævder indvendingen, fordi det vil føre til, at politiet negativt forskelsbehandler sårbare minoriteter.

Hvad betyder det, at ansigtsgenkendelse har bias? Bias i ansigtsgenkendelse er et eksempel på såkaldt "algoritmisk bias".

Algoritmisk bias betyder, lidt forenklet, at

en algoritme virker bedre for nogle grupper og dårligere for andre grupper.⁶⁰ Algoritmisk bias i ansigtsgenkendelse har været intenst diskuteret det seneste årti, fordi en lang række tests har vist, at ansigtsgenkendelse typisk virker bedre for visse grupper og ringere for andre grupper.⁶¹ Ansigtsgenkendelse kan for eksempel være bedre til at identificere mænd end kvinder, bedre til at identificere ældre end yngre, eller bedre til at identificere personer med lys hud end personer med mørk hud.

Indvendingen rejser to centrale spørgsmål. For det første: hvor meget bias vil ansigtsgenkendelse have for forskellige grupper, hvis dansk politi anvender det? Argumentet er alt andet lige en stærkere indvending, hvis ansigtsgenkendelse har meget bias, mens det er en svagere indvending, hvis ansigtsgenkendelse har mindre bias. For det andet, vil bias føre til dataetisk problematisk negativ forskelsbehandling?

Dansk politi har ikke offentliggjort test af de ansigtsgenkendelses-systemer politiet anvender, men der findes internationale test af bias i ansigtsgenkendelse, som kan give en indikation af, hvor meget bias man kan forvente. Både den britiske test fra National Physics Laboratory og de amerikanske NIST tests har undersøgt bias i ansigtsgenkendelse.

Den britiske test viste en statistisk signifikant forskel i falsk negative fejl for forskellige aldersgrupper, idet ansigtsgenkendelse virkede bedre for ældre personer (over 42 år) og dårligere for yngre personer. Der var også forskelle i antallet af falsk negative på tværs af køn og etnicitet, således at ansigtsgenkendelse virkede bedre for mænd

Bias

Politiets brug af AGT vil have bias.

Det er vigtigt at politiets værktøjer ikke har bias, fordi dette vil føre til negativ forskelsbehandling af sårbare minoriteter.

Derfor bør politiet ikke bruge AGT.

⁶⁰ For overblik over diskussionen af algoritmisk bias, se: Fazelpour & Danks 2021. Carey & Wu 2023.

⁶¹ Khalil, et al. 2020; Yucer, et al. 2024.

end for kvinder, og bedre for "hvide" end for "sorte", men disse forskelle var ikke statistisk signifikante. På samme vis lavede ansigtsgenkendelse i testen flere falsk positive fejl for mænd, "sorte", og yngre, men disse forskelle var kun statistisk signifikante, når ansigtsgenkendelse blev indstillet således, at den lavede usædvanligt mange falsk positive fejl. Samlet set indikerede testen, at ansigtsgenkendelse havde visse bias, men at de for de fleste grupper var så svage, at det er vanskeligt at vurdere, hvor stor effekten er.

NIST tester bias i 1:1 genkendelse på store datasæt.⁶² En måde at vurdere bias, er at se på hvor mange falsk positive fejl et ansigtsgenkendelses-system laver for den demografiske gruppe, hvor det klarer sig bedst, og sammenligne med antallet af falsk positive fejl for den demografiske gruppe, hvor det klarer sig dårligst. NISTs tests opdateres løbende, men i 2025 lavede de 20 ansigtsgenkendelse-systemer, som overordnet klarede sig bedst i NISTs tests, cirka 0.5-2% flere falske positive fejl. Et system kan for eksempel lave falsk positive fejl i 0.006% af tests med Østeuropæiske mænd, og 2.15% af tests med Vestafrikanske kvinder. Forskellen er mindre i NISTs test af falsk negative fejl. De bedste ansigtsgenkendelses-systemer laver fejl i cirka 0.05% flere tests for de demografiske grupper, hvor de klarer sig dårligst. Et system laver for eksempel falsk negative fejl i 0.11% af tests for Centralamerikanske personer og 0.16% af tests for Sydasiatiske personer.⁶³

Det næste spørgsmål er, hvornår bias fører til dataetisk problematisk forskelsbehandling af en gruppe. Der har det seneste årti været en intens diskussion af dette spørgsmål.⁶⁴ Ét muligt synspunkt er, at en hvilken som helst form for bias i ansigtsgenkendelse i sig selv udgør dataetisk problematisk forskelsbehandling. Dette synspunkt møder imidlertid en række udfordringer. For det første, at det typisk er matematisk umuligt at få en algoritme til at virke lige godt for alle grupper i alle henseender.⁶⁵ For det andet, at det er nødvendigt at definere de relevante grupper, og forklare hvorfor det er bias mod netop disse grupper, som ansigtsgenkendelse skal undgå. For det tredje at det kan virke tvivlsomt, at bias er uetisk forskelsbehandling af personer fra en gruppe, hvis det ikke har negative konsekvenser for de pågældende. Hvis eksempelvis ansigtsgenkendelse har vanskeligt ved at identificere eftersøgte kriminelle fra en bestemt gruppe, stiller dette i udgangspunktet kriminelle fra denne gruppe *bedre*.

62 Se https://pages.nist.gov/frvt/html/frvt_demographics.html

63 For begge typer tests kalibreres AGT-systemerne til at have en ensartet overordnet præcision, således at testresultaterne kan sammenlignes.

64 For et delvist overblik, se Fazelpour & Danks 2021.

65 Kleinberg, et al. 2016; Chouldechova 2017; Lipton, et al. 2018.

For det fjerde, at synspunktet betyder, at det kan være dataetisk, at træne ansigtsgenkendelse til at fungere dårligere for nogle grupper, selv hvis dette ikke får det til at virke bedre for andre grupper.⁶⁶

Et andet muligt synspunkt er, at bias er dataetisk problematisk, når det har negative konsekvenser for en gruppe. Nogle grupper kan være særligt relevante, fordi de er sårbare minoriteter, som bliver negativt påvirket af bias på en måde, som andre grupper ikke bliver. Hvis man accepterer dette synspunkt, så afhænger indvendingen ikke blot af om ansigtsgenkendelse har bias, men også af hvad konsekvenserne af denne bias er. For at vurdere hvor stærk indvendingen er, vil det derfor ifølge denne forståelse være nødvendigt at afklare både bias og eventuelle negative konsekvenser af bias.

Ligesom for indvendingen at ansigtsgenkendelse vil begå fejl, må en samlet vurdering af indvendingen, at ansigtsgenkendelse har bias, derfor afhænge af både hvor meget bias ansigtsgenkendelse har i det konkrete brugsscenarie, og hvilke negative konsekvenser dette bias har for berørte personer. Og ligesom ved fejl kan det være relevant at sammenligne med, hvor meget og hvilke bias som findes hvis ansigtsgenkendelse ikke anvendes, ganske enkelt fordi også mennesker kan have kognitive og affektive bias.

Politiets brug af ansigtsgenkendelse vil afskrække uskyldig adfærd

En tredje mulig indvending er, at politiets brug af ansigtsgenkendelse vil have en uønsket afskrækkende effekt. Et centralt argument for brug af ansigtsgenkendelse er, at det kan afskrække potentielle kriminelle fra at begå forbrydelser. Indvendingen hævder, at brug af ansigtsgenkendelse også vil afskrække uskyldig adfærd. Det kaldes ofte at overvågning har en "afkølende" effekt (eng. "chilling").

Afkøling

Politiets brug af AGT vil afskrække uskyldig adfærd.

Det er vigtigt at politiets ikke afskrækker uskyldig adfærd, fordi dette begrænser borgernes frihed og sociale goder.

Derfor bør politiet ikke bruge AGT.

Det er vigtigt ikke at afskrække uskyldig adfærd, kan indvendingen hævde, både for at give borgerne frihed til at udfolde deres liv, og fordi sådan adfærd kan skabe livskvalitet og socialt gavnlige konsekvenser.

⁶⁶ Mittelstadt, et al. 2023.

Det kan umiddelbart virke troværdigt, at øget overvågning kan påvirke adfærd. Det virker også rimeligt at det kan være vigtigt, ikke at begrænse uskyldige former for adfærd. Indvendingens styrke afhænger imidlertid af hvor stor den afskrækkende effekt er, hvilken adfærd den påvirker, og hvor vigtigt det er at undgå, at afskrække denne adfærd.

Den såkaldte afkølede effekt af overvågning er blevet studeret i flere årtier.⁶⁷ Der er næppe tvivl om at overvågning i kombination med trusler om sanktioner kan påvirke adfærd.⁶⁸ Det er imidlertid vanskeligt at måle præcis hvilke adfærdseffekter overvågning har, især i de tilfælde hvor den ikke kombineres med en konkret trussel om sanktioner, både fordi det kan være vanskeligt at måle den relevante adfærd, og fordi det kan være svært at vurdere, hvordan adfærden ville have set ud uden overvågning. De mest kendte studier fokuserer på personers holdninger snarere end adfærd, eller på begrænsede adfærdseffekter; nogle studier viser at selv når der er effekter, så kan de aftage over tid.⁶⁹ Det er således i almindelighed vanskeligt både at vurdere hvor stor den afkølede effekt er for forskellige typer overvågning, og vise at den faktisk findes for en given type overvågning.⁷⁰

Det har ikke været muligt at identificere studier af om politiets brug af ansigtsgenkendelse kan have en selvstændig afkølede effekt. Vurderinger af ansigtsgenkendelses afkølede effekt er derfor nødvendigvis spekulative. Offentlighedens holdning til ansigtsgenkendelse kan imidlertid tænkes at give en vis indikation, fordi den afkølede effekt antageligt vil være større, jo mere bekymrende almindelige borgere mener, at politiets brug af ansigtsgenkendelse er. Denne holdning findes der både danske og internationale studier af.

I England har Ada Lovelace Institute gennemført undersøgelser i 2019, 2023, og 2025 om holdninger til AI, som også inkluderer spørgsmål om politiets brug af ansigtsgenkendelse.⁷¹ Storbritannien er særligt interessant i denne sammenhæng, fordi britisk politi har været blandt de første i Europa til at bruge ansigtsgenkendelse.

67 Penney 2016; Penney 2017; Stoycheff, et al. 2019; Büchi, et al. 2022.

68 Dette var kernen i den europæiske menneskerettighedsdomstols dom i Glukhin v. Russia, hvor anvendelsen af ansigtsgenkendelse på politiske demonstrationer kombineret med anholdelser og fængselsstraffe af domstolen formodedes at udgøre en så markant trussel, at det krænkede centrale demokratiske og politiske rettigheder. Se European Court of Human Rights 2023.

69 En gruppe studier fokuserer på adfærdsendringer og holdninger i kølvandet på Edward Snowdens afsløringer i 2013 af amerikanske efterretningstjenesters systematiske overvågning af borgere i vestlige lande. Et studie viser eksempelvis et dyk i internettrafik til hjemmesider relateret til terrorisme (e.g. Wikipedia artikler om terrorgrupper), men også at trafikken til sådanne sider på relativt kort tid kan vende tilbage til det forhenværende niveau. Se: Penney 2016.

70 For et overblik over udfordringerne med at dokumentere en afkølede effekt, se: Büchi, et al. 2022. For et kritisk studie af den afkølede effekt, se: Bedi 2021.

71 Ada Lovelace Institute 2019. Tallene i dette afsnit er trukket fra det fulde datasæt på: <https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Ada-Lovelace-Institute-Beyond-face-value-survey-results-for-publication-FINAL.xlsx> Modhvadia, et al. 2023; Modhvadia, et al. 2025.

I undersøgelsen fra 2019 bliver deltagerne bedt om at indikerer hvor "komfortable" de er med, at politiet anvender ansigtsgenkendelse på en skala fra 1-10, hvor 1 indikerer "overhovedet ikke komfortabel" og 10 "meget komfortabel".

"Hvor komfortabel er du med, at politiet anvender ansigtsgenkendelse?" (2019)

1	2	3	4	5	6	7	8	9	10
9%	2%	4%	4%	10%	9%	14%	16%	7%	21%
15%			37%				44%		

Undersøgelsen spurgte også om deltagerne var enige eller uenige i mere konkrete spørgsmål om politiets brug af ansigtsgenkendelse, blandt andet om "politiet bør kunne bruge ansigtsgenkendelse på menneskemængder og i det offentlige rum, hvis det hjælper med at reducere kriminalitet?"

"Politiet bør kunne bruge ansigtsgenkendelse på menneskemængder og i det offentlige rum, hvis det hjælper med at reducere kriminalitet." (2019)

Stærkt uenig	Lidt uenig	Hverken eller	Lidt enig	Stærkt enig
8%	8%	9%	32%	38%

I Ada Lovelace Instituttets nyere undersøgelser fra 2023 og 2025 blev deltagerne spurgt om hvilke af 17 forskellige AI systemer de oplevede som henholdsvis gavnlige og bekymrende. Politiets brug af ansigtsgenkendelse blev vurderet som det tredje mest gavnlige, næst efter AI til kræftdiagnoser og ansigtsgenkendelse til grænsekontrol, og det 11. mest bekymrende, nogenlunde på niveau med brug af ansigtsgenkendelse til at låse op for en mobiltelefon.

"I hvilken udstrækning tror du, at politiets brug af ansigtsgenkendelse vil være gavnlig?" (2023 / 2025)

Overhovedet ikke	Ikke særligt	Rimeligt	Meget
3% / 2%	4% / 4%	41% / 42%	45% / 49%

"I hvilken udstrækning er du bekymret for politiets brug af ansigtsgenkendelse?" (2023 / 2025)

Meget	Rimeligt	Ikke særligt	Overhovedet ikke
8% / 7%	26% / 32%	37% / 40%	25% / 19%

I Danmark har Algoritmer, Data og Demokrati-projektet undersøgt danske borgeres holdninger til ansigtsgenkendelse i befolkningsundersøgelser i 2021 og 2023.

I den første undersøgelse besvarede deltagerne spørgsmål om deres holdning til ansigtsgenkendelse kvalitativt.⁷² Besvarelsene viste stor spredning fra meget positive til moderat negative, men undersøgelsen kan ikke kvantificere hvordan svarene fordeler sig. I den nyere undersøgelse fra 2023 benyttede undersøgelsen en 7-trinsskala fra meget negativt stemt (1) til meget positivt stemt (7).⁷³

"Hvordan ser du på ansigtsgenkendelsesteknologi fx til at åbne din smartphone eller MitID?"

1	2	3	4	5	6	7
4%	6%	7%	13%	18%	17%	28%

Undersøgelserne synes at vise, at et stort flertal er positivt stemte og relativt ubekymrede ved ansigtsgenkendelse, i de britiske undersøgelser også ved specifikt politiets brug af ansigtsgenkendelse. Ikke desto mindre findes der et mindretal, som oplever ansigtsgenkendelse som bekymrende og ukomfortabel, og som i de britiske undersøgelser ikke ønsker, at politiet skal have mulighed at bruge ansigtsgenkendelse i det offentlige rum. Hvis man tentativt vil slutte fra sådanne undersøgelser af borgernes holdninger, kunne man således antage, at der vil forekomme en afkølende effekt for en mindre gruppe borgere. Præcis hvilken type afkølende effekt, og hvor stor den vil være, er imidlertid usikkert.

Det næste spørgsmål er, hvor vigtigt det er, at undgå en afkølende effekt. Hvilken vægt bør vi give til det dataetiske hensyn om, ikke at afskrække uskyldig adfærd? To forhold

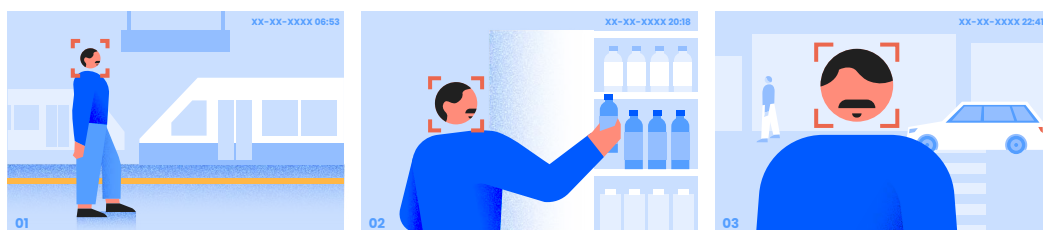
⁷² Se: <https://algoritmer.org/befolkningsundersoegelse/forside/2021-2/ansigtsgenkendelse/>

⁷³ Se: <https://algoritmer.org/befolkningsundersoegelse/forside/2023-2/nye-teknologier/> Undersøgelsen spurgte også en gruppe af digitalt udsatte borgere. Her er holdningerne mere delte, idet 32% er overvejende positive og 30% overvejende negative. For begge grupper fordeler de øvrige besvarelser sig på deltagere som er "neutrale", og deltagere som har svaret, at de ikke kender teknologien. Den sidste gruppe udgør 7% af spørgeskemadeltagere, og hele 29% af de digitalt udsatte deltagere.

kunne tænkes at påvirke dette spørgsmål. Dels hvilken adfærd der er tale om, og dels hvilken trussel politiets brug af ansigtsgenkendelse reelt udgør.

Det forekommer oplagt, at spørgsmålet kan afhænge af hvilken adfærd der er tale om. Det er alt andet lige vigtigere ikke at begrænse adfærd, som er en udøvelse af centrale demokratiske rettigheder, eller som er afgørende for personers livskvalitet, end det er ikke at begrænse adfærd, som er mindre vigtig for samfundet og den enkelte. For at vide hvilken vægt man skal give til indvendingen, må man derfor vurdere hvilken specifik adfærd den påvirker, og hvor vigtigt det er, at undgå at afskrække netop denne adfærd.

Man kan også forestille sig, at nogen vil have lyst til at skelne mellem adfærd som afskrækkes fordi ansigtsgenkendelse påfører personer en omkostning eller risiko, og adfærd som afskrækkes uden grund. Et ofte diskuteret eksempel på uskyldig adfærd, som ansigtsgenkendelse kunne risikere at afskrække, er borgernes deltagelse i lovlige demonstrationer. I nogle situationer gør politiets brug af ansigtsgenkendelse det mere risikabelt at deltage i en lovlig demonstration, og kan derved afskrække borgere fra at udøve deres demokratiske rettigheder og støtte social udvikling. Borgere i et land med et autoritært regime løber en betragtelig risiko ved at deltage i en demonstration. Hvis politiet bruger ansigtsgenkendelse til at identificere deltagere i demonstrationen, så stiger denne risiko. Borgere, som af den grund afskrækkes fra at deltage i en demonstration, reagerer rationelt på en reel stigning i truslen om sanktioner. Men man kan også forestille sig borgere i et liberalt samfund, som bliver afskrækket fra at deltage i en demonstration, fordi politiet bruger ansigtsgenkendelse, selvom politiet ikke anvender ansigtsgenkendelse til at identificere deltagere ved lovlige demonstrationer, og selvom staten ikke udøver repressalier mod borgere som deltager i demonstrationer. Politiets brug af ansigtsgenkendelse kan i teorien have afkølede effekter, som ikke er rationelle. I den situation kunne nogle mene, at de afkølede effekter ikke bør tale imod politiets brug af ansigtsgenkendelse, for eksempel med den begrundelse, at afskrækkelsen egentlig skyldes ubegrundet mistillid, som den enkelte selv er ansvarlig for. Hvis man indtager dette synspunkt er det nødvendigt at skelne mellem afkølede effekter som skyldes en øget risiko, og afkølede effekter som skyldes for eksempel misinformation.



Politiets brug af ansigtsgenkendelse vil reducere borgeres privatliv

En fjerde indvending er, at politiets brug af ansigtsgenkendelse vil reducere borgeres privatliv. Politiets brug af ansigtsgenkendelse kan medvirke til at indsamle, analysere og dele personlige informationer. Det virker oplagt, at dette kan reducere borgeres privatliv. Men det kan være værd at spørge præcis hvordan brug af ansigtsgenkendelse reducerer privatliv? Er der for eksempel nogle måder at bruge ansigtsgenkendelse, som i højere grad reducerer privatlivet end andre?

Privatliv

Politiets brug af AGT vil reducere borgeres privatliv.

Det er vigtigt at politiet ikke reducerer borgeres privatliv.

Derfor bør politiet ikke bruge AGT.

Indvendingen hævder videre, at det er vigtigt, at politiet ikke reducerer borgeres privatliv. Det vil mange nok umiddelbart opfatte som et troværdigt synspunkt. Man kan ikke desto mindre udfordre synspunktet ved at pege på, at vi i mange situationer accepterer, at politiet reducerer borgeres privatliv. Hvorfor, kunne en kritiker spørge, er det anderledes eller værre, at reducere en borgers privatliv ved at bruge ansigtsgenkendelse, end når politiet på andre måder får kendskab til personlige informationer?

For at vurdere hvor stærk indvendingen er, må man derfor forholde sig til både hvornår brug af ansigtsgenkendelse reducerer privatliv, og hvilke grunde vi har til at beskytte borgeres privatliv.

Man kan have forskellige syn på, hvad det vil sige at have privatliv.⁷⁴ Ét synspunkt kunne være, at en person mister privatliv alene ved, at ansigtsgenkendelse behandler et billede af personen. Hvis man har dette syn på privatliv, så reducerer al brug af ansigtsgenkendelse privatlivet for de personer, hvis billeder behandles. En udfordring for synspunktet kan være, at ansigtsgenkendelse kan behandle en persons billede, uden at nogen af den grund får kendskab til personlige informationer om vedkommende. Eksempelvis kan ansigtsgenkendelse bruges til eftersøgning, og sammenligne billeder af mange andre personer med et referencebillede af en eftersøgt, men vil blot konkludere, at de ikke er identiske med den eftersøgte. Det kan i dette tilfælde lyde underligt at sige, at de pågældende personer har mistet privatliv, selvom ansigtsgenkendelse ikke identificerer dem, og ingen får kendskab til personlige informationer om dem.

⁷⁴ Se Dataetisk Råds etiksplainer Dataetik og privatliv.

Et andet synspunkt kunne være, at brug af ansigtsgenkendelse først reducerer en persons privatliv, hvis politiet derved får kendskab til personlige informationer om personen. I så fald behøver personer ikke at miste privatliv alene fordi ansigtsgenkendelse behandler et billede af dem. Men mange af de måder politiet kan bruge ansigtsgenkendelse har til formål at hjælpe politiet med at få informationer om personer, for eksempel når ansigtsgenkendelse identificerer personer i billedmateriale. Derved kan politiet få kendskab til for eksempel hvor personer har opholdt sig, hvad de har foretaget sig, og hvem de omgås. Ifølge dette synspunkt fører brug af ansigtsgenkendelse i nogle situationer til tab af privatliv, om end kun for denne mere begrænsede gruppe personer.

Uanset hvilket synspunkt man anlægger på spørgsmålet om hvornår personer mister privatliv, er det værd at overveje hvorfor det er dataetisk problematisk, hvis politiets brug af ansigtsgenkendelse reducerer en persons privatliv. Én mulighed er at indtage det synspunkt, at ethvert tab af privatliv er dataetisk problematisk. Dette synspunkt møder imidlertid den udfordring, at der synes at være mange situationer, hvor personer mister privatliv, som ikke er etisk problematiske.⁷⁵ Hvis man skal forklare hvorfor privatliv er dataetisk vigtigt kunne man derfor i stedet pege på, at det kan være ubehageligt eller ydmygende, at andre får kendskab til personlige informationer, at det kan være stressende at føle sig overvåget, og bekymrende ikke at vide hvilke private informationer andre kan få kendskab til. Endvidere kan tab af privatliv gøre personer sårbare.⁷⁶ Et simpelt eksempel kunne være en borger i et land med et autoritært regime, som anonymt kritiserer regimet på sociale medier. I denne situation kan det udgøre en alvorlig risiko, hvis politiet får kendskab til systemkritikerens identitet.

Selvom der er dataetiske grunde til at beskytte privatlivet kunne man spørge, om politiets brug af ansigtsgenkendelse udgør en særlig udfordring? Politiet reducerer ofte på forskellig vis borgeres privatliv som del af almindeligt politiarbejde. Hvis eksempelvis politiet leder efter et vidne til en forbrydelse, baseret på et billede af vedkommende i nærheden af gerningsstedet, så kan man forsøge at identificere vidnet på flere måder. Man kan for eksempel vise billedet til lokale beboere og erhvervsdrivende i håb om, at en af disse kender vidnet og kan identificere personen. Man kunne også bruge ansigtsgenkendelse på en stor referencedatabase, i håb om at personen findes i databasen. I begge tilfælde vil succes betyde, at politiet får kendskab til vidnets identitet. Derved mister vedkommende privatliv. Det er imidlertid sjældent, at politiet

⁷⁵ Se eksempelvis Ryberg 2007; Doyle 2009.

⁷⁶ Se Citron & Solove 2022; Solove 2006.

kritiseres for at identificere vidner med konventionelle metoder, og det kan være vanskeligt at se, hvorfor den ene metode skulle være værre end den anden med hensyn til vidnets privatliv.

Et argument for, at politiets brug af ansigtsgenkendelse rejser særlige udfordringer for privatlivet kunne være, at brug af ansigtsgenkendelse vil gøre det langt nemmere at indsamle, analysere og dele personlige informationer. Konventionelle metoder til at identificere personer er ofte ressourcekrævende. Det begrænser naturligt reduktion af privatlivet til de relativt få situationer, hvor politiet har tungtvejende grunde til at identificere en person. Brug af ansigtsgenkendelse gør det principielt muligt for politiet at indsamle, analysere og dele personlige informationer i langt flere situationer, og derfor også i situationer hvor der ikke nødvendigvis er tungtvejende grunde til at reducere personers privatliv (se også indvendingen nedenfor om en dataetisk problematisk glidebane). I denne fortolkning er kernen i indvendingen, at ansigtsgenkendelse kan være dataetisk problematisk når (og hvis) det enten fører til mere omfattende tab af privatliv end konventionelt politiarbejde, eller når det fører til tab af privatliv med hensyn til personlige informationer, som vi har stærkere dataetiske grunde til at beskytte, for eksempel fordi deling af disse informationer gør personer sårbare.



Vi accepterer normalt, at politiet i nogle situationer har tilstrækkeligt gode grunde til at indsamle, analysere og dele personlige informationer til, at det er etisk acceptabelt, at reducere en persons privatliv. Omvendt mener vi typisk også, at der kunne være indgreb i privatlivet, som er så omfattende, eller så dårligt begrundede, at de ikke kan retfærdiggøres. Hvis man anlægger samme syn på hensynet til privatliv i denne sammenhæng, så må man afveje på den ene side de grunde vi har til at beskytte personers personlige informationer, og på den anden side de grunde politiet har til at behandle netop disse personlige informationer. En samlet vurdering af indvendingen forudsætter således, at man forholder sig til hvor meget privatliv personer mister ved at politiet anvender ansigtsgenkendelse i et konkret brugsscenarie, og hvordan dette tab af privatliv påvirker de berørte personer.

Politiets brug af ansigtsgenkendelse vil kunne misbruges

Den femte mulige indvending er, at politiets systemer til ansigtsgenkendelse vil kunne misbruges. Selv hvis politiets egentlige brug af ansigtsgenkendelse er dataetisk, hævder indvendingen, så vil sådanne systemer kunne misbruges på måder som er dataetisk problematiske.

Misbrug

Politiets brug af AGT vil åbne for misbrug af teknologien.

Det er vigtigt at AGT ikke misbruges.

Derfor bør politiet ikke bruge AGT.

Indvendingen kan på et overordnet niveau tænkes at dreje sig om tre forskellige typer misbrug. For det første den situation, hvor individuelle ansatte i politiet misbruger teknologien til private formål, for eksempel til at indsamle information om personer de kender privat, eller kendte personer som politikere, sportsstjerner, musikere og skuespillere.⁷⁷

For det andet den situation, hvor politiet gradvist kommer til at anvende ansigtsgenkendelse i stadigt større omfang, på en måde som ikke var intenderet, da man indførte teknologien. Det kaldes for funktionsskred (eng. "function creep").⁷⁸

⁷⁷ Der har i dansk sammenhæng bl.a. været eksempler på en polititjenestemand, som i 2019 modtog bødestraf for uberettigede opslag på sin ekskone og dennes nye partner i politiets registre, sundhedsfaglige medarbejdere, som i 2023 blev fyret for usaglige opslag i journalen for en 13-årig pige, der var offer for kidnapning, og en læge, som i 2023 blev dømt for godt 1200 ulovlige opslag i patientjournaler, herunder opslag i 14 forskellige kendte personers journaler. I en amerikansk sag fra staten Minnesota blev en kvindelig politibetjent i 2013 tildelt erstatning efter at 58 af hendes kollegaer over en periode på fire år havde foretaget usaglige opslag på hendes fødselsregisterinformationer. Se: Associated Press 2024; Redaktionen 2023a; Den Uafhængige Politiklagemyndighed 2019; Redaktionen 2023b.

⁷⁸ Se: Brey 2004. En anklage om sådant funktionsskred fremkom eksempelvis i 2017 i forbindelse med dansk politis anvendelse af nummerpladescannere. Se: Stræde & Andersen 2017.

For det tredje den situation, hvor danske myndigheder eller andre, for eksempel hackere eller fremmede efterretningstjenester, systematisk misbruger ansigtsgenkendelse til at indhente informationer på en dataetisk problematisk måde, for eksempel om aktivister, systemkritikere, oppositionspolitikere, eller journalister. Sådanne informationer kan misbruges til at afsløre samarbejdspartnere, arbejdsmetoder, strategier og personlige sårbarheder, som for eksempel kan udnyttes til miskreditering eller afpresning.⁷⁹

Hvorfor er det vigtigt at undgå de forskellige former for misbrug? Man kan forestille sig flere mulige forklaringer. For det første er misbrug per definition i modstrid med de regler, som sætter rammerne for brug af teknologien. Man kan mene, at det i sig selv er dataetisk problematisk at bruge en teknologi som ansigtsgenkendelse i modstrid med reglerne. Dertil kunne man indvende, at regler ikke er til for egen skyld, og at det snarere er de dataetiske hensyn, som motiverer reglerne, der forklarer hvorfor misbrug er dataetisk problematisk. Man kunne således også mene, at misbrug af ansigtsgenkendelse er dataetisk problematisk, når det for eksempel reducerer borgernes privatliv uden god grund, afskrækker uskyldig adfærd, gør personer sårbare, eller på anden måde har uetiske konsekvenser. Ifølge denne forklaring er risikoen for misbrug dataetisk relevant, når og fordi et sådant misbrug har negative konsekvenser.

For at vurdere hvor stærk indvendingen er, må man således både forholde sig til hvor stor risikoen er for forskellige typer misbrug i forskellige brugsscenarier, og hvor dataetisk problematisk forskellige typer misbrug vil være.

Politiets brug af ansigtsgenkendelse vil føre til en uetisk glidebane

Den sidste mulige indvending mod politiets brug af ansigtsgenkendelse er, at anvendelse vil føre til en uetisk glidebane. Argumentet hævder, at selv hvis der findes dataetisk acceptable måder at bruge teknologien, så vil konsekvensen af at tillade denne form for brug være en normalisering af teknologien. Denne normalisering vil føre til stadigt mere omfattende brug af ansigtsgenkendelse. Og

Glidebane

Politiets brug af AGT vil føre til en glidebane mod stadigt mere omfattende og/eller indgribende brug.

Det er vigtigt at undgå denne glidebane.

Derfor bør politiet ikke bruge AGT.

⁷⁹ Denne form for misbrug kendes bedst fra fiktionens spionfilm, men bekymringen er eksempelvis blevet fremført i dansk kontekst i forbindelse med danske myndigheders køb af kinesisk-producerede overvågningskameraer. Se: Kristensen & Yding 2021.

nogle af de måder, man vil ende med at bruge ansigtsgenkendelse, vil være dataetisk problematiske. Det kunne for eksempel være, at det var dataetisk uproblematisk, at lade politiet bruge ansigtsgenkendelse til automatiseret paskontrol i lufthavnen, men at denne brug på sigt førte til, at politiet brugte teknologien til systematisk overvågning af alle danske borgere i det offentlige rum.

Glidebaneargumenter betragtes ofte af flere grunde med en vis skepsis.⁸⁰ For det første, at det næsten altid er muligt at formulere et glidebaneargument, som hævder, at hvis man gør noget bestemt, så vil det føre til en glidebane mod katastrofale konsekvenser. Men det er ikke altid troværdigt, at der findes en glidebane. Datidens kritikere hævdede eksempelvis, at tildeling af stemmeret til kvinder ville føre til socialt sammenbrud, og at legalisering af homoseksuelle vielser ville føre til opløsning af kernefamilien. Begge dele har naturligvis vist sig at være faktisk forkerte, og de fleste vil nok i dag mene, at det allerede i datiden burde have været tydeligt, at konsekvenserne ikke ville forekomme. På lignende vis udgør det kun en god indvending, imod politiets brug af ansigtsgenkendelse i ét brugsscenarie, at dette vil føre til en glidebane mod meget problematiske anvendelser, hvis det faktisk er tilfældet, at den første anvendelse vil have disse konsekvenser.

Den første betingelse for et glidebaneargument er således, at de konsekvenser, argumentet peger på, faktisk er *sandsynlige*. Omvendt svækkes et glidebaneargument, jo vanskeligere det er at pege på solid evidens for, at de relevante konsekvenser faktisk vil indtræde. Når man skal vurdere indvendingen, er det første spørgsmål man bør stille derfor, hvordan det begrundes, at konsekvenserne vil følge af det første skridt?

Den anden konventionelle udfordring for glidebaneargumenter er, at glidebanen faktisk skal ende med konsekvenser, som det er etisk vigtigt at undgå. Historisk argumenterede kritikere eksempelvis, at kvinders stemmeret ville føre til kvindelige politikere og regeringsoverhoveder, og til at også andre minoriteter ville få bedre muligheder for at stemme. Selvom datidens kritikere øjensynligt betragtede disse mulige konsekvenser som katastrofale, så er det nok de færreste som i dag mener, at det udgør et etisk problem, hvis kvinders stemmeret faktisk har haft disse konsekvenser. Tilsvarende udgør det kun en god indvending, at politiets brug af ansigtsgenkendelse på sigt vil have en bestemt konsekvens, hvis der faktisk er stærke grunde til at undgå denne konsekvens.

80 Se eksempelvis van der Burg 1991; Enoch 2001; LaFollette 2005; Douglas 2010. For overblik, se Jefferson 2014; Walton 2017.

Den anden betingelse for et glidebaneargument er således, at de konsekvenser, argumentet peger på, faktisk er *etisk problematiske*. Omvendt svækkes et glidebaneargument, jo mindre klart det er, at vi har etiske grunde til at undgå konsekvenserne. Når man skal vurdere indvendingen er det andet spørgsmål, man bør stille derfor, hvordan det begrundes, at konsekvenserne vil være etisk problematiske?

For at vurdere hvor stærk indvendingen er, må man derfor tage stilling til to forhold. For det første, hvor sandsynligt det er, at en bestemt måde at bruge ansigtsgenkendelse vil føre til, at politiet også bruger ansigtsgenkendelse på en eller flere andre måder. For det andet, hvor dataetisk problematisk det vil være, hvis politiet bruger ansigtsgenkendelse på disse måder. En sådan vurdering bør principielt foretages i forhold til det konkrete brugsscenarie, som er på spil. Selv hvis det er rigtigt, at ét brugsscenarie ville føre til en etisk problematisk glidebane, følger det ikke deraf, at det samme vil gøre sig gældende i andre brugsscenarier.

Argumenter mod politiets brug af ansigtsgenkendelse

Der findes både i faglitteraturen og den offentlige debat en række almindelige indvendinger mod, at lade politiet bruge ansigtsgenkendelse. Mange indvendinger er umiddelbart plausible, fordi ansigtsgenkendelse for eksempel kan begå fejl, have bias, og reducere borgeres privatliv. Men indvendingerne kan være stærkere eller svagere.

Indvendingernes styrke må vurderes i hvert enkelt brugsscenarie, ved at kigge på hvordan ansigtsgenkendelse virker, og hvilke effekter det har, i det konkrete scenarie.

Nogle indvendinger peger på negative effekter af at bruge ansigtsgenkendelse, som fortsat er underbelyste eller principielt vanskelige at sandsynliggøre. Disse effekter er således behæftet med væsentlig usikkerhed.

For at vurdere en indvending kan det også være relevant at sammenligne med alternativer. Det udgør eksempelvis en alvorlig svaghed ved indvendingen at ansigtsgenkendelse har bias, hvis alternativet er, at opgaven udføres af mennesker, som har endnu stærkere bias.

5. Dataetisk Råds position og anbefalinger⁸¹

Der er behov for bedre regulering af og information om eksisterende anvendelser af ansigtsgenkendelse.

Det er Dataetisk Råds opfattelse og udgangspunkt, at det er afgørende at værne om borgernes privatliv. Samtidig kan politiets brug af ansigtsgenkendelse være dataetisk forsvarlig i visse brugsscenarier, såfremt visse betingelser er opfyldt.

Politiets brug af ansigtsgenkendelse rejser risici for både fejl og bias. Det er rådets opfattelse, at disse risici i visse brugsscenarier vil kunne reduceres til et niveau, hvor de udgør en mindre tungtvejende indvending mod politiets anvendelse af teknologien. Dette forudsætter, at politiet mitigerer disse risici teknisk, samt at der etableres de nødvendige kontrolfunktioner med "et-menneske-i-kredsløbet".

Politiets brug af ansigtsgenkendelse kan også rejse risici for sikkerhedsbrud og misbrug. Det er rådets opfattelse, at disse risici i visse brugsscenarier vil kunne reduceres til et forsvarligt niveau ved at indføre relevante sikkerhedsforanstaltninger, herunder teknisk sikring af adgang til systemerne og logning af brug. Forudsat at tilstrækkelige sikkerhedsforanstaltninger er til stede, vurderer Dataetisk Råd, at disse risici udgør et mindre tungtvejende argument imod at lade politiet anvende ansigtsgenkendelse.

Endelig er det rådets opfattelse, at brugen af ansigtsgenkendelse i visse brugsscenarier, udover at være problematisk i sig selv, også skaber risici for en udvikling i retning af en omfattende og meget indgribende anvendelse af ansigtsgenkendelse. Det ville i særlig grad gøre sig gældende for brug af ansigtsgenkendelse til realtids eftersøgning i det offentlige rum og til identifikation af ukendte personer i fysiske interaktioner, fordi det første forudsætter etablering af den tekniske kapacitet til realtids overvågning ved særligt alvorlig kriminalitet, som efterfølgende kan anvendes også i forbindelse med andre typer kriminalitet, og det andet forudsætter etablering af en referencedatabase, som efterfølgende kan anvendes til identifikation i andre sammenhænge. Dataetisk

⁸¹ Rådsmedlem Peter Damm har grundet sin stilling ved Milestone Systems ikke deltaget i Dataetisk Råds positionering i dette projekt. "Dataetisk Råd" omfatter derfor i denne sammenhæng de 14 øvrige rådsmedlemmer, som er enedes om de her fremførte vurderinger og anbefalinger.

Råd anerkender, at der kan være nødsituationer, hvor det vil være dataetisk forsvarligt at anvende ansigtsgenkendelse på mere indgribende vis, for eksempel for at afværge alvorlige trusler mod personers liv i forbindelse med et terrorangreb. Det er imidlertid rådets opfattelse, at sådanne undtagelser bør behandles som nødretslike, og derfor bør tillades når de faktisk falder under sådanne bestemmelser, i stedet for som almindelige brugsscenarier.

Dataetisk Råd vurderer, på baggrund af disse betragtninger, at det er dataetisk forsvarligt, at lade dansk politi anvende ansigtsgenkendelse i begrænsede brugsscenarier som automatiseret paskontrol, offergenkendelse i materiale med seksuelt misbrug af børn, retrospektiv eftersøgning i materiale fra det offentlige rum i sager om særligt alvorlig, personfarlig kriminalitet, samt retrospektiv billedsøgning i materiale fra relevante personer i efterforskning af sager om særligt alvorlig, personfarlig kriminalitet. Dette er de tre brugsscenarier for politiets brug af ansigtsgenkendelse, som faktisk findes i Danmark i 2025, samt et nærliggende scenarie, som har været afprøvet. Rådets opfattelse er således, at politiets aktuelle brug af ansigtsgenkendelse i udgangspunktet vil være dataetisk forsvarlig for så vidt Folketinget giver anvendelsen klar lovhjemmel. Det er dog værd at bemærke, at retrospektiv eftersøgning i materiale fra det offentlige rum i 2025 fortsat er et pilotprojekt ved Københavns Politi, og at en endelig stillingtagen til dette brugsscenarie derfor må afhænge af hvordan pilotprojektet evalueres.

Omvendt vurderer rådet, på baggrund af disse betragtninger, at det ikke ville være dataetisk forsvarligt, at lade dansk politi bruge ansigtsgenkendelse til eftersøgning i realtid i det offentlige rum i sager om særligt alvorlig, personfarlig kriminalitet, eller til identifikation af ukendte personer i fysiske interaktioner. Dette er brugsscenarier, som ikke aktuelt findes i Danmark, og som det altså er rådets opfattelse, heller ikke bør introduceres i dansk sammenhæng.

Det er Dataetisk Råds vurdering, at dansk politis anvendelse af ansigtsgenkendelse skal have en klar lovhjemmel, idet rådet bemærker, at den aktuelle anvendelse finder sted indenfor mere generelle bestemmelser om politiets virke. Rådet anbefaler derfor, at Folketinget og Regeringen indfører regulering af politiets brug af ansigtsgenkendelse, som præciserer i hvilke brugsscenarier politiet har og ikke har tilladelse til at anvende teknologien. En sådan lov bør efter rådets opfattelse eksplicit tillade ansigtsgenkendelse til automatiseret paskontrol, offergenkendelse i materiale med seksuelt misbrug af børn, retrospektiv eftersøgning i materiale fra det offentlige rum i sager om særligt alvorlig, personfarlig kriminalitet, samt retrospektiv billedsøgning i materiale fra relevante personer i efterforskning af sager om særligt alvorlig, personfarlig kriminalitet. Lovgivning bør tilsvarende eksplicit forbyde mere vidtgående

anvendelse af ansigtsgenkendelse herunder til eftersøgning i realtid i det offentlige rum og identifikation af ukendte personer i fysiske interaktioner.

Dataetisk Råd anbefaler i denne forbindelse, at Folketinget og Regeringen tager stilling til, hvilke betingelser der skal stilles for politiets brug af ansigtsgenkendelse, herunder hvornår anvendelsen bør underlægges krav om at indhente dommerkendelse, således at sådanne krav om nødvendigt kan stilles i reguleringen. Et krav om dommerkendelse kan efter rådets opfattelse være særligt relevant i forbindelse med anvendelse af ansigtsgenkendelse til retrospektiv eftersøgning i materiale fra det offentlige rum.

Dataetisk Råd anbefaler også, at ny lovgivning pålægger politiet at offentliggøre detaljeret information om hvordan man anvender ansigtsgenkendelse, herunder beskrivelse af brugsscenarier og relevante tekniske specifikationer, såsom aggregerede oplysninger om mængden af anvendelse og behandlet data, fejlrate, og systemiske bias. I visse tilfælde kan oplysning om hvordan sådanne systemer fungerer og anvendes udgøre en risiko for politiets anvendelse. Rådet anerkender således, at der kan være behov for at undlade at dele information om systemerne, men anbefaler at der stilles krav til, at sådanne undtagelser begrundes præcist og defineres så snævert som muligt.

Dataetisk Råd anbefaler også, at lovgivningen stiller krav til både anvendelse og de tekniske systemer for at begrænse risici for fejl, bias og misbrug, herunder krav om at brugeres aktivitet i de relevante systemer logges, og at det i den forbindelse registreres hvilken sag anvendelse er knyttet til, samt tekniske standarder for både systemernes kvalitet med hensyn til eksempelvis risici for fejl og bias, og dokumentation af systemernes kvalitet på de relevante parametre.

Dataetisk Råd anbefaler endvidere, at Folketinget og Regeringen samtidig ajourfører eksisterende lovgivning, herunder evaluerer og om nødvendigt opdaterer bestemmelserne om politiets muligheder for at indhente billedmateriale. Disse bestemmelser er udviklet i en tid, hvor det var langt mindre almindeligt og langt mere ressourcekrævende, at foretage videoovervågning, og hvor det var vanskeligere at dele data fra sådan overvågning. Politiets muligheder for at indhente billedmateriale er således vokset dramatisk i den mellemliggende periode.

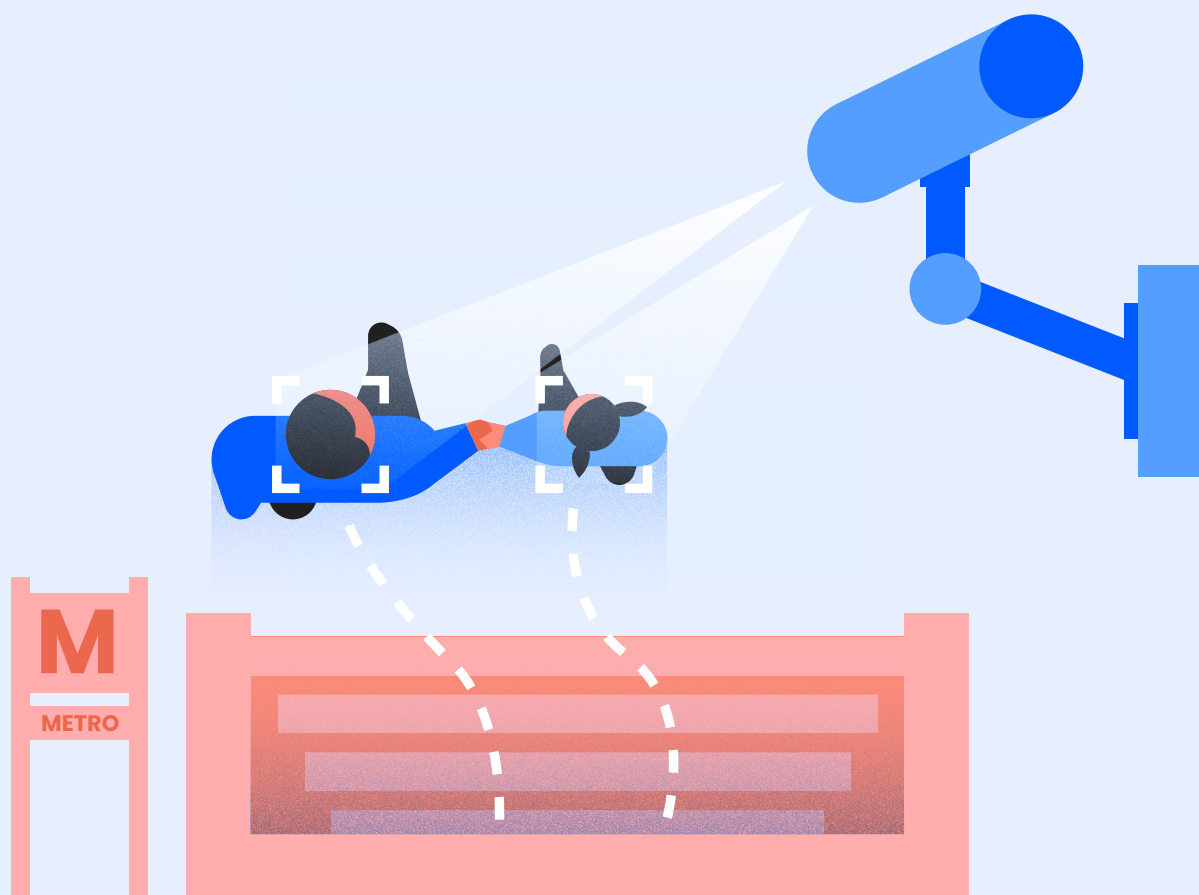
Konklusion

Dataetisk Råd vurderer, at politiets brug af ansigtsgenkendelse kan være dataetisk forsvarlig i fire brugsscenarier: automatiseret paskontrol, offergenkendelse i materiale med seksuelt misbrug af børn, retrospektiv eftersøgning i materiale fra det offentlige rum i sager om særligt alvorlig, personfarlig kriminalitet, samt retrospektiv billedsøgning i materiale fra relevante personer i efterforskning af sager om særligt alvorlig, personfarlig kriminalitet. Omvendt vurderer Dataetisk Råd, at dansk politis anvendelse af ansigtsgenkendelse ikke ville være dataetisk forsvarlig til realtids eftersøgning i det offentlige eller til identifikation af ukendte personer i fysiske interaktioner.

Dataetisk Råd anbefaler, at Folketinget og Regeringen regulerer politiets brug af ansigtsgenkendelse, herunder:

- **EksPLICIT tillader** anvendelse af ansigtsgenkendelse til automatiseret paskontrol, offergenkendelse i materiale med seksuelt misbrug af børn, retrospektiv eftersøgning i materiale fra det offentlige rum i sager om særligt alvorlig, personfarlig kriminalitet, samt retrospektiv billedsøgning i materiale fra relevante personer i efterforskning af sager om særligt alvorlig, personfarlig kriminalitet.
- **EksPLICIT forbyder** mere vidtgående anvendelse af ansigtsgenkendelse, herunder realtids eftersøgning i det offentlige og identifikation af ukendte personer i fysiske interaktioner.
- **Tager stilling til**, hvilke krav der skal stilles til politiets brug af ansigtsgenkendelse. Herunder hvornår der skal indhentes dommerkendelse, hvilket i særlig grad er aktuelt ved anvendelse til retrospektiv eftersøgning i materiale fra det offentlige rum.
- **Stiller krav om** offentliggørelse af detaljeret information om hvordan politiet anvender ansigtsgenkendelse, herunder dokumentation for hvordan systemerne virker.
- **Stiller krav til** hvilke tekniske standarder systemerne skal møde, og hvordan dette skal dokumenteres.

Dataetisk Råd anbefaler i denne forbindelse, at Folketinget og Regeringen evaluerer og om nødvendigt ajourfører eksisterende lovgivning for politiets indhentning af billedmateriale.



Litteratur

Access Now, Amnesty International, European Digital Rights, Human Rights Watch, Internet Freedom Foundation & Instituto Brasileiro de Defesa do Consumidor (2021). Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance. <https://www.amnesty.org/en/documents/doc10/4254/2021/en/>

Ada Lovelace Institute (2019). Beyond face value: public attitudes to facial recognition technology. London, Ada Lovelace Institute.

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

Associated Press (2024). Minnesota cop is awarded \$585,000 by jury after 58 fellow officers broke privacy laws by searching her private data 87 times in four years. Daily Mail. <https://www.dailymail.co.uk/news/article-7168311/Jury-awards-585K-Minnesota-officer-license-lookups.html>

Bacchini, F. & Lorusso, L. (2019). "Race, again: how face recognition technology reinforces racial discrimination." Journal of Information, Communication and Ethics in Society 17(3): 321-335 DOI: 10.1108/JICES-05-2018-0050.

Bech-Nielsen, P. C. (2024). På Vestegnen brugte politiet allerede ansigtsgenkendelse i 2022. Stik imod alle anvisninger. Radar. <https://radar.dk/artikel/paa-vestegnen-brugte-politiet-allerede-ansigtsgenkendelse-i-2022-stik-imod-alle-anvisninger>

Bedi, S. (2021). "The myth of the chilling effect." Harvard Journal of Law and Technology 35: 267.

Big Brother Watch. (2023, May 22). "Understanding live facial recognition statistics." from <https://bigbrotherwatch.org.uk/blog/understanding-live-facial-recognition-statistics/>

Braga, A. A. & Weisburd, D. L. (2012). "The Effects of Focused Deterrence Strategies on Crime: A Systematic Review and Meta-Analysis of the Empirical Evidence." Journal of Research in Crime and Delinquency 49(3): 323-358 DOI: 10.1177/0022427811419368.

Brey, P. (2004). "Ethical aspects of facial recognition systems in public places." Journal of Information, Communication and Ethics in Society 2(2): 97-109 DOI: 10.1108/14779960480000246.

Büchi, M., Festic, N. & Latzer, M. (2022). "The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda." Big Data & Society 9(1): 20539517211065368 DOI: 10.1177/20539517211065368.

Carey, A. N. & Wu, X. (2023). "The statistical fairness field guide: perspectives from social and formal sciences." AI and Ethics 3(1): 1-23 DOI: 10.1007/s43681-022-00183-3.

Chouldechova, A. (2017). "Fair prediction with disparate impact: A study of bias in recidivism prediction instruments." Big Data 5(2): 153–163. <https://ui.adsabs.harvard.edu/\#abs/2016arXiv161007524C>

Citron, D. K. & Solove, D. J. (2022). "Privacy harms." Boston University Law Review 102: 793.

Den Uafhængige Politiklagemyndighed (2019). Politiklagemyndighedens årsberetning 2019. <https://www.ft.dk/samling/20191/almdel/REU/bilag/395/2190294/index.html>

Devantier, N. (2015). Ny paskontrol i Københavns Lufthavn: Sådan virker det. Finans.dk. <https://finans.dk/tech/ECE8132325/Ny-paskontrol-i-K%C3%B8benhavns-Lufthavn-S%C3%A5dan-virker-det/>

Douglas, T. (2010). "Intertemporal Disagreement and Empirical Slippery Slope Arguments." Utilitas 22(2): 184–197 DOI: 10.1017/S0953820810000087.

Doyle, T. (2009). "Privacy and perfect voyeurism." Ethics and Information Technology 11(3): 181–189 DOI: 10.1007/s10676-009-9195-9.

Enoch, D. (2001). "Once You Start Using Slippery Slope Arguments, You're on a Very Slippery Slope." Oxford Journal of Legal Studies 21(4): 629–647.

European Court of Human Rights (2023). Glukhin v. Russia. <https://hudoc.echr.coe.int/eng?i=001-225655>

Fazelpour, S. & Danks, D. (2021). "Algorithmic bias: Senses, sources, solutions." Philosophy Compass 16(8): 1–16 DOI: <https://doi.org/10.1111/phc3.12760>

Gerell, M. (2021). "CCTV in deprived neighbourhoods – a short-time follow-up of effects on crime and crime clearance." Nordic Journal of Criminology 22(2): 221–239 DOI: 10.1080/2578983X.2020.1816023.

Goddard, K., Roudsari, A. & Wyatt, J. C. (2011). "Automation bias: a systematic review of frequency, effect mediators, and mitigators." Journal of the American Medical Informatics Association 19(1): 121–127 DOI: 10.1136/amiajnl-2011-000089 %J Journal of the American Medical Informatics Association.

Grother, P., Ngan, M. & Hanaoka, K. (2019). Face recognition vendor test (fvrt): Part 3, demographic effects, National Institute of Standards and Technology Gaithersburg, MD.

Heikkilä, M. (2022). "The walls are closing in on Clearview AI." MIT Technology Review. <https://www.technologyreview.com/2022/05/24/1052653/clearview-ai-data-privacy-uk/>

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." *Scientific Reports* 12(1): 10688 DOI: 10.1038/s41598-022-14981-6.

Jefferson, A. (2014). "Slippery Slope Arguments." *Philosophy Compass* 9(10): 672-680 DOI: <https://doi.org/10.1111/phc3.12161>

Johnson, T. L., Johnson, N. N., Topalli, V., McCurdy, D. & Wallace, A. (2024). "Police facial recognition applications and violent crime control in U.S. cities." *Cities* 155: 105472 DOI: <https://doi.org/10.1016/j.cities.2024.105472>

Justitsministeriet (2018). Endelig besvarelse af spørgsmål nr. 926 (Alm. del). <https://www.ft.dk/samling/2017/almdel/reu/spm/926/svar/1505668/1928805/index.html>

Justitsministeriet (2024a). Endelig besvarelse af spørgsmål nr. 1344 (Alm. del) fra Folketingets Retsudvalg. <https://www.ft.dk/samling/2023/almdel/reu/spm/1345/svar/2086547/2933863/index.html>

Justitsministeriet (2024b). Orientering om politiets forsøg med digitaliseret offergenkendelse i efterforskning af sager om seksuelt misbrug af børn. <https://www.ft.dk/samling/2023/almdel/DIU/bilag/145/2885095/index.html>

Justitsministeriet (2024c). Politiet får grønt lys til ansigtsgenkendelse. <https://www.justitsministeriet.dk/pressemeddelelse/politiet-faar-groent-lys-til-ansigtsgenkendelse/>

Kaur, M. & Kumar, M. (2024). "Facial emotion recognition: A comprehensive review." *Expert Systems* 41(10): e13670 DOI: <https://doi.org/10.1111/exsy.13670>

Kennedy, D. M. (2009). *Deterrence and Crime Prevention: Reconsidering the Prospect of Sanction*, Routledge.

Khalil, A., Ahmed, S. G., Khattak, A. M. & Al-Qirim, N. (2020). "Investigating Bias in Facial Analysis Systems: A Systematic Review." *IEEE Access* 8: 130751-130761 DOI: 10.1109/ACCESS.2020.3006051.

Khare, S. K., Blanes-Vidal, V., Nadimi, E. S. & Acharya, U. R. (2024). "Emotion recognition and artificial intelligence: A systematic review (2014–2023) and research recommendations." *Information Fusion* 102: 102019 DOI: <https://doi.org/10.1016/j.inffus.2023.102019>

Kim, J. & Joo, H. (2025). Facial Recognition Technology in Law Enforcement: Regulations, Crime Clearance, and Bias. *AMCIS 2025 Proceedings*. https://aisel.aisnet.org/amcis2025/sig_odis/sig_odis/4

Kleinberg, J., Mullainathan, S. & Raghavan, M. (2016) "Inherent Trade-Offs in the Fair Determination of Risk Scores." *arXiv e-prints*. <https://ui.adsabs.harvard.edu/\#abs/2016arXiv160905807K>

Ko, B. C. (2018). "A Brief Review of Facial Emotion Recognition Based on Visual Information." *Sensors* 18(2): 401. <https://www.mdpi.com/1424-8220/18/2/401>

Kortli, Y., Jridi, M., Al Falou, A. & Atri, M. (2020). "Face Recognition Systems: A Survey." Sensors 20(2): 342. <https://www.mdpi.com/1424-8220/20/2/342>

Kristensen, A. M. & Yding, H. (2021). Ekspert kan ikke udelukke, at Kina kan overvåge danskere gennem sikkerhedskameraer: "Jeg kan aldrig vide mig sikker". DR.dk. <https://www.dr.dk/nyheder/regionale/oestjylland/eksperter-kan-ikke-udelukke-kina-kan-overvaage-danskere-gennem>

Kulager, F. (2021). Nu aflæser butikker dit humør, køn, alder og etnicitet. Zetland. <https://www.zetland.dk/historie/semEIG5L-aOZj67pz-4f9da>

LaFollette, H. (2005). "Living on a Slippery Slope." The Journal of Ethics 9(3-4): 475-499.

Laperruque, J. (2025). Status of State Laws on Facial Recognition Surveillance: Continued Progress and Smart Innovations. TechPolicy.Press. <https://www.techpolicy.press/status-of-state-laws-on-facial-recognition-surveillance-continued-progress-and-smart-innovations/>

Latkowski, T. C. (2024). Facing Facts: The Effect of Facial Recognition Bans on Policing Effectiveness. McCourt School of Public Policy, Georgetown University. Master of Public Policy. https://repository.digital.georgetown.edu/handle/10822/1088629?utm_source=chatgpt.com

Li, L., Mu, X., Li, S. & Peng, H. (2020). "A Review of Face Recognition Technology." IEEE Access 8: 139110-139120 DOI: 10.1109/ACCESS.2020.3011028.

Li, S. & Deng, W. (2020). "Deep facial expression recognition: A survey." IEEE transactions on affective computing 13(3): 1195-1215.

Lipton, Z. C., Chouldechova, A. & McAuley, J. (2018). Does mitigating ML's impact disparity require treatment disparity? 32nd Conference on Neural Information Processing Systems.

Lyell, D. & Coiera, E. (2017). "Automation bias and verification complexity: a systematic review." Journal of the American Medical Informatics Association 24(2): 423-431 DOI: 10.1093/jamia/ocw105.

Mansfield, T. (2023). Facial Recognition Technology in Law Enforcement Equitability Study Final Report, National Physics Laboratory. https://science.police.uk/site/assets/files/3396/frt-equitability-study_mar2023.pdf

Metropolitan Police, S. (2025). "Live Facial Recognition Annual Report 2025." <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/other-lfr-documents/live-facial-recognition-annual-report-2025.pdf>

Mittelstadt, B., Wachter, S. & Russell, C. (2023). "The Unfairness of Fair Machine Learning: Leveling Down and Strict Egalitarianism by Default." Mich. Tech. L. Rev. 30: 1.

Modhvadia, R., Colom, A., Strait, A., Field Reid, O. & Peppin, A. (2023). How do people feel about AI? London, Ada Lovelace Institute. <https://www.adalovelaceinstitute.org/wp-content/uploads/2023/06/Ada-Lovelace-Institute-The-Alan-Turing-Institute-How-do-people-feel-about-AI.pdf>

Modhvadia, R., Sippy, T., Field Reid, O. & Margetts, H. (2025). How do people feel about AI? Wave two of a nationally representative survey of UK attitudes to AI. London, The Ada Lovelace Institute & The Alan Turing Institute. <https://attitudestoai.uk/findings-2025>

Molnar, C. (2019). Interpretable machine learning. A guide for making black box models explainable.

Nagin, D. S. (2013). "Deterrence in the Twenty-First Century." *Crime and Justice* 42(1): 199–263 DOI: doi:10.1086/670398.

Oxley, G., Uwazuruike, A., Lalic, M., Samuel, H. & Downs, W. (2024). "Police use of live facial recognition technology: Debate pack 11 November 2024 (CDP 2024/0144)." House of Commons Library Research Briefing. <https://researchbriefings.files.parliament.uk/documents/CDP-2024-0144/CDP-2024-0144.pdf>

Penney, J. W. (2016). "Chilling effects: Online surveillance and Wikipedia use." *Berkeley Technology & Law Journal* 31(1): 118–182.

Penney, J. W. (2017). "Internet surveillance, regulation, and chilling effects online: a comparative case study." *Internet Policy Review* 6(2): 1–39.

Pereira, R., Mendes, C., Ribeiro, J., Ribeiro, R., Miragaia, R., Rodrigues, N., Costa, N. & Pereira, A. (2024). "Systematic Review of Emotion Detection with Computer Vision and Deep Learning." *Sensors (Basel)* 24(11) DOI: 10.3390/s24113484.

Piza, E. L., Welsh, B. C., Farrington, D. P. & Thomas, A. L. (2019). "CCTV surveillance for crime prevention." *Criminology & Public Policy* 18(1): 135–159 DOI: <https://doi.org/10.1111/1745-9133.12419>

Rahman, M. & Kehtarnavaz, N. (2008). "Real-Time Face-Priority Auto Focus for Digital and Cell-Phone Cameras." *Consumer Electronics, IEEE Transactions on* 54: 1506–1513 DOI: 10.1109/TCE.2008.4711194.

Redaktionen (2023a). Læge dømt for at snage i 1.230 personers journaler. Sundhedspolitisk Tidsskrift. <https://sundhedspolitisktidsskrift.dk/nyheder/sundhedspolitik/8131-retssag-laege-ankla-get-for-at-snage-i-1-230-personers-journaler.html>

Redaktionen (2023b). Snageri i 13-årigs journaler: Regioner har fyret en stribe medarbejdere. Sundhedspolitisk Tidsskrift. <https://sundhedspolitisktidsskrift.dk/nyheder/sundhedspolitik/7690-snageri-i-13-arigs-journaler-regioner-har-fyret-en-strib-medarbejdere.html>

Rehman, A., Mujahid, M., Elyassih, A., AlGhofaily, B. & Bahaj, S.-A.-O. (2025). "Comprehensive Review and Analysis on Facial Emotion Recognition: Performance Insights into Deep and Traditional Learning with Current Updates and Challenges." *Computers, Materials & Continua* 82(1): 41--72. <http://www.techscience.com/cm/v82n1/59239>

Rigspolitiet (2025). Politiet tager objekt- og ansigtsgenkendelsesteknologi i brug i et pilotforsøg. <https://politi.dk/rigspolitiet/nyhedsliste/politiet-tager-objekt-og-ansigtsgenkendelsesteknologi-i-brug-i-et-pilotforsog/2025/03/07>

Ringrose, K. (2019). "Law Enforcement's Pairing of Facial Recognition Technology with Body-Worn Cameras Escalates Privacy Concerns." Virginia Law Review Online 105(Online 57). <https://virginiawreview.org/articles/law-enforcements-pairing-facial-recognition-technology-body-worn-cameras-escalates/>

Robinson, J. P., Livitz, G., Henon, Y., Qin, C., Fu, Y. & Timoner, S. (2020). Face recognition: too bias, or not too bias? Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops.

Ryberg, J. (2007). "Privacy Rights, Crime Prevention, CCTV, and the Life of Mrs. Aremac." Res Publica 13(2): 127-143.

Seacrest, L. & Snider, J. (2025). The Past, Present, and Future of Police Body Cameras, R Street Institute. <https://www.rstreet.org/research/the-past-present-and-future-of-police-body-cameras/>

Selinger, E. & Leong, B. (2024). "The ethics of facial recognition technology." The Oxford Handbook of Digital Ethics. Carrisa Veliz. Oxford, Oxford University Press: 590-610.

Skovgaard, L. (2021). Kæmpebøde til kontroversiel ansigsgenkendelse. Version2. <https://www.version2.dk/artikel/kaempeboede-til-kontroversiel-ansigsgenkendelse-datatilsyn-straffer-clear-view-ai>

Smith, M. & Miller, S. (2022). "The ethical application of biometric facial recognition technology." AI and Society 37(1): 167-175.

Solove, D. J. (2006). "A Taxonomy of Privacy." University of Pennsylvania Law Review 154(3): 477-560.

Solove, D. J. (2007). "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy." San Diego Law Review 44: 745-772.

Stoycheff, E., Liu, J., Xu, K. & Wibowo, K. (2019). "Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects." New Media & Society 21(3): 602-619 DOI: 10.1177/1461444818801317.

Stræde, M. K. & Andersen, L. S. (2017). Danskere med bil bliver udsat for omfattende overvågning af politiet, selv om de ikke er mistænkt for noget. Information. <https://www.information.dk/indland/2017/07/danskere-bil-udsat-omfattende-overvaagning-politiet-mistaenkt>

Taskiran, M., Kahraman, N. & Erdem, C. (2020). "Face recognition: Past, present and future (a review)." Digital Signal Processing 106: 102809 DOI: 10.1016/j.dsp.2020.102809.

Thomas, A. L., L., P. E., C., W. B. & and Farrington, D. P. (2022). "The internationalisation of cctv surveillance: Effects on crime and implications for emerging technologies." International Journal of Comparative and Applied Criminal Justice 46(1): 81-102 DOI: 10.1080/01924036.2021.1879885.

UNICRI & INTERPOL (2025). Toolkit for Responsible AI Innovation in Law Enforcement: Technical Reference Book. https://unicri.org/sites/default/files/2025-03/Tech%20Ref_Book_Mar25.pdf

van der Burg, W. (1991). "The slippery slope argument." *Ethics* 102(1): 42–65.

Von Hirsch, A., Bottoms, A. E., Burney, E. & Wikström, P.-O. (1999). *Criminal Deterrence and Sentence Severity*. Cambridge, Hart Publishing.

Waelen, R. & Brey, P. (2022). "Ethical Dimensions of Facial Recognition and Video Analytics in Surveillance." *Ethics in the AI, Technology, and Information Age*. Michael Boylan & Wanda Teays, Rowman & Littlefield Publishers: 15.

Walton, D. (2017). "The Slippery Slope Argument in the Ethical Debate on Genetic Engineering of Humans." *Science and Engineering Ethics* 23(6): 1507–1528.

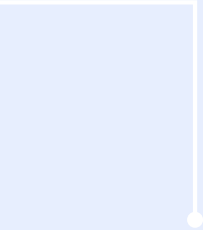
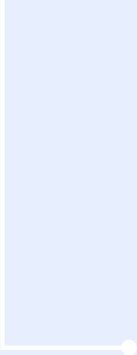
Wang, M. & Deng, W. (2021). "Deep face recognition: A survey." *Neurocomputing* 429: 215–244 DOI: <https://doi.org/10.1016/j.neucom.2020.10.081>

Wang, Y. & Kosinski, M. (2018). "Deep neural networks are more accurate than humans at detecting sexual orientation from facial images." *Journal of personality and social psychology* 114(2): 246–257.

Welsh, B. C. & Farrington, D. P. (2009). "Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis." *Justice Quarterly* 26(4): 716–745.

Yucer, S., Tektas, F., Moubayed, N. A. & Breckon, T. (2024). "Racial Bias within Face Recognition: A Survey." *ACM Comput. Surv.* 57(4): Article 105 DOI: 10.1145/3705295.

Zheng, X., Guo, Y., Huang, H., Li, Y. & He, R. (2020). "A Survey of Deep Facial Attribute Analysis." *Int. J. Comput. Vision* 128(8–9): 2002–2034 DOI: 10.1007/s11263-020-01308-z.



Dataetisk Råd 2025

Dataetisk Råd er en offentlig myndighed ved Nationalt Center for Etik, som rådgiver og skaber debat om etisk udvikling og anvendelse af digitale løsninger, data og kunstig intelligens.

København, 3. december 2025