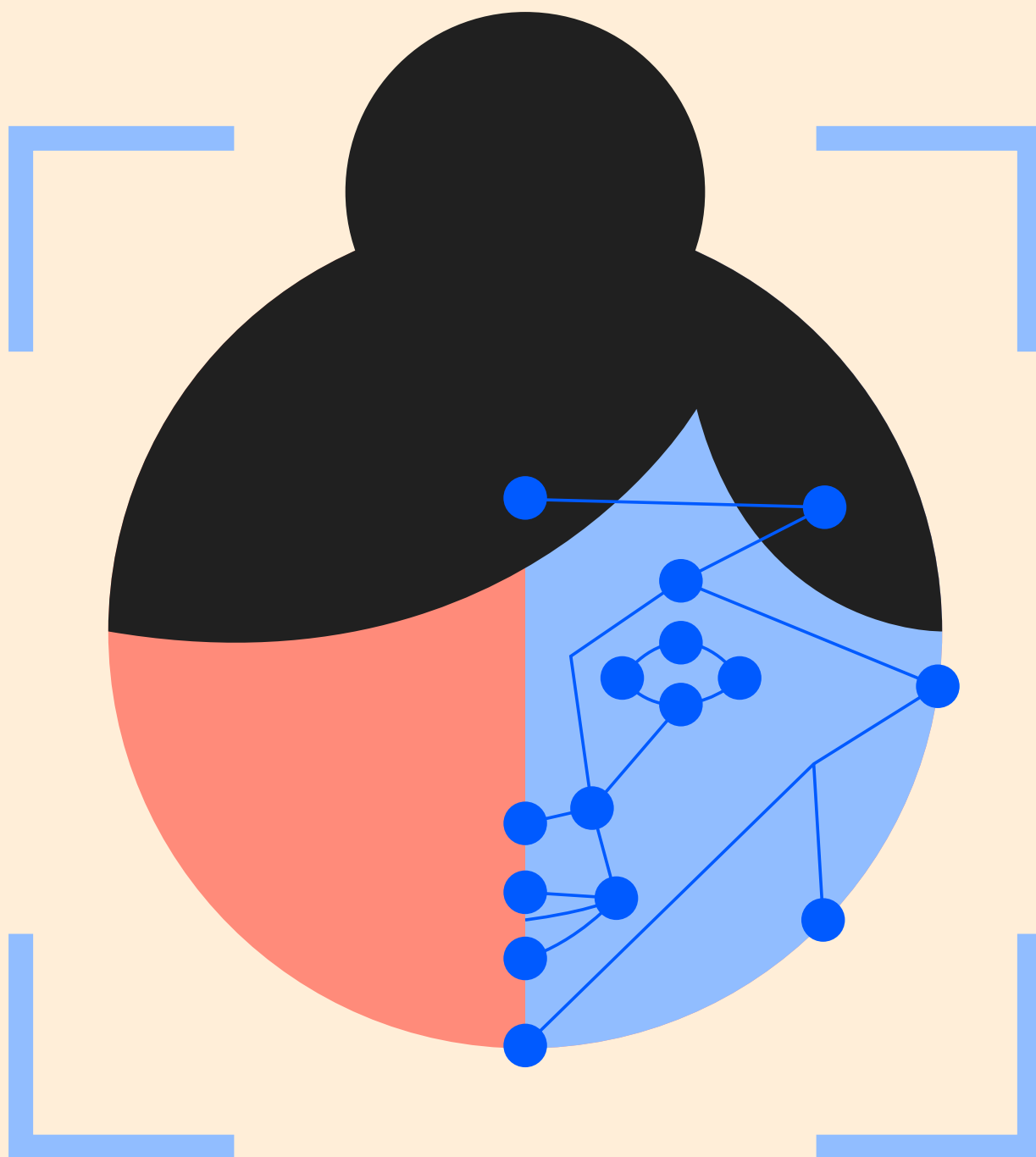


TECHSPLAINER

Hvad er ansigtsgenkendelse?

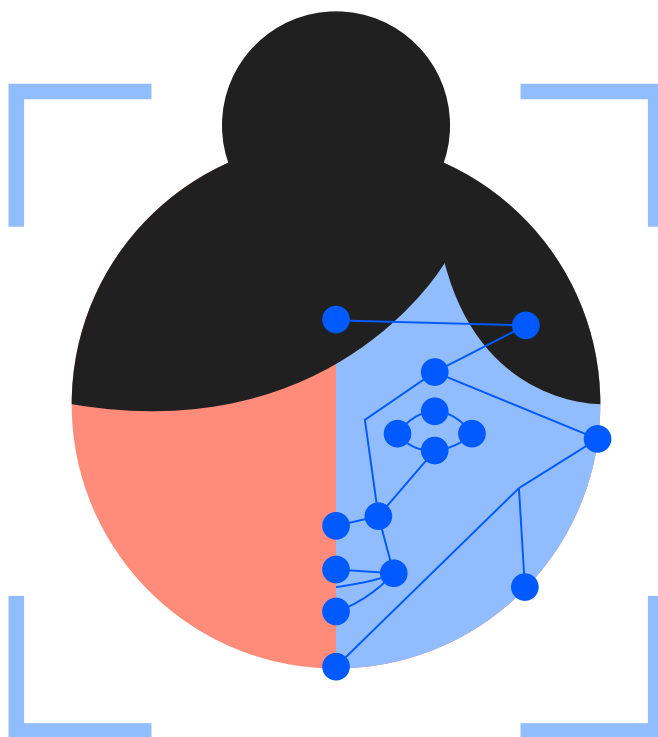


Hvad er ansigtsgenkendelse?

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.

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 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.

Ansigtsgenkendelse kan 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.

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.

Pixel

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

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**.¹

Billedanalyse

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

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 kattekill- ing 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.

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

- **Ansigtsoptagelse**, som opdager hvor der findes ansigter i et billede
- **Biometrisk analyse**, som laver matematiske aftryk af ansigterne
- **Personidentifikation**, som sammenligner ansigtsaftryk²

¹ I den engelsksprogede faglitteratur tales om "object recognition" og "object classification".

² 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.

Ansigtsopdagelse

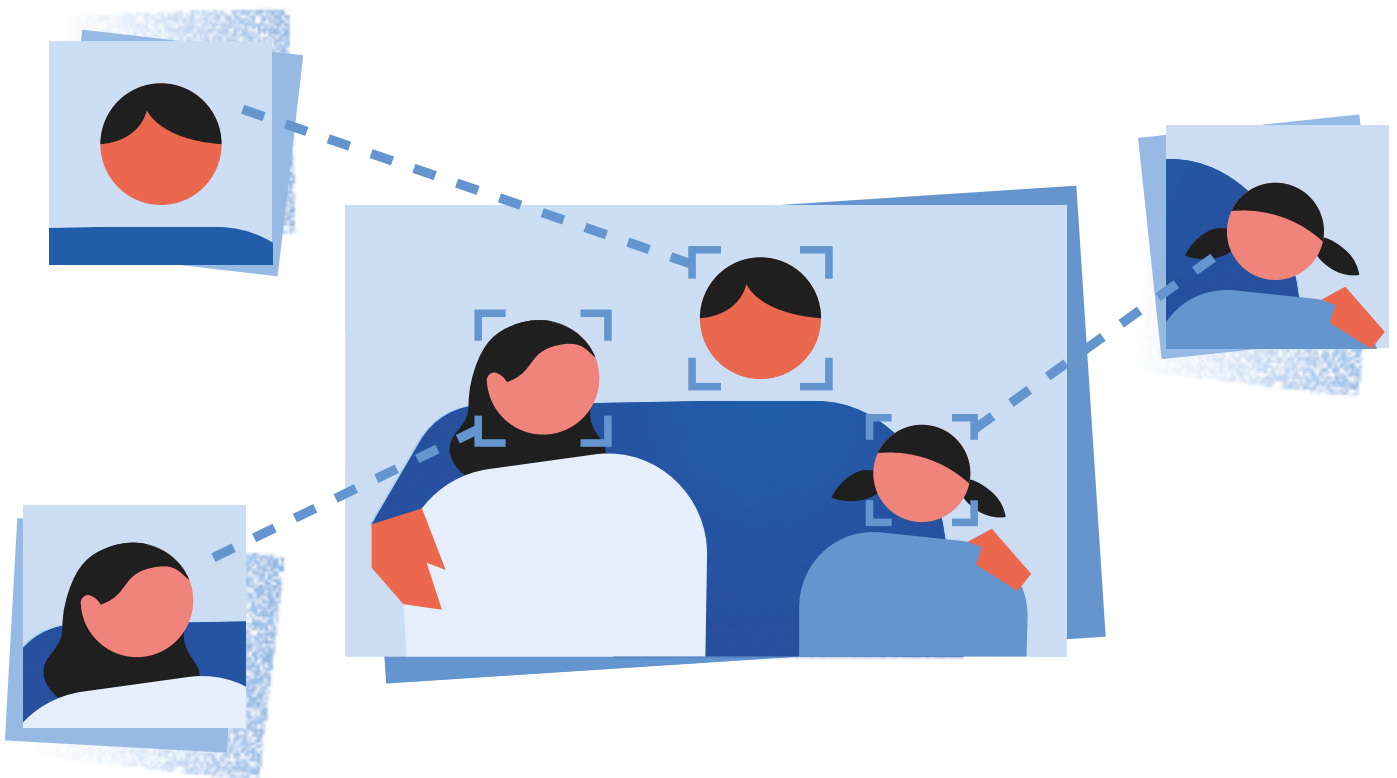
Den mest grundlæggende opgave for ansigtsgenkendelse er at opdage hvor i billeddata, der findes ansigter. Først når den har fundet ud af, hvor der findes et ansigt, kan den kunstige intelligens løse eventuelle andre opgaver.

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.

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)

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



Biometrisk analyse

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

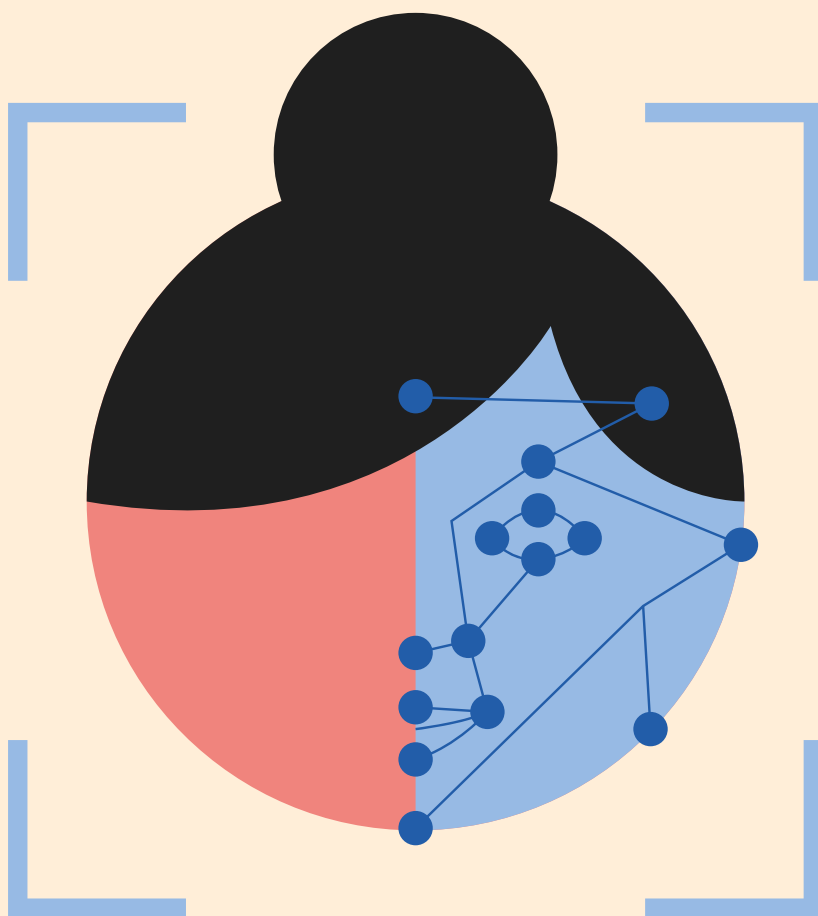
Den kunstige intelligens analyserer billedet for at finde en række målepunkter på ansigtet – for eksempel let genkendelige steder på panden, ørerne, kindbenene, læberne og mundvigene, øjenkrogene, hagen, næseryggen og næseborene. I alt måles typisk cirka 80 målepunkter.³

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

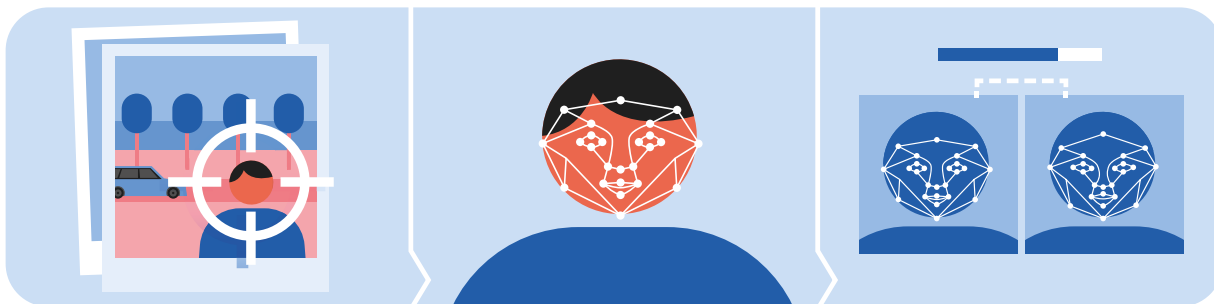
Et matematisk kort over et ansigt baseret på et sæt af målepunkter, som findes på alle ansigter.



³ Se UNICRI & INTERPOL 2025.

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.

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. Ansigtsgenkendelse kan kun identificere en person, hvis personens ansigtsaftryk er en reference i databasen. Hver gang den sammenligner et ansigtsaftryk med en reference, 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.⁴

Reference

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

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.

⁴ Se Kortli, et al. 2020; Li, et al. 2020.



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.

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.

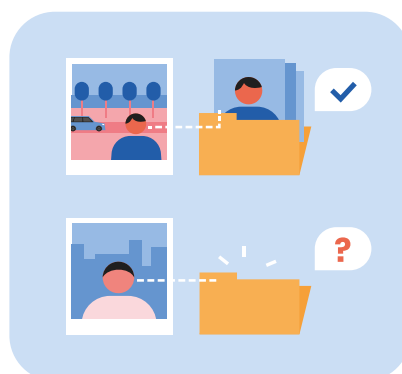
Automatisk billedsortering og -tagging

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.

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.



Til 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.

Andre former for ansigtsanalyse

Ansigtsgenkendelse handler om at identificere personer, men kunstig intelligens kan også bruges til andre slags analyser af ansigter. To almindelige eksempler er demografisk analyse og affektanalyse. De minder teknisk set om ansigtsgenkendelse, men tjener andre formål.

Demografisk identifikation

Kunstig intelligens kan bruges til at analysere billeder af ansigter, for at finde ud af personers karaktertræk, for eksempel 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.⁵

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.

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)

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.

⁵ Se Zheng, et al. 2020.

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, ved at se på hvad ansigtet udtrykker. En kunstig intelligens kan forsøge at gøre mennesker kunsten efter, ved at også analysere disse udtryk. Det kaldes at den kunstige intelligens identificerer menneskers affekt eller følelser.

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 normalt er forbundet med glæde.⁶

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. Og ligesom demografisk identifikation har opgaven vist sig at være teknisk vanskelig.⁷

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)

⁶ Se Ko 2018; Li & Deng 2020.

⁷ Se Khare, et al. 2024; Kaur & Kumar 2024; Pereira, et al. 2024; Rehman, et al. 2025.

Tre eksempler på ansigtsgenkendelse i Danmark



Adgangsbegrænsning til fodboldstadion

Et af de mest kendte eksempler på ansigtsgenkendelse i Danmark findes på Brøndby Stadion. Brøndby stadion bruger ansigtsgenkendelse til at identificere fans, som har fået karantæne fra stadion, for eksempel fordi de har begået hærværk. Systemet tager billeder af tilskuerne, når de er på vej ind på stadion.

Ansigtsgenkendelse sammenligner tilskuerne på disse billeder med billeder af de fans, som er blevet bortvist fra stadion. Hvis systemet genkender en person, som er blevet bortvist, giver det besked til kontrollører ved indgangen, som kan afvise den pågældende person. (Andersen 2020) Datatilsynet vurderede i 2019, at denne anvendelse er lovlig, og lignende systemer er i 2025 blevet udbredt til en række andre stadion i Danmark. (Datatilsynet 2019)

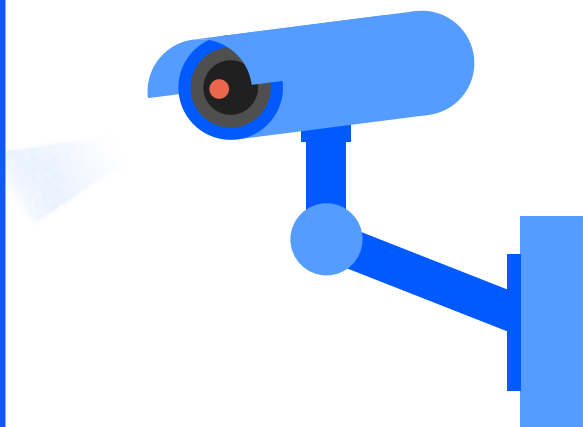
Adgangskontrol i fitnesscentre

Nogle danske fitnesscentre anvender ansigtsgenkendelse til at give kunder adgang til centret.

I nogle tilfælde er dette et valgfrit alternativ til en adgangskode eller et nøglekort, i andre tilfælde skal alle kunder bruge ansigtsgenkendelse for at få adgang.

Datatilsynet udtalte i en afgørelse fra 2022 en advarsel til et fitnesscenter, som anvendte ansigtsgenkendelse på denne vis, fordi kunder ikke blev anmodet om samtykke til brugen af ansigtsgenkendelse til indsamling af statistisk information, og fordi kameraet var placeret ved centerets indgang således, at det kunne filme personer, som ikke var kunder i centeret, og som derfor ikke havde samtykket til databehandlingen. (Datatilsynet 2022)

Til gengæld vurderede Datatilsynet at centerets anvendelse af ansigtsgenkendelse til brug for adgangskontrol var lovlig, for de kunder som havde afgivet informeret samtykke til dette.



Politiets brug af ansigtsgenkendelse

Meget af både den danske og internationale debat om ansigtsgenkendelse, har handlet om politiets brug af teknologien. Politi i blandt andet USA og UK har anvendt ansigtsgenkendelse i kropskameraer båret af politifolk på patrulje, og i stationære kameraer opsat på offentlige steder. (Woodhams 2021; U.S. Government Accountability Office 2021; Lee & Chin-Rothmann 2022)

Dansk politi har siden 2016 anvendt ansigtsgenkendelse til automatisk paskontrol i Kastrup lufthavn. (Devantier 2015; Justitsministeriet 2018) Paskontrollen scanner pas-set, og sammenligner ansigtsaftrykket i dette med ansigtet på den person, som står i paskontrollen. Hvis de to ansigtsaftryk minder tilstrækkeligt meget om hinanden, så verificerer ansigtsgenkendelse den rejsendes identitet.

I 2023 igangsatte politiets Nationale center for Særlig Kriminalitet (NSK) et pilotprojekt med ansigtsgenkendelse til identifikation af ofre i billed- og videomateriale med seksuelt misbrug af børn. (Justitsministeriet 2024a)

Og i begyndelsen af 2025 er Københavns politi begyndt at anvende ansigtsgenkendelse til identifikation af eftersøgte i forbindelse med særligt farlig kriminalitet. (Rigspolitiet 2025; Justitsministeriet 2024b)



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.⁸

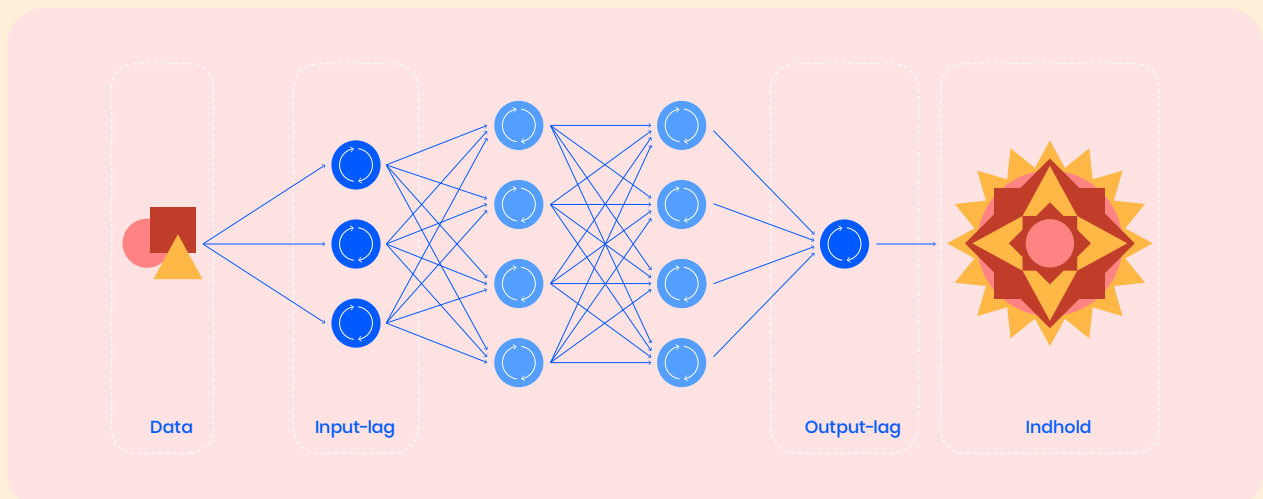
Et **neuralt netværk** er en bestemt måde at designe en computeralgoritme, som ofte bruges til at lave kunstig intelligens. Et neuralt netværk består af knudepunkter – ”digitale neuroner” – som er forbundet med hinanden.

Hvert af knudepunkterne i et neuralt netværk

Neuralt netværk

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

Modtager data, udfører en matematisk operation på det, og sender nye data videre i netværket. Det 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.



⁸ Se Li, et al. 2020; Taskiran, et al. 2020; Wang & Deng 2021.

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.⁹

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

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

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 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.

⁹ Se Hupont, et al. 2022; Zheng, et al. 2020.

Hvilke dataetiske udfordringer rejser ansigtsgenkendelse?



Brugen af ansigtsgenkendelse har i nogle tilfælde været kontroversiel. Kritikere har blandt andet argumenteret for, at ansigtsgenkendelse indskrænker menneskers privatliv, og kan afskrække uskyldig adfærd.¹⁰

De har også peget på, at teknologien er uigennemskueligt kompleks, så det er svært for mennesker at forstå, hvordan den virker, samt at den kan begå alvorlige fejl og have bias, så den virker bedre for nogle grupper og værre for andre grupper.¹¹

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.¹²

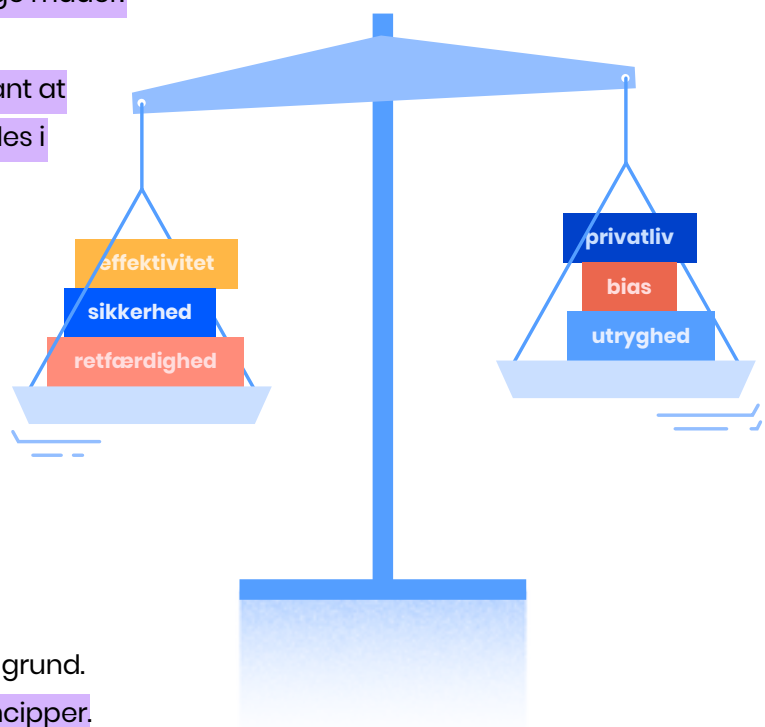
Ansigtsgenkendelse er imidlertid ikke én ting, men en teknologi som kan bruges på mange forskellige måder.

Når man skal vurdere om anvendelse af ansigtsgenkendelse er dataetisk, er det relevant at kigge på præcis hvordan teknologien anvendes i det enkelte tilfælde.

For at tage etisk stilling til en bestemt brug af ansigtsgenkendelse, er det nødvendigt at lave en dataetisk vurdering. Dataetisk Råd har lavet en introduktion til at udføre dataetiske vurderinger:

"Dataetik – sådan gør du".

Dataetiske vurderinger afhænger af de dataetiske principper, som man lægger til grund. Dataetisk Råd arbejder med 12 dataetiske principper.



¹⁰ Se Access Now, et al. 2021; Skovgaard 2021; Heikkilä 2022.

¹¹ Se Bacchini & Lorusso 2019; Grother, et al. 2019; Robinson, et al. 2020; Molnar 2019.

¹² Se Waelen & Brey 2022; Smith & Miller 2022.

Faktor	Eksempler	
Aktør	Hvem anvender teknologien?	Offentlige myndigheder, virksomheder; privatpersoner
Formål	Hvad er den intenderede effekt af at anvende teknologien?	Adgangsbegrænsning; eftersøgning af en specifik person; kundesegmentering
Målgruppe	Hvem anvendes teknologien på?	Børn og unge; patienter; kunder; medarbejdere; personer i det offentlige rum
Anvendelse	Hvor anvendes teknologien?	Det offentlige rum; arbejdspladser; fængsler; butikker; uddannelsesinstitutioner
Samtykke	Har de personer, som teknologien anvendes på, samtykket til anvendelsen?	Samtykke med mulighed for at tilgå den samme tjeneste uden anvendelse af ansigtsgenkendelse hvis samtykke nægtes; samtykke obligatorisk for at tilgå en tjeneste; intet samtykke
Dataproduktion	Hvilke data genererer ansigtsgenkendelsen?	Ansigtsopdagelse; biometrisk ansigtsaftryk; en-til-en verifikation; en-til-mange identifikation; demografiske data; udtryks- og/eller affektdata
Kvalitet	Hvor mange og hvilke fejl begår teknologien?	Specialiserede træningsdatabaser; syntetiske data; sociale medier; offentlige registre; brugerdata
Adgang til data	Hvem har adgang til de data som teknologien anvender og genererer?	Data lagres lokalt og kan kun tilgås af den enkelte bruger; data lagres centralt og kan tilgås af udviklere
Information	Hvordan oplyses målgruppen?	Skiltning om anvendelse; ingen oplysning; hjemmeside med oplysninger om anvendelse, formål, software, databaser, og kontakt til aktøren.
Kvalitet	Hvor mange og hvilke fejl begår teknologien?	Præcision; genkald; F1-score; AUC
Konsekvenser ved fejl	Hvilke data trækker teknologien på i trænings- og anvendelsesfaserne?	Bruger kan ikke låse sin mobil op; forkert person identificeres som eftersøgt; kamerafokus fungerer dårligt for visse grupper
Bias	Virker teknologien lige godt for alle grupper?	Statistisk uafhængighed; statistisk separation; statistisk tilstrækkelighed

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/>.

Andersen, T. (2020). Sådan fungerer Brøndby Stadions ansigtsgenkendelse. Version2. <https://www.version2.dk/artikel/saadan-fungerer-broendby-stadions-ansigtsgenkendelse>.

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.

Datatilsynet (2019). Tilladelse til behandling af biometriske data ved brug af automatisk ansigtsgenkendelse ved indgange på Brøndby Stadion. <https://www.datatilsynet.dk/afgoerelser/tilladelser/2019/maj/tilladelse-til-behandling-af-biometriske-data-ved-brug-af-automatisk-ansigtsgenkendelse-ved-indgange-paa-broendby-stadion>.

Datatilsynet (2022). Datatilsynet har truffet afgørelse i en sag om brugen af et system til ansigtsgenkendelse <https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/mar/datatilsynet-har-truffet-afgoerelse-i-en-sag-om-brugen-af-et-system-til-ansigtsgenkendelse>.

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/>.

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.

Justitsministeriet (2018). Endelig besvarelse af spørgsmål nr. 926 (Alm. del). <https://www.ft.dk/samling/20171/almdel/reu/spm/926/svar/1505668/1928805/index.htm>.

Justitsministeriet (2024a). Orientering om politiets forsøg med digitaliseret offergenkendelse i efterforskning af sager om seksuelt misbrug af børn. <https://www.ft.dk/samling/20231/almdel/DIU/bilag/145/2885095/index.htm>.

Justitsministeriet (2024b). 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>.
- 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>.
- 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>.
- Kulager, F. (2021). Nu aflæser butikker dit humør, køn, alder og etnicitet. Zetland. <https://www.zetland.dk/historie/semEIG5L-aOZj67pz-4f9da>.
- Lee, N. T. & Chin-Rothmann, C. (2022). Police surveillance and facial recognition: Why data privacy is imperative for communities of color, Brookings Institute. <https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/>.
- 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.
- Molnar, C. (2019). Interpretable machine learning. A guide for making black box models explainable.
- 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.
- 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.
- 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/cmcc/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>.
- 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*.

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.

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.

U.S. Government Accountability Office (2021). Federal Law Enforcement Agencies Should Have Better Awareness of Systems Used By Employees. <https://www.gao.gov/products/gao-21-105309>.

UNICRI & INTERPOL (2025). Toolkit for Responsible AI Innovation in Law Enforcement: Technical Reference Book. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://unicri.org/sites/default/files/2024-02/07_Tech%2520Ref_Book_Feb24.pdf&ved=2ahUKEw-jph4L6g8GNAXU9cfEDHffwJycQFnoECBkQAQ&usg=AOvVaw2NGEQI8L3DMaXQBBSGxsCA.

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.

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.

Woodhams, S. (2021). London is buying heaps of facial recognition tech. *WIRED*. <https://www.wired.com/story/met-police-facial-recognition-new/>.

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

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

Læs mere på **dataetiskraad.dk**

Illustrationer ved Grobowski

København 6. Oktober 2025.