



Birgitte Arent Eiriksson
Direktør
Justitia

POLITIETS ANVENDELSE AF ANSIGTSGENKENDELSESTEKNOLOGI

ANSIGTSGENKENDELSESTEKNOLOGI

Ansigtsgenkendelse:

- En form for biometrisk identifikation, der anvender algoritmer til at analysere og genkende unikke træk og mønstre i ansigter mhp. at *verificere* (en til en), *identificere* (en til mange) eller *kategorisere* (bestemte grupper, profilering, følelser) ansigter.

Retrospektiv anvendelse:

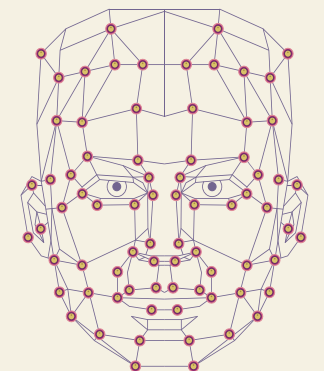
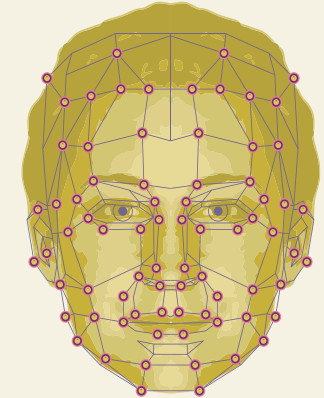
- Efterfølgende identifikation – ansigtsdata optages og sammenlignes efterfølgende med data i en database.

Anvendelse i realtid:

- Øjeblikkelig identifikation - ansigter udskilles konstant fra live-optagelser og sammenlignes automatisk med ansigter i referencedatabaser.
- Særligt indgribende.

Dilemmaet:

- Potentiel styrkelse af sikkerhed og effektiv retshåndhævelse, men rejser også alvorlige bekymringer om individets ret til privatliv og beskyttelse af data, fordi der sker indsamling og behandling af biometriske data, som kan anvendes til intens overvågning og profilering på individniveau.



DEN RETLIGE RAMME



Bredt og uklart retsgrundlag for politiets anvendelse ansigtsgenkendelse

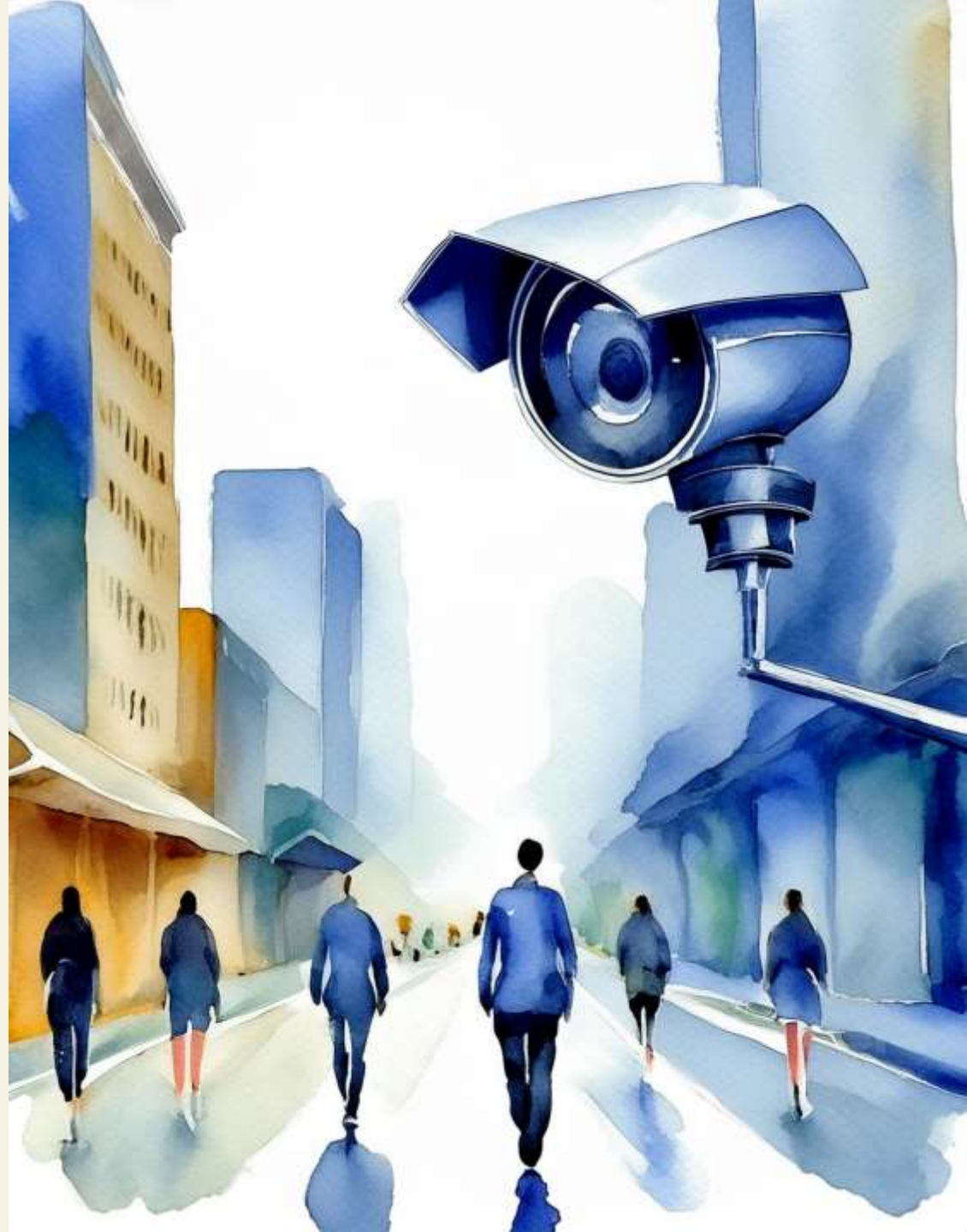
- **Retshåndhævelsesloven:** Politiet kan alene behandle biometriske data, når det er strengt nødvendigt mhp. at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger, fuldbyrde strafferetlige sanktioner, herunder for at beskytte mod eller forebygge trusler mod den offentlige sikkerhed eller beskytte personers vitale interesser, *eller* hvis data tydeligvis er offentliggjort af den registrerede.
- **Tv-overvågningsloven:** Politiet kan iværksætte tv-overvågning i det offentlige rum og andre frit tilgængelige steder (proportionalitetsvurdering). På ikke frit tilgængeligt sted gælder retsplejelovens regler om observation. Politiets kan få adgang til tv-overvågning, der foretages af myndigheder og private. Politiets kan også i særlige tilfælde overtage deres tv-overvågning.

Den kommende EU's forordning om kunstig intelligens (AI Act)

- Politiets anvendelse af ansigtsgenkendelse i **real tid** må kun ske, når det er strengt nødvendigt til 1) eftersøgning af ofre for visse kriminalitetstyper eller forsvundne, 2) forebyggelse af væsentlig overhængende trussel mod liv eller sikkerhed eller en reel aktuel/forudsigelig terrortrussel eller 3) eftersøgning af personer der har begået visse former for kriminalitet med en strafferamme på mindst 4 år. Krav om retskendelse.
- Også krav om retskendelse ved politiets **retrospektive anvendelse** af ansigtsgenkendelse til eftersøgning af personer, der er mistænkt eller dømt, medmindre der er tale om indledende identifikation af potentielt mistænkt.
- Forventes at træde i kraft primo 2025. **OBS: dansk retsforbehold.**

UDFORDRINGER

- 1. Privatlivets fred:**
 - Trussel mod borgernes ret til privatliv og beskyttelse af personoplysninger.
- 2. Overvågningssamfund:**
 - Egnede til at fremkalde følelse af konstant overvågning og indirekte afskrække fra udøvelsen af forsamlingsfrihed, ytringsfrihed mv. Ca. 1,5 mio. kameraer i DK.
- 3. Bredt og uklart retsgrundlag samt manglende retsgarantier:**
 - Ifølge EMD skærpede krav til hjemmelgrundlag ved realtid.
- 4. Kan anvendes til profilering:**
 - Overvågningsdata kan sammen med andre persondata skabe detaljerede personprofiler, særligt med POL-INTEL.
- 5. Diskrimination:**
 - Risiko for bias og fejl, som kan føre til diskrimination.
- 6. Misbrug:**
 - Fare for ulovlig indsamling og deling af biometriske oplysninger.
- 7. Samfundsmæssig tillid:**
 - Mulig underminering af tilliden til myndighederne og manglende accept fra samfundet.



JUSTITIAS ANBEFALINGER I

1. Behov for klar regulering:

- Grundig afklaring af politiets anvendelse af ansigtsgenkendelse.
- Etablering af klar og præcis national lovhjemmel for at sikre, at anvendelsen er proportional og nødvendig.

2. Forbud mod realtidsanvendelse:

- Anbefaling om forbud mod politiets realtidsanvendelse af ansigtsgenkendelse.
- Støttet af European Data Protection Board, CAHAI og FN.
- Alternativt begrænset til situationer, hvor der er tale om overhængende fare for tab af liv

3. Begrænsning af retrospektiv anvendelse:

- Retrospektiv anvendelse bør begrænses til lovovertrædelser, der kan straffes med fængsel i 8 år eller derover, og som kan medføre eller har medført fare for menneskers liv eller legeme.



JUSTITIAS ANBEFALINGER II



4. Generelle anbefalinger:

- Udvidelse af politiets anvendelse af ansigtsgenkendelse forudsætter bred og åben demokratisk samtale samt dataetisk konsekvensanalyse.
- Bør reguleres som et straffeprocessuelt indgreb i retsplejeloven, der kræver retskendelse, og reguleres nærmere i politiloven.
- Der skal ikke ske lagring af biometriske ansigtsdata.
- Der skal laves løbende kortlægning af politiets samlede tv-overvågning i det offentlige rum og andre frit tilgængelige steder, inklusiv anvendelse af ansigtsgenkendelse i realtid. Kortlægning skal være offentlig tilgængelig.
- Undersøgelse af behov for regulering af politiets observation i det offentlige rum.
- Kortlægning af politiets overtagelse af kameraovervågning fra offentlige myndigheder og private
- Undersøgelse af, hvordan der kan sikres en effektiv klageadgang for borgere, der er blevet overvåget af politiet med anvendelse af ansigtsgenkendelse.
- Evaluering af politiets anvendelse af ansigtsgenkendelse i realtid og retrospektivt efter 2 år.

SPØRGSMÅL?