INSTITUT FOR MENNESKE RETTIGHEDER

ANALYSE

FEBRUAR 2024

POLITIETS BRUG AF ANSIGTSGENKENDELSE I DET OFFENTLIGE RUM

Regeringen har meldt ud, at det er vigtigt, at politiet kan anvende ansigtsgenkendelse på offentlige steder.[1] Regeringen har også meldt ud, at man ikke anser det for nødvendigt at inddrage Folketinget om enhver brug af ansigtsgenkendelse.[2]

Politiets brug af ansigtsgenkendelse til kriminalitetsbekæmpelse udgør et alvorligt indgreb i de grundlæggende rettigheder til privatliv- og databeskyttelse. Det skyldes, at der er tale om automatisk og teknologisk avanceret behandling af følsomme personoplysninger til brug for retshåndhævelse.[3] Hvis teknologien anvendes på offentlige steder, er der tilmed en risiko for, at borgerne kan føle sig overvåget, og at det kan få en afskrækkende effekt og afholde borgere fra at bruge deres ytrings- og forsamlingsfrihed (chilling effect).[4]

Data indsamlet med ansigtsgenkendelsesteknologi kan desuden i kombination med øvrige oplysninger om borgeren, f.eks. indsamlet fra sociale medier eller fra politiets egne registre, bruges til at foretage præcise kortlægninger af borgernes private forhold og færden i det offentlige rum (profilering).

Det er Institut for Menneskerettigheders vurdering, at der i Danmark bør gennemføres udtrykkelige og detaljerede regler for politiets brug af ansigtsgenkendelse til kriminalitetsbekæmpelse. Brugen af teknologien på offentlige steder bør desuden begrænses til situationer, hvor det er strengt nødvendigt og står mål med kriminalitetens alvor. Endelig bør der være stærke retsgarantier mod misbrug og vilkårlig anvendelse.

Den nye EU-forordning om kunstig intelligens (AI-forordningen) kommer bl.a. til at forbyde politiets brug af ansigtsgenkendelse på offentlige steder i realtid (se faktaboks).[5] Danmark står dog uden for denne del af AI-forordningen på grund af det danske retsforbehold. Forbuddet kommer derfor ikke til at gælde i Danmark.

ANBEFALINGER

Institut for Menneskerettigheder anbefaler, at politiets brug af ansigtsgenkendelse

- sker på baggrund af klar og præcis hjemmel i politi- og retsplejelov.
- på offentlige steder begrænses til situationer, hvor det er strengt nødvendigt og står mål med kriminalitetens alvor.

- ledsages af krav om retskendelse, et effektivt tilsyn og klageadgang for berørte borgere.

HVAD ER ANSIGTSGENKENDELSE?

Ansigtsgenkendelse er baseret på teknologi, der opfanger biometriske data til at identificere fysiske personer. Biometriske data er personfølsomme oplysninger ligesom f.eks. DNA. Teknologien kan bruges til alt fra sammenligning af et billede med en enkeltperson (verifikation) til bredere overvågning af borgerne og sammenligning af ansigtsbilledet med større databaser (identifikation).[6]

Ansigtsgenkendelse kan både bruges til at gennemse materiale på nettet eller på andet billedmateriale (identifikation) og til at overvåge borgere i det offentlige rum via kameraer opstillet på f.eks. offentlige pladser og trafikknudepunkter (fjernidentifikation). Teknologien kan anvendes i realtid, dvs. med ingen eller minimal forsinkelse, eller efterfølgende. Endelig kan det anvendes uden at et menneske gennemser materialet (fuldautomatiseret) eller ved, at der undervejs eller efterfølgende føres en vis menneskelig kontrol.

Ligesom øvrige teknologiske værktøjer, som bruges i politiarbejdet – f.eks. DNA-analyser – er der også i selv den mest avancerede ansigtsgenkendelsesteknologi visse fejlmarginer. Teknologien er blandt andet blevet kritiseret for at identificere særligt kvinder og personer med et ikke-vestligt udseende forkert.[7]

MENNESKERETLIGE KRAV TIL ANSIGTSGENKENDELSE

Retten til respekt for privatliv og personoplysninger, er bl.a. beskyttet i EMRK artikel 8 og i EU's Charter om Grundlæggende Rettigheder i artikel 7 og 8.

Ansigtsgenkendelsesteknologi gør brug af borgernes biometriske data, der i databeskyttelsesretlig forstand er følsomme personoplysninger, ligesom f.eks. DNA. Politiets brug af ansigtsgenkendelse er omfattet af retshåndhævelseslovens regler om politiets behandling af følsomme personoplysninger. Herefter må politiet kun behandle sådanne oplysninger, når det er strengt nødvendigt for bl.a. efterforskning.[8]

Den Europæiske Menneskerettighedsdomstol (EMD) har i Glukhin mod Rusland (2023) haft anledning til at forholde sig til politiets brug af ansigtsgenkendelse til kriminalitetsbekæmpelse. EMD fandt, at brugen af ansigtsgenkendelse udgjorde et indgreb i retten til privatliv. På grund af til indgrebets (alvorlige) karakter, kræver

menneskeretten, at der er detaljerede regler for teknologiens anvendelse og udstrækning og stærke retsgarantier mod misbrug og vilkårlig magtanvendelse. EMD fandt det derfor problematisk, at national ret hverken indeholdt begrænsninger i forhold til de situationer, hvor teknologien kunne anvendes, formålene hermed, de kategorier af personer, den kunne anvendes, eller regler om behandling af følsomme personoplysninger. Der forelå heller ikke oplysninger om processuelle garantier så som procedurer for tilladelse til at indsamle og behandle oplysningerne, tilsynsbeføjelser eller adgang til retsmidler.[9]

Politiets brug af ansigtsgenkendelse på offentlige steder kan bruges til at foretage præcise kortlægninger af borgernes færden og kan derfor rent menneskeretligt sammenlignes med logning af borgernes teledata (trafik- og lokaliseringsdata). EU-Domstolen har udtalt, at generel og udifferentieret logning kan bruges til detaljeret profilering af borgerne og er egnet til at skabe en følelse hos de berørte personer af at være under konstant overvågning. Dette kan have en afskrækkende effekt på udøvelsen af deres ytringsfrihed og skal begrænses til det strengt nødvendige.[10]

BEHOV FOR UDTRYKKELIG LOVHJEMMEL

Politiets brug af ansigtsgenkendelse indebærer et alvorligt indgreb i retten til respekt for privatliv og databeskyttelse. Det skyldes, at der er tale om automatisk (og teknologisk avanceret) behandling af følsomme personoplysninger til brug for retshåndhævelse. Menneskeretten stiller derfor krav om detaljeret regulering af politiets brug af ansigtsgenkendelse.

Menneskeretten stiller som udgangspunkt krav om detaljeret regulering af politiets brug af ansigtsgenkendelse, hvor reguleringen opregner de situationer og formål, hvortil teknologien kan anvendes (kriminalitetens art og truslens karakter) og de kategorier af personer, den kan anvendes på (graden af mistanke) samt indeholde regler for behandlingen af de indsamlede data, herunder adgangen hertil samt opbevaring og sletning.

Det er instituttets vurdering, at disse krav bedst efterkommes ved at fastsætte en udtrykkelig hjemmel til politiets brug af ansigtsgenkendelse i politi- og retsplejelov.

KRAV OM STRENG NØDVENDIGHED OG SAMMENHÆNG MED KRIMINALITETENS ALVOR

Alt afhængigt af hvordan og i hvilken udstrækning ansigtsgenkendelse bruges, kan det føre til mere eller mindre intensive indgreb i privatlivet. Jo mere intensivt indgrebet er, des mere tungtvejende skal modhensynet være, for at det kan anses for proportionalt. Det har derfor betydning, om overvågningen centreres om én bestemt person, som er under en grad af mistanke for at have begået kriminelle handlinger (målrettet overvågning), eller om den bruges til generel overvågning i

det offentlige rum (masseovervågning).[11] I begge tilfælde vil det være afgørende, at brugen begrænses tidsmæssigt og geografisk.

Kriminalitetstypen har også betydning. Der er således forskel på, hvilke redskaber der lovligt kan bruges til at fange en terrormistænkt fremfor en cykeltyv.

Politiets brug af ansigtsgenkendelse på offentlige steder kan bruges til at foretage præcise kortlægninger af borgernes færden (profilering). Det kan give de berørte personer en følelse af at være under konstant overvågning og kan – ligesom generel og udifferentieret logning – have en afskrækkende effekt på udøvelsen af deres ytrings- og forsamlingsfrihed (chilling effect) hvis de er usikre på, om de bliver overvåget og om de mulige konsekvenser heraf.[12]

Det er på denne baggrund instituttets vurdering, at ansigtsgenkendelse ikke bør anvendes til generel og udifferentieret overvågning af det offentlige rum, men begrænses til det strengt nødvendige og stå mål med kriminalitetens alvor.

BEHOV FOR STÆRKE RETSGARANTIER

Politiets overvågning via ansigtsgenkendelse kan blive vilkårlig, hvis den ikke er ledsaget af effektive og præcist udmøntede retsgarantier, herunder krav til kontrol med indsamling og øvrig behandling af personoplysninger. I fraværet af effektive retsgarantier kan den blotte risiko for, at man bliver overvåget efter omstændighederne føre til en krænkelse.[13]

Indsamlingen af biometriske data aktualiserer risikoen for, at data om borgerne "flyder" på tværs af forskelligartede formål. Det er problematisk og i visse tilfælde ulovligt, hvis data, som er indsamlet med henblik på én – alvorlig – kriminalitetstype, bruges til efterforskning af en anden – mindre alvorlig – type af kriminalitet.[14] Disse udfordringer skal i Danmark ses i lyset af politiets brug af analyseplatformen POL-INTEL, som muliggør tværgående informationsanalyser (samkøring og netværksanalyse) af massive mængder data fra politiets registre og øvrige kilder som led i bl.a. efterforskning og prioritering af politiets indsatser.[15]

EMD stiller krav om, at brugen af ansigtsgenkendelse ledsages af stærke retsgarantier mod misbrug og vilkårlig magtanvendelse. Det er instituttets vurdering, at der for at sikre menneskeretten bedst muligt stilles krav om retskendelse, der som det klare udgangspunkt skal være forudgående. Herudover bør der fastsættes regler om tilsyn, klageadgang for berørte borgere.

SLUTNOTER

[1] Udvalget for Digitalisering og It, samråd om regeringens forhandlingsmandat på kunstig intelligensforordningen, DIU Alm.del – endeligt svar på spørgsmål 82, tilgængelig på: https://www.ft.dk/aktuelt/webtv/video/20231/diu/td.2006008.aspx?as=1.

[2] Udvalget for Digitalisering og It 2023-24, DIU Alm.del – endeligt svar på spørgsmål 61, tilgængelig på: https://www.ft.dk/samling/20231/almdel/diu/spm/61/svar/2011449/2805362.pdf

[3] EMD's dom i Glukhin mod Rusland, 4. juli 2023, præmis 74 ff., tilgængelig på: https://hudoc.echr.coe.int/eng?i=001-225655.

[4] Samme, præmis 88ff.

[5] Artificial intelligence – Questions and Answers, 12. december 2023, tilgængelig på: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683?utm_source=substack&utm_medium=email.

[6] Se Dataetisk Råd (2022) Hvad er ansigtsgenkendelse? tilgængelig her: https://nationaltcenterforetik.dk/Media/638037688341688364/Data-Etisk-Raad_Ansigtsgenkedelse_2022.pdf.

[7] Se f.eks. Essex Universitets rapport af juni 2019, tilgængelig her: https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf samt EU's Agentur for Grundlæggende Rettigheders rapport om ansigtsgenkendelse, december 2019, tilgængelig her: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf.

[8] § 10, stk. 1 og 2, i lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger (retshåndhævelsesloven), tilgængelig her: https://www.retsinformation.dk/eli/lta/2017/410

[9] EMD's dom i Glukhin mod Rusland, 4. juli 2023, præmis 74 ff. (note 3).

[10] EU-Domstolens dom i forenede sager C-203/15 og C-698/15, Tele2 Watson, 21. december 2016, præmis 100, tilgængelig her: https://curia.europa.eu/juris/document/document.jsf;jsessionid=2115F730212719092C515ECDB00BCDF6?text=&docid=186492&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=2009821. Se i øvrigt Institut for Menneskerettigheder, "Logning af teledata i et menneskeretligt perspektiv", 11. september 2023, tilgængelig på: https://menneskeret.dk/files/media/document/Logning%20af%20teledata%20i%20et%20menneskeretligt%20perspektiv%20notat.pdf.

[11] Se f.eks. EU-Domstolens dom i forenede sager C-203/15 og C-698/15, Tele2 Watson, 21. december 2016 (note 13) eller Europarådets faktaark om masseovervågning, tilgængelig her: https://rm.coe.int/factsheet-on-mass-surveillance-july2018-docx/16808c168e.

[12] I Glukhin mod Rusland, 4. juli 2023, præmis 88 ff. (note 3), fandt EMD derfor, at brugen af ansigtsgenkendelse til at identificere og anholde en fredelig demonstrant ikke svarede til "a pressing social need".

[13] Se EMD's dom i Klass mod Tyskland, 6. september 1978, præmis 38, tilgængelig her: http://hudoc.echr.coe.int/eng?i=001-57510.
[14] De forenede sager C-511/18, C-512/18 og C-520/18 (La Quadrature du Net), præmis 166, tilgængelig her: https://curia.europa.eu/juris/document/document.jsf;jsessionid=9FB631E5147091DE5F41684E1AF7CB42?text=&docid=232084&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=426628, som bekræftet i sag C-140/20, Commissioner of An Garda Síochána m.fl., 5. april 2022, tilgængelig her https://curia.europa.eu/juris/document/document.jsf?text=&docid=257242&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=54549.
[15] Se Institut for Menneskerettigheders høringssvar af 9. marts 2017 om politiets anvendelse af databaserede analyseredskaber mv., tilgængelig her: https://menneskeret.dk/sites/menneskeret.dk/files/03_marts_17/hoeringssvar_til_udkast_til_forslag_til_lov_om_aendring_af_politiets_virksomhed_og_toldloven.pdf.