DECEMBER 2019

ANSIGTSGENKENDELSE OG BEKÆMPELSE AF KRIMINALITET

Institut for Menneskerettigheder anbefaler, at regeringen venter med at indføre ansigtsgenkendelse til kriminalitetsbekæmpelse, indtil vi kender de menneskeretlige konsekvenser for bl.a. retten til privatliv, retten til beskyttelse af personoplysninger samt forsamlingsfriheden. Notatet giver et overblik over de menneskeretlige problemstillinger.

Ansigtsgenkendelse er en særligt intensiv og indgribende metode, der udfordrer beskyttelsen af privatlivets fred og persondatabeskyttelsen. Ansigtsgenkendelse kan være forbundet med store retssikkerhedsrisici, hvis der ikke er fornødne retsgarantier. Brugen kan også potentielt udfordre forsamlingsfriheden, hvis den bruges til masseovervågning.

En eventuel brug af ansigtsgenkendelse vil skærpe de retssikkerhedsmæssige betænkeligheder, som tv-overvågning allerede rejser.

Netop nu pågår der drøftelser og undersøgelser af teknologiens konsekvenser for menneskerettighederne i EU, Europarådet, FN[1] og i europæiske lande, som ønsker eller allerede har indført adgang for politiet (eller andre myndigheder) til at bruge ansigtsgenkendelsesteknologi. Hverken EU- eller Menneskerettighedsdomstolen har endnu haft lejlighed til at vurdere lovligheden af ansigtsgenkendelse. Det betyder, at vi ikke véd under hvilke omstændigheder politiets brug af ansigtsgenkendelse vil være lovlig.

Lovligheden afhænger overordnet af om:

1. Der er tilstrækkelige retsgarantier mod uberettigede indgreb,
2. Teknologien bruges til kriminalitetsbekæmpelse eller andre myndighedsopgaver,
3. Overvågning centreres om mistænkte eller bruges til masseovervågning,
4. Teknologien bruges til opklaring af alvorlig kriminalitet eller mindre forseelser,
5. Brugen er tidsmæssigt og geografisk afgrænset eller generel tilgængelig for politiet.

Justitsministeren har sagt, at ansigtsgenkendelse rejser principielle spørgsmål[2] og forventer, at Folketinget på et tidspunkt kommer til at drøfte ansigtsgenkendelse.[3] Senest er der blevet fremsat et beslutningsforslag i Folketinget om at forbyde offentlige myndigheders anvendelse af ansigtsgenkendelsesteknologi i det offentlige rum.[4]

Institut for Menneskerettigheder anbefaler i lyset heraf at:

- ansigtsgenkendelsesteknologi ikke bruges som led i politiets efterforsknings- og kriminalitetsbekæmpelsesarbejde, før der er afklaring om teknologiens vidtrækkende menneskeretlige konsekvenser og klarhed om, hvordan disse imødegås.

- ansigtsgenkendelsesteknologi ikke bruges i efterforsknings- og kriminalitets-bekæmpelsesarbejde til indsamling, behandling mv. af biometriske data om borgere, som der ikke er rettet nogen mistanke mod.

I det følgende gives et kort juridisk overblik over de menneskeretlige problem-stillinger, som lovgiverne bør være opmærksomme på.

BRUGEN AF ANSIGTSGENKENDELSE I UDLANDET OG DANMARK

Kina er et af de lande i verden, hvor ansigtsgenkendelse er mest udbredt. Ansigtsgenkendelse bruges både i kommercielle sammenhænge, til myndighedernes administrative opgaver, og af politiet. For eksempel er ansigtsgenkendelse netop blevet obligatorisk i Kina når man køber et SIM-kort. Sammen med andre overvågningsteknologier betyder det, at masseovervågning af befolkningen er udbredt i Kina. I USA er ansigtsgenkendelse også vidt anvendt af myndighederne. I den seneste tid er der dog blevet nedlagt flere og flere forbud mod brugen i enkelte stater og byer. Senest har man i Californien nedlagt et forbud mod politiets brug af teknologien i kropskameraer i de næste tre år. I EU er politiets brug af ansigtsgenkendelse blevet testet eller i færd med at blive afprøvet i UK, Frankrig, Holland og Tyskland. De fleste af disse lande har afprøvet muligheden for at overvåge/tracke udvalgte personers færden i det offentlige rum. I Sverige har politiet netop fået en forhåndsgodkendelse af det svenske datatilsyn til at bruge ansigtsgenkendelse til kriminalitetsbekæmpelse.

I dag bruger dansk politi ansigtsgenkendelse til verifikation af personers identitet i Kastrup Lufthavn. Det indebærer alene en automatisering af den eksisterende grænsekontrol i lufthavnen og sker ikke som led i politiets efterforskning af kriminalitet. Politiet bruger i dag ikke ansigtsgenkendelsesteknologi som led i efterforskningen eller andet arbejde med kriminalitetsbekæmpelse.[5]

Brugen af ansigtsgenkendelse til verifikation af en persons identitet i en lufthavn rejser ikke de principielle betænkeligheder, som en eventuel brug til kriminalitetsbekæmpelse eller til øvrige politiopgaver.

INSTITUT FOR MENNESKE RETTIGHEDER

MENNESKERETLIGE KRAV TIL POLITIETS BRUG AF ANSIGTSGENKENDELSE

Ansigtsgenkendelse indebærer først og fremmest et indgreb i retten til privatliv og beskyttelsen af personoplysninger. Af beskyttelsen af privatliv og personoplysninger følger, at der kun må gøres indgreb i rettighederne, hvis der er lovhjemmel, et legitimt formål og indgrebet i øvrigt står mål med dette formål (proportionalitet).

Ansigtsgenkendelsesteknologi gør brug af borgernes biometriske data. Biometriske data er i persondataretlig forstand følsomme personoplysninger, ligesom for eksempel DNA.

Hvis politiet gør brug af ansigtsgenkendelse til kriminalitetsbekæmpelse gælder retshåndhævelseslovens § 10, stk. 1. I denne bestemmelse er der et klart udgangspunkt om, at det er forbudt for politiet at behandle biometriske oplysninger, hvis det sker for at identificere en fysisk person.

Det er dog muligt at gøre undtagelser til dette forbud efter § 10, stk. 2, hvis det er strengt nødvendigt for efterforskningen eller retsforfølgelsen jf. § 1, stk. 1. Dette indebærer, at brugen af teknologien i konkrete tilfælde kan tillades.

Hvad er ansigtsgenkendelse?

Ansigtsgenkendelse er baseret på teknologi, der opfanger biometriske data til at identificere fysiske personer. Teknologien kan bruges til alt fra sammenligning af et billede med en enkeltperson (såkaldt "en til en"-sammenligning) til bredere overvågning af borgerne og sammenligning af ansigtsbilledet med større databaser ("en til mange"-sammenligning). Ansigtsgenkendelse kan både bruges til at gennemse materiale på nettet og til at overvåge borgere i det offentlige rum. Teknologien kan 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 – eksempel 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.[6]

Af retshåndhævelseslovens § 4, stk. 6, følger, at indsamlede oplysninger ikke må opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles.

Data indsamlet med ansigtsgenkendelses-teknologi kan, i kombination med øvrige oplysninger om borgeren, danne detaljerede profiler. Det gælder både data på internettet, for eksempel indsamlet via sociale medier og i registre mv., der er tilgængelige for politiet. Sammenholdes al denne data, vil det blive muligt for politiet at foretage meget præcise kortlægninger af borgernes private forhold.

Retten til privatliv
Retten til respekt for privatliv er blandt andet beskyttet i Den Europæiske Menneskerettighedskonventions artikel 8. Retten er også beskyttet i EU's Charter om Grundlæggende Rettigheder, artikel 7. Chartrets artikel 8 beskytter personoplysninger. Chartret finder anvendelse på politiets indsamling af oplysninger til brug for efterforskning, da dette er reguleret i retshåndhævelses-loven, som gennemfører EU's retshåndhævelsesdirektiv.[7]

EU- OG MENNESKERETTIGHEDSDOMSTOLENS DOMME OM OVERVÅGNING

En indgående overvågning af borgerne kan som nævnt føre til kendskab om den enkelte persons aktiviteter og overbevisninger, herunder kendskab til følsomme – og for formålet uvedkommende – personoplysninger.

EU-Domstolen har udtalt, at en generel og udifferentieret lagring af data om borgerne er egnet til at skabe en følelse hos de berørte personer af, at deres privatliv konstant er genstand for overvågning.[8]

Den Europæiske Menneskerettighedsdomstol har udtalt, at myndighedernes hemmelige overvågning af borgerne kun er forenelig med menneskeretten, hvis overvågningen er strengt nødvendig.[9]

Om politiets anvendelse af ansigtsgenkendelsesteknologi er lovlig, afhænger derfor samlet set af, om brugen i det konkrete tilfælde er proportional, herunder også af, om et eventuelt indgreb giver borgerne de fornødne retsgarantier.

KRAV OM PROPORTIONALITET

Alt afhængigt af, hvordan ansigtsgenkendelse bliver brugt, kan den føre til mere eller mindre intensive indgreb i beskyttelsen af privatlivet. Jo mere intensivt indgrebet er, des mere tungtvejende skal modhensynet være, for at det kan anses for proportionalt.

Bruges teknologien inden for kriminalitetsbekæmpelse, har det betydning, om overvågningen centreres om én bestemt person, som der er anledning til at mistænke, eller om teknologien bruges til generel overvågning af borgerne i det offentlige rum (masseovervågning).

Masseovervågning er overvågning, der ikke rettes mod én eller flere bestemte personer, men derimod indsamler oplysninger på generel og udifferentieret vis.[10]

Der er også forskel på proportionalitetsvurderingen alt afhængig af kriminalitetstypen. Der er forskel på, hvilke redskaber der er lovlige at bruge for at fange en cykeltyv frem for en terrormistænkt.

Det vil også kunne have betydning, om ansigtsgenkendelse er tidsmæssigt og geografisk afgrænset, herunder om det bruges til alle eller udvalgte overvågningskameraer, som politiet har eller kan få adgang til, og om det kun er stationære eller også mobile kameraer, droner mv. politiet kan anvende teknologien på.

Herudover har det især betydning for proportionalitetsvurderingen, om der findes tilstrækkelige retsgarantier mod uberettigede indgreb.

KRAV OM RETSGARANTIER

Politiets overvågning kan blive vilkårlig, hvis der ikke er effektive og præcist udmøntede retssikkerhedsgarantier tilknyttet brugen. Effektive retsgarantier stiller navnlig krav til kontrollen med og brugen, delingen og sletningen af personoplysninger.

Disse retsgarantier gælder, uanset, om overvågningen vedrører én bestemt person, som der er anledning til at mistænke, eller om teknologien bruges til generel overvågning af borgerne i det offentlige rum (masseovervågning).

Den Europæiske Menneskerettighedsdomstol har fastslået, at statens hemmelige overvågning som udgangspunkt bør være underlagt domstolskontrol eller anden effektiv kontrol for at være forenelig med artikel 8 i Den Europæiske Menneskerettighedskonvention.[11]

Domstolen har udtalt, at i fraværet af effektive retsgarantier for overvågningen kan den blotte risiko for, at man bliver overvåget efter omstændighederne føre til en krænkelse af retten til respekt for privatliv, uden at borgeren behøver at bevise, at vedkommende rent faktisk er blevet overvåget.[12]

Det følger også af EU's Charter om Grundlæggende Rettigheder, artikel 8, stk. 3, at overholdelsen af beskyttelsen af personoplysninger skal være underlagt en uafhængig myndigheds kontrol.

En eventuel brug af ansigtsgenkendelse skærper de retssikkerhedsmæssige betænkeligheder, som øget tv-overvågning indebærer. Se i den forbindelse

instituttets notat om regeringens nyligt lancerede udspil om tryghed og sikkerhed i det offentlige rum, som indebærer øget adgang til tv-overvågning.[13]

Brugen af biometriske data aktualiserer også andre særegne spørgsmål om retsgarantier. Som eksempel kan nævnes risikoen for, at data om borgerne "flyder" på tværs af forskelligartede formål. Det er problematisk, hvis data, som er indsamlet med henblik på én – alvorlig – kriminalitetstype, bruges med henblik på efterforskning af en anden – mindre alvorlig – type af kriminalitet. På samme måde skal der være retsgarantier mod, at data indsamlet som led i andre opgaver end kriminalitetsbekæmpelse, automatisk kan indgå i en efterforskningssammenhæng.

Den Europæiske Menneskerettighedsdomstol har fremhævet, at der skal være tydelig hjemmel til enhver brug af videooptagelser eller andet billedmateriale, som bliver brugt af politiet, herunder navnlig, hvis politiet bruger materialet til et andet formål, end det, som materialet oprindeligt blev indhentet til.[14]

Retssikkerhedsudfordringerne ved ansigtsgenkendelse skal blandt andet ses i lyset af politiets øgede brug af intelligence-led policing. Det gælder for eksempel politiets brug af et redskab som analyseplatformen POLINTEL, som muliggør bearbejdning af en massiv mængde data om personer.[15] Oplysninger analyseret ud fra sådanne redskaber kan ikke blot bruges til egentlig efterforskning, men potentielt også til såkaldt predictive policing, hvor politiet analyserer data for at forudse kommende kriminalitet eller uro uden forudgående mistanke om en kriminel handling.[16]

Hertil kommer forøgede risici for sikkerhedsbrud og misbrug, når data deles af politimyndigheder på tværs af landegrænser, eller når private aktører udvikler og sælger teknologi til brug for overvågning. I værste fald kan det føre til, at følsomme oplysninger om borgerne tilgår andre aktører end staten.

Retssikkerhedsudfordringerne har fået FN's specialrapportør for ytringsfrihed til at foreslå et komplet forbud mod blandt andet brug, eksport og salg af indgribende former for overvågningsteknologi udviklet af private aktører, som for eksempel ansigtsgenkendelse, indtil menneskeretlige retsgarantier er sikret i fornøden grad.[17]

INSTITUT FOR MENNESKE RETTIGHEDER

FORSAMLINGS- OG YTRINGSFRIHED

Politiets intensive overvågning kan potentielt få indflydelse på forsamlingsfriheden og til dels ytringsfriheden.[18]

Brugen af ansigtsgenkendelsesteknologi til for eksempel en demonstration kan potentielt komme til at afsløre en række forskellige oplysninger om personer, herunder også følsomme oplysninger som politisk tilhørsforhold.

Forsamlingsfrihed
Forsamlingsfriheden er blandt andet beskyttet i Den Europæiske Menneskerettighedskonventions artikel 11 og grundlovens § 79, og indebærer, at enhver har ret til at samles med flere personer, der har fredelige hensigter, om et fælles formål.

FN-ADVARSLER MOD ANSIGTSGENKENDELSE

Både FN's specialrapportør for forenings- og forsamlingsfrihed og FN's specialrapportør for ytringsfrihed[19] har advaret mod brug af ansigtsgenkendelsesteknologi.

Specialrapportøren for forenings- og forsamlingsfrihed har udtalt, at brugen af overvågningsteknikker til vilkårlig overvågning af personer, der gør brug af deres forsamlingsfrihed, bør forbydes. Dette er begrundet i, at identifikationen og dataindsamlingen fjerner muligheden for anonymitet i det offentlige rum, og kan få en "chilling effect" på borgernes beslutning om at deltage i offentlige forsamlinger.[20] Dette kan for eksempel være af frygt for, at deres deltagelse vil blive registreret i en politidatabase. Rapportøren anfører, at denne "chilling effect" kan intensiveres, hvis demonstrationen omhandler holdninger, der afviger fra flertallets holdninger.[21]

Politiet kan i dag lovligt orientere sig om forløbet af en demonstration og føre en vis kontrol. Politiet bruger i den forbindelse videooptagelser til dokumentation af eksempelvis politiindgreb og personer med mistænkelig adfærd i større forsamlinger.[22] I Danmark gælder der desuden ved deltagelse i demonstrationer et maskeringsforbud efter straffelovens § 134 b.

Ansigtsgenkendelsen indebærer imidlertid en så øget intensivering af overvågningen, at det efter Institut for Menneskerettigheders vurdering næppe kan sammenlignes med hverken regulære videooptagelser eller med hensynet bag maskeringsforbuddet i straffelovens § 134 b. Teknologien afslører følsomme oplysninger og om langt flere mennesker, end hvad gældende ret muliggør i dag. Dette udfordrer proportionalitetsprincippet.

SLUTNOTER

1 Se navnlig: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf , https://rm.coe.int/0900001680973a5d og https://undocs.org/A/HRC/41/35

2 Svar på § 20-spørgsmål nr. S 190, 31. oktober 2019, tilgængeligt her: https://www.ft.dk/samling/20191/spoergsmaal/s190/index.htm

3 Svar på § 20-spørgsmål S 288, 20. november 2019, tilgængeligt her: https://www.ft.dk/samling/20191/spoergsmaal/s288/index.htm

4 B 46 Forslag til folketingsbeslutning om at forbyde offentlige myndigheders anvendelse af ansigtsgenkendelsesteknologi i det offentlige rum fremsat den 27. november 2019, tilgængeligt her: https://www.ft.dk/samling/20191/beslutningsforslag/B46/som_fremsat.htm

5 Se navnlig endeligt svar på spørgsmål 926 fra Retsudvalget, 21. august 2018, tilgængeligt her: https://www.ft.dk/samling/20171/almdel/reu/spm/926/index.htm samt endeligt svar på spørgsmål 927 fra Retsudvalget, 21. august 2018, tilgængeligt her: https://www.ft.dk/samling/20171/almdel/reu/spm/927/index.htm

6 Se for eksempel Essex Universitets rapport af juni 2019 som er tilgængelig her: https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf samt EU's Agentur for Grundlæggende Rettigheder i deres rapport om ansigtsgenkendelse, december 2019 tilgængelig her: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf

7 Se lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger, tilgængelig her: https://www.retsinformation.dk/Forms/R0710.aspx?id=189891#id4f473848-6de6-4956-bd58-2252db5363a7.

8 EU-Domstolens dom i forenede sager C-203/15 og C-698/15, Tele2 Watson, 21. december 2016, præmis 100, tilgængelig her: http://curia.europa.eu/juris/document/document.jsf;jsessionid=2115F730212719092C515ECDB00BCD-F6?text=&docid=186492&pageIndex=0&doclang=DA&mode=lst&dir=&occ=first&part=1&cid=2009821

9 Se Domstolens dom i Rotaru mod Rumænien, 4. maj 2000, præmis 47 tilgængelig her: http://hudoc.echr.coe.int/eng?i=001-58586

10 Se for eksempel EU-Domstolens dom i forenede sager C-203/15 og C-698/15, Tele2 Watson, 21. december 2016 herom, tilgængelig her: http://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 eller Europarådets faktaark om masseovervågning, tilgængeligt her: https://rm.coe.int/factsheet-on-mass-surveillance-july2018-docx/16808c168e

11 Se Domstolens dom i Rotaru mod Rumænien, 4. maj 2000, præmis 57ff, tilgængelig her: http://hudoc.echr.coe.int/eng?i=001-58586

12 Se Domstolens dom i Klass mod Tyskland, 6. september 1978, præmis 38, tilgængelig her: http://hudoc.echr.coe.int/eng?i=001-57510

13 Instituttets notat og nyhed er tilgængeligt her: https://menneskeret.dk/nyheder/regeringens-sikkerhedsudspil-begraenser-borgernes-frihedsrettigheder
14 Se Domstolens dom i Peck mod UK, 28. januar 2003 (44647/98), præmis 61-62 tilgængelig her: https://hudoc.echr.coe.int/eng#{"itemid":["001-60898"]} samt Perry v. UK, 17. juli 2003,Præmis 47-48 tilgængelig her: https://hudoc.echr.coe.int/eng#{"itemid":["001-61228"]}
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
16 Se endeligt svar på spørgsmål nr. 52 fra Retsudvalg med gennemgang af såvel intelligence-led og predictive policing, 25. november 2016 tilgængeligt her: https://www.ft.dk/samling/20161/almdel/reu/spm/52/svar/1362234/1693008/index.htm
17 FN's Menneskerettighedsråd, " Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", 28. maj 2019, A/HRC/41/35, tilgængelig her: https://undocs.org/A/HRC/41/35
18 Se for eksempel FN's Menneskerettighedsråd, "The right to privacy in the digital age - Report of the Office of the United Nations High Commissioner for Human Rights", 30. Juni 2014, A/HRC/27/37, tilgængelig her: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf
19 FN's Menneskerettighedsråd, "Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", 28. maj 2019, A/HRC/41/35, tilgængelig her: https://undocs.org/A/HRC/41/35.
20 FN's Menneskerettighedsråd, "Rights to freedom of peaceful assembly and of association - Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association", 17. maj 2019, A/HRC/41/41, punkt 56-57 og 76, tilgængelig her: https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/41/41
21 Ibid.
22 Endeligt svar på spørgsmål 388 fra Retsudvalget, 29. oktober 2019, tilgængeligt her: https://www.ft.dk/samling/20182/almdel/reu/spm/388/index.htm