JUSTITSMINISTERIET

Folketinget
Udvalget for Digitalisering og It
Christiansborg
1249 København K
DK Danmark

Dato: 12. september 2024
Kontor: Politikontoret
Sagsbeh: Ida Schiøler
Sagsnr.: 2024-06738
Dok.: 3387841

Besvarelse af spørgsmål nr. 165 (Alm. del) fra Folketingets Udvalg for Digitalisering og It

Hermed sendes besvarelse af spørgsmål nr. 165 (Alm. del), som Folketingets Udvalg for Digitalisering og It har stillet til justitsministeren den 17. maj 2024. Spørgsmålet er stillet efter ønske fra Lisbeth Bech-Nielsen (SF).

Peter Hummelgaard

/

Maria Carlsson

Slotsholmsgade 10
1216 København K.

T +45 7226 8400

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 165 (Alm. del) fra Folketingets Udvalg for Digitalisering og It:

> ”Vil ministeren redegøre for den svenske og britisk praksis med og erfaringer fra anvendelse af ansigtsteknologi? Mener ministeren, at der er andre lande, hvis erfaringer bør inddrages som grundlag for en dansk beslutning om politiets anvendelse af ansigtsteknologi?”

Svar:

1. Som det fremgår af Justitsministeriets besvarelse af 26. juni 2024 af spørgsmål nr. 165 (Alm. del) fra Folketingets Udvalg for Digitalisering og It, har Justitsministeriet foretaget en høring af de danske ambassader i Sverige og Storbritannien.

Justitsministeriet har i den forbindelse anmodet om at få oplyst, hvad de pågældende landes juridiske rammer er for brugen af ansigtsgenkendelsesteknologi til retshåndhævelsesformål, om ansigtsgenkendelsesteknologi bliver brugt af de retshåndhævende myndigheder til realtidsovervågning, hvorvidt der er specifikke begrænsninger for brugen af realtidsovervågning, om ansigtsgenkendelsesteknologi bruges af de retshåndhævende myndigheder retrospektivt, og om der er specifikke begrænsninger for brugen af ansigtsgenkendelsesteknologi retrospektivt.

Justitsministeriet har endvidere anmodet om at få oplyst, hvordan de pågældende lande sikrer beskyttelsen af den enkeltes privatliv og datasikkerhed i forbindelse med implementeringen af systemer, der anvender ansigtsgenkendelsesteknologi, om landene har eksempler på sager, hvor ansigtsgenkendelsesteknologi er blevet brugt til at opklare forbrydelser eller forbedre den offentlige sikkerhed, og hvilke foranstaltninger der tages for at forhindre misbrug af ansigtsgenkendelsesteknologi fra de retshåndhævende myndighedernes side. En sammenfatning fremgår nedenfor.

<u>Sverige</u>
Den danske ambassade i Stockholm har indhentet oplysninger fra det svenske Justitiedepartement, der har oplyst, at politiets brug af ansigtsgenkendelsesteknologi ikke specifikt er reguleret, men at de almindelige regler om behandling af personoplysninger, herunder

biometrisk data, finder anvendelse. Sverige har implementeret Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 (retshåndhævelsesdirektivet) gennem en rammelov, "brottsdatalagen (20118:177)" og love om de forskellige retshåndhævende myndigheders behandling af personoplysninger, f.eks. "lagen om polisens behandling av personuppgifter inom brottsdatalagens område (2018:1693)". Artikel 10 i retshåndhævelsesdirektivet fastsætter specifikke krav til behandling af bl.a. biometriske data med det formål entydigt at identificere en fysisk person. Disse krav er implementeret i de nævnte love, f.eks. i kapitel 2, § 12 i "brottsdatalagen". Ifølge denne bestemmelse må biometriske data kun behandles, hvis det er specifikt foreskrevet, og hvis det er absolut nødvendigt for formålet med behandlingen.

Det svenske Justitiedepartement har endvidere oplyst, at de retshåndhævende myndigheder i Sverige i øjeblikket ikke bruger ansigtsgenkendelsesteknologi i realtid.

I nogle tilfælde bruger politiet automatiserede billedanalyseværktøjer, der kan indebære behandling af biometrisk data, som f.eks. ansigtsgenkendelse. Der anvendes kun ansigtsgenkendelsesteknologi retrospektivt, hvor det anses for absolut nødvendigt, og kun på billeder, der er blevet indsamlet og behandlet til specifikke formål, f.eks. som led i en igangværende efterforskning af et strafbart forhold.

Beskyttelsen af fysiske personers privatliv og datasikkerhed i forbindelse med behandling af biometriske data er sikret bl.a. ved ovennævnte regulering, herunder bestemmelsen om, at biometrisk data kun må behandles, hvis det er absolut nødvendigt for formålet med behandlingen.

Det indebærer endvidere, at politiet i visse tilfælde er forpligtet til at foretage en konsekvensanalyse og høre tilsynsmyndigheden (Integritetsskyddsmyndigheten i Sverige), inden der iværksættes en ny type behandling eller væsentlige ændringer af en allerede igangværende behandling af personoplysninger, jf. kapitel 3, § 7 i "brottsdatalagen". Tilsynsmyndigheden kan derefter give skriftlig rådgivning, hvis myndigheden mener, at den planlagte behandling er i strid med lov eller anden vedtægt, jf. kapitel 5, § 3 i "brottsdataförordingen (2018:1202)". Tilsynsmyndigheden har også mulighed for at pålægge en bøde i tilfælde af overtrædelser.

Politiet bruger et egenudviklet AI-værktøj (Alfa) til at analysere store mængder billed- og videomateriale. Der kan f.eks. søges efter personer eller bilers nummerplader. Værktøjet bruges ofte i efterforskningen af alvorlige forbrydelser. Det er f.eks. blevet brugt til at identificere gerningspersoner på forskellige steder, der er relevante for konkrete efterforskninger. Værktøjet er bl.a. blevet brugt til at fastlægge et hændelsesforløb og antallet af gerningspersoner. I forbindelse med optøjerne i flere svenske byer i påsken 2022 var AI-værktøjet i stand til at søge i billedmateriale i beslaglagte telefoner. AI-værktøjet fandt bl.a. billeder og video, hvor den mistænkte kunne identificeres på gerningsstedet.

Politiet har foretaget en konsekvensanalyse og en forudgående høring af tilsynsmyndigheden vedrørende deres brug af billedanalyse, herunder ansigtsgenkendelsesteknologi, ved efterforskning af lovovertrædelser. Før ansigtsgenkendelse anvendes i en konkret sag, vurderes det, om det er absolut nødvendigt at bruge teknologien. Derudover er det kun et begrænset antal specialuddannede medarbejdere, der har adgang til ansigtsgenkendelsesværktøjerne, og al brug af teknologien bliver registreret.

Storbritannien

Den danske ambassade i London har været i kontakt med det britiske indenrigsministerium, der har henvist til åbne kilder på internettet, som den danske ambassade har anvendt til besvarelsen.

Det kan i den forbindelse oplyses, at ansigtsgenkendelsesteknologi til retshåndhævelsesformål ikke er underlagt specifik lovgivning, men at det retlige grundlag til at anvende ansigtsgenkendelsesteknologi udspringer bl.a. fra politiets beføjelser under sædvaneretten (”common law powers”) og ”Police and Criminal Evidence Act 1984 (PACE) Section 64A”.

Brugen af ansigtsgenkendelsesteknologi til retshåndhævelsesformål er omfattet af flere forskellige retsakter, herunder ”Human Rights Act 1998”, ”Equality Act 2010”, ”Data Protection Act 2018”, ”Protection of Freedoms Act 2012” og ”Freedom of Information Act 2000”. Ansigtsgenkendelsesteknologien kan kun bruges til politimæssige formål, hvor det er nødvendigt, proportionalt og retfærdigt.

Der er indtil videre tre politikredse, der har benyttet realtidsovervågning. Alle anvendelser af ansigtsgenkendelse i realtidsovervågning er målrettede,

efterretningsbaserede, tidsbegrænsede og geografisk begrænsede. Før politiet anvender ansigtsgenkendelsesteknologi i realtidsovervågning, informerer politiet offentligheden om, hvor politiet har til hensigt at bruge teknologien, og hvor man kan få mere information om dens anvendelse. Hvis politiet i en efterforskning anvender ansigtsgenkendelse i realtidsovervåning og får et hit på deres søgning, er det altid en politibetjent, der beslutter, hvilken handling, hvis nogen, der skal tages. Som i andre efterforskninger skal den efterforskende betjent have begrundet mistanke om, at den identificerede person står bag en lovovertrædelse, og at der er grundlag for en anholdelse.

Standardprocedurer for efterforskning – bevisindsamling, anholdelse, sigtelse og retsforfølgelse – skal følges. Hvis realtidsovervågningssystemet ikke matcher en person med politiets overvågningsliste under en politioperation, slettes personens biometriske data straks og automatisk. Politiets overvågningsliste destrueres, når den konkrete politioperation er afsluttet. Det er en operativ beslutning for de enkelte politikredse, hvordan og hvornår ansigtsgenkendelse ved realtidsovervågning skal bruges, hvilket er i overensstemmelse med den nationale vejledning (Authorised Professional Practice) fra College of Policing. Vejledningen beskriver de tilfælde, hvor politiet kan bruge realtidsovervågning, og hvilke kategorier af personer de kan søge efter.

Et eksempel på politiets anvendelse af ansigtsgenkendelsesteknologi ved realtidsovervågning er set i forbindelse med kroningen af Kong Charles 3., hvor en eftersøgt seksualforbryder blev identificeret på billedmateriale fra overvågningen. Billedet af vedkommendes ansigt på overvågningen matchede billedet af en eftersøgt, og på det grundlag blev vedkommende anholdt for at have overtrådt vilkårene for sin løsladelse.

For så vidt angår brug af ansigtsgenkendelsesteknologi retrospektivt benyttes det tilsyneladende af flere politikredse, herunder Metropolitan Police, der er den største politikreds i Storbritannien. I tilfælde af et potentielt match gennemgår en uddannet operatør billedmaterialet med henblik på at bekræfte matchet. En efterforsker gennemgår ligeledes matchet for at bekræfte nøjagtigheden.

Et eksempel på en sag, hvor ansigtsgenkendelsesteknologi er blevet anvendt retrospektivt, er set i forbindelse med efterforskningen af et drab begået på en natklub i Coventry. Her blev billedmateriale fra en borger, der opholdt

sig på natklubben, matchet med en person i politiets nationale database. Offerets blod blev efterfølgende fundet på personens tøj, og personen blev dømt til fængsel på livstid.

2. Som jeg tidligere har givet udtryk for, er ansigtsgenkendelse en teknologi, som kan benyttes på mange forskellige måder**.** Anvendelsen strækker sig lige fra simple sikkerhedsfunktioner, såsom at låse sin iPhone op, til udbygget og avanceret overvågning af det offentlige rum.

I øjeblikket anvender de retshåndhævende myndigheder ansigtsgenkendelsesteknologi i meget begrænset omfang. En mere systematisk eller omfattende anvendelse af ansigtsgenkendelsesteknologi forudsætter, at myndighederne har gjort sig relevante juridiske, praktiske og principielle overvejelser. I den forbindelse er det naturligt, at myndighederne inddrager andre landes overvejelser og erfaringer med teknologien. En eventuel justering af den retlige ramme vil naturligvis ske under sædvanlig inddragelse af Folketinget.

Der henvises endvidere til REU Alm. del – Bilag nr. 311 (folketingsåret 2023-24) om politiets brug af ansigtsgenkendelsesteknologi i efterforskning som oversendt til Folketingets Retsudvalg den 5. september 2024.