Rådets perspektiv

Vigtige problemstillinger i forhold til ansigtsgenkendelse i politiets arbejde

I september 2024 indgik regeringen sammen med SF, Danmarksdemokraterne, Det Konservative Folkeparti og Dansk Folkeparti en aftale om at give politiet øget mulighed for at implementere ansigtsgenkendelsesteknologi i efterforskningen.

Ifølge justitsministerens orientering til Folketingets Retsudvalg (5.9.24) vil den digitale løsning i første omgang blive implementeret i Københavns Politi med henblik at underbygge og kvalificere, hvorvidt og under hvilke rammer brugen af henholdsvis objekt- og ansigtsgenkendelsesteknologi i givet fald kan udbredes nationalt i dansk politi. Det forventes, at løsningen vil være implementeret i Københavns Politi senest ved udgangen af 2024. De øvrige politikredse vil have mulighed for at anvende den digitale løsning, hvis videomaterialet fra politikredsene bliver sendt eller bragt til Københavns Politi.

Rådet for Digital Sikkerhed mener principielt, at politiets anvendelse af digital teknologi, herunder kunstig intelligens i efterforskningsøjemed bør være på et højt teknisk niveau, både fordi kriminaliteten i stigende omfang overskrider landegrænser og finder sted i det digitale miljø, men også af den simple grund, at politiet skal have tidssvarende ressourcer til efterforskning. Samtidig er det en central opgave for politiet at være foregangseksempel på forsvarlig anvendelse af digital teknologi i tråd med menneskerettighederne.

I det lys vil Rådet for Digital Sikkerhed hverken blåstemple eller afvise den politiske aftale, men i stedet pege på vigtige problemstillinger som politiet bør iagttage i forbindelse med øget anvendelse af ansigtsgenkendelse i efterforskningen.

Hovedpunkter i den politiske aftale om politiets anvendelse af ansigtsgenkendelse

- Politiet får mulighed for at søge efter objekter og ansigter på tværs af videomateriale, som politiet indhenter i forbindelse med efterforskning af en konkret sag, men ikke for at anvende ansigtsgenkendelse i realtid.
- Politiet vil i første omgang bruge ansigtsgenkendelsesteknologi i efterforskningen af alvorlig personfarlig kriminalitet som for eksempel drab og voldtægt samt i sager af betydning for statens sikkerhed og i særlige operative situationer. Det gælder blandt andet såkaldte ”manhunt”-situationer, hvor politiet eftersøger en farlig gerningsperson.
- De retlige rammer for behandling af personoplysninger – herunder behandling af biometriske data som for eksempel ansigtsgenkendelse – følger af databeskyttelsesdirektivet samt retshåndhævelsesloven for retshåndhævende myndigheder. Politiet har mulighed for at anvende ansigtsgenkendelse inden for disse rammer.
- Politiet anvender i dag ansigtsgenkendelsesteknologi som et værktøj til digitaliseret offergenkendelse af børn, der udsættes for seksuelt misbrug.

- Skulle der opstå behov at ændre den retlige ramme, vil det ske under sædvanlig inddragelse af Folketinget.

Vigtige problemstillinger

Formål og procedurer i forbindelse med ansigtsgenkendelse
Som det fremgår af aftalen, har aftalepartierne tilstræbt en afgrænsning af de kriminalitetsformer, hvor ansigtsgenkendelse kan komme i anvendelse. Nu da aftaleteksten ikke mere krystalklart afgrænser anvendelsesmulighederne, bør risikoen for formålsforskydning være et opmærksomhedspunkt hos politiet såvel som aftalepartierne.

Aftaleteksten omtaler ikke eventuelle krav til politiets procedurer i forhold til ansigtskendelse. Der kunne fx være tale om procedurer for validering af genkendelsesdata, da ansigtsgenkendelse rummer risiko for falske positiver (og negativer) samt procedurer for lagring, adgang, logning, videregivelse, kryptering og sletning af videomateriale med personoplysninger, når efterforskningen er afsluttet.

Både Institut for Menneskerettigheder og Justitia har peget på disse problemstillinger.

Databeskyttelse
På baggrund af aftalen har Datatilsynet fundet det nødvendigt at få afklaret, om politiet har iagttaget de relevante databeskyttelsesretlige regler. I september har Datatilsynet derfor fremsendt spørgsmål til Rigspolitiet om hvilke overvejelser politiet har gjort sig i forhold til overholdelse af retshåndhævelsesloven.

I et brev til Datatilsynet, som Ingeniørforeningen IDA har fået aktindsigt i, skriver Rigspolitiet, at det endnu ikke er besluttet, hvilket system der skal indkøbes. På den baggrund afviser Rigspolitiet på forhånd at konkretisere, hvilke "behandlingsaktiviteter, garantier, sikkerhedsforanstaltninger og mekanismer, der kan sikre beskyttelse af personoplysninger". Se IDAs pressemeddelelse 21.10.24.

Rådet for Digital Sikkerhed kan i den forbindelse tilslutte sig Datatilsynets henvisning til Det europæiske Databeskyttelsesråds vurdering, *"…at udvikling og brug af ansigtsgenkendelsesteknologi i de fleste tilfælde har en iboende høj risiko for de registreredes rettigheder, og at den dataansvarlige – foruden at udarbejde en konsekvensanalyse – også bør høre den relevante tilsynsmyndighed forud for ibrugtagen af systemet."*

Kort sagt finder Rådet for Digital Sikkerhed, at politiet allerede som led i indkøbsforberedelserne bør opstille klare kriterier for databeskyttelse og dataetik.

Realtid vs retroperspektiv anvendelse af videomateriale
Den politiske aftale understreger, at politiets øgede muligheder for ansigtsgenkendelse alene vedrører retroperspektiv anvendelse og ikke overvågning i realtid.

Det er Rådets opfattelse, at denne adskillelse bør opretholdes tydeligt efter ibrugtagning af den nye teknologi. Ansigtsgenkendelse i realtid har vidtrækkende perspektiver i forhold til privatlivets fred, forsamlingsfriheden og den generelle overvågning i samfundet.